

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR



FACULTAD DE INGENIERÍA

**MAESTRÍA EN REDES DE COMUNICACIÓN**

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

**TEMA:**

***“Análisis y optimización de una RED SAN para el transporte de copias de respaldo seguridad y restauración de información y propuesta de mejoramiento del esquema de backup basado en software Data Protector”***

***Juan Carlos Chitan Quilca***

Quito – 2016

## AUTORÍA

Yo, *Juan Carlos Chitan Quilca*, portador de la cédula de ciudadanía No. *1711394476*, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

---

*Juan Carlos Chitan Quilca*

## Contenido

1.	Introducción .....	8
2.	Justificación .....	10
3.	Antecedentes .....	12
4.	Objetivos .....	14
5.	Desarrollo Caso de Estudio .....	15
5.1.	<i>Estado del arte de las Redes SAN</i> .....	15
5.1.1.	<i>Definición de Red SAN</i> .....	15
5.1.2.	<i>Estructura de una Red SAN</i> .....	17
5.1.3.	<i>Protocolos de la Red SAN</i> .....	20
5.1.4.	<i>Características principales de la Red SAN.</i> .....	21
5.1.5.	<i>Importancia de la Red SAN.</i> .....	23
5.1.6.	<i>Equipos que conforman la Red SAN.</i> .....	23
5.1.7.	<i>Ventajas y desventajas de la Red SAN</i> .....	24
5.2.	<i>Herramienta de Backup Data Protector</i> .....	25
5.2.1.	<i>Beneficios</i> .....	26
5.2.2.	<i>Requerimientos para la instalación del Cell Manager de Data Protector.</i> .....	26
5.2.3.	<i>Arquitectura de Data Protector.</i> .....	29
5.2.4.	<i>Cell Manager.</i> .....	30
5.3.	<i>Arquitectura, componentes del sistema de copias de seguridad y restauraciones.</i> .....	32
5.3.1.	<i>Librerías</i> .....	34
5.3.2.	<i>Storage.</i> .....	35
5.3.3.	<i>Directores y SAN Switch.</i> .....	35
5.4.	<i>Análisis de la red SAN y la herramienta de copias de seguridad Data Protector.</i> .....	37
5.4.1.	<i>Análisis de la red SAN.</i> .....	37
5.4.2.	<i>Resumen ejecutivo.</i> .....	38
5.4.3.	<i>Objetivos del documento.</i> .....	38
5.4.4.	<i>Necesidades y requerimientos.</i> .....	39
5.4.5.	<i>Análisis de la red SAN.</i> .....	39
5.4.6.	<i>Estado actual de los equipos SAN.</i> .....	40
5.4.7.	<i>Análisis de la configuración actual de la red SAN, SANSW_BP11.</i> .....	42
5.4.7.1.	<i>Análisis de puertos.</i> .....	42
5.4.7.2.	<i>Análisis de zonas.</i> .....	44

5.4.7.3.	<i>Análisis de topología.</i>	46
5.4.8.	<i>Análisis de la configuración actual de la red SAN, SANSW_BP12.</i>	47
5.4.8.1.	<i>Análisis de puertos.</i>	47
5.4.8.2.	<i>Análisis de zonas.</i>	48
5.4.9.	<i>Análisis del consumo de Ancho de banda.</i>	51
5.4.10.	<i>Alertas y errores reportados por SAN health.</i>	56
5.4.11.	<i>Análisis de Data Protector.</i>	57
5.5.	<i>Estudio comparativo entre las diferentes herramientas de copias de seguridad y restauración existentes en el mercado.</i>	65
5.6.	<i>Recomendaciones para optimizar el tiempo de ejecución de los respaldos y mejoramiento de la red SAN.</i>	67
6.	<i>Conclusiones y Recomendaciones</i>	70
6.1	<i>Conclusiones</i>	70
6.2	<i>Recomendaciones</i>	70
	<i>Bibliografía:</i>	72
	<i>Anexos:</i>	73
	<i>Análisis de la red SAN por Brocade SAN Health.</i>	76
	<i>Análisis de la red SAN por DELLEMC Data Protector.</i>	80

## Índice de Figura

FIGURA 1 DISEÑO DE RED SAN.....	15
FIGURA 2 ESTRUCTURA DE UNA RED SAN.....	17
FIGURA 3 CAPAS DE LA RED SAN.....	18
FIGURA 4 REDES FIBRE CHANNEL.....	19
FIGURA 5 TOPOLOGÍA DE RED SAN.....	23
FIGURA 6 EQUIPOS DE UNA RED SAN.....	24
FIGURA 7 HP DATA PROTECTOR.....	25
FIGURA 8 ARQUITECTURA DE DATA PROTECTOR.....	30
FIGURA 9 CELL MANAGER DATA PROTECTOR.....	31
FIGURA 10 MENÚ PRINCIPAL DE DATA PROTECTOR.....	31
FIGURA 11 INFRAESTRUCTURA DEL SISTEMA DE COPIAS DE SEGURIDAD Y RESTAURACIONES.....	33
FIGURA 12 LIBRERÍA MSL6480.....	34
FIGURA 13 SAN SWITCH.....	36
FIGURA 14 FAMILIA DE EQUIPOS BROCADE.....	37
FIGURA 15 SAN SUMMARY DATAILS FOR SAN.....	41
FIGURA 16 SUMMARY DE SWITCHES.....	42
FIGURA 17 MÉTRICAS DE LAS ZONAS Y ALIAS.....	43
FIGURA 18 PUERTOS UTILIZADOS DIRECTOR 1.....	43
FIGURA 19 PUERTOS UTILIZADOS.....	43
FIGURA 20 TOPOLOGÍA DIRECTOR 1.....	46
FIGURA 21 MÉTRICA DE LAS ZONAS.....	47
FIGURA 22 PUERTOS USADOS.....	47
FIGURA 23 PUERTOS UTILIZADOS.....	48
FIGURA 24 TOPOLOGÍA DIRECTOR 2.....	50
FIGURA 25 RESUMEN CONSUMO ANCHO DE BANDA SW1.....	52
FIGURA 26 ANCHO DE BANDA SW1.....	53
FIGURA 27 ESTADÍSTICA DEL CONSUMO DE ANCHO DE BANDA EN HORARIO PICO.....	53
FIGURA 28 RESUMEN CONSUMO ANCHO DE BANDA SW2.....	54
FIGURA 29 CONSUMO DEL ANCHO DE BANDA SW2.....	55
FIGURA 30 ESTADÍSTICA DEL CONSUMO DE ANCHO DE BANDA EN HORARIO PICO SW2.....	55
FIGURA 31 ERROR SWITCH REPORTADO.....	56
FIGURA 32 ERRORES SAN 2.....	56
FIGURA 33 BACKUP POR MEDIO DE DATA PROTECTOR.....	57
FIGURA 34 TOP ECBRHCP1.....	61
FIGURA 35 ACTIVIDAD DE DATA PROTECTOR.....	61
FIGURA 36 TAREAS PROGRAMADAS EN DATA PROTECTOR.....	62
FIGURA 37 RECOMENDACIONES A IMPLEMENTAR SOBRE DATA PROTECTOR.....	62
FIGURA 38 POLÍTICAS APLICADAS A DATA PROTECTOR.....	63
FIGURA 39 MÉTRICAS DEL CONSUMO DE LA RED – LICENCIAS.....	63
FIGURA 40 CAPACIDAD DE BACKUPS.....	64
FIGURA 41 CONSUMO PROMEDIO POR MES.....	64
FIGURA 42 PERFORMANCE DE DATA PROTECTOR.....	65
FIGURA 43 SUMMARY RED SAN.....	73
FIGURA 44 SUMMARY DE LICENCIAS – PUERTOS.....	73
FIGURA 45 ZONAS DE LA RED SAN.....	73
FIGURA 46 TOPOLOGÍA DIRECTOR 1.....	74
FIGURA 47 TOPOLOGÍA DIRECTOR 2.....	75

FIGURA 48 ANÁLISIS DE LA RED SAN .....	76
FIGURA 49 DETALLE RESUMIDO DE LA RED SAN.....	77
FIGURA 50 ERRES DE LA RED SAN.....	77
FIGURA 51 RESUMEN DE LA CONFIGURACIÓN DEL DIRECTOR 1 .....	78
FIGURA 52 RESUMEN DE LA CONFIGURACIÓN DEL DIRECTOR 2. ....	79

## Índice de Tablas

TABLA 1 TIEMPO DE RETENCIÓN DE LA INFORMACIÓN. ....	32
TABLA 2 SUMMARY RED SAN. ....	41
TABLA 3 VERSIÓN DE FIRMWARE DE SWITCH CON ERROR.....	42
TABLA 4 VELOCIDAD DE LOS PUERTOS DEL SAN SWITCH.....	44
TABLA 5 ALIAS NO DEFINIDOS.....	46
TABLA 6 VELOCIDAD DE LOS PUERTOS DEL SAN SWITCH.....	48
TABLA 7 ALIAS NO DEFINIDOS.....	50
TABLA 8 SERVIDORES TOP DATA PROTECTOR. ....	60
TABLA 9 COMPARACIONES ENTRE HERRAMIENTAS DE BACKUP.....	67

## 1. Introducción

El presente trabajo investigativo trata sobre el estudio de una red SAN, con el objetivo de optimizar la obtención de las copias de seguridad y recuperación que se realizan mediante la herramienta de respaldo de HP Data Protector para los servidores que se hallan dentro de la plataforma UNIX en los ambientes de producción y test de la empresa Tata Consultancy Services, TCS es una empresa que se dedica a brindar soporte IT, soluciones de negocios y tercerización a las principales entidades bancarias del país.

La empresa inicia y se constituye en el país de la India y se ha posesionado en todo el mundo, en América del sur se encuentra en los siguientes países: Argentina, Brasil, Chile, Colombia, Ecuador, Perú, Uruguay. En el país, TCS, se encuentra establecida como empresa aproximadamente hace 15 años, brindando servicios de IT, servicios de infraestructura IT, soluciones empresariales, soluciones Business Process Outsourcing (BPO), inteligencia empresarial y gestión del rendimiento, servicios industriales y de ingeniería, Bancs.

La herramienta de respaldos seleccionada para el caso investigativo se denomina Data Protector la cual es proporcionada por la empresa mundialmente conocida como Hewlett-Packard y que generalmente se la reconoce por sus siglas HP. Data Protector es una herramienta que facilita la obtención de respaldos o backup y restauraciones de manera eficiente unificada e inteligente y en tiempo real, cuenta con una interfaz gráfica mediante la cual se puede configurar aspectos fundamentales tales como: respaldos programados, calendarización de eventos, integración con base de datos y lo principal que es una herramienta multiplataforma que se ha integrado con varios sistemas operativos tales como HP - UX, Linux, Aix, Windows y puede ser instalado en los servidores de tipo físico como también para servidores virtualizados. Las características y funciones principales sobre Data Protector, infraestructura, la red SAN, se las tratará en el transcurso y desarrollo de presente documento.

El caso de estudio planteado tiene como base una institución financiera en la cual el servicio de copias de seguridad y recuperación es un punto crítico y de importancia significativa, siendo necesario mantener óptimo y operativo un sistema de backup, el cual debe estar alineado con las nuevas tecnologías y tendencias modernas, enmarcado en las buenas prácticas y cuente con procesos de gobernabilidad IT.

Los servidores que se analizarán corresponden a la plataforma UNIX, en los cuales se podrá encontrar equipos que han sido preparados con sistemas operativos como: HP - UX, Linux y Aix, estos servidores se encuentran inter conectados por medio de una red SAN hacía los dispositivos de almacenamiento como librerías y storages, dispositivos de los cuales se ha obtenido la información necesaria para realizar el estudio de la red SAN y poder determinar el

consumo de ancho de banda, tiempo de ejecución, entre otros y determinar las posibles mejoras para optimizar y minimizar los tiempos que tardan en ejecutarse las copias de seguridad.

Al finalizar el proceso de estudio se entregará un documento donde conste el análisis de la red SAN y las sugerencias para minimizar el tiempo de ejecución de las copias de seguridad y restauración.

## 2. Justificación

Las nuevas tendencias tecnológicas y la constante evolución permiten que las necesidades sean cada vez más elaboradas, exigentes y requieran de soluciones inteligentes e innovadoras, soluciones en las cuales permitan fácilmente ajustarse y acoplarse a la realidad y a las demandas de las empresas, es por tal razón que hoy en día las compañías buscan medios y soluciones que garanticen un adecuado y correcto procedimiento para la obtención de copias de seguridad de sus aplicaciones, archivos e información de gran importancia para su negocio, pero de nada sería útil mantener un sistema de copias de seguridad si no existe un mecanismo mediante el cual se pueda restaurarse la información obtenida del backup.

Teniendo en cuenta el objetivo que representa tener un sistema que permita obtener copias de seguridad y de restauración, se ve la obligación de generar procedimientos y sistemas que cumplan con las expectativas de las empresas, recordando que se debe apoyar en herramientas o software especializados, los cuales permitan mantener de forma centralizada toda la información que se considera de importancia para la línea de negocio de la empresa, además debe reflexionar que también es necesario disponer de un conjunto de equipos en los cuales se pueda almacenar una gran cantidad de información, producto de las copias de seguridad planificadas y generadas por la herramienta de respaldos, debe también considerarse como primordial el sistema de restauración, ya que en algún momento del tiempo y en base a las necesidades del negocio, también es posible se solicite una restauración de la información obtenida mediante la copia de seguridad. Sin copia de seguridad es imposible realizar una restauración.

En el caso del estudio planteado sobre el análisis de la Red SAN para la obtención de copias de seguridad y restauración por medio de data protector es primordial y fundamental primeramente conocer la infraestructura que la constituye, para poder coleccionar la información de los equipos que la conforman y determinar las recomendaciones y mejoras para minimizar el tiempo de ejecución del respaldo y el uso del canal de transmisión y mejorar el consumo del ancho de banda.

Para la obtención de las copias de seguridad y su posterior restauración es necesario disponer del equipamiento necesario para llevar a cabo la actividad de respaldos adicional debe contemplar un sitio donde pueda almacenar una gran cantidad de información, por lo que se dispone de una librería HP MSL 6480 de 20 drives, particionados de la siguiente manera 16 driver en LTO4 y 4 driver en LTO6, lo que permite obtener restauraciones de cintas históricas, en ocasiones y por tareas específicas también es óptimo tener espacio en disco, para lo cual se dispone de un storage para su almacenamiento o recuperación, los discos son presentados y

zonificados bajo demanda y depende de la criticidad del evento, el área analiza el préstamo de las cuotas y espacio para su incremento.

Es por este motivo que se realiza el análisis del tráfico en los equipos que conforman la red SAN y la herramienta de copias de seguridad y restauración Data Protector para poder determinar mejoras en los tiempos de ejecución y garantizar el correcto funcionamiento del sistema de respaldos, el análisis da a conocer información útil para emitir recomendaciones y sugerencias que puedan ser consideradas para la toma de decisiones en beneficio de la empresa y de la línea de negocio y su continuo mejoramiento.

### 3. Antecedentes

Mantener un sistema de copias de seguridad y restauraciones en una empresa es de importancia significativa, debido a que conservar la información de manera ordenada y centralizada, agiliza y mejora el proceso de restauraciones en caso de desastre o pérdida de información sensible.

El sistema de copias de seguridad que se analiza está instalado en una empresa que presta servicios tecnológicos a las principales entidades bancarias del país, por cerca de 15 años aproximadamente, motivo por el cual se debe mantener respaldos periódicos de los sistemas operativos, files system, directorios, e información de importancia para la línea de negocio y que es de uso exclusivo para el cliente, también se debe considerar que existen bases de datos, en las cuales se almacena información de los cuenta ahorristas. Esta data es utilizada para evitar casos de fraude, desvíos de fondo, pérdidas de dinero, entre los casos más relevantes y que las entidades regulatorias del gobierno nacional como la superintendencia de bancos y el SRI solicitan.

Una de las actividades que se realiza constantemente es el tema de actualizaciones a los diferentes sistemas bancarios como la banca virtual, cajeros electrónicos, entre los más utilizados, se procede con actualizaciones periódicas que se realizan mediante proyectos y controles de cambios internos que garantizan la seguridad e integridad de la información para evitar plagios y ataques.

Cuando las actualizaciones no salen como se espera viene el proceso de reverso de los cambios realizados y puede darse que los datos se corrompan y se requiera realizar un procedimiento denominado roll back, esta tarea es un mecanismo mediático que no es más que la reinstalación de los archivos modificados o recuperados de las copias de seguridad, así se agiliza y se minimiza los tiempos de respuesta y de servicio que banco mantiene a sus clientes.

Por estas razón por la cual es necesario buscar mecanismos que permitan mantener el sistema de copias de seguridad y la red SAN en óptimas condiciones, para lo cual se analiza ha realizado un análisis del tráfico entre los componentes tales como switch que conforman la red SAN, los dispositivos de almacenamiento y data protector que es la herramienta que realiza el proceso de obtención de los respaldos y restauraciones para sugerir procesos que mejoren los tiempos del proceso de las copias de seguridad.

El caso de estudio cumple con los lineamientos elementales para un análisis del comportamiento del sistema y se podrá obtener datos relevantes para emitir recomendaciones aplicables para un continuo mejoramiento y una optimización constante del sistema de

respaldos y red SAN, actualmente las empresas invierten recursos destinados a buscar soluciones ágiles, inteligentes y especializadas con el objetivo de disponer sistemas eficientes estructurados, donde se pueda mantener gran cantidad de información de alta importancia y crucial para la empresa de manera organizada y centralizada.

## 4. Objetivos

### ***Objetivo General:***

Realizar un estudio del comportamiento de la Red SAN como medio de transporte para la obtención de copias de seguridad y restauración de información por medio data protector, con el fin de optimizar y mejorar la red SAN para reducir los tiempos de ejecución del respaldo.

### ***Objetivos Específicos:***

1. Presentar el estado del arte de las redes SAN.
2. Estudiar la estructura, protocolos y características principales de la red SAN.
3. Presentar los equipos que conforman una red SAN.
4. Estudiar la arquitectura y los componentes que constituyen el sistema de copias de seguridad y restauración.
5. Analizar la red SAN y la herramienta de copias de seguridad Data Protector.
6. Analizar el consumo de Ancho de banda en la red SAN y de la herramienta de Data Protector.
7. Realizar un estudio comparativo entre las diferentes herramientas de copias de seguridad y restauración existentes en el mercado.
8. Presentar las recomendaciones necesarias para optimizar el tiempo de ejecución de los respaldos.
9. Presentar las recomendaciones necesarias para optimizar la red SAN.

## 5. Desarrollo Caso de Estudio

### 5.1. Estado del arte de las Redes SAN

#### 5.1.1. Definición de Red SAN

Una red SAN es una red de área de almacenamiento cuyas siglas en inglés son Storage Área Network (SAN). Es una red dedicada y exclusiva para conectar servidores, matrices, arreglos de discos y librerías de soporte. La red SAN es destinada a transportar datos entre servidores y recursos de almacenamiento a grandes velocidades, generalmente las conexiones se dan entre: servidor a equipo de almacenamiento, entre equipos de almacenamiento y de servidor a servidor.

El almacenamiento compartido simplifica la administración de la red SAN, lo que permite que sea muy flexible, esto se debe a que el cableado y los dispositivos de almacenamiento no necesitarán moverse de un servidor a otro. Cada dispositivo de la SAN es propiedad de un solo servidor o un computador.

Una SAN tiende a maximizar el aprovechamiento de almacenamiento, puesto que varios servidores pueden utilizar el mismo espacio reservado para crecimiento.<sup>1</sup>

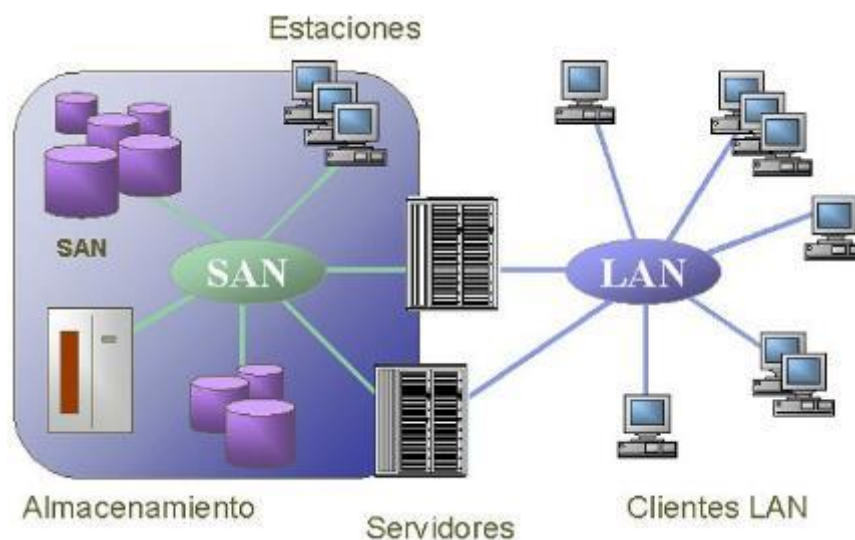


Figura 1 Diseño de red SAN.<sup>2</sup>

La red SAN enlaza los servidores o las estaciones de trabajo a los dispositivos, generalmente por Fibre Channel, un transporte versátil de alta velocidad. El modelo de red de área de almacenamiento (SAN) pone el almacenamiento en su propia red

<sup>1</sup> Mundo Cisco, ¿Qué es una Red SAN?, recuperado de:  
<http://www.mundocisco.com/2009/09/que-es-una-red-SAN.html>

<sup>2</sup> Google.com, Redes SAN, recuperado de:  
[https://www.google.com.ec/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjSksa4l\\_7QAhXFOhQKHbVaAMgQjRwIBw&url=https%3A%2F%2Fwww.ecured.cu%2FRed\\_de\\_%25C3%25A1rea\\_de\\_almacenamiento&psig=AFQjCNEOuKEVvOw9PYOEHmOtG\\_F0Utu3jQ&ust=1482165637414218](https://www.google.com.ec/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjSksa4l_7QAhXFOhQKHbVaAMgQjRwIBw&url=https%3A%2F%2Fwww.ecured.cu%2FRed_de_%25C3%25A1rea_de_almacenamiento&psig=AFQjCNEOuKEVvOw9PYOEHmOtG_F0Utu3jQ&ust=1482165637414218)

dedicada, eliminando el acaparamiento de datos tanto del bus SCSI del servidor a disco como de la red de usuario principal.

La red SAN incluye uno o más hosts que proporcionan un punto de la interfaz con los usuarios de LAN, así como (en el caso de SAN grandes) uno o más fabric switches y hubs de SAN para acomodar un gran número de dispositivos de almacenamiento.

Una red con el almacenamiento compartido que es visible para todos los servidores en SAN. Un paradigma de red que proporciona fácilmente conectividad reconfigurable entre cualquier subconjunto de equipos, almacenamiento en disco y hardware de interconexión, como switches.<sup>3</sup>

Los protocolos de red utilizados en una SAN son Fibre Channel e iSCSI. Una red de canal de fibra es una red muy rápida aislada normalmente del tráfico de la red LAN de la empresa. Sin embargo, es muy cara. Las tarjetas de canal de fibra óptica cuestan alrededor de mil dólares cada una. También requieren dispositivos especiales de canal de fibra.

**Fibre Channel:** Es un tipo de red de alta velocidad integrada por fibra óptica o cable de cobre y la implementación del protocolo de Fibra Canal. Un nombre generalizado para la tecnología de fibra óptica que es de uso frecuente para configurar una red de área de almacenamiento (SAN) o un entramado virtual (VSAN).

Un conjunto de estándares capaces de transferir datos entre los puertos y a través de los dispositivos de red en altas velocidades y sobre distancias perceptiblemente mayores que la tecnología SCSI, Fibre Channel admite las tecnologías de punto a punto, de bucle y de entramado.

**iSCSI:** Es una nueva tecnología que envía comandos SCSI sobre una red TCP/IP. Este método no es tan rápido como una red Fibre Channel, pero ahorra costes, ya que utiliza un hardware de red de menor costo.<sup>4</sup>

A partir de eventos críticos de desastre, como los atentados terroristas a los Estados Unidos del 11 de septiembre de 2001, los administradores de TI han tomado acciones al respecto, con servicios de cómo recuperarse ante un desastre, cómo recuperar miles de datos y lograr la continuidad del negocio, una de las opciones es contar con la red SAN; sin embargo, las compañías se pueden enfrentar a cientos de ataques, por lo que es necesario contar con un plan en caso de contingencia.

Es de vital importancia que el sitio donde se encuentre la SAN, se encuentre en un área geográfica distinta a donde se ubican los servidores que contienen la información crítica. Además, se trata de un modelo centralizado fácil de administrar, puede tener un bajo costo de expansión y administración, lo que la hace una red fácilmente

---

<sup>3</sup> Symantec Corporation, *SAN (red de área de almacenamiento)*, 1995 - 2016, Recuperado de: [https://www.symantec.com/es/mx/security\\_response/glossary/define.jsp?letter=s&word=SAN-storage-area-network](https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=s&word=SAN-storage-area-network)

<sup>4</sup> Symantec Corporation, *Fibre Channel*, 2016, Recuperado de: [https://www.symantec.com/es/mx/security\\_response/glossary/define.jsp?letter=f&word=fibre-channel](https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=f&word=fibre-channel)

escalable; fiabilidad, debido a que se hace más sencillo aplicar ciertas políticas para proteger a la red.

### 5.1.2. Estructura de una Red SAN

Las redes SAN proveen conectividad de E/S a través de las computadoras host y los dispositivos de almacenamiento combinando los beneficios de tecnologías Fibre Channel y de las arquitecturas de redes brindando así una aproximación más robusta, flexible y sofisticada que supera las limitaciones de DAS empleando la misma interfaz lógica SCSI para acceder al almacenamiento.

En el almacenamiento de conexión directa, Direct Attached Storage (DAS), el almacenamiento es local al sistema de ficheros, mientras que en SAN, el almacenamiento es remoto.



Figura 2 Estructura de una red SAN.<sup>5</sup>

La red SAN utiliza diferentes protocolos de acceso como Fibre Channel y Gigabit Ethernet. En el lado opuesto se encuentra la tecnología Network-Attached Storage (NAS), donde las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos Server Message Block (CIFS) y Network File System (NFS).

Las redes SAN se componen de tres capas:

1. **Capa Host:** esta capa consiste principalmente en servidores, dispositivos o componentes (HBA, GBIC, GLM) y software (sistemas operativos).

---

<sup>5</sup> Google.com, *Storage Área Network, Estructura de una red SAN*, recuperado de: [https://www.google.com.ec/search?q=La+red+de+almacenamiento+SAN&biw=1366&bih=700&source=lms&tbm=isch&sa=X&ved=0ahUKEwjRkuaOjeHQAhXGeCYKHxeCqQQ\\_AUIBigB#imgsrc=giMv9LQMj4KXWM%3A](https://www.google.com.ec/search?q=La+red+de+almacenamiento+SAN&biw=1366&bih=700&source=lms&tbm=isch&sa=X&ved=0ahUKEwjRkuaOjeHQAhXGeCYKHxeCqQQ_AUIBigB#imgsrc=giMv9LQMj4KXWM%3A)

2. **Capa Fibra:** esta capa la conforman los cables (fibra óptica) así como SAN switches como punto central de conexión para la SAN.
3. **Capa Almacenamiento:** esta capa la componen las formaciones de discos (Disk Arrays, memoria caché, RAID) y cintas empleados para almacenar datos.

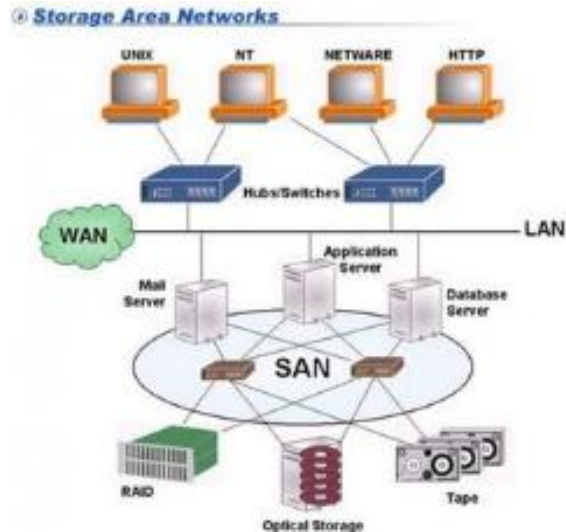


Figura 3 Capas de la red SAN.<sup>6</sup>

La red de almacenamiento puede ser de dos tipos:

- **Red Fibre Channel.**  
La red fibre channel es la red física de dispositivos Fibre Channel que emplea Fibre Channel Switches y directores y el protocolo Fibre Channel Protocol (FCP) para transporte (SCSI-3 serial sobre canal de fibra).
- **Red IP.**  
Emplea la infraestructura del estándar LAN con switches Ethernet interconectados. Una red SAN IP emplea iSCSI para transporte (SCSI-3 serial sobre IP).<sup>7</sup>

Canal de fibra (Fibre Channel): es un estándar, que transporta en gigabits, está optimizado para almacenamiento y otras aplicaciones de alta velocidad. Actualmente la velocidad que se maneja es de alrededor de 1 gigabit (200 MBps full-duplex). Fibre Channel soportará velocidades de transferencia full duplex arriba de los 400 MBps.

Hay tres topologías basadas en Fibre Channel.

1. Punto a punto (Point to Point).
2. Bucle Arbitrado (Arbitrated Loop).
3. Tejido Conmutado (Switched Fabric).

<sup>6</sup> Google.com, *Storage Área Network*, recuperado de:  
<https://www.google.com.ec/search?q=estructura+red+SAN&biw=1366&bih=700&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwjU1NfSi-HQAhVSgCYKHaRpBwoQ7AkIPQ#imgrc=nA5V2n-alwmURM%3A>

<sup>7</sup> Wikipedis.com, *Fibra Canal*, recuperado de:  
[https://es.wikipedia.org/wiki/Canal\\_de\\_fibra](https://es.wikipedia.org/wiki/Canal_de_fibra)

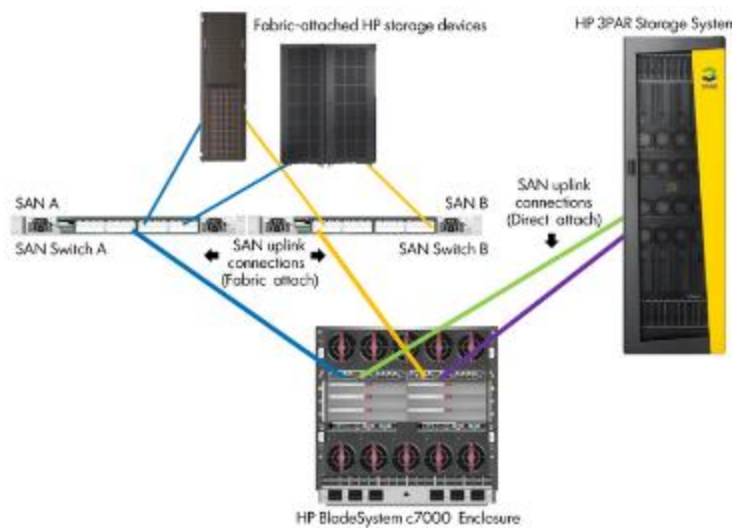


Figura 4 redes Fibre Channel.<sup>8</sup>

### Fibre Channel Fabric.

El “Tejido de Canal de Fibra” (Fibre Channel Fabric) fue diseñado como una interfaz genérica entre cada nodo y la interconexión con la capa física de ese nodo. Con la adhesión de esta interfaz, cualquier nodo "canal de fibra", puede comunicarse sobre el Tejido, sin que sea requerido un conocimiento específico del esquema de interconexión entre los nodos.

### Fibre Channel Arbitrated Loop.

Esta topología, se refiere a la compartición de arquitecturas, las cuales soportan velocidades full-duplex de 100 MBps o inclusive de hasta 200 MBps. Análogamente a la topología Token Ring, múltiples servidores y dispositivos de almacenamiento, pueden agregarse a mismo segmento del bucle.

Hasta 126 dispositivos pueden agregarse a un FC-AL (Fibre Channel Arbitrated Loop). Ya que el bucle es de transporte compartido, los dispositivos deben ser arbitrados, esto es, deben ser controlados, para el acceso al bucle de transporte, antes de enviar datos.

### Servicios Brindados por una Fabric.

Cuando un dispositivo se une a una Fabric su información es registrada en una base de datos, la cual es usada para su acceso a otros dispositivos de la Fabric, así mismo mantiene un registro de los cambios físicos de la topología. A continuación se presentan los servicios básicos dentro de una Fabric.

<sup>8</sup> Hewlett-Packard Development Company, L.P., *Fibre Channel networks*, recuperado de: [http://h17007.www1.hp.com/docs/enterprise/servers/oneview1.2/cic/en/content/s\\_cicug-netoverview-fc-about-fusion.html](http://h17007.www1.hp.com/docs/enterprise/servers/oneview1.2/cic/en/content/s_cicug-netoverview-fc-about-fusion.html)

**Login Service:** este servicio se utiliza para cada uno de los nodos cuando estos realizan una sesión a la Fabric (FLOGI). Para cada una de las comunicaciones establecidas entre nodos y la fábrica se envía un identificador de origen (S\_ID) y del servicio de conexión se regresa un D\_ID con el dominio y la información del puerto donde se establece la conexión.

**Name services:** toda la información de los equipos "logueados" en la Fabric son registrados en un servidor de nombre que realiza PLOGIN. Esto con la finalidad de tener todas las entradas registradas en una base de datos de los residentes locales.

**Fabric Controller:** es el encargado de proporcionar todas las notificaciones de cambio de estado a todos los nodos que se encuentren dados de alta dentro de la Fabric utilizando RSCNs (registro notificación de estado de cambio).

**Management Server:** el papel de este servicio es proporcionar un punto de acceso único para los tres servicios anteriores, basado en "contenedores" llamados zonas. Una zona es una colección de nodos que define a residir en un espacio cerrado.

### **5.1.3. Protocolos de la Red SAN**

Existen protocolos básicos usados en una red de área de almacenamiento:

1. FC-AL
2. FC-SW
3. SCSI
4. FCoE

**FC-AL. Protocolo Fibre Channel Arbitrated Loop:** usado en hubs, en el SAN hub este protocolo es el que se usa por excelencia, el protocolo controla quién puede comunicarse, sólo uno a la vez.

**FC-SW Protocolo Fibre Channel Switched:** usado en switches, en este caso varias comunicaciones pueden ocurrir simultáneamente. El protocolo se encarga de conectar las comunicaciones entre dispositivos y evitar colisiones.

**SCSI:** Usado por las aplicaciones, es un protocolo usado para que una aplicación de un equipo se comunique con el dispositivo de almacenamiento.

En la SAN, el SCSI se encapsula sobre FC-AL o FC-SW. SCSI trabaja diferente en una SAN que dentro de un servidor, SCSI fue originalmente diseñado para comunicarse dentro de un mismo servidor con los discos, usando cables de cobre. Dentro de un servidor, los datos SCSI viajan en paralelo y en la SAN viajan serializados.

**FCoE:** Es una tecnología de red de computadoras que encapsula las tramas de canal de fibra a través de redes Ethernet. Esto permite al canal de fibra utilizar 10 redes Gigabit Ethernet (o velocidades más altas), preservando el protocolo Fibre Channel. La

especificación fue parte del Comité Internacional de Estándares de Tecnologías de Información T11 FC-BB-5 estándar publicado en 2009.<sup>9</sup>

#### **5.1.4. Características principales de la Red SAN.**

Las principales características de la red SAN se detallan a continuación:

- **Latencia:** una de las diferencias y principales características de las SAN es que son construidas para minimizar el tiempo de respuesta del medio de transmisión.
- **Conectividad:** permite que múltiples servidores sean conectados al mismo grupo de discos o librerías de cintas, permitiendo que la utilización de los sistemas de almacenamiento y los respaldos sean válidos.
- **Distancia:** las SAN al ser construidas con fibra óptica heredan los beneficios de esta, por ejemplo, las SAN pueden tener dispositivos con una separación de hasta 10 km sin repetidores.
- **Velocidad:** el rendimiento de cualquier sistema de cómputo dependerá de la velocidad de sus subsistemas, es por ello que las SAN han incrementado su velocidad de transferencia de información, desde 1 Gigabit, hasta actualmente 4 y 8 Gigabits por segundo.
- **Disponibilidad:** una de las ventajas de las SAN es que al tener mayor conectividad, permiten que los servidores y dispositivos de almacenamiento se conecten más de una vez a la SAN, de esta forma, se pueden tener "rutas" redundantes que a su vez incrementarán la tolerancia a fallos.
- **Seguridad:** la seguridad en las SAN ha sido desde el principio un factor fundamental, desde su creación se notó la posibilidad de que un sistema accediera a un dispositivo que no le correspondiera o interfiriera con el flujo de información, es por ello que se ha implementado la tecnología de zonificación, la cual consiste en que un grupo de elementos se aíslan del resto para evitar estos problemas, la zonificación puede llevarse a cabo por hardware, software o ambas, siendo capaz de agrupar por puerto o por WWN (World Wide Name), una técnica adicional se implementa a nivel del dispositivo de almacenamiento que es la Presentación, consiste en hacer que una LUN (Logical Unit Number) sea accesible sólo por una lista predefinida de servidores o nodos (se implementa con los WWN).

Una parte esencial de la seguridad de las redes de área de almacenamiento es la ubicación física de todos y cada uno de los componentes de la red. La construcción de un data center es sólo la mitad del desafío, es el hecho de decidir dónde se instalará los componentes de la red (tanto software como hardware) la otra mitad y la más difícil.

---

<sup>9</sup> WIKIPEDIA, Red de área de almacenamiento, recuperado de:  
[https://es.wikipedia.org/wiki/Red\\_de\\_%C3%A1rea\\_de\\_almacenamiento](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento)

Los componentes críticos de la red, como pueden ser los switches, matrices de almacenamiento o hosts los cuales deben estar en el mismo data center. Al implementar seguridad física, sólo los usuarios autorizados pueden tener la capacidad de realizar cambios tanto físicos como lógicos en la topología, cambios como pueden ser: cambio de puerto de los cables, acceso a reconfigurar algún equipo, agregar o quitar dispositivos, entre otros.

La planificación también debe tomar en cuenta las cuestiones del medio ambiente como puede ser la refrigeración, la distribución de energía y los requisitos para la recuperación de desastres. Al mismo tiempo se debe asegurar que las redes IP que se utilizan para gestionar los diversos componentes de la SAN son seguras y no son accesibles para toda la compañía. También tiene sentido cambiar las contraseñas por defecto que tienen los dispositivos de la red para así prevenir el uso no autorizado.

- **Componentes:** los componentes primarios de una SAN son: switches, directores, HBAs, servidores, ruteadores, gateways, matrices de discos y librerías de cintas.
- **Topología:** cada topología provee distintas capacidades y beneficios las topologías de SAN son:
  - Cascada (cascade).
  - Anillo (ring).
  - Malla (meshed).
  - Núcleo/borde (core/edge).

**ISL (Inter Switch Link, enlace entre switch):** actualmente las conexiones entre los switches de SAN se hacen mediante puertos tipo "E" y pueden agruparse para formar una troncal (trunk) que permita mayor flujo de información y tolerancia a fallos.

- **Arquitectura:** los canales de fibra actuales funcionan bajo dos arquitecturas básicas, FC-AL (Fibre Channel Arbitrated Loop) y Switched Fabric, ambos esquemas pueden convivir y ampliar las posibilidades de las SAN. La arquitectura FC-AL puede conectar hasta 127 dispositivos, mientras que switched fabric hasta 16 millones teóricamente.<sup>10</sup>

---

<sup>10</sup> Wikipedia, *Red de área de almacenamiento*, recuperado de:  
[https://es.wikipedia.org/wiki/Red\\_de\\_%C3%A1rea\\_de\\_almacenamiento](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento)

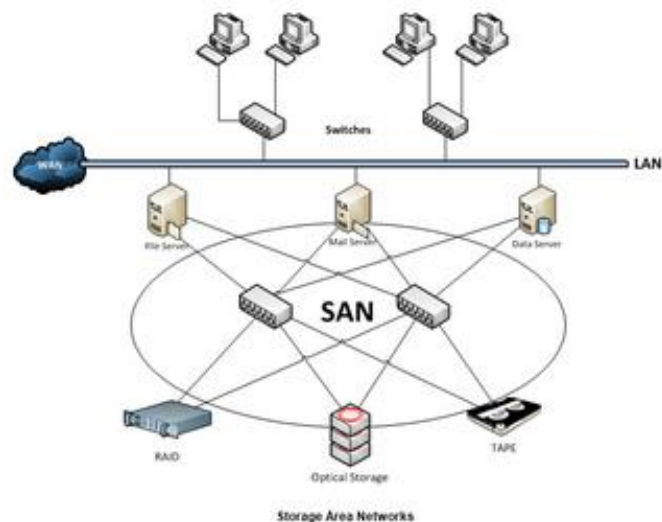


Figura 5 Topología de Red SAN.<sup>11</sup>

#### 5.1.5. Importancia de la Red SAN.

La importancia de mantener una red SAN se debe a la seguridad y velocidad de transmisión de información, no todos pueden acceder fácilmente a los equipos, menormente a la información almacenada, brindando un blindaje al acceso no autorizado, esto garantiza la integridad y disponibilidad de la información en caso de desastre.

La red SAN es independiente de la red LAN, los hosts se encuentran en redes distintas, los servidores de la red SAN, se encuentran dentro de una misma ubicación y en el mismo segmento de la red SAN.

#### 5.1.6. Equipos que conforman la Red SAN.

Los equipos que conforman una red SAN son servidores, dispositivos de almacenamiento y los equipos de interconexión, los cuales se describen a continuación.

- **Servidores:** Una red de almacenamiento debe ser una red abierta y heterogénea en la que entre a formar parte todo tipo de servidores con todo tipo de sistemas operativos que puedan acceder al almacenamiento de la red.
- **Dispositivos de almacenamiento:** Los dispositivos de almacenamiento son la base de la SAN. La SAN libera el almacenamiento de tal manera que ya no forma parte de un bus particular de un servidor, es decir, el almacenamiento se externaliza y su funcionalidad se distribuye. Tantas unidades de cinta magnética o librerías y robots de cintas como cabinas de discos se conectan directamente a la red Fibre Channel.

<sup>11</sup> Google.com, *Storage Área Network, Estructura de una red SAN*, recuperado de: [http://ensamblemantenimientocampoalto.blogspot.com/p/blog-page\\_12.html](http://ensamblemantenimientocampoalto.blogspot.com/p/blog-page_12.html)

- **Elementos de Interconexión:** Toda la terminología de una red de datos se hereda en el mundo de las SAN para definir los dispositivos y elementos usados para interconectar los servidores con el almacenamiento. Cualquier dispositivo conectado a un puerto de un conmutador puede conectarse con cualquier otro dispositivo de la red.

El hecho de que servidores y sistemas de almacenamiento compartan la misma red permite la transferencia de datos de tres maneras distintas:

1. **Entre servidor y almacenamiento:** Es el modelo tradicional de interacción, aunque en el caso de una SAN el mismo dispositivo de almacenamiento puede ser accedido por múltiples servidores.
2. **Entre servidores:** La propia SAN puede usarse como medio de comunicaciones entre servidores.
3. **Entre dispositivos de almacenamiento:** La SAN permite la transferencia de datos entre sistemas de almacenamiento sin intervención directa de los servidores.

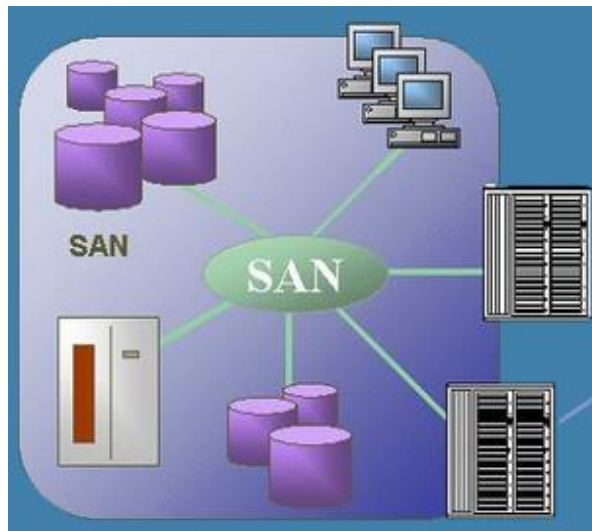


Figura 6 Equipos de una red SAN.<sup>12</sup>

### 5.1.7. Ventajas y desventajas de la Red SAN

El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza. En el caso de una red de canal de fibra, el ancho de banda es de aproximadamente 100 megabytes/segundo (1.000 megabits/segundo) y se puede extender aumentando la cantidad de conexiones de acceso. La capacidad de una SAN se puede extender de manera casi ilimitada y puede alcanzar cientos y hasta miles de terabytes.

<sup>12</sup> Sistemas Informáticos III, *Redes de Almacenamiento SAN*, recuperado de: <https://nikenver.wordpress.com/2014/04/23/tipos-de-redes/>

Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones que funcionan como una interfaz entre la red de datos (generalmente un canal de fibra) y la red de usuario (por lo general Ethernet).

Por otra parte, una SAN es mucho más costosa que una NAS ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara. Normalmente, cuando una compañía estima el TCO (Coste total de propiedad) con respecto al coste por byte, el coste se puede justificar con más facilidad.

## 5.2. Herramienta de Backup Data Protector.

Data Protector es un software licenciado perteneciente a la empresa HPE, Data Protector es una herramienta especializada en obtener copias de seguridad y recuperación de datos completa, con análisis en tiempo real y opciones de optimización que permite una administración amigable y confiable.

Data Protector es una herramienta diseñada para infraestructuras a nivel empresarial que unifica y aprovecha al máximo la automatización para obtener copias de seguridad y restauración de manera centralizada e inteligente. Permite estandarizar las copias de seguridad y la restauración de varias plataformas como HP-UX, AIX y Windows permitiendo canalizarlas a medios de almacenamiento robustos como librerías o storage.

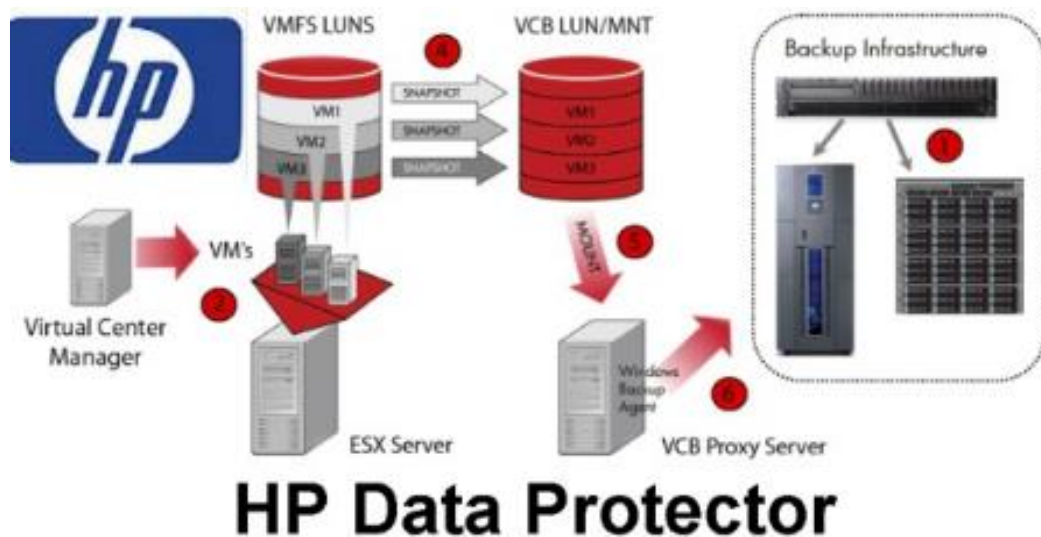


Figura 7 HP Data Protector.<sup>13</sup>

<sup>13</sup> HPE.com, *Best Backup Softwares*, recuperado de: [https://encrypted-tbn3.gstatic.com/images?q=tbn:AND9GcQjV2xQebQkgVvRW-NvB\\_wgE-G87mapBCSjgk7jqB73LLK34Hj3Eg](https://encrypted-tbn3.gstatic.com/images?q=tbn:AND9GcQjV2xQebQkgVvRW-NvB_wgE-G87mapBCSjgk7jqB73LLK34Hj3Eg)

### **5.2.1. Beneficios.**

Entre los principales beneficios que Data Protector brinda, se puede mencionar los siguientes:

- Análisis avanzados para obtener una mejor información y valor empresarial.
- La matriz de soporte completo simplifica su experiencia de copia de seguridad y recuperación.
- Obtención de copias de seguridad de manera centralizada.
- Las opciones de recuperación avanzadas le permiten satisfacer las estrictas expectativas de nivel de servicio y recuperación.
- La de duplicación federada optimiza el almacenamiento de copia de seguridad y reduce los costes.
- La protección basada en políticas automatizada para ambientes virtuales reduce la exposición a la pérdida de datos y mejora la gobernabilidad de TI.
- Protección de instantánea de copia de seguridad de tiempo de inactividad cero para satisfacer fácilmente las demandas de ventana de backup decrecientes.
- La arquitectura de recuperación por niveles optimiza el coste general de la copia de seguridad.<sup>14</sup>

### **5.2.2. Requerimientos para la instalación del Cell Manager de Data Protector.**

#### **Cell Manager Unix.**

La cuenta para instalar data protector debe tener permisos de ROOT.

Tener el protocolo TCP/IP instalado y funcional, el protocolo debe ser capaz de resolver los sistemas clientes involucrados en la solución de Backup por HOSTNAME.

Los siguientes puertos deben estar libres (no pueden estar asignados o usados por otras aplicaciones) y sin restricciones (firewall):

- 5555 — Puerto default comunicaciones Data Protector.
- 7112 — Puerto Servicio de la IDB (Internal Database).
- 7113 — Puerto conexión del Pooler de la Internal Database (IDB CP).
- 7116 — Puerto Application Server (HTTPS AS).
- 9999 — Puerto administración Application Server.

Soportar nombres largos para los archivos.

Servicio Telnet habilitado y funcional.

Demonio INETD o XINETD (según aplique) instalado y funcional.

---

<sup>14</sup> HPE, *HPE Data Protector*, recuperado de:  
<http://www8.hp.com/ec/es/software-solutions/data-protector-backup-recovery-software/>

Crear el grupo de usuarios hpdp y la cuenta de usuario dedicada hpdp configurado en el sistema operativo para que puedan ser usados por Data protector.

Soportar rexec.

Recomendado usar LFS (large file Support) en los filesystem.

El espacio en disco recomendado es de 100 Gb o superior para el punto de montaje que almacenara la Internal database (IDB) de modo que permita el crecimiento de esta.

Para HP - UX debe setear el parámetro de Kernel shmmax no menor 2,5 Gb, ejecutando: kusage shmmax

Para HP - UX debe setear el parámetro de Kernel maxdsiz o maxdsiz\_64 como mínimo en 134217728 bytes (128 MB).

Para HP-UX setear el parámetro de Kernel semmnu no menor de 256.

Para Linux setear el parámetro de Kernel shmmax no menor de 2,5 Gb, verifíquelo con: cat /proc/sys/kernel/shmmax

En Solaris se recomienda configurar el parámetro de kernel shmsys: shminfo\_shmmax (máximum shared memory segment size (SHMMAX)) en /etc/system a 67108864 bytes (64 MB).

Recomendado adicionar la ruta /opt/omni/lib/man a la variable MANPATH para poder acceder a la ayuda desde cualquier path.

Las librerías físicas de cintas deben estar conectadas a través de la SAN al Cell manager (core) y los clientes que vayan a enviar sus backup por SAN. Estos deben poder ver los drives y la robótica de la librería desde su sistema operativo.

Las librerías virtuales (VTL's) emuladas en un dispositivo D2D o B6XXX deben poderse ver los drivers y la robótica de librería desde su sistema operativo en el Cell manager (core) y los clientes que vayan a enviar sus backup por SAN.

#### **Cientes a tomar backup unix:**

Usuario con permisos de root.

Archivo hosts referenciando al cell manager por su nombre completo e IP.

TCP/IP habilitado y funcional.

Servicio de telnet instalado y funcional.

Rexec habilitado y funcional.

En el caso de tener firewall definir rango de puertos (adicionales a los ya mencionados) por el que no existan restricciones para la transmisión bidireccional de datos entre el cliente y el cell manager.

### **Cell Manager Windows.**

Usuario con permisos de ADMINISTRATOR.

Permisos de acceso de red seteados en la política local de seguridad del servidor.

Tener el protocolo TCP/IP instalado y funcional, el protocolo debe ser capaz de resolver los sistemas clientes involucrados en la solución de Backup por HOSTNAME, el nombre del computador y el de su HOSTNAME deben ser exactamente iguales.

Tener una IP estática asignada, si por alguna razón el servidor debe de usar DHCP debe de configurarse adicionalmente un servidor DHCP para que reserve una IP estática para el sistema.

Los siguientes puertos deben estar libres (no pueden estar asignados o usados por otras aplicaciones) y sin restricciones (firewall):

- 5555 — Puerto default comunicaciones Data Protector
- 7112 — Puerto Servicio de la IDB (Internal Database)
- 7113 — Puerto conexión del Pooler de la Internal Database (IDB CP)
- 7116 — Puerto Application Server (HTTPS AS)
- 9999 — Puerto administración Application Server

Soportar nombres largos para los archivos.

Cliente Telnet habilitado y funcional.

En Windows Server, en el Firewall del Sistema Operativo debe estar configurado para aceptar "Remote Service Administration" (NP) connections (port 445).

Terminal services habilitado y funcional para el caso que se necesite desplegar remotamente el cell manager, agentes y/o binarios.

Se recomienda usar filesystems tipo NTFS para el crecimiento de los datafiles de la base de datos interna.

El espacio en disco recomendado es de 100 Gb o superior para el punto de montaje que almacenara la Internal database (IDB) de modo que permita el crecimiento de esta.

Se recomienda en Windows que exista un segundo disco o en su defecto sea partición lógica de un disco físico distinto al disco C:\ para albergar la IDB de modo que no se pierdan los archivos de configuración si se presentase un fallo en el sistema operativo.

Las librerías físicas de cintas deben estar conectadas a través de la SAN al Cell Manager (core) y a los clientes que vayan a enviar sus backup por SAN. Estos deben de poder ver los drives y la robótica de la librería desde la sección de dispositivos (panel de control).

Las librerías virtuales (VTL's) emuladas en un dispositivo D2D o B6XXX deben poderse ver los drives y la robótica de la librería desde la sección de dispositivos (panel de control) en el Cell Manager (core) y los clientes que vayan a enviar sus backup por SAN y puedan verla.

#### **Cientes a tomar backup Windows:**

Usuario con permisos de Administrador.

Archivo hosts referenciando al cell manager por su nombre completo e IP.

TCP/IP habilitado y funcional.

Ciente telnet instalado y funcional.

En el caso de tener firewall definir rango de puertos (adicionales a los ya mencionados) por el que no existan restricciones para la transmisión bidireccional de datos entre el cliente y el Cell Manager.

#### **5.2.3. Arquitectura de Data Protector.**

La arquitectura de data protector está definida por los siguientes aspectos.

**Arquitectura escalable y altamente flexible.** Data Protector puede utilizarse en ambientes que van desde un único sistema hasta miles de sistemas en varios sitios. Debido al concepto de componente de red de Data Protector, los elementos de la infraestructura de respaldo pueden colocarse en la topología de acuerdo con los requisitos del usuario. Las numerosas opciones de backup y alternativas a la creación de una infraestructura de respaldo permiten la implementación de prácticamente cualquier configuración. Data Protector también se integra perfectamente con los dispositivos de respaldo HP StoreOnce y HP StoreEver.

**Administrador de Cell de Data Protector.** Una celda de HP Data Protector es un conjunto de sistemas con una política de copia de seguridad común existente en la misma LAN / SAN. Cell Manager es el sistema principal que es el punto central para administrar este entorno de red. Contiene la base de datos interna de HP Data Protector (IDB) y ejecuta el software principal de HP Data Protector y los administradores de sesión. La base de datos interna realiza un seguimiento de los archivos de copia de seguridad y la configuración de la celda.

**Ciente Data Protector.** Un sistema host se convierte en un cliente de HP Data Protector cuando uno o más de los componentes de software de HP Data Protector están instalados en el sistema. Los sistemas cliente con discos que necesitan una copia

de seguridad deben tener instalado un componente adecuado de Data Protector Disk Agent.

El agente de discos le permite hacer una copia de seguridad de los datos del disco cliente o restaurarlos. Los sistemas cliente que están conectados a un dispositivo de copia de seguridad deben tener instalado un componente de agente multimedia. Este software gestiona dispositivos y medios de copia de seguridad.<sup>15</sup>

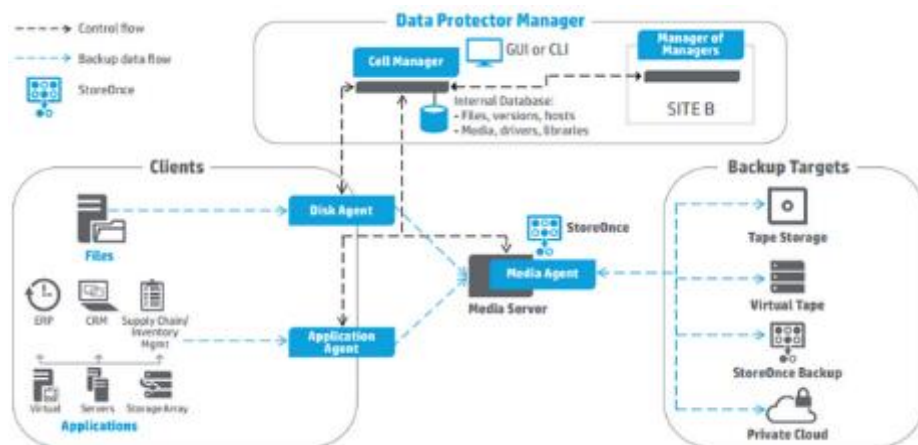


Figura 8 Arquitectura de Data Protector.<sup>16</sup>

Data protector maneja su propia base de datos donde almacena localmente las configuraciones de los job o tareas programadas que han sido creadas y que son asociados a los servidores de los cuales se obtendrá una copia de seguridad, almacena datos de las sesiones realizadas para ser utilizadas en las restauraciones futuras.

#### 5.2.4. Cell Manager.

El Cell Manager de Data Protector es el entorno gráfico por medio del cual permite la configuración necesaria para la obtención de las copias de seguridad y restauraciones, es un ambiente amigable en el cual puede generar y programar actividades personalizadas que le permitirán una mejor administración del producto y mejor administración a nivel de tareas planificadas.

A continuación en la imagen se puede apreciar de mejor manera como Data Protector utiliza un menú para su navegación y configuración, de manera general se comentara algunas de sus opciones, ya que el punto focal del caso de estudio es conocer a detalle la red SAN que constituye el sistema de respaldos.

<sup>15</sup> HP, *Student Book, HP Arquitectura Data Protector*, recuperado de: <http://hpstudentworkbook.blogspot.com/2014/11/hp-data-protector-architecture.html>

<sup>16</sup> HP Student, *Arquitectura de Data Protector*, recuperado de: <http://hpstudentworkbook.blogspot.com/2014/11/hp-data-protector-architecture.html>

La ventana principal de Cell Manager cuenta con un menú donde están opciones como: Clientes, Usuarios, Devices & Media Backup, Object Operations, Monitor, Restore, Instant Recovery, Reporting, y la internal data base.

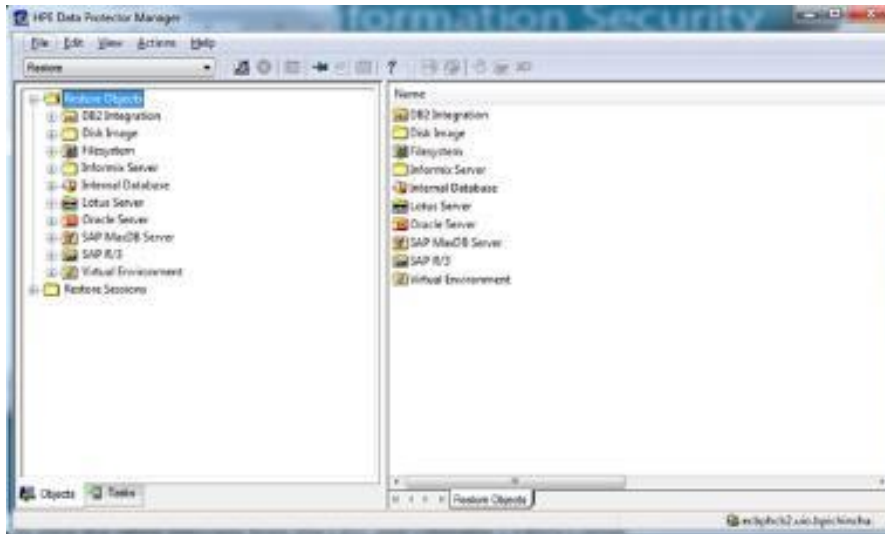


Figura 9 Cell Manager Data Protector.



Figura 10 Menú principal de data protector.

Cada una de sus opciones está diseñada para la administración del producto y obtener el mayor provecho de la herramienta, así se pone en consideración los siguientes puntos más relevantes.

- **Clientes:** En la presente opción lista todos los clientes que se encuentran asociados al Cell Manager de data protector, la lista solo muestra los equipos que utilizan la red SAN para la obtención de copias de seguridad y restauración.
- **Usuarios:** Creación de usuarios y perfiles de acceso a la herramienta de data protector donde define los privilegios, permisos y acciones de los usuarios.
- **Device & Media:** Son los dispositivos de almacenamiento tales como librerías que se encuentran ligadas al data protector, previamente se debe realizar la

zonificación para que los dispositivos se puedan reconocer y visualizar es el medio físico mediante el cual la herramienta data protector obtendrá o recuperará la información procedente de la copia de seguridad.

- **Backup:** pestaña en la cual se configura las diferentes opciones para poder realizar las copias de seguridad, también puede configurar las tareas planificadas y calendarizarlas.
- **Monitor:** Pestaña en la cual indica las actividades que está realizando la herramienta de copias de seguridad y restauraciones. Se puede visualizar en tiempo real si está realizando una tarea de backup o de restauración.
- **Restore:** Aquí se puede ver las sesiones que han sido restauradas, también consta del pool de trabajo en la cual detalla las políticas y los grupos de ejecución para cada restauración.

Las políticas son generadas a un grupo de servidores que comparten afinidad en la política, esta también ocasiona una desventaja, debido a que si un servidor se modifica o elimina, el job devuelve un error.

Una tarea planificada hace referencia a la calendarización de una copia de seguridad determinada en un espacio del tiempo ya definido. La definición está dada por el ambiente, la permanencia de retención del backup y la criticidad de la información.

Siendo el caso se puede determinar la siguiente tabla de contención de la información:

AMBIENTE	Diario FS	Mensual FS	DB	FS
<b>Producción</b>	30 días	90 días	10 años	1 año
<b>Test</b>	30 días	90 días	10 años	1 año
<b>Desarrollo</b>	30 días	90 días	10 años	1 año

*Tabla 1 Tiempo de retención de la información.*

Data protector está en monitoreo constante y será considerado como la herramienta principal para el tema de copias de seguridad y restauraciones, cotidianamente conviven también herramientas como: Arcserve y Netbackup, TSM, herramientas que han sido evaluadas por varios meses y no se ha obtenido la estabilidad y los beneficios que Data Protector ha proporcionado.

### **5.3. Arquitectura, componentes del sistema de copias de seguridad y restauraciones.**

La empresa TCS, cuenta con un sistema de copias de seguridad y restauraciones para dos ambientes principales definidos de la siguiente manera; el ambiente de producción donde alberga la mayor cantidad de información y los equipos con mejores características que son destinados a brindar servicios y aplicaciones y facilitan la interoperabilidad entre las entidades bancarias y los usuarios o cuenta ahorristas, seguidamente también dispone de un ambiente de test, el cual es destinado a las pruebas previas al paso a producción.

Existe un ambiente de desarrollo que es donde nacen las aplicaciones y los servicios; los cuales posteriormente pasaran al ambiente de testing para su valoración y control de calidad y seguidamente ser implementados y puestos en ejecución en el ambiente productivo, para el ambiente de desarrollo aún no existe una política definida para la obtención de copias de seguridad y solo se lo aplica a ciertos equipos que se consideran importantes, esta es una de las razones por la cual el nivel de carga aumenta en la red SAN y ocasiona que se produzca una saturación en el sistema de respaldos.

Los equipos de se involucran en el sistema de copias de seguridad y restauraciones conviven en una infraestructura compuesta por los siguientes dispositivos, dos directores y varios switches SAN, unidades de almacenamiento como librería y la conexión a los distintos servidores en sus diferentes plataformas, así se tiene equipos con HP-UX, AIX, Linux, el servidor de respaldos está integrado con un Cell Manager, que es la consola grafica de administración y configuración de data protector, en el desarrollo de esta punto se mencionará y describirá cada uno de sus componentes y se definirá conceptos fundamentales de la red SAN y Data Protector.

La Figura 11 representa la red SAN, en la cual se centrará el análisis para determinar las recomendaciones y sugerencias necesarias que permitan mitigar la demora en la obtención de las copias de seguridad y restauración.

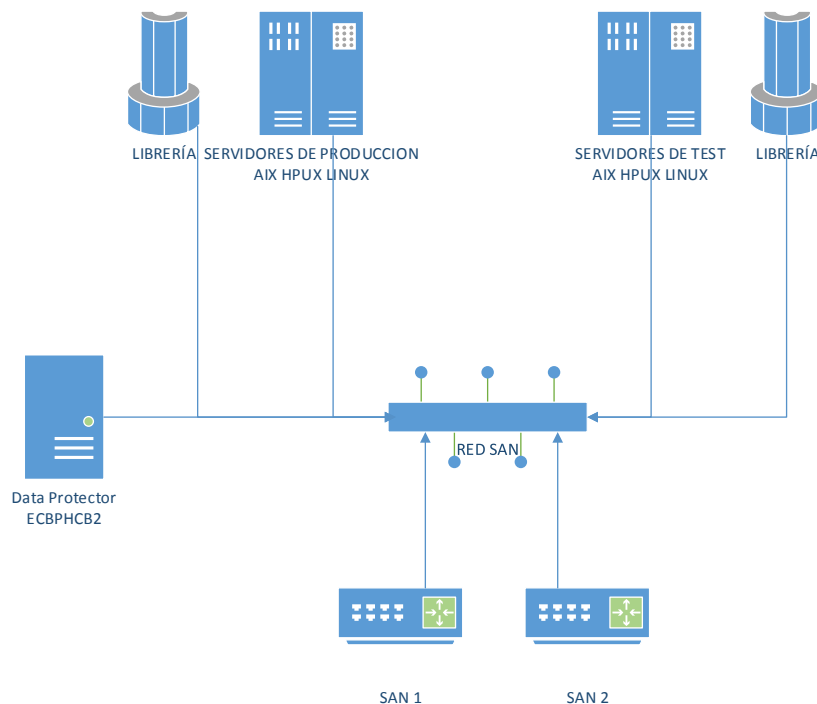


Figura 11 Infraestructura del sistema de copias de seguridad y restauraciones.

Brevemente se presentan los equipos de almacenamiento y los equipos que se encargan de la asignación de espacio de provisión de discos para la utilización de cada uno de los servidores.

### 5.3.1. Librerías

Son equipos de almacenamiento de información que se conectan entre los directores, los equipos de almacenamiento y los servidores para la obtención de las copias de seguridad por medio de data protector, en la empresa la más utilizada es la librería MSL 6480 que cumple con características aceptables para la automatización y trabajo requerido.



*Figura 12 Librería MSL6480.*

#### **Principales características y ventajas.**

- Escalabilidad en el sector con el fin de obtener una mejor solución de cinta.
- La librería de cintas HP MSL6480 preserva su inversión de capital inicial con una solución única que se amplía sin discontinuidades para adaptarse a sus necesidades. Puede abordar sus necesidades de almacenamiento a corto y largo plazo sin esfuerzo y responder a cambios, servicios o crecimiento de naturaleza impredecible.
- La librería de cintas MSL6480 presenta una arquitectura ampliable, la cual le permite pagar a medida que crece, solo tiene que añadir nuevos módulos para aumentar la capacidad y el rendimiento sin invertir en una librería nueva completa. En caso necesario, las actualizaciones se realizan de manera rápida y sin interrupciones. Puede ampliar verticalmente de 80 a 560 ranuras de cartuchos para almacenar hasta 3,5 PB en un único rack de 19 pulgadas; añada entre 1 y 42 unidades Fibre Channel (FC) o SAS LTO-5 o LTO-6 de media altura para obtener velocidades de hasta 60,4 TB/h, una LTO-6 con una compresión de datos de 2,5:1, lo que permite ahorrar mucho tiempo.
- Las librerías de cintas HP MSL le permiten gestionar con facilidad los soportes dentro y fuera de la librería de cintas mediante un lector de código de barras estándar y cargadores de 10 ranuras configurables.
- Reduce el tiempo de administración: capacidad de gestión y fiabilidad de clase empresarial
- La librería de cintas HP MSL6480 libera sus recursos con capacidades de protección y archivo de datos simplificado, consolidado y automatizado que reducen la intervención y los errores humanos, con la consiguiente mejora de sus resultados

finales. Sus administradores pueden gestionar, configurar y usar la librería desde cualquier parte de la oficina o del mundo con las exclusivas herramientas de diagnóstico y gestión a distancia basadas en la Web de HP.

- Los administradores pueden supervisar de manera proactiva e inteligente el uso, el rendimiento operativo y la vida útil y el estado global de la librería, las unidades y los soportes de su infraestructura de cintas con el software HP StoreEver TapeAssure Advanced.
- La división en particiones permite una mayor utilización de los activos, al consolidarse varias librerías y aplicaciones en una sola librería de cintas.
- Reduce costes de hardware, espacio físico, refrigeración y energía
- La librería de cintas HP MSL6480 ofrece hasta 81 TB por 1U de espacio en rack utilizando unidades LTO-6, además de brindar la más alta densidad de unidad de cinta por módulo de cualquier librería de cinta de gama media.
- La librería de cintas MSL6480 ofrece escalabilidad de 80 a 560 ranuras con una única librería ampliable, por lo que no es necesario quitar y reemplazar a medida que crezcan sus necesidades de almacenamiento.
- En el caso de los clientes de librería MSL existentes, reutilice los recipientes de unidades de cinta HP MSL2024, MSL4048, MSL8048 y MSL8096 en la librería de cintas MSL6480 para aprovechar las inversiones existentes.

### **5.3.2. Storage.**

Una red de área de almacenamiento, en inglés Storage Área Network (SAN), es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad de canal de fibra o iSCSI.
- Un equipo de interconexión dedicado entre directores, switches.

La función Data Storage es el conjunto de especificaciones que sirven para definir cómo, cuándo y qué se almacena. En toda organización, independientemente del sector o el tamaño, puede observarse que los datos crecen a un ritmo exponencial y eso genera un problema a la hora de almacenarlos. Ya no es suficiente con almacenar, sino que hay que definir una estrategia que sienta las bases del almacenamiento.

La función de Data Storage busca implementar buenas prácticas y políticas que cumplan con los objetivos fijados desde el Data Governance, de forma que no se pierda alineación con las políticas de cada empresa.

### **5.3.3. Directores y SAN Switch.**

En el campo de almacenamiento, un switch Fibre Channel es un equipo de red compatible con el protocolo Fibre Channel (FC). Permite la creación de un tejido Fibre Channel, que actualmente es el componente principal de la mayoría de las redes de área de almacenamiento SAN.

El tejido es una red de dispositivos Fibre Channel que permite la comunicación muchos-a-muchos, búsqueda de nombre de dispositivo, seguridad y redundancia. Los switch FC implementan la zonificación, un mecanismo que deshabilita el tráfico no deseado entre determinados nodos de tejido.

Un director de canal de fibra es, por convención actual, un switch no menor de 128 puertos. No difiere de un switch en la funcionalidad del protocolo FC central.

Los switch Fibre Channel se pueden implementar uno a la vez o en configuraciones de switch múltiples más grandes. Los administradores de SAN suelen añadir nuevos switch a medida que crecen sus necesidades de servidor y almacenamiento, conectando los switch a través de un cable de fibra óptica utilizando los puertos estándar del dispositivo.

Varios de los proveedores de switch ahora ofrecen puertos dedicados de apilamiento de alta velocidad para manejar conexiones inter-switch (similares a los switch Ethernet apilables existentes), permitiendo crear configuraciones de switch múltiples de alto rendimiento con menor número de switch en general.

Los principales fabricantes de switch Fibre Channel son: Brocade, Cisco Systems, Dell y QLogic.

En la figura 13 se aprecia un equipo SAN Switch de marca HP, un equipo de gama alta dedicado a empresa con enfoque y visión de calidad y manejo de información a grandes velocidades.



*Figura 13 San Switch.<sup>17</sup>*

---

<sup>17</sup> NetStorageWorks.com, *HP StoreFabric 8/80 SAN Switch*, recuperado de: <http://www.netstorageworks.com/images/StoreFabric/HP-8-80-Base.png>

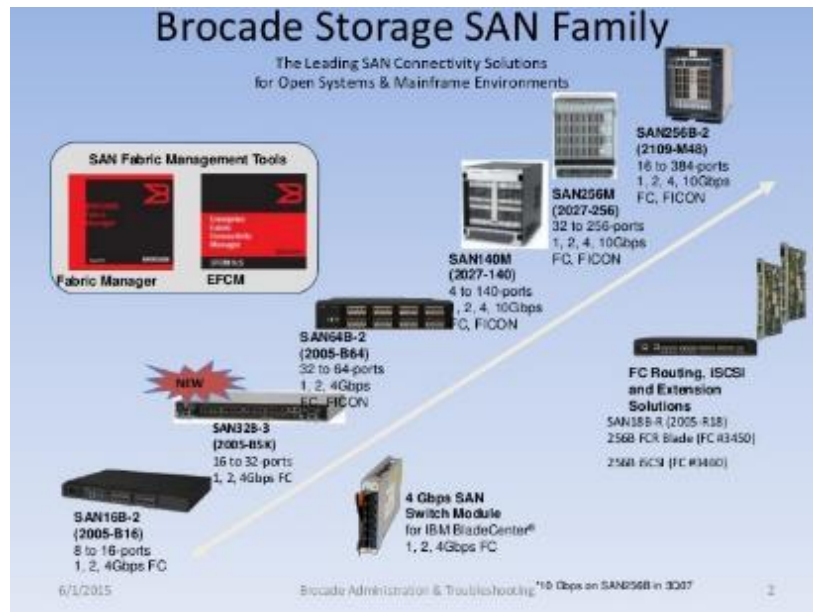


Figura 14 Familia de equipos Brocade.<sup>18</sup>

#### 5.4. Análisis de la red SAN y la herramienta de copias de seguridad Data Protector.

El análisis en el presente caso de estudio se ha considerado realizarlo en los siguientes dispositivos SAN switch y el servidor de data protector.

Como preámbulo se indicará que el SAN switch tiene las siguientes características técnicas.

- SANSwitch: SANSWBP12 IP: 10.151.16.131
- SANSwitch: SANSWBP11 IP: 10.151.16.134

El servidor de data protector es un equipo físico donde está instalado HP-UX como sistema operativo y es el servidor principal donde se situó la versión 9 del producto mencionado

- Procesador 8 cores.
- Memoria 25 Gb.
- Sistema Operativo HP-UX 11.31

##### 5.4.1. Análisis de la red SAN.

###### Información General.

Para el análisis de la red SAN, se consideró realizar el estudio de la situación actual de la infraestructura de los directores, SAN switches y la conexión con los servidores, se tomó como punto de inicio el estudio del comportamiento de servidor de data protector y su asociación con los equipos de almacenamiento.

<sup>18</sup> Brocade Storage, *Brocade Storage San Family*, recuperado de: <http://image.slidesharecdn.com/d4e1327a-d364-4901-a356-3962b429dc1f-150601133900-lva1-app6892/95/brocade-administration-troubleshooting-2-638.jpg?cb=1433166402>

Para la realización de esta tarea fue necesario realizarlo por medio de herramientas dedicadas y especializadas en la obtención de métricas y análisis de consumos de anchos de banda, la información obtenida será interpretada para la generación de un reporte de fácil entendimiento y sus datos puedan ser puestos a consideración para la toma de decisiones empresariales.

La recolección de la información fue obtenida mediante SAN Health, la investigación de la data fue enviada de manera encriptada a los servidores de análisis de Brocade SAN, con el motivo de ver a detalle el tráfico que cruza por el dispositivo y determinar desconexiones o errores de comunicación o de red procedentes entre los equipos seleccionados.

El tiempo de análisis de la información estuvo determinado por el número de equipos, siendo así el caso que la herramienta fue configurada para que analice durante un lapso prudencial y que se ajuste a los instantes de mayor carga, se tomó como referencia un tiempo de una semana y se consideró que lo oportuno era realizarlo en un fin de semana, donde los backup son más extensos y de manera full, se aprovechó el tiempo de mayor concurrencia y demanda de servicios.

El sistema de backup trabaja todos los días durante los 365 días y durante las 24 horas, en fin de semana se programan los respaldos por temas de depuraciones a las bases de datos y aplicaciones y se utiliza el tiempo nocturno para no incurrir en la operación de online.

#### **5.4.2. Resumen ejecutivo.**

La infraestructura que dispone y ofrece la empresa TCS, está diseñada de manera escalable y garantiza la alta disponibilidad de acceso a los datos, hay que mencionar que la empresa garantiza la redundancia con el diseño propuesto, por tal razón es necesario realizar el análisis para poder determinar si existen errores o fallas en la red SAN para poder emitir las recomendaciones y sugerencias correspondientes para evitar fallas en la red SAN.

En el presente estudio se procedió con el análisis de la red SAN de la siguiente manera.

- Recolección de datos por medio de la herramienta SAN Health Brocade.

El análisis permite identificar el puerto de los equipos que se encuentran conectados, el firmware instalado, la zona a las que corresponden, el nivel de concurrencia, redundancia a las fabric configuradas.

#### **5.4.3. Objetivos del documento.**

A continuación se detalla los objetivos del análisis de la red SAN de TCS:

- Analizar la situación actual de la estructura de la red SAN TCS con el soporte de herramientas que permitan obtener la información de la estructura lógica y física de la red SAN.

- Analizar el estado de los componentes de la red SAN con el objetivo de identificar errores y fallas de conexión de la red SAN.
- Analizar la configuración de las zonas presentes y los dispositivos que corresponden a cada una de éstas para comprobar las configuraciones que no representan importancia.
- Analizar las alertas presentes para plantear recomendaciones que admitan mejorar el performance de la red SAN.
- Emitir recomendaciones para mejorar los servicios de la red SAN de TCS.

#### **5.4.4. Necesidades y requerimientos.**

La necesidad de realizar un análisis técnico del estado de la red SAN actual, permitirá:

Identificar la estructura lógica y componentes que integran la red SAN. Con este propósito se realizó un análisis detallado del sistema por medio de la utilización de herramientas que proporciona la marca de los dispositivos Brocade SAN, especializados en recolectar registros de la operación de los equipos en un horario flexible y de mayor congestión del funcionamiento de la red SAN.

Posterior al análisis de la información, el presente documento reflejará los resultados encontrados que servirán para la emisión de sugerencias y recomendaciones con el fin de que TCS cuente con una infraestructura de red SAN optimizada para la carga de tráfico actual y futura.

#### **5.4.5. Análisis de la red SAN.**

Se realizó un análisis de la situación actual de los Directores y Switches Brocade, de la siguiente manera:

- Recolección de información de operación de la red SAN en horario normal y en horas pico, durante el lapso de una semana de estudio.
- Procesamiento de la información de operación de la red SAN, representación gráfica y posterior análisis del informe emitido por el fabricante a través del portal de propiedad de Brocade SAN Health, el cual envía los reportes con los datos procesados.
- Análisis de reportes, en el que se identifica los dispositivos conectados a los puertos de cada Switch Brocade.
- Análisis de miembros que están formando parte de una zona.
- Análisis de las versiones de firmware de los switches integrantes de cada Fabric.
- Análisis de la configuración actual de las zonas, en el que se identifica configuraciones que no se encuentran activas.
- Análisis de errores y alertas de los equipos SAN.
- Recomendaciones en la red SAN para garantizar un correcto funcionamiento de la infraestructura.

#### 5.4.6. Estado actual de los equipos SAN.

La empresa TCS cuenta con una red SAN, configurada de forma redundante para garantizar la disponibilidad de los servicios y la obtención de las copias de seguridad y restauraciones a dos instituciones bancarias como el Banco del Pichicha y Banco General Rumiñahui, la red SAN ha escalado vertiginosamente gracias a la necesidad de incluir más dispositivos, por lo que es posible demostrar un crecimiento de los componentes de la red SAN de manera insegura y poco estructurada, lo que ha ocasionado que exista errores de hardware y de configuración que por el momento ha degradado el rendimiento de la red SAN.

El análisis que se pretende realizar en los componentes que conforman la red SAN permitirá identificar posibles errores, que serán el eje para realizar una adecuada reestructuración lógica y física de la red SAN y emitir las recomendaciones más acertadas que beneficien en medida el rendimiento de la red SAN.

Del análisis de la red SAN permitirá cumplir con los objetivos propuestos al inicio de la investigación, entre los objetivos más relevantes se iniciara con:

- Análisis de situación inicial de la red SAN.
- Análisis del estado de los equipos que conforman la red SAN, en busca de fallas de conexión y soporte.
- Análisis de la configuración de las zonas y la conexión a los equipos de interconexión, con el propósito de mejorar las configuraciones.
- Del análisis de las alertas se emitirá las sugerencias y recomendaciones que permitan optimizar la red SAN.

La situación de la red SAN en la empresa TCS es la siguiente:

Cuenta con una infraestructura de red SAN, que es utilizada como medio de comunicación entre los dispositivos de almacenamiento y respaldo con los servidores respectivos.

La presente tabla determina los fabric name constituidos por el director 1 y director 2, respectivamente para mantener la redundancia entre los dispositivos.

Fabric Name	Sw Name	Sw Domain	IP Address	World Wide Name	Spd (Sw Speed)	OSVer (SO Ver)
Director1	c7000-sw7	1	10.151.16.70	10:00:00:05:1e:c6:17:cd	8G	7.4.1c
Director1	c7000-sw5	2	10.151.16.72	10:00:00:05:1e:c5:42:a4	8G	7.4.1c
Director1	c7001-sw5	3	10.151.16.92	10:00:00:05:33:43:bf:da	8G	7.4.1c
Director1	c7001-sw7	4	10.151.16.95	10:00:00:05:33:4a:01:68	8G	7.4.1c
Director1	c7002-sw5	7	10.151.16.100	10:00:00:05:33:49:f7:bd	8G	7.4.1c
Director1	c7002-sw7	8	10.151.16.102	10:00:00:05:33:49:e9:a1	8G	7.4.1c
Director1	SANsw_bp1 1	11	10.151.16.131	10:00:00:05:33:c0:f8:00	16G	7.4.1c

Director1	SANsw_bp13	13	10.151.16.234	10:00:00:27:f8:60:29:68	8G	7.4.1c
Director1	sw5-xp24000	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	8G	7.0.1a
Director2	c7000-sw8	1	10.151.16.73	10:00:00:05:1e:c6:1e:62	8G	7.4.1c
Director2	c7000-sw6	2	10.151.16.71	10:00:00:05:1e:c6:33:c0	8G	7.4.1c
Director2	c7001-sw6	3	10.151.16.26	10:00:00:05:33:42:00:86	8G	7.4.1c
Director2	c7002-sw6	7	10.151.16.101	10:00:00:05:33:49:f7:d0	8G	7.4.1c
Director2	c7002-sw8	8	10.151.16.103	10:00:00:05:33:49:fc:a8	8G	7.4.1c
Director2	SANsw_bp12	12	10.151.16.134	10:00:00:05:33:81:9e:00	16G	7.4.1c
Director2	SANsw_bp14	14	10.151.16.235	10:00:00:27:f8:60:0a:dc	8G	7.4.1c
Director2	c7001-sw8	48	10.151.16.28	10:00:00:05:33:49:fa:14	8G	7.4.1c

Tabla 2 Summary Red SAN.

La figura 15 detalla las conexiones de las fabric name hacia los diferentes equipos, el reporte es generado por Brocade SAN Health, donde se evidencia el dominio, la IP del equipo, modelos de quipo, velocidad de sus tarjetas de red y numero de puertos, versión del firmware, entre la información que más se destaca y es de interés para el análisis de la red SAN.

SAN SUMMARY DETAILS FOR JC														Table Of Contents	
SWITCHES IN SAN jc															
Fabric Name	Switch Name	Dom	IP Address	World Wide Name	Model	Spd	OSVer	Status	DaysUp	Pwr[W]	Serial Number	Ports (Total)	Unusd	UnLicd	
Director1	c7000-sw7	1	10.151.16.70	10:00:00:05:1e:c6:17:cd	5480	8G	7.4.1c	Healthy	120	36	ALE0442E06B	24 (24)	17	0	
Director1	c7000-sw5	2	10.151.16.72	10:00:00:05:1e:c5:42:a4	5480	8G	7.4.1c	Healthy	120	36	ALE0442E06K	24 (24)	16	0	
Director1	c7001-sw5	3	10.151.16.92	10:00:00:05:33:43:bf:da	5480	8G	7.4.1c	Healthy	119	36	ALE0448F0F5	24 (24)	5	0	
Director1	c7001-sw7	4	10.151.16.95	10:00:00:05:33:4a:01:68	5480	8G	7.4.1c	Healthy	119	36	ALE0448F0F7	24 (24)	8	0	
Director1	c7002-sw5	7	10.151.16.100	10:00:00:05:33:49:f7:bd	5480	8G	7.4.1c	Healthy	119	36	ALE0448F0F4	24 (24)	15	0	
Director1	c7002-sw7	8	10.151.16.102	10:00:00:05:33:49:e9:a1	5480	8G	7.4.1c	Healthy	119	36	ALE0448F0ED	24 (24)	18	0	
Director1	sansw_bp11	11	10.151.16.131	10:00:00:05:33:c0:f8:00	DCX-8510-4	16G	7.4.1c	Healthy	119	1104	ANN2502H01S	192 (256)	9	0	
Director1	sansw_bp13	13	10.151.16.234	10:00:00:27:f8:60:29:68	5480	8G	7.4.1c	Healthy	120	36	ALE0408J010	24 (24)	5	14	
Director1	sw5-xp24000	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	5100	8G	7.0.1a	Healthy	284	84	ALM0640E02K	40 (40)	33	0	
Director2	c7000-sw8	1	10.151.16.73	10:00:00:05:1e:c6:1e:62	5480	8G	7.4.1c	Healthy	118	36	ALE0442E02S	24 (24)	16	0	
Director2	c7000-sw6	2	10.151.16.71	10:00:00:05:1e:c6:33:c0	5480	8G	7.4.1c	Healthy	118	36	ALE0442E040	24 (24)	17	0	
Director2	c7001-sw6	3	10.151.16.26	10:00:00:05:33:42:00:86	5480	8G	7.4.1c	Healthy	118	36	ALE0448F0E1	24 (24)	5	0	
Director2	c7002-sw6	7	10.151.16.101	10:00:00:05:33:49:f7:d0	5480	8G	7.4.1c	Healthy	118	36	ALE0448F0F1	24 (24)	15	0	
Director2	c7002-sw8	8	10.151.16.103	10:00:00:05:33:49:fc:a8	5480	8G	7.4.1c	Healthy	118	36	ALE0448F0G7	24 (24)	18	0	
Director2	sansw_bp12	12	10.151.16.134	10:00:00:05:33:81:9e:00	DCX-8510-4	16G	7.4.1c	Healthy	118	1104	ANN2528G02S	192 (256)	8	0	
Director2	sansw_bp14	14	10.151.16.235	10:00:00:27:f8:60:0a:dc	5480	8G	7.4.1c	Healthy	118	36	ALE0408J023	24 (24)	5	14	
Director2	c7001-sw8	48	10.151.16.28	10:00:00:05:33:49:fa:14	5480	8G	7.4.1c	Healthy	118	36	ALE0448F0G8	24 (24)	8	0	

Figura 15 San summary details for SAN.

También se detallan los switch que se relacionan con los directores de la red SAN, los switches están formando una topología en cascada, para mayor detalle puede encontrar en la parte de los anexos la topología descubierta por SAN Health.

En el siguiente punto analizado se puede observar que el análisis determina un switch con un firmware que no está actualizado y requiere la instalación del parche para su mayor optimización, lo que se pretende es lograr que le equipo este trabajando al 100 % y con todas sus ventajas.

La tabla 3 detalla la versión recomendada para la actualización del firmware en el director 1.

SWITCHES THAT ARE NOT ON TARGET PATH RELEASES								
Fabric Name	Switch Name	Domain	IP Address	World Wide Name	Model	Current OS Ver	Target Path OS Version	FICON in use
Director1	sw5-xp24000	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	5100	7.0.1a	7.2.0d, 7.1.0c	

Tabla 3 Versión de Firmware de Switch con error.

La figura 16 muestra en resumen de las velocidades de los puertos, información indispensable para canalizar las concurrencias y determinar posibles errores en su tarjetería.

SUMMARY FOR 17 SWITCHES WITH 760 PORTS ( LICENSED PORTS - 732) THAT ARE 70 % UTILIZED																			
Fabric Name	Switch Count							Port Count							Port Use Metrics				
	2G	4G	8G	10G	16G	32G	Total	2G	4G	8G	10G	16G	32G	Total	ISL Ports	Device Ports	Devices	Unused	Utilization
Director1	0	0	8	0	1	0	9	2	84	300	0	0	0	400	22	252	602	126	67 %
Director2	0	0	7	0	1	0	8	2	47	297	0	0	0	360	20	248	597	92	73 %
<b>TOTALS</b>	<b>0</b>	<b>0</b>	<b>15</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>17</b>	<b>4</b>	<b>131</b>	<b>597</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>760</b>	<b>42</b>	<b>500</b>	<b>1199</b>	<b>218</b>	<b>70 %</b>

Figura 16 Summary de Switches.<sup>19</sup>

El número total de puertos en los directores es de 760 puertos de los cuales trabajan a velocidades de 2Gb, 4Gb, 8Gb brindando servicio a cerca de 1199 dispositivo, donde a velocidades de 8 Gb, tiene 15 tarjetas, de 16 Gb tan solo dos, de los cual se deduce que el director 1 trabaja y negocia velocidades de 9Gb y el director 2 a solo 8Gb. Teniendo un promedio de trabajo del 70%, se sugiere incrementar tarjetas HBA de 8Gb.

#### 5.4.7. Análisis de la configuración actual de la red SAN, SANSW\_BP11.

El resultado del análisis de la topología de la red SAN, configuración de alias, zonas y errores que se encontraron en el san switch sansw\_bp11.

##### 5.4.7.1. Análisis de puertos.

Existen al momento un total de 766 miembros o alias definidos en la configuración del san switch sansw\_bp11. Cada miembro representa a un dispositivo conectado a un puerto del switch, pudiendo ser un servidor, un almacenamiento, una librería. De los cuales, 266 no están definidos, debido a que no existen físicamente al momento de realizar el levantamiento de información durante el periodo de estudio. Esto indicaría que estos dispositivos no están presentes y ya no forman parte de la red SAN, por tanto estos puertos constarían como libres y se los podría reutilizar. La figura 17 hace referencia a las zonas que se encuentran activas y configuradas, muestra el número total de alias que al momento están usadas e identifica varios puertos que no reconoce lo que ayudaría a ser utilizados.

<sup>19</sup> Brocade, San Health, Análisis de métricas.

ZONING METRICS													
Fabric Name	Zone Database Use	Aliases Statistics				Zone Statistics				Config Statistics			
		Aliases	Avg Mems	Max Mems	Hang Mems	Zones	Avg Mems	Max Mems	Hang Mems	Configs	Avg Mems	Max Mems	Hang Mem
Director1	14.7%of10452748	766	1.01	2	266	922	2.72	11	349	1	857	857	259
Director2	14.4%of10452748	735	1	2	240	914	2.74	11	362	1	841	841	253
<b>TOTALS</b>		<b>1501</b>	<b>1</b>	<b>2</b>	<b>506</b>	<b>1836</b>	<b>2.7</b>	<b>11</b>	<b>711</b>	<b>2</b>	<b>849</b>	<b>857</b>	<b>512</b>

Figura 17 Métricas de las zonas y alias.<sup>20</sup>

Los puertos usados se visualizan en la figura 18, se puede apreciar un número de 400 puertos, en los cuales se han conectado 495 hosts, 34 discos, 11 tapes, 6 Appliance, y 56 gateway, de los cuales 126 puertos se encuentran libres y 14 no han sido autorizados, la distancia promedio es de 10 Km, el análisis realizado evidencia que alrededor de 400 dispositivos están conectados a distancias de 10 Km.

PORT USE																						
Fabric Name	Port Counts			Attached Device Types						Inter Switch Links				Fan Out Ratios			Long Distance Modes					
	Total	Unusd	Unlocd	Disk	Tape	Host	Appliance	Gateway	ISLs	IFLs	Trnk Mstr	Trnk Slv	Host:Disk	Non-ISL:ISL	Device:ISL	10km	25km	50km	100k	300k	Auto	
Director1	400	126	14	34	11	495	6	56	22	0	0	0	14.56:1	17.18:1	27.36:1	400	0	0	0	0	0	
Director2	360	92	14	35	11	490	6	55	20	0	0	0	14:1	17:1	29.85:1	360	0	0	0	0	0	
<b>TOTALS</b>	<b>760</b>	<b>218</b>	<b>28</b>	<b>69</b>	<b>22</b>	<b>985</b>	<b>12</b>	<b>111</b>	<b>42</b>	<b>0</b>	<b>0</b>	<b>0</b>				<b>760</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	

Figura 18 Puertos utilizados Director 1.

La figura 19 determina un total de 400 puertos, los cuales trabajan a velocidades desde los 2 Gb hasta un máximo de 8Gb, se puede evidenciar que el san switch sansw\_bp11, pinta de color azul lo indica que es el equipo con una tarjetería ya obsoleta y se debe analizar su actualización y mejorar las características de sus tarjetas, menciona un acceso concurrente hacia el director 1, mediante los puertos 48 y 64 del san switch sansw\_bp11.

PORT USE																										
Switch Name	Port Counts			Attached Device Types				Inter Switch Links				Fan Out Ratios			Port Speeds						Long Distance Modes					
	Total	Unusd	Unlocd	Disk	Tape	Host	Applnc	Gtww	ISL	TrkMstr	TrkSlv	Hst:Trg	Dvc:ISL	2G	4G	8G	16G	32G	1GE	10GE	10km	25km	50km	100k	300k	Auto
c7000-sw7	24	17	0	0	0	6	0	1	0	0	6:0	6:1	0	4	20	0	0	0	0	24	0	0	0	0	0	
c7000-sw5	24	16	0	0	0	7	0	1	1	0	7:1	8:1	0	4	20	0	0	0	0	24	0	0	0	0	0	
c7001-sw5	24	5	0	0	0	15	0	4	0	0	15:0	3.75:1	0	1	23	0	0	0	0	24	0	0	0	0	0	
c7001-sw7	24	8	0	0	0	15	0	1	0	0	15:0	15:1	0	0	24	0	0	0	0	24	0	0	0	0	0	
c7002-sw5	24	15	0	0	0	8	0	1	0	0	8:0	8:1	0	3	21	0	0	0	0	24	0	0	0	0	0	
c7002-sw7	24	18	0	0	0	5	0	1	0	0	5:0	5:1	0	3	21	0	0	0	0	24	0	0	0	0	0	
sansw_bp11	192	9	0	34	11	429	6	55	11	0	4.05:1	48.64:1	2	29	161	0	0	0	0	192	0	0	0	0	0	
sansw_bp13	24	5	14	0	0	4	0	1	0	0	4:0	4:1	0	0	10	0	0	0	0	24	0	0	0	0	0	
sw5-xp24000	40	33	0	0	0	6	0	1	0	0	6:0	6:1	0	40	0	0	0	0	0	40	0	0	0	0	0	
<b>TOTALS</b>	<b>400</b>	<b>126</b>	<b>14</b>	<b>34</b>	<b>11</b>	<b>495</b>	<b>6</b>	<b>56</b>	<b>22</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>84</b>	<b>300</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>400</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	

Figura 19 Puertos utilizados.<sup>21</sup>

Realizando un resumen con relación a la velocidad de sus tarjetas se tiene un total de 400 puertos en la tabla 4 se presenta a detalle las velocidades y el número de tarjetas a las que se debe dar prioridad de mejoramiento.

<sup>20</sup> Brocade, San Health, Análisis de métricas.

<sup>21</sup> Brocade, San Health, Análisis de métricas.

VELOCIDAD DEL PUERTO	TOTAL
2G	2
4G	84
8G	300
Sub Total =	386
NO autorizadas =	14
<b>TOTAL=</b>	<b>400</b>

Tabla 4 Velocidad de los puertos del San Switch

#### 5.4.7.2. Análisis de zonas.

A continuación un análisis de la zonas que se encuentran configuradas en la presente red SAN. La tabla 5 zonas y alias, se detalla las zonas y los wwn asociados entre ellos, donde se aprecia que existe varios que no están correctamente definidos o no se relacionan entre sí, de este resultados se puede empezar por la depuración de las zonas que tal vez ya no estén presentes o ya no sean necesarias pero que aún constan como configuradas en los directores.

Fabric Name	Active Zone Config	Alias Name	Alias Member(s)	Alias Status	Zoned Status
Director1	XP24000	ALI_3PAR_ECBPSTG05_N0S2P1_PEERMOTION	20:21:02:02:ac:00:ac:61	Hanging	NOT ZONED
Director1	XP24000	ALI_3PAR_ECBPSTG05_N1S2P1_PEERMOTION	21:21:02:02:ac:00:ac:61	Hanging	NOT ZONED
Director1	XP24000	ALI_3PAR_ECBPSTG05_N4S2P3_PeerMotion	24:23:02:02:ac:00:ac:61	Hanging	NOT ZONED
Director1	XP24000	ALI_BANCSAPP_HPUXPOC	50:01:4c:24:00:00:00:02	Hanging	NOT ZONED
Director1	XP24000	ALI_BANCSDB_HPUXPOC	50:01:4c:24:00:00:00:00	Hanging	NOT ZONED
Director1	XP24000	ALI_CARRETAS_XP12K_7A	50:06:0e:80:04:76:76:60	Hanging	NOT ZONED
Director1	XP24000	ALI_CARRETAS_XP24K_1F	50:06:0e:80:05:70:bb:05	Hanging	NOT ZONED
Director1	XP24000	ALI_CARRETAS_XP24K_3F	50:06:0e:80:05:70:bb:25	Hanging	NOT ZONED
Director1	XP24000	ALI_CARRETAS_XP24K_5A	50:06:0e:80:05:70:bb:40	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCBA_fcd0	50:01:4c:25:00:00:00:02	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCBA_fcd7	50:01:4c:25:00:00:00:06	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCBA_fcpl4	50:01:4c:24:00:00:00:73	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCF5_PCI4P1	50:06:0b:00:00:6a:36:a8	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCF5_PCI5P1	50:01:43:80:03:c0:f7:e0	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCF5_PCI6P1	50:01:43:80:03:c0:e7:a0	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCMF_c7001_sw7	50:01:43:80:21:dd:2c:ec	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCP5_PCI4P1	50:01:43:80:03:c1:16:80	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCP5_PCI5P1	50:01:43:80:03:c0:f9:c4	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCP5_PCI6P1	50:01:43:80:03:c1:15:e8	Hanging	NOT ZONED

Director1	XP24000	ALI_ECBPHCT1_fcd4	50:01:43:80:03:3a:2c:74	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPHCT3_fcd0	50:01:4c:25:00:00:00:09	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCDP2	50:01:4c:23:00:00:00:15	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCIBM1_APP_P1	10:00:00:00:c9:d9:10:e1	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCIBM2_BDD_P1	10:00:00:00:c9:da:65:47	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCIBM_APP_P2	10:00:00:00:c9:d9:10:e0	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCIBM_BDD_P2	10:00:00:00:c9:da:65:46	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCIBM_LIB_TSM	20:02:00:0e:11:14:51:cf	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCIBM_TSM_TSM	10:00:00:00:c9:d7:fd:58	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPOCVP1_FCD0	50:01:4c:23:00:00:00:10	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPRSX21_HBA2_PORT1	50:06:0b:00:00:c2:62:8c	Hanging	NOT ZONED
Director1	XP24000	ALI_ECBPPRSX22_HBA2_PORT1	50:06:0b:00:00:c2:62:14	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP1_FCS0	c0:50:76:05:fe:e4:00:20	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP1_FCS2	c0:50:76:05:fe:e4:00:40	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP1_P770_FCS0	c0:50:76:04:38:c8:00:18	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP1_P770_FCS2	c0:50:76:04:38:c8:00:1c	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP3_FCS0	c0:50:76:05:fe:e4:00:24	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP3_FCS2	c0:50:76:05:fe:e4:00:48	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP3_P770_FCS0	c0:50:76:04:38:c8:00:22	Hanging	NOT ZONED
Director1	XP24000	ALI_HABP3_P770_FCS2	c0:50:76:04:38:c8:00:26	Hanging	NOT ZONED
Director1	XP24000	ALI_HATP2_FCS0	c0:50:76:05:fe:e4:00:2c	Hanging	NOT ZONED
Director1	XP24000	ALI_HATP2_FCS2	c0:50:76:05:fe:e4:00:4e	Hanging	NOT ZONED
Director1	XP24000	ALI_HATP2_P770_FCS0	c0:50:76:04:38:c8:00:00	Hanging	NOT ZONED
Director1	XP24000	ALI_HATP2_P770_FCS2	c0:50:76:04:38:c8:00:04	Hanging	NOT ZONED
Director1	XP24000	ALI_LAB1_HPUX_P1	50:01:4c:27:00:00:00:1c	Hanging	NOT ZONED
Director1	XP24000	ALI_MPX_BL1_FC1	21:00:00:c0:dd:23:e3:0e	Hanging	NOT ZONED
Director1	XP24000	ALI_MPX_BL2_FC2	21:00:00:c0:dd:23:e3:19	Hanging	NOT ZONED
Director1	XP24000	ALI_MPX_TARGET1_BL1	21:04:00:c0:dd:23:e3:0e	Hanging	NOT ZONED
Director1	XP24000	ALI_MPX_TARGET2_BL2	21:04:00:c0:dd:23:e3:19	Hanging	NOT ZONED
Director1	XP24000	ALI_MQSP3_FCS0	c0:50:76:05:fe:e4:00:28	Hanging	NOT ZONED
Director1	XP24000	ALI_MQSP3_FCS2	c0:50:76:05:fe:e4:00:4a	Hanging	NOT ZONED
Director1	XP24000	ALI_MQSP3_P770_FCS0	c0:50:76:04:38:c8:00:10	Hanging	NOT ZONED
Director1	XP24000	ALI_MQSP3_P770_FCS2	c0:50:76:04:38:c8:00:14	Hanging	NOT ZONED
Director1	XP24000	ALI_MSBP2_FCS0	c0:50:76:05:fe:e4:00:1e	Hanging	NOT ZONED
Director1	XP24000	ALI_MSBP2_FCS2	c0:50:76:05:fe:e4:00:3c	Hanging	NOT

					ZONED
Director1	XP24000	ALI_MSBP2_P770_FCS0	c0:50:76:04:38:c8:00:08	Hanging	NOT ZONED
Director1	XP24000	ALI_MSBP2_P770_FCS2	c0:50:76:04:38:c8:00:0c	Hanging	NOT ZONED
Director1	XP24000	ALI_TELCONET_XP24K_1F	50:06:0e:80:15:25:ce:05	Hanging	NOT ZONED
Director1	XP24000	ALI_TELCONET_XP24K_3F	50:06:0e:80:15:25:ce:25	Hanging	NOT ZONED
Director1	XP24000	ALI_VIOSAS720_FCS5	c0:50:76:05:fe:e4:00:56	Hanging	NOT ZONED
Director1	XP24000	SX46_sw5	50:01:43:80:12:0f:30:e4	Hanging	NOT ZONED
Director1	XP24000	SX46_sw7	50:01:43:80:12:0f:85:44	Hanging	NOT ZONED
Director1	XP24000	SX53_sw5	50:01:43:80:04:c0:9f:e8	Hanging	NOT ZONED

Tabla 5 Alias no definidos.<sup>22</sup>

### 5.4.7.3. Análisis de topología.

La topología de la red SAN correspondiente al director 1, dispone de 922 zonas, conectadas a 8 switch que disponen de tarjetería que trabaja a velocidades de 8Gb/s, la ventaja es que el director se conecta con los switch generando la cascada y minimizando el número de saltos, la recomendación es que para que una red SAN trabaje con un buen rendimiento debe tener en menor número de saltos posibles. En la siguiente Figura, la representación gráfica de la topología referente al director 1.

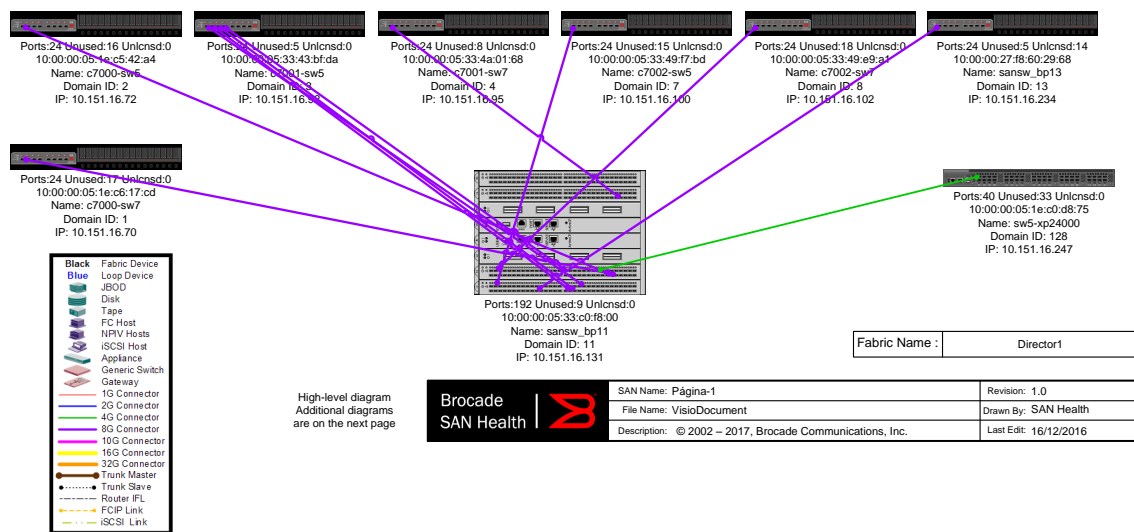


Figura 20 Topología Director 1<sup>23</sup>

La conexión que se representa de color verde trabaja a una velocidad de 4G, es un equipo que se debe de considerar para migrar o actualizar su tarjeta de conexión para estandarizar la velocidad de transmisión a 8G, es un equipo que cuenta con

<sup>22</sup> Brocade, San Health, Análisis de métricas.

<sup>23</sup> Brocade, San Health, Análisis de métricas, Topología.

40 puertos y 33 de ellos no están siendo utilizados, por tal razón se analizara las redes y servicios que por este san switch cruzan y optimizar la red SAN.

En el apartado de los anexos puede encontrar las topologías detalladas que hacen referencia a la Figura 20 y Figura 24, respectivamente.

#### 5.4.8. Análisis de la configuración actual de la red SAN, SANSW\_BP12.

El resultado del análisis de la topología de la red SAN, configuración de alias, zonas y errores que se encontraron en la sansw\_bp12.

##### 5.4.8.1. Análisis de puertos.

Existen al momento un total de 1501 miembros o alias definidos en la configuración del san switch sansw\_bp11. Cada miembro representa a un dispositivo conectado a un puerto del switch, pudiendo ser un servidor, un almacenamiento, una librería. De los cuales, 506 no están definidos, debido a que no existen físicamente al momento de realizar el levantamiento de información durante el periodo de estudio. Esto indicaría que estos dispositivos no están presentes y ya no forman parte de la red SAN, por tanto estos puertos constarían como libres y se los podría reutilizar. La figura 17 hace referencia a las zonas que se encuentran activas y configuradas, muestra el número total de alias que al momento están usadas e identifica varios puertos que no reconoce lo que ayudaría a ser utilizados.

ZONING METRICS													
Fabric Name	Zone Database Use	Aliases Statistics				Zone Statistics				Config Statistics			
		Aliases	Avg Mems	Max Mems	Hang Mems	Zones	Avg Mems	Max Mems	Hang Mems	Configs	Avg Mems	Max Mems	Hang Mem
Director1	14.7%of10452748	766	1.01	2	266	922	2.72	11	349	1	857	857	259
Director2	14.4%of10452748	735	1	2	240	914	2.74	11	362	1	841	841	253
<b>TOTALS</b>		<b>1501</b>	<b>1</b>	<b>2</b>	<b>506</b>	<b>1836</b>	<b>2.7</b>	<b>11</b>	<b>711</b>	<b>2</b>	<b>849</b>	<b>857</b>	<b>512</b>

Figura 21 Métrica de las zonas.

Los puertos usados se visualizan en la figura 22, se puede apreciar un número de 360 puertos, en los cuales se han conectado 490 hosts, 35 discos, 11 tapes, 6 Appliance, y 55 gateway, de los cuales 126 puertos se encuentran libres y 14 no han sido autorizados, la distancia promedio es de 10 Km, el análisis realizado evidencia que alrededor de 360 dispositivos están conectados a distancias de 10 Km.

PORT USE																							
Fabric Name	Port Counts			Attached Device Types					Inter Switch Links					Fan Out Ratios			Long Distance Modes						
	Total	Unusd	Unlcl	Disk	Tape	Host	Appliance	Gateway	ISLs	IFLs	Trnk	Mstr	Trnk	Slv	Host/Disk	Non-ISL	ISL/Device	ISL	10km	25km	50km	100k	300k
Director1	400	126	14	34	11	495	6	56	22	0	0	0	0	14.56:1	17.18:1	27.36:1	400	0	0	0	0	0	0
Director2	360	92	14	35	11	490	6	55	20	0	0	0	0	14:1	17:1	29.85:1	360	0	0	0	0	0	0
<b>TOTALS</b>	<b>760</b>	<b>218</b>	<b>28</b>	<b>69</b>	<b>22</b>	<b>985</b>	<b>12</b>	<b>111</b>	<b>42</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>				<b>760</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

Figura 22 Puertos usados.

La figura 23 determina un total de 3600 puertos, los cuales trabajan a velocidades desde los 2 Gb hasta un máximo de 8Gb, se puede evidenciar que el san switch sansw\_bp12, pinta de color azul indicando que es el equipo con una tarjetería ya obsoleta y se debe analizar su actualización y mejorar las características de sus tarjetas, menciona un acceso concurrente hacia el director 1, mediante los puertos 53 y 6 del san switch sansw\_bp12.

Switch Name	Port Counts			Attached Device Types						Inter Switch Links				Fan Out Ratios		Port Speeds						Long Distance Modes					
	Total	Unusd	Unloc	Disk	Tape	Host	Aplnc	Gtww	ISL	TrkMst	TrkSlv	Hst:Trg	Dvc:ISL	2G	4G	8G	16G	32G	1GE	10GE	10km	25km	50km	100k	300k	Auto	
c7000-sw8	24	16	0	0	0	7	0	0	1	0	0	7:0	7:1	0	4	20	0	0	0	0	24	0	0	0	0	0	
c7000-sw6	24	17	0	0	0	6	0	1	1	0	0	6:1	7:1	0	4	20	0	0	0	0	24	0	0	0	0	0	
c7001-sw6	24	5	0	0	0	15	0	0	4	0	0	15:0	3:75:1	0	1	23	0	0	0	0	24	0	0	0	0	0	
c7002-sw6	24	15	0	0	0	8	0	0	1	0	0	8:0	8:1	0	3	21	0	0	0	0	24	0	0	0	0	0	
c7002-sw8	24	18	0	0	0	5	0	0	1	0	0	5:0	5:1	0	3	21	0	0	0	0	24	0	0	0	0	0	
sansw_bp12	192	8	0	35	11	430	6	54	10	0	0	4:06:1	53:6:1	2	32	158	0	0	0	0	192	0	0	0	0	0	
sansw_bp14	24	5	14	0	0	4	0	0	1	0	0	4:0	4:1	0	0	10	0	0	0	0	24	0	0	0	0	0	
c7001-sw8	24	8	0	0	0	15	0	0	1	0	0	15:0	15:1	0	0	24	0	0	0	0	24	0	0	0	0	0	
<b>TOTALS</b>	<b>360</b>	<b>92</b>	<b>14</b>	<b>35</b>	<b>11</b>	<b>490</b>	<b>6</b>	<b>55</b>	<b>20</b>	<b>0</b>	<b>0</b>			<b>2</b>	<b>47</b>	<b>297</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>360</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	

Figura 23 Puertos utilizados.<sup>24</sup>

Realizando un resumen con relación a la velocidad de sus tarjetas se tiene un total de 400 puertos en la tabla 4 se presenta a detalle las velocidades y el número de tarjetas a las que se debe dar prioridad de mejoramiento.

VELOCIDAD DEL PUERTO	TOTAL
<b>2G</b>	<b>2</b>
<b>4G</b>	<b>47</b>
<b>8G</b>	<b>297</b>
<b>Sub Total =</b>	<b>346</b>
<b>NO autorizadas =</b>	<b>14</b>
<b>TOTAL=</b>	<b>360</b>

Tabla 6 Velocidad de los puertos del San Switch

#### 5.4.8.2. Análisis de zonas.

A continuación un análisis de las zonas que se encuentran colgadas y no se encuentran zonificadas en la presente red SAN. La tabla 7 zonas y alias, se detalla las zonas y los wwn asociados entre ellos, donde se aprecia que existe varios que no están correctamente definidos o no se relacionan entre sí, de estos resultados se puede empezar por la depuración de las zonas que tal vez ya no estén presentes o ya no sean necesarias pero que aún constan como configuradas en los directores.

Name	Fabric	Active Zone Config	Alias Name	Alias Member(s)	Alias Status	Zoned Status
Director2		XP24000	ALI_3PAR_ECBPSTG01_N3S2P2_PeerMotion	23:22:02:02:ac:00:5e:53	Hanging	NOT ZONED
Director2		XP24000	ALI_3PAR_ECBPSTG01_N3S2P4_PeerMotion2	23:24:02:02:ac:00:5e:53	Hanging	NOT ZONED
Director2		XP24000	ALI_CARRETAS_XP12K_8A	50:06:0e:80:04:76:76:70	Hanging	NOT ZONED
Director2		XP24000	ALI_CARRETAS_XP24K_2F	50:06:0e:80:05:70:bb:15	Hanging	NOT ZONED
Director2		XP24000	ALI_CARRETAS_XP24K_4F	50:06:0e:80:05:70:bb:35	Hanging	NOT ZONED

<sup>24</sup> Brocade, San Health, Análisis de métricas.

Director2	XP24000	ALI_CARRETAS_XP24K_6A	50:06:0e:80:05:70:bb:50	Hanging	NOT ZONED
Director2	XP24000	ALI_CARRETAS_XP24K_8A	50:06:0e:80:05:70:bb:70	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCBA_fcd6	50:01:4c:25:00:00:00:05	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCF5_PCI4P2	50:06:0b:00:00:6a:36:aa	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCF5_PCI6P2	50:01:43:80:03:c0:e7:a2	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCF5_PCI7P2	50:01:43:80:03:c0:e7:6e	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCP5_PCI4P2	50:01:43:80:03:c1:16:82	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCP5_PCI6P2	50:01:43:80:03:c1:15:ea	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPHCP5_PCI7P2	50:01:43:80:03:c0:f4:8e	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPPOCDP2_fcd1	50:01:4c:23:00:00:00:16	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPPRCST1	50:01:43:80:02:a3:24:02	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPPRSX21_HBA2_PORT2	50:06:0b:00:00:c2:62:8e	Hanging	NOT ZONED
Director2	XP24000	ALI_ECBPPRSX22_HBA2_PORT2	50:06:0b:00:00:c2:62:16	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP1_FCS1	c0:50:76:05:fe:e4:00:22	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP1_FCS3	c0:50:76:05:fe:e4:00:42	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP1_P770_FCS1	c0:50:76:04:38:c8:00:1a	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP1_P770_FCS3	c0:50:76:04:38:c8:00:1e	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP3_FCS1	c0:50:76:05:fe:e4:00:46	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP3_FCS3	c0:50:76:05:fe:e4:00:44	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP3_P770_FCS1	c0:50:76:04:38:c8:00:20	Hanging	NOT ZONED
Director2	XP24000	ALI_HABP3_P770_FCS3	c0:50:76:04:38:c8:00:24	Hanging	NOT ZONED
Director2	XP24000	ALI_HATP2_FCS1	c0:50:76:05:fe:e4:00:2e	Hanging	NOT ZONED
Director2	XP24000	ALI_HATP2_FCS3	c0:50:76:05:fe:e4:00:50	Hanging	NOT ZONED
Director2	XP24000	ALI_HATP2_P770_FCS1	c0:50:76:04:38:c8:00:02	Hanging	NOT ZONED
Director2	XP24000	ALI_HATP2_P770_FCS3	c0:50:76:04:38:c8:00:06	Hanging	NOT ZONED
Director2	XP24000	ALI_MQSP3_FCS1	c0:50:76:05:fe:e4:00:2a	Hanging	NOT ZONED
Director2	XP24000	ALI_MQSP3_FCS3	c0:50:76:05:fe:e4:00:4c	Hanging	NOT ZONED
Director2	XP24000	ALI_MQSP3_P770_FCS1	c0:50:76:04:38:c8:00:12	Hanging	NOT ZONED
Director2	XP24000	ALI_MQSP3_P770_FCS3	c0:50:76:04:38:c8:00:16	Hanging	NOT ZONED
Director2	XP24000	ALI_MSBP2_FCS1	c0:50:76:05:fe:e4:00:1c	Hanging	NOT ZONED
Director2	XP24000	ALI_MSBP2_FCS3	c0:50:76:05:fe:e4:00:3e	Hanging	NOT ZONED
Director2	XP24000	ALI_MSBP2_P770_FCS1	c0:50:76:04:38:c8:00:0a	Hanging	NOT ZONED
Director2	XP24000	ALI_MSBP2_P770_FCS3	c0:50:76:04:38:c8:00:0e	Hanging	NOT ZONED
Director2	XP24000	ALI_TELCONET_XP24K_2F	50:06:0e:80:15:25:ce:15	Hanging	NOT ZONED
Director2	XP24000	ALI_TELCONET_XP24K_4F	50:06:0e:80:15:25:ce:35	Hanging	NOT

					ZONED
Director2	XP24000	SX46_sw6	50:01:43:80:12:0f:85:46	Hanging	NOT ZONED
Director2	XP24000	SX46_sw8	50:01:43:80:12:0f:30:e6	Hanging	NOT ZONED
Director2	XP24000	SX53_sw6	50:01:43:80:04:c0:9f:ea	Hanging	NOT ZONED

Tabla 7 Alias no definidos.<sup>25</sup>

### 5.4.8.3. Análisis de topología.

La topología de la red SAN correspondiente al director 2, dispone de 766 zonas, conectadas a 7 switch que disponen de tarjetería que trabaja a velocidades de 8Gb/s, la ventaja es que el director se conecta con los switch generando la cascada y minimizando el número de saltos, la recomendación es que para que una red SAN trabaje con un buen rendimiento debe tener en menor número de saltos posibles. En la siguiente Figura, la representación gráfica de la topología referente al director 2.

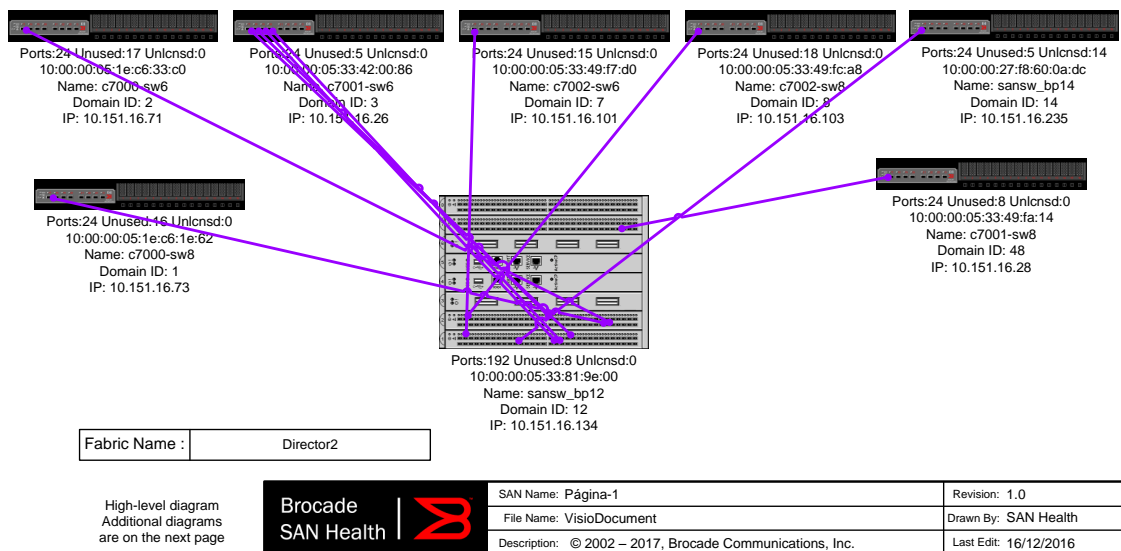


Figura 24 Topología Director 2.<sup>26</sup>

La conexión que se representa de color purpura trabaja a una velocidad de 8G, es un equipo que cuenta con 192 puertos y 8 de ellos no están siendo utilizados, por tal razón se analizara las redes y servicios que por este san switch cruzan y se recomienda un depuración de las zonas ahí configuradas.

En el apartado de los anexos puede encontrar las topologías detalladas que hacen referencia a la Figura 20 y Figura 21, respectivamente.

<sup>25</sup> Brocade, San Health, Análisis de métricas.

<sup>26</sup> Brocade, San Health, Análisis de métricas, topología.

#### **5.4.9. Análisis del consumo de Ancho de banda.**

El análisis realizado al consumo de ancho de banda por medio de la herramienta SAN Health, determina que existe un alto índice en el empleo del recurso, en los dos SAN Switches se puede evidenciar que existe un gran número de dispositivos conectados a la red SAN, el consumo de los canales y del ancho de banda es utilizado dependiendo de la configuración que se realiza sobre el storage, los medios de almacenamiento y los servidores mediante su tarjetería y va a depender de los parámetros de time out que pueda soportar el servidor, para el caso exclusivo de Data Protector el servidor se encuentra configurado con un time out del 1200 ms, así será dependiente de la aplicación, las necesidades o requerimientos y responderá a la concurrencia que se desarrolla en cada uno de sus puertos.

La concurrencia se verá afectada por la masiva solicitud de requerimientos, depende también del tipo de información que viaja por la red SAN, se recuerda que la información que viaja mediante el llamado desde la aplicación o servicio que se encuentre disponible en los servidores, la data puede ser procedente de desde las bases de datos transaccionales o históricas donde el tiempo de respuesta debe ser inmediato, la red SAN es utilizada como medio de comunicación mediante el cual el sistema de backup realiza su operación.

En las siguientes imágenes visualizar un sumario del SAN Switch, donde se evidencia el consumo del ancho de banda que se provoca en horarios pico, se determina las concurrencias a los puertos y determinar una solución acorde a la necesidad y los requerimientos de la empresa.

SWITCH SUMMARY DETAILS FOR SANSW\_BP11

Table Of Contents

SANSW_BP11 IN FABRIC DIRECTORI					
ESSENTIAL SWITCH ATTRIBUTES					
Switch Name	sansw_bp11	World Wide Name	10:00:00:05:33:c0:f8:00	Number Of Ports	192
Model Number	DCX-8510-4	Model Name	Brocade DCX-8510-4	Switch Speed	16G
Domain ID	11	Fabric Name	Director1	Fabric Principal	10:00:00:05:33:c0:f8:00
IP Address	10.151.16.131	Vendor/Support	BROCADE	Serial Number	ANN2502H01S
OEM Serial Number	USB202C01S	Chassis Serial Num	ANP2551G00K	Logical Fabric ID	128
Logical Switch Role	BaseSwitch:No DefaultSwitch:Yes Address	Power Usage	1104	Switch Date	12/12/2016 11:51:39
Switch State	Online	Health Status	Healthy	Switch Role	Principal
ADDITIONAL SWITCH ATTRIBUTES					
Chassis Type	2	Switch ID	ffic0b	Model Sub Number	3
Switch Type	121	Buffer Credits	16	Data Field Size	2112
Error Detect Timeout	2000	Res Allocatn Timeout	10000	Long Distance Mode	0
Port ID Format	1	Delay On ReRoutes	Enabled	Sticky ReRoutes	Set
Inteop Mode	0	Hop Count To Far Pnt	1	Preferred Domain	1
Insistent Domain	0	Domain RSCN	0	Switch Mode	Native
Adv Perf Tuning Policy	3	odeName ZoneCheck	0	DCFM Versions	838186778, 0;, -511108013, 0;, -9529219
Fan 1 State	Ok	Fan 2 State	Ok	Temp Sensor 1	Ok 30C 86F
Temp Sensor 2	Ok 29C 84F	Temp Sensor 3	Ok 31C 87F	Temp Sensor 4	Ok 17C 62F
Temp Sensor 5	Ok 20C 68F	Temp Sensor 6	Ok 26C 78F	Temp Sensor 7	Ok 29C 82F
Temp Sensor 8	Ok 23C 84F	Temp Sensor 9	Ok 33C 91F	Temp Sensor 10	Ok 31C 87F
Network Time Protocol	LOCL	FICDN	InUse	FC Routing	disabled
iSCSI	n/a	RADIUS Authentication	No	LDAP Authentication	No
Port Based Routing	NotInUse	xchange Based Routin	InUse	Fabric Watch	Disabled
MAPS	InUse	MAPS Active Policy	dlit_base_policy	Syslog Server	Not In Use
SNMP Trap Recipient	Community1	SNMP IP Address 1	10.0.0.141	SNMP Trap Recipient 2	Community2
SNMP IP Address 2	10.0.3.9	SNMP Trap Recipient 3	Community3	SNMP IP Address 3	10.70.80.31
CPU load (One Minute)	0.30	Active Firmware	7.4.1c	Total Chassis Slots	8
Vacant Chassis Slots	1	CP0 State	Standby, Healthy	CP1 State	Active, Warm Recovered
HA State	HA enabled, Heartbeat Up, HA State sync	SCC Policy Count	0	DCC Policy Count	0
FCS Policy Count	0	2G Ports	2	4G Ports	29
8G Ports	161	Unused Ports	9	Inter-Switch-Links	11
Total Devices	535	Disk Ports	34	Host Ports	429
Tape Ports	11	Appliance Ports	6	Gateway Ports	55
Host : Target ports	4:05:1	Device : ISL ports	48:64:1	No Active Licenses	Exists

Figura 25 Resumen consumo ancho de banda SW1

La Figura 25 Resumen del consumo de ancho de banda, evidencia los datos anteriormente mencionados, tales como:

- Ip del dispositivo
- Nombre del dispositivo
- WWN
- 192 Puertos
- Fabric name al que corresponde

Información necesaria para localizar e identificar el equipo dentro de las instalaciones del centro de datos y procesamiento, ubicado en las instalaciones de Telconet.

La figura 26 Ancho de banda sw1, describe el comportamiento y el uso del ancho de banda en horas normales y pico, se logró evidenciar que el consumo oscila entre el 60 % del su rendimiento total, pero existe un punto que se debe evaluar y buscar una solución inmediata, en la imagen muestra al SAN switch sansw\_bp11, que presenta niveles altos en el consumo del ancho de banda llegando a ocupar el 62 % del recurso, esto se debe a que el puerto 23 del slot 2, se conecta con el SAN switch sw5-xp24000, el cual trabaja a una velocidad de 4G, lo que ocasiona que haya momentos de saturación, retardo y retención de información en horario pico, su tasa de transmisión es de 497.7 MB/s, lo que evidencia un punto de quiebre en el performance de la red SAN, se sugiere una actualización oportuna de sus componentes de conexión. Para mejorar el rendimiento de la red SAN y llegar al estándar de transmisión de 8G.

ISL / TRUNK SUMMARY															
From Switch			To Switch				ISL or	FSPF	Farthest	Dynamic	Available Bandwidth and Utilization				
Name	Dom Area	Slot/Port	Name	Dom Area	Slot/Port	Trunk Type	Cost	Pri (Hops)	or Static	Speed	BW	Average	% Use	Peak	% Use
sansw_bp11	11	1	c7002-sw5	7	17	Normal ISL	500	1	D	8 Gbps	8	126.4 MB/s	8%	551.6 MB/s	34%
sansw_bp11	11	20	c7001-sw5	3	17	Normal ISL	500	1	D	8 Gbps	8	80.5 MB/s	5%	264.5 MB/s	17%
sansw_bp11	11	42	sansw_bp13	13	17	Normal ISL	500	1	D	8 Gbps	8	12.3 MB/s	1%	133.4 MB/s	8%
sansw_bp11	11	49	c7001-sw5	3	18	Normal ISL	500	1	D	8 Gbps	8	80.7 MB/s	5%	257.4 MB/s	16%
sansw_bp11	11	50	c7001-sw5	3	19	Normal ISL	500	1	D	8 Gbps	8	80.7 MB/s	5%	263.6 MB/s	16%
sansw_bp11	11	65	c7002-sw7	8	17	Normal ISL	500	1	D	8 Gbps	8	17.4 MB/s	1%	137.3 MB/s	9%
sansw_bp11	11	80	c7001-sw5	3	20	Normal ISL	500	1	D	8 Gbps	8	80.8 MB/s	5%	262.5 MB/s	16%
sansw_bp11	11	87	sw5-xp24000	128	0	Normal ISL	500	1	D	4 Gbps	4	4.3 MB/s	1%	497.7 MB/s	62%
sansw_bp11	11	122	c7000-sw5	2	17	Normal ISL	500	1	D	8 Gbps	8	195.5 MB/s	12%	826.5 MB/s	52%
sansw_bp11	11	123	c7000-sw7	1	17	Normal ISL	500	1	D	8 Gbps	8	102.1 MB/s	6%	494.9 MB/s	31%
sansw_bp11	11	188	c7001-sw7	4	17	Normal ISL	500	1	D	8 Gbps	8	3.5 MB/s	0%	144.8 MB/s	9%

Figura 26 Ancho de banda sw1

Estadísticamente se puede demostrar lo anteriormente expuesto, la figura 27 Estadística del consumo de ancho de banda en horario pico, revela los resultados obtenidos de la captura y procesamiento de la información, el análisis emitido por DELL EMC, identifica alto consumo de ancho de banda en el puerto 23 del slot 2, se conecta con el SAN switch sw5-xp24000, la tasa de consumo se eleva hasta el 62% del consumo total de la red SAN, los demás equipos muestran un comportamiento normal y bajas tasas de consumo, de similar manera evidencio los picos, y se determina que la velocidad de transmisión en ese punto es crítico y debe ser analizado para su actualización y mejora del performance del equipo, para obtener mayor rendimiento en la red SAN.

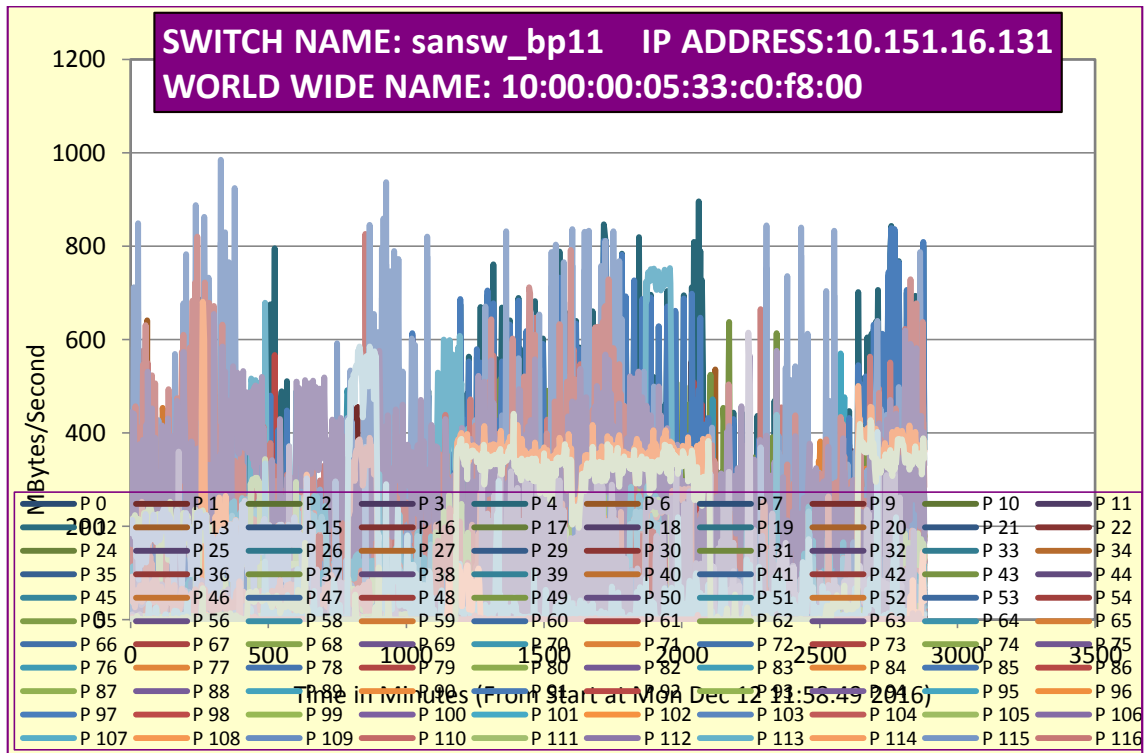


Figura 27 Estadística del consumo de ancho de banda en horario pico.

En la figura 28 resumen del consumo ancho de banda SW2, se puede visualizar un sumario del SAN Switch, donde se evidencia el consumo del ancho de banda que se

provocan en horarios pico, se determina las concurrencias a los puertos, esto da como resultado poder determinar una solución acorde a la necesidad y los requerimientos de la empresa.

SWITCH SUMMARY DETAILS FOR SANSW_BP12				Table Of Contents	
SANSW_BP12 IN FABRIC DIRECTOR2					
ESSENTIAL SWITCH ATTRIBUTES					
Switch Name	sansw_bp12	World Wide Name	10:00:00:05:33:81:9e:00	Number Of Ports	192
Model Number	DCX-8510-4	Model Name	Brocade DCX-8510-4	Switch Speed	16G
Domain ID	12	Fabric Name	Director2	Fabric Principal	10:00:00:05:33:81:9e:00
IP Address	10.151.16.134	Vendor/Support	BROCADE	Serial Number	ANN25286025
DEM Serial Number	USB128C025	Chassis Serial Num	ANP2523G00M	Logical Fabric ID	128
Logical Switch Role	BaseSwitch:No DefaultSwitch:Yes Address	Power Usage	1104	Switch Date	12/12/2016 11:51:39
Switch State	Online	Health Status	Healthy	Switch Role	Principal
ADDITIONAL SWITCH ATTRIBUTES					
Chassis Type	2	Switch ID	lffc0c	Model Sub Number	3
Switch Type	121	Buffer Credits	16	Data Field Size	2112
Error Detect Timeout	2000	Res Allocain Timeout	10000	Long Distance Mode	0
Port ID Format	1	Delay On ReRoutes	Enabled	Sticky ReRoutes	Set
Inteop Mode	0	Hop Count To Far Pnt	1	Preferred Domain	1
Insistent Domain	0	Domain RSCN	0	Switch Mode	Native
Adv Perf Tuning Policy	3	odeName_ZoneCheckin	0	DCFM Versions	695500879_0; -588834778_0; -6539902
Fan 1 State	Ok	Fan 2 State	Ok	Temp Sensor 1	Ok 31C 87F
Temp Sensor 2	Ok 30C 86F	Temp Sensor 3	Ok 32C 89F	Temp Sensor 4	Ok 18C 64F
Temp Sensor 5	Ok 21C 69F	Temp Sensor 6	Ok 27C 80F	Temp Sensor 7	Ok 29C 84F
Temp Sensor 8	Ok 29C 84F	Temp Sensor 9	Ok 33C 91F	Temp Sensor 10	Ok 31C 87F
Network Time Protocol	LOCL	FICON	InUse	FC Routing	disabled
ISCSI	n/a	RADIUS Authentication	No	LDAP Authentication	No
Port Based Routing	NotInUse	xchange Based Routing	InUse	Fabric Watch	Disabled
MAPS	InUse	MAPS Active Policy	dflt_base_policy	Syslog Server	Not In Use
SNMP Trap Recipient	Community1	SNMP IP Address 1	10.0.0.141	SNMP Trap Recipient 2	Community2
SNMP IP Address 2	10.0.3.9	SNMP Trap Recipient 3	Community3	SNMP IP Address 3	10.70.80.31
CPU load (One Minute)	0.33	Active Firmware	7.4.1c	Total Chassis Slots	8
Vacant Chassis Slots	7	CP0 State	Active, Warm Recovered	CP1 State	Standby, Healthy
HA State	HA enabled, Heartbeat Up, HA State sync	SCC Policy Count	0	DCC Policy Count	0
FCS Policy Count	0	2G Ports	2	4G Ports	32
8G Ports	158	Unused Ports	78	Inter-Switch-Links	10
Total Devices	536	Disk Ports	35	Host Ports	430
Tape Ports	11	Appliance Ports	6	Gateway Ports	54
Host : Target ports	4.06:1	Device : ISL ports	53.6:1	No Active Licenses	Exists
SWITCH COMPONENTS					

Figura 28 Resumen consumo ancho de banda SW2

La Figura 25 Resumen del consumo de ancho de banda, evidencia los datos anteriormente mencionados, tales como:

- Ip del dispositivo
- Nombre del dispositivo
- WWN
- 192 Puertos
- Fabric name al que corresponde

Información necesaria para localizar e identificar el equipo dentro de las instalaciones del centro de datos y procesamiento, ubicado en las instalaciones de Telconet.

La figura 29 Ancho de banda sw1, describe el comportamiento y el uso del ancho de banda en horas normales y pico, se logró evidenciar que el consumo oscila entre el 50 % del su rendimiento total, Para el mejorar y rendimiento óptimo de la red SAN el equipo trabaja con estándar de transmisión de 8G.

ISL / TRUNK SUMMARY																	
From Switch			To Switch			ISL or Trunk Type	FSFP Cost	Farthest Pnt (Hops)	Dynamic or Static	Available Bandwidth and Utilization							
Name	Dom Area	Slot/Port	Name	Dom Area	Slot/Port					Speed	BW	Average	% Use	Peak	% Use		
sansw_bp12	12	1	1/1	c7002-sw6	7	17	17	Normal ISL	500	1	D	8 Gbps	8	126.4 MB/s	8%	782.8 MB/s	49%
sansw_bp12	12	20	1/20	c7001-sw6	3	17	17	Normal ISL	500	1	D	8 Gbps	8	82.7 MB/s	5%	303.2 MB/s	19%
sansw_bp12	12	42	1/42	sansw_bp14	14	17	17	Normal ISL	500	1	D	8 Gbps	8	5.4 MB/s	0%	58.5 MB/s	4%
sansw_bp12	12	49	1/49	c7001-sw6	3	19	19	Normal ISL	500	1	D	8 Gbps	8	82.8 MB/s	5%	298.4 MB/s	19%
sansw_bp12	12	50	1/50	c7001-sw6	3	20	20	Normal ISL	500	1	D	8 Gbps	8	82.8 MB/s	5%	309.8 MB/s	19%
sansw_bp12	12	65	2/1	c7002-sw8	8	17	17	Normal ISL	500	1	D	8 Gbps	8	17.7 MB/s	1%	185.6 MB/s	12%
sansw_bp12	12	80	2/16	c7001-sw6	3	18	18	Normal ISL	500	1	D	8 Gbps	8	82.4 MB/s	5%	313.1 MB/s	20%
sansw_bp12	12	122	2/58	c7000-sw8	1	17	17	Normal ISL	500	1	D	8 Gbps	8	139.5 MB/s	9%	715.9 MB/s	45%
sansw_bp12	12	123	2/59	c7000-sw6	2	17	17	Normal ISL	500	1	D	8 Gbps	8	120.6 MB/s	8%	703.3 MB/s	44%
sansw_bp12	12	188	7/60	c7001-sw8	48	17	17	Normal ISL	500	1	D	8 Gbps	8	37.9 MB/s	2%	254.1 MB/s	16%

Figura 29 Consumo del ancho de banda sw2.

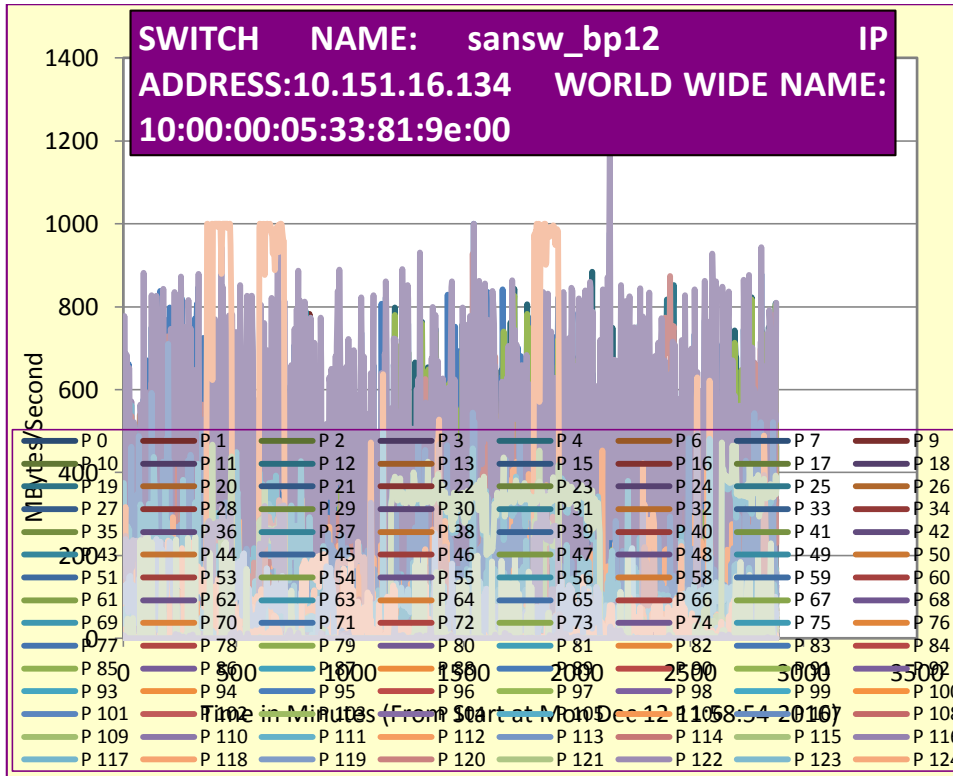


Figura 30 Estadística del consumo de ancho de banda en horario pico sw2.

Estadísticamente se puede demostrar lo anteriormente expuesto, la figura 30 Estadística del consumo de ancho de banda en horario pico sw2, revela los resultados obtenidos de la captura y procesamiento de la información, el análisis emitido por DELL EMC, identifica alto consumo de ancho de banda en el puerto 124, la tasa de consumo se eleva hasta el 100% del consumo total de la red SAN, los demás equipos muestran un comportamiento normal y bajas tasas de consumo.

Para este caso en particular, se identificó un error en su chasis, lo que no fácilmente se puede emitir una solución adecuada sin la participación del proveedor externo quien con su experticia indicara la solución y los pasos a seguir, el error encontrado se lo comentara en el 5.4.10 alertas y errores.

Gracias al estudio de la red SAN por medio del análisis de Brocade SAN Health, se pudo identificar de manera certera los inconvenientes que se producen de manera imperceptible, pero que están ocasionando problemas en el rendimiento y performance de la red SAN.

### 5.4.10. Alertas y errores reportados por SAN health.

El análisis permitió reconocer una alerta sobre un switch sw5-xp2400, que presenta su firmware desactualizado, la recomendación para el caso es realizar un upgrade, por lo cual se generara una ventana de tiempo para logra corregir el errores reportado y causar el menor impacto posible en la disponibilidad de los servicios críticos del cliente.

SWITCHES THAT ARE NOT ON TARGET PATH RELEASES								
Fabric Name	Switch Name	Domain	IP Address	World Wide Name	Model	Current OS Ver	Target Path OS Version	FICON in use
Director1	sw5-xp2400	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	5100	7.0.1a	7.2.0d, 7.1.0c	

Figura 31 Error Switch reportado.<sup>27</sup>

Del análisis realizado se puede determinar que se debe realizar una depuración fina de la conexión con los directores y los switches SAN, con el propósito de reutilizar los puertos, eliminar zonas y alias que ya no son parte de la red SAN, con la depuración se estima que el rendimiento mejoraría considerablemente, debido a que en sus tablas solo constaría los datos de los equipos en los cuales debe asociarse, evitando carga de procesamiento en los dispositivos de la red SAN.

La siguiente figura 33, se visualiza los puertos en los cuales el error encontrado produce fallas en la red SAN, el error Brocade\_DCX4S S7 hace referencia a fallas en el chasis, por lo que se recomienda la visita de un especialista para su valoración y posterior reparación.

IMPORTANT ALERTS AND WARNINGS																				
Date Stamp	Error Level	Process	Description																	
Thu Sep 29 19:51:13 2015	ERROR	C2:1001	Brocade DCX4S S7																	
Sat Oct 15 22:29:03 2015	ERROR	EM-1034	Brocade DCX4S PS 2 set to faulty																	
Sat Oct 15 22:34:43 2015	ERROR	EM-1034	Brocade DCX4S PS 2 set to faulty																	
Sun Oct 16 00:13:53 2015	ERROR	EM-1034	Brocade DCX4S PS 1 set to faulty																	
Sun Oct 16 00:19:23 2015	ERROR	EM-1034	Brocade DCX4S PS 1 set to faulty																	
Sat Oct 29 18:52:36 2015	ERROR	EM-1034	Brocade DCX4S PS 1 set to faulty																	
Sat Oct 29 19:41:00 2015	ERROR	EM-1034	Brocade DCX4S PS 1 set to faulty																	
Sun Oct 30 18:47:11 2015	ERROR	EM-1034	Brocade DCX4S PS 2 set to faulty																	
FRAME ERROR COUNTS																				
Port	Slot	Port Name / Alias / Zone	Port World Wide Name	Transmit	Receive	Enc In	CRC	Short	Long	EndFram	Enc Out	ClassID	Link Fail	IsrSigs	IsrSig	Reject	Busy	Avg Pkt	Peak Pkt	
0	W0	ALI_ECIBPFRMB1_data	2100:00:24:H50:acde	1.9g	1.9g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	W1	c7002-ev6	80:00:00:05:33:49:17:c0	2.5g	362.5m	0	0	0	0	0	0	0	1.2k	0	0	0	0	0	0	0
2	W2	ALI_VIOS0P770_FC59	80:00:00:00:c3:b4:61:43	4.3g	175.7m	0	0	0	0	0	0	0	4.2g	0	0	0	0	0	0	0
3	W3	ALI_TELCONET_XP24K_2C	50:06:0e:80:15:25:ce:12	2.8g	2.8g	0	0	0	0	0	0	0	10.3k	0	0	0	0	0	0	0
4	W4	(EM_DS8870_FC_002C_E3E	50:05:07:43:06:03:94:0f	543.1m	1.1g	0	0	0	0	0	0	0	83.2k	0	0	0	0	0	0	0
5	W5	ALI_VIOS0P770_FC59	80:00:00:00:c3:b4:76:ef	14.8m	6.7m	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	W6	ALI_FLASH_P02	60:06:07:60:5e:82:08:82	1.6g	1.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	W7	ALI_FLASH_P02	60:06:07:60:5e:82:08:82	1.6g	1.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	W8	ALI_FLASH_P02	60:06:07:60:5e:82:08:82	1.6g	1.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	W9	ALI_3PAR_ECIBPSTG04_NMS2	20:22:00:02:ac:00:5e:63	3.9g	1.1g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	W10	ALI_3PAR_ECIBPSTG04_NMS2	20:22:00:02:ac:00:5e:63	2.4g	2.4g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	W11	slot1 port1	20:1100:10:a0:00:78:46	1.9g	2.8g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	W12	slot1 port2	20:1100:10:a0:00:84:c5	317.0m	1.8g	0	0	0	0	0	0	0	260	0	0	0	0	0	0	0
13	W13	slot1 port3	20:12:00:70:a0:00:84:c5	3.4g	4.8g	0	0	0	0	0	0	0	367	0	0	0	0	0	0	0
14	W14	ALI_FLASH_P02	60:06:07:60:5e:82:08:82	1.6g	1.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	W15	ALI_FLASH_P02	60:06:07:60:5e:82:08:82	1.6g	1.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	W16	ALI_ECIBPFRMB2_P3	2100:00:24:H50:acde	395.8m	194.4m	0	0	0	0	0	0	0	475.4k	4.2g	4	558	0	0	0	0
17	W17	ALI_ECIBPFRMB2_P3	2100:00:24:H50:acde	3.2g	3.6g	0	0	0	0	0	0	0	50.9k	0	0	0	0	0	0	0
18	W18	ALI_T53280_DFWV2	25:05:00:0e:11:H:59:5e	2.5g	1.3g	6	7	0	0	0	0	0	7.9k	52.9k	0	1	0	0	0	0
19	W19	ALI_T53280_DFWV4	25:05:00:0e:11:H:59:5e	1.0g	2.4g	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0
20	W20	c7002-ev6	80:00:00:05:33:49:17:c0	2.5g	3.5g	0	0	0	0	0	0	0	20.8k	3	0	0	0	0	0	0
21	W21	ALI_3PAR_ECIBPSTG03_NMS2	24:32:00:02:ac:00:81:97	2.5g	1.9g	0	0	0	0	0	0	0	30	69	0	0	0	0	0	0
22	W22	ALI_3PAR_ECIBPSTG03_NMS2	24:32:00:02:ac:00:81:97	2.5g	3.9g	0	0	0	0	0	0	0	0	36	0	0	0	0	0	0
23	W23	ALI_VIOS0G_FC51	80:00:00:00:c3:b4:78:27	550.7m	1.4g	0	0	0	0	0	0	0	39	4.2g	0	12	0	0	0	0
24	W24	ALI_VIOS02G_FC51	80:00:00:00:c3:b7:b7:c7	97.5m	60.4m	0	0	0	0	0	0	0	7	4.2g	0	18	0	0	0	0
25	W25	slot1 port5	80:00:00:30:a7:74:e4:3c	2.8g	1.4g	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0
26	W26	slot1 port6	80:00:00:30:a7:74:e3:68	3.8g	279.6m	0	0	0	0	0	0	0	39	0	0	0	0	0	0	0
27	W27	slot1 port7	80:00:00:00:c3:b8:21:58	507.5m	2.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	W28	ALI_HAB02_1	80:00:00:00:c3:b7:b7:c7	1.2g	1.9g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	W29	ALI_HAB02_2	80:00:00:00:c3:b7:b7:c7	774.2m	1.2g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	W30	ALI_ECIBPFRMB2_P1_LB1	2100:00:24:H50:acde	1.1g	1.3g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	W31	ALI_ECIBPFRMB2_P2_LB1	2100:00:24:H50:acde	4.3g	547.8m	0	0	0	0	0	0	0	28	4.2g	0	33	0	0	0	0
32	W32	ALI_TELCONET_XP24K_2A	50:06:0e:80:15:25:ce:10	1.6g	1.8g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	W33	ALI_TELCONET_XP24K_4A	50:06:0e:80:15:25:ce:30	1.6g	1.3g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	W34	ALI_TELCONET_XP24K_3B	50:06:0e:80:15:25:ce:11	107.2m	1.4g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	W35	ALI_ECIBPFRMB2_P3_server	2100:00:24:H50:acde	1.1g	684.7m	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	W36	ALI_VIOS0P770_FC51D	80:00:00:00:c3:b4:7e:4b	4.3g	2.5g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	W37	ALI_VIOS02P780_FC51D	80:00:00:00:c3:b8:84:80	2.8g	1.1g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	W38	ALI_VIOS02P780_FC51D	80:00:00:00:c3:b8:84:80	2.8g	1.1g	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figura 32 Errores SAN 2.

<sup>27</sup> Brocade, San Health, Análisis de métricas.

**5.4.11. Análisis de Data Protector.**

El análisis realizado al servidor de data protector pudo evidenciar anomalías en varios equipos tales como servidores en los cuales sus componentes principales como memoria, disco y tarjetería reportaron saturación y la recomendación para estos casos fue el aumento considerable de procesador, cambio de tarjetas por unas de mayor velocidad de transmisión.

El reporte más relevante está incluido como anexos y medio de sustento del análisis realizado sobre data protector, la parte principal es el estudio de la red SAN, lo que por ningún motivo ha de ser de importancia la validación del sistema de obtención de copias de seguridad y restauración mediante data protector y su adecuado almacenamiento en la librerías relacionadas.

La Figura 34 backup por medio de data protector identifica el tipo de backup realizados por la herramienta de color azul muestra los backup de manera incremental y lo de color rojo los backup de manera full.

Seguidamente el top de los servidores que realizan copias de seguridad y restauraciones utilizando data protector.



Figura 33 Backup por medio de data protector.<sup>28</sup>

<sup>28</sup> Brocade San Health, Análisis de métricas Data Protector.



Server	Pool	Type	# Media	# Full	Written (TB)	Avg Full Media Util (GB)
ecbphcb2.uio.bpichincha.com	PRD_P013BANS_FULLLMES	LTO-Ultrium	15		1	
ecbphcb2.uio.bpichincha.com	PRD_P013BANS_FULLLMES_2	LTO-Ultrium	20		3	
ecbphcb2.uio.bpichincha.com	PRD_P013BANS_FULLSEM	LTO-Ultrium	58		5	
ecbphcb2.uio.bpichincha.com	PRD_P013BANS_MIG_ANTES	LTO-Ultrium	1		0	
ecbphcb2.uio.bpichincha.com	PRD_P014BANR_FULLDIA	LTO-Ultrium	3		12	
ecbphcb2.uio.bpichincha.com	PRD_P014BANR_FULLLMES	LTO-Ultrium	39		108	
ecbphcb2.uio.bpichincha.com	PRD_P014BANR_FULLSEM	LTO-Ultrium	141		187	
ecbphcb2.uio.bpichincha.com	PRD_P014BANR_MIG_ANTES	LTO-Ultrium	2		4	
ecbphcb2.uio.bpichincha.com	PRD_P016BANH_MIG_ANTES	LTO-Ultrium	1		4	
ecbphcb2.uio.bpichincha.com	PRD_PAGUEYA_FULLDIA	LTO-Ultrium	3		3	
ecbphcb2.uio.bpichincha.com	PRD_PAGUEYA_FULLSEM	LTO-Ultrium	12		22	
ecbphcb2.uio.bpichincha.com	TST_4048_BS_IgniteServer	LTO-Ultrium	2		1	
ecbphcb2.uio.bpichincha.com	TST_4048_DESA_BPDBFULLSEM	LTO-Ultrium	15		44	

<b>ecbphcb2.uio.bpichincha.com</b>	TST_4048_DESA_BRDBFULLSEM	LTO-Ultrium	2		1	
<b>ecbphcb2.uio.bpichincha.com</b>	TST_4048_ECBPHCD2_FULLLDIA	LTO-Ultrium	1		2	
<b>ecbphcb2.uio.bpichincha.com</b>	TST_4048_ECBPHCD2_FULLSEM	LTO-Ultrium	2		5	
<b>ecbphcb2.uio.bpichincha.com</b>	TST_4048_ECBPHCQ1_FULLLDIA	LTO-Ultrium	1		1	

*Tabla 8 Servidores top Data Protector. <sup>29</sup>*

---

<sup>29</sup> EMCI, Análisis métricas Data Protector.

En la siguiente figura 25 el análisis de data protector y los canales de conexión permitió identificar que existe concurrencia de un servidor denominado ECBRHCP1, durante el análisis el servidor mostro fallas en su procesamiento la acción mediática fue levantar el servidor de contingencia y se mitigo el error, al momento se aumentó memoria y procesamiento en los siguientes días se iniciara la puesta en producción el servidor principal.

## Top Client - Sizing Summary

Host	Operating System	Policy Type	# Policies	Simple Peak Daily (GiB)	Peak Daily by Policy Type (GiB)	Peak Daily Manuals plus Peak by Policy Stream (GiB)
precbphcdb.uio.bpichincha.com	ibm rs6000 aix-7.1	FileSystem, Oracle8	17	10,085	10,779	4,708
ecuio197h02.uio.bpichincha.com	microsoft amd64 wNT-6.0-S	WinFS	1	3,769	3,769	3,769
ecbphcsp2.uio.bpichincha.com	hp ia64 hp-ux-11.31	FileSystem	8	1,311	1,311	2,197
ecbphcp2.uio.bpichincha.com	hp s800 hp-ux-11.11	FileSystem, Oracle8	21	10,317	10,856	2,068
ecbrhcp3.bgr.com	hp ia64 hp-ux-11.31	FileSystem	2	2,064	2,064	1,337
ecbrhcp1.bgr.com	hp s800 hp-ux-11.11	FileSystem	4	1,530	1,530	1,182
ecbphcqa.uio.bpichincha.com	hp s800 hp-ux-11.11	FileSystem, Oracle8	11	2,332	2,334	554
ecuio197h01.uio.bpichincha.com	microsoft i386 wNT-5.0-S	WinFS	1	476	476	476
ecbphcop.uio.bpichincha.com	hp ia64 hp-ux-11.31	FileSystem, Oracle8	15	248	249	297
ecbpbxy1	gpl x86_64 linux-2.6.18-164.el5	FileSystem	2	570	570	268
ecbphcmp.uio.bpichincha.com	hp ia64 hp-ux-11.31	FileSystem, Oracle8	11	152	203	197
ecbphcb2.uio.bpichincha.com	hp ia64 hp-ux-11.31	FileSystem, IDB	2	462	463	183
ecbphcd2.uio.bpichincha.com	hp s800 hp-ux-11.11	FileSystem	3	896	896	147
ecbphcmt.uio.bpichincha.com	hp ia64 hp-ux-11.31	FileSystem	3	110	110	136
ecbpxmat1.uio.bpichincha.com	gpl x86_64 linux-2.6.32-504.el6.x86_64	FileSystem	2	104	104	95

Figura 34 Top ECBRHCP1

Del análisis realizado a la herramienta de data protector considerando los días de mayor carga, se puede apreciar como en los días de fin de semana trabaja al 100%, en base a lo evidenciado se recomendara realizar las copias en horarios nocturnos diferentes tomando en consideración el ambiente de producción, el cual se ejecutara sincronizadamente y con las normas de IT, para garantizar la disponibilidad del servicio y evitando el tiempos de retardo, se toma también en consideración el tema de las depuraciones mensuales y trimestrales a las bases de datos.

## Activities

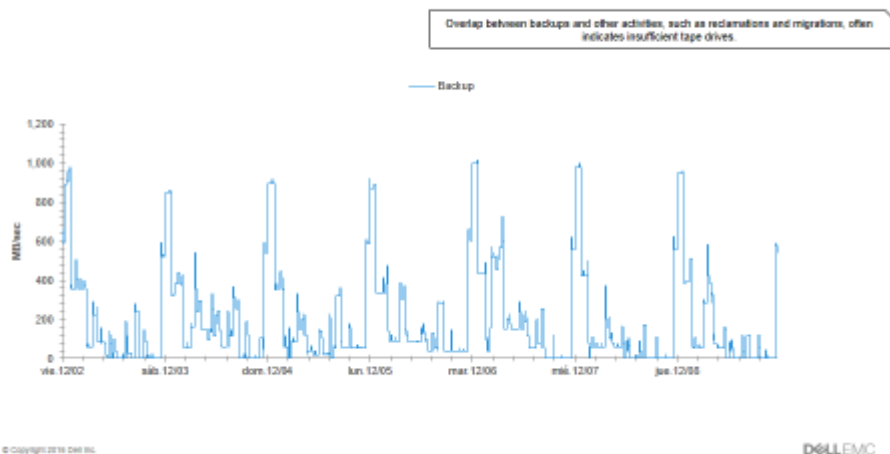


Figura 35 Actividad de Data Protector.

Se puede apreciar también que se tiene que depurar los Jobs de manera de que pueda aplicarse a grupos de servidores afines, ya que una modificación en el job hace que el backup no ejecute con normalidad, retrasando la operatividad del ambiente, los criterios de la generación de las tareas son coordinadas con el departamento de centro de cómputo para su análisis y posterior toma de decisión para una mejora continua.

## Backup Job Summary

Long backups are a sign of unhealthy and overloaded backup servers

Server	ecbphcb2.uio.bpichincha.com
Clients	28
# Jobs	37,992
# Clients > 8 Hours	6
# Clients > 12 Hours	5
# Clients > 24 Hours	3
Backed Up (TB)	470.81
# Files	124,647,668

Figura 36 Tareas programadas en Data Protector.

La figura 27 resumen las acciones a reparar para que el sistema de copias de seguridad y restauraciones mejore en su rendimiento y eficacia, el análisis recomienda un análisis de los respaldos que se realizan a las bases de datos transaccionales, y que son ejecutadas por comandos propios de Oracle, comandos como rman, los cuales son interpretados en las conexiones de la red SAN directamente con el servidor de respaldos, revisión en la parte de los dominios, recomienda que solo debe gobernar un solo dominio en la red, por lo que se recomienda la separación de los dominios y la creación de los servidores dentro de cada dominio correspondiente, una revisión para optimizar el ambiente virtual, tomando en consideración la parte de UNIX que en HP - UX, conviven contenedores asociados a la vpar, en todos los ambientes conocidos.

## Recommended Assessments

- [Data Domain](#): Utilization trends, performance and client data change rates
- [VMware](#): VM to Backup Relationships
- [Oracle RMAN](#): Directly measure client size, backup duration, and change rates
- [SAN Health](#): Understand how the SAN impacts backups

Figura 37 Recomendaciones a implementar sobre Data Protector.

El análisis pudo reflejar de manera generalizada las políticas que se imponen en el sistema de copias de seguridad y restauración, mostrando un análisis para su depuración y mejor organización, la figura 28 presenta a detalle lo sugerido.

## Policy Types Peak Summary

Server	Operating System	Policy Type	# Clients	Peak Daily (GB)
ectphcb2.uio.bpichincha.com	gpl x86_64 linux-2.6.18-164.el5	FileSystem	1	570
ectphcb2.uio.bpichincha.com	gpl x86_64 linux-2.6.32-504.el6.x86_64	FileSystem	4	166
ectphcb2.uio.bpichincha.com	gpl x86_64 linux-2.6.32-504.el6.x86_64	Oracle8	2	129
ectphcb2.uio.bpichincha.com	gpl x86_64 linux-2.6.32-573.7.1.el6.x86_64	FileSystem	2	35
ectphcb2.uio.bpichincha.com	gpl x86_64 linux-2.6.32-573.7.1.el6.x86_64	Oracle8	1	22
ectphcb2.uio.bpichincha.com	hp ia64 hp-ux-11.31	FileSystem	8	4,092
ectphcb2.uio.bpichincha.com	hp ia64 hp-ux-11.31	IDB	1	154
ectphcb2.uio.bpichincha.com	hp ia64 hp-ux-11.31	Oracle8	2	175
ectphcb2.uio.bpichincha.com	hp s800 hp-ux-11.11	FileSystem	5	3,922
ectphcb2.uio.bpichincha.com	hp s800 hp-ux-11.11	Oracle8	2	11,723
ectphcb2.uio.bpichincha.com	ibm rs6000 aix-7.1	FileSystem	1	695
ectphcb2.uio.bpichincha.com	ibm rs6000 aix-7.1	Oracle8	1	10,085
ectphcb2.uio.bpichincha.com	microsoft amd64 wNT-6.0-S	WinFS	1	3,769
ectphcb2.uio.bpichincha.com	microsoft i386 wNT-5.0-S	WinFS	1	476
ectphcb2.uio.bpichincha.com	microsoft i386 wNT-5.2-S	WinFS	4	89
ectphcb2.uio.bpichincha.com	sun sparc solaris-5.10	Oracle8	1	92
				36,193

Figura 38 Políticas aplicadas a Data Protector.

La capacidad de la red también fue analizada por medio del estudio de Data Protector, sus resultados se visualizan en la siguiente imagen donde se evidencia el consumo promedio de la red y servirá también de referencia para la emisión de las sugerencias y recomendaciones para la mejora de la red SAN.

## NetWorker Capacity Licensing Metrics - Type

All sizes are after any client-side compression, including RMAN compression.

Operating System	Policy Type	Peak Daily - App (GB)	Peak Daily - Unique or Manual Filesystem (GB)	Total Largest Fulls - Filesystems (GB)	Capacity Estimate (GB)
gpl x86_64 linux-2.6.18-164.el5	FileSystem	0	0	570	570
gpl x86_64 linux-2.6.32-504.el6.x86_64	FileSystem	0	0	166	166
gpl x86_64 linux-2.6.32-504.el6.x86_64	Oracle8	129	0	0	129
gpl x86_64 linux-2.6.32-573.7.1.el6.x86_64	FileSystem	0	0	35	35
gpl x86_64 linux-2.6.32-573.7.1.el6.x86_64	Oracle8	22	0	0	22
hp ia64 hp-ux-11.31	FileSystem	0	0	5,651	5,651
hp ia64 hp-ux-11.31	IDB	154	0	0	154
hp ia64 hp-ux-11.31	Oracle8	191	0	0	191
hp s800 hp-ux-11.11	FileSystem	0	0	3,845	3,845
hp s800 hp-ux-11.11	Oracle8	11,723	0	0	11,723
ibm rs6000 aix-7.1	FileSystem	0	0	695	695
ibm rs6000 aix-7.1	Oracle8	10,085	0	0	10,085
microsoft amd64 wNT-6.0-S	WinFS	0	0	3,769	3,769
microsoft i386 wNT-5.0-S	WinFS	0	0	476	476
microsoft i386 wNT-5.2-S	WinFS	0	0	89	89
sun sparc solaris-5.10	Oracle8	92	0	0	92

Figura 39 Métricas del consumo de la red – Licencias.

La capacidad de retención y almacenamiento de la información se dio a conocer gracias al análisis realizado, se procederá con un estudio para verificar si la información almacenada es de importancia y será utilizada a futuro, se analizará el riesgo que

conlleve la perdida de la misma. La figura 30 demuestra y evidencia el análisis reportado.

## Daily Capacity by Type Backup

Use fewer pools to improve drive and tape utilization, and to simplify media management.



Figura 40 Capacidad de backups.

## Media Consumption by Month

Does not include any Disk/Boost/OST media

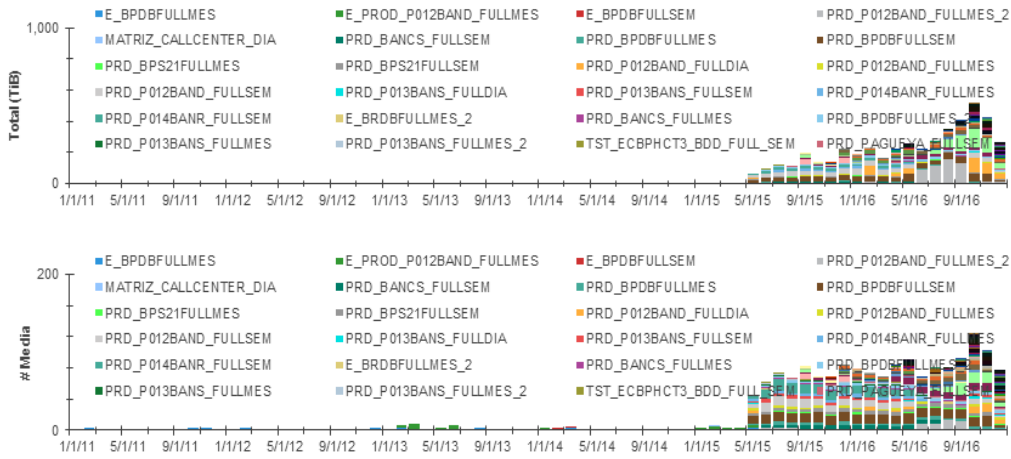


Figura 41 Consumo promedio por mes.

# Backup Throughput

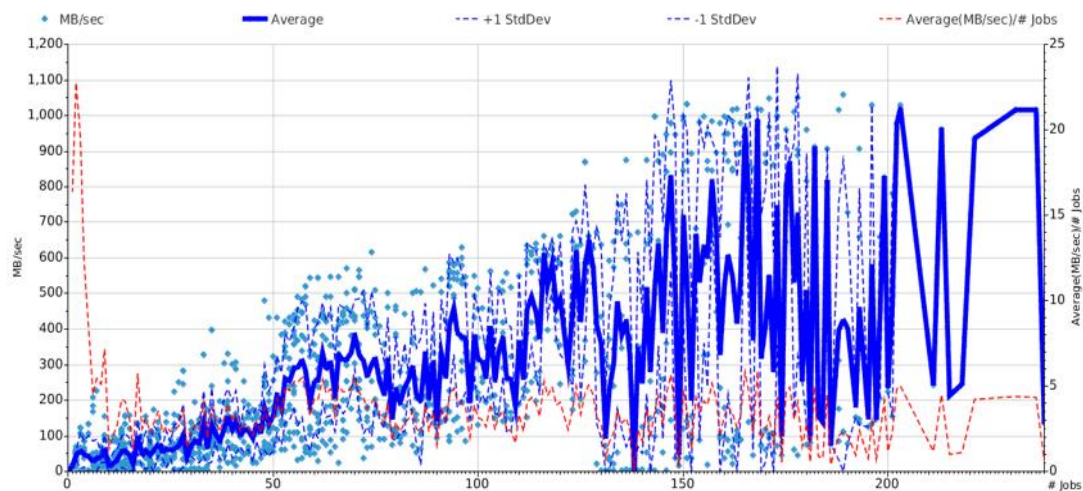


Figura 42 Performance de Data Protector.

En el espacio de los anexos usted puede encontrar el informe completo sobre el análisis de Data Protector, transcurso de la investigación se presentaron inconvenientes tales como:

Demora en el backup: evento producido por falta de memoria en el servidor ECBRHPC2, el cual consta en este caso de estudio retraso la operación cerca de 3 Horas, lo que ocasiona pérdidas económicas para la empresa, los niveles y políticas garantizan que se debe solucionar en un tiempo menor de una hora, al momento se incrementó memoria y procesador al servidor en mención.

El estudio ha sido de gran ayuda en la validación de los errores y casos reportados por temas de retraso con la herramienta de copias de seguridad y restauración

## 5.5. Estudio comparativo entre las diferentes herramientas de copias de seguridad y restauración existentes en el mercado.

Dentro de la empresa conviven otras herramientas que permiten la obtención de copias de seguridad y restauración, las cuales están siendo analizadas para determinar si continúan en funcionamiento o son reemplazadas por otra, en el caso puntual data protector ha sido elegida como la herramienta principal y se ha puesto en estudio Netbackup. La segunda herramienta no ha brindado la confiabilidad y estabilidad con referencia a data protector, Netbackup ha tenido varias dificultades desde su origen, no se ha adaptado a una de sus características principales que es la operatividad en múltiples plataforma, el caso está siendo analizado por la empresa Conecta, empresa responsable de la adquisición y soporte dedicado de Netbackup.

Las herramientas utilizadas en TCS son Arcserve, Netbackup, TSM y Data Protector, como se lo menciono anteriormente en el presente documento se debe tener en consideración que se debe tener un ambiente de restauración por cada herramienta, en caso de que salgan de producción hay que proveer un ambiente alternativo para restaurar los históricos que se soliciten, en especial de Arcserv que esta por ser remplazada por Netbackup, la decisión depende de los resultados que se obtengan en el periodo de pruebas finales que se llevará a cabo desde el mes de enero del 2017, y los beneficios que representa mantener data protector y permitir la convivencias de Netbackup y data protector.

Las herramientas utilizadas se diferencian en costo y beneficio, siendo necesario realizar un análisis detallado donde se pueda evidenciar las mejoras obtenidas al utilizar una sola herramienta.

A continuación en siguiente tabla se describe cada una de las herramientas que se utiliza como medio de obtención de copias de seguridad y se hará una comparación entre ellas para determinar ventajas y desventajas que a futuro servirán en la toma de decisiones y la adecuada selección de la herramienta idónea para la tarea indicada.

<i>BACKUP</i>	<i>VENTAJAS</i>	<i>DESVENTAJAS</i>	<i>LICENCIAMIENTO</i>	<i>SOPORTE</i>
<i>TSM</i>	<ul style="list-style-type: none"> <li>• <i>Respaldo programados</i></li> <li>• <i>Respaldo de Base de datos db2 propias de del producto</i></li> <li>• <i>Respalda FS</i></li> </ul>	<i>No respalda base de datos transaccionales</i>	<i>Licenciamiento adicional por cada base</i> <i>Licenciamiento por cada servidor</i>	<i>Si</i>
<i>Arcserve</i>	<ul style="list-style-type: none"> <li>• <i>Respalda base de datos Sql</i></li> <li>• <i>Respaldo de file system</i></li> <li>• <i>Plataforma solaris</i></li> </ul>	<i>No respalda base de datos transaccionales</i>	<i>Licenciamiento perpetuo</i>	<i>no</i>
<i>Netbackup</i>	<ul style="list-style-type: none"> <li>• <i>Ambientes virtuales</i></li> <li>• <i>File system Exchange</i></li> <li>• <i>Sql</i></li> <li>• <i>Oracle</i></li> <li>• <i>Producción</i></li> <li>• <i>Integración Multiplataforma</i></li> </ul>	<i>Respalda base de datos transaccionales.</i> <i>Errores con integraciones Oracle</i>	<i>Por espacio</i> <i>Por agente</i>	<i>SI</i>
<i>Data Protector</i>	<ul style="list-style-type: none"> <li>• <i>Respalda File system</i></li> <li>• <i>Respalda Base de datos transaccionales</i></li> </ul>	<i>Al ocurrir pérdida o fallas en su base interna el producto no funciona.</i>	<i>Por cada concurrencia a las bases un licenciamiento.</i> <i>Errores que requiere soporte</i>	<i>Si</i>

	<ul style="list-style-type: none"> <li>• <i>Incluye su propia base</i></li> <li>• <i>Respalda bases en línea</i></li> <li>• <i>Tareas programadas</i></li> <li>• <i>Administración gráfica.</i></li> <li>• <i>Integración Multi plataforma</i></li> <li>• <i>Producción</i></li> </ul>		<i>especializado</i>	
--	--	--	----------------------	--

*Tabla 9 Comparaciones entre herramientas de backup.*

La tabla 6 comparaciones entre herramientas de backup, representa resumidamente las fortalezas y opciones de las diferentes herramientas de copias de seguridad y restauración que actualmente conviven en la empresa y dentro del sistema de las red SAN, lo que se trata de evidencias que Data protector tiene mejores beneficios en comparación con las demás, pero el estudio solo mencionará como sugerencias y recomendaciones que luego de un análisis gerencial referente al costo beneficio las jefaturas y gerencias decidirán que herramienta será la que gobierne en toda la infraestructura y se tomara en consideración los riesgos que contemple las nuevas implementaciones.

**5.6. Recomendaciones para optimizar el tiempo de ejecución de los respaldos y mejoramiento de la red SAN.**

Luego del análisis realizado en la red SAN, se determina las siguientes recomendaciones.

- Para una mejor optimización y administración del sistema de copias de seguridad y restauración se debe considerar la separación de las redes de los ambientes existentes, es decir que se debe separa el ambiente de producción con los ambientes de test y desarrollo.
- El cliente debe mejorar sus equipos, iniciando desde los más elementales o básicos, tratando de unificar su tarjetería de comunicación, al igual que sus equipos de transmisión de datos, de nada sirve mejorar la tasa de transmisión y uno o varios equipos trabajan a velocidades mínimas.
- En el análisis realizado por DELLEMCI relacionado a las métricas de Data protector se pudo identificar que el tema de procesamiento de datos es también un cuello de botella que puede ocasionar retención de data y no culminar el proceso exitosamente y dentro de las tiempos estimados, al momento se está validando la posibilidad de incremento de cores y memoria en los equipos de producción, tomando énfasis en los servidores de nivel crítico, cuyo tiempo de recuperación debe ser mínimo el cliente deberá realizar un estudio de costo beneficio para lograr estabilizar el ambiente, al tratarse de una empresa que brinda servicios masivos y por la políticas internas establecidas iniciarían en los equipos que conforman el ambiente de test para

posteriormente ser aplicados a la plataforma de online o producción. Pero basados en el siguiente estudio la recomendación aplica al ambiente productivo y se deja a libre decisión por parte del cliente, quien decidirá y aplica directamente el incremento de cores y memoria o se rige a las políticas internas.

- Realizar un cronograma establecido y periódico para la realización de mantenimientos a las librerías y todo el equipamiento que conforma el sistema de copias de seguridad y restauración.
- Se recomienda la separación de las entidades bancarias y contemplar un sistema propio de copias de seguridad y restauración que garantice la obtención y retención de la información por separado, es decir la cada empresa debería tener su servidor de copia y su servidor de restauración por cada herramienta y su respectivo ambiente.
- Elegir una sola herramienta de copias de seguridad y restauración, al momento conviven dos herramientas más como el Arcserve y Netbackup dentro de toda la infraestructura. Si data protector es elegida como herramienta principal debería considerar mantener un servidor para data protector y otro para restauraciones, recordando que cada herramienta restaura desde el origen del backup, por ejemplo si se contiene una copia de seguridad por medio de data protector solo puede restaurar los backup obtenidos por dicha herramienta.
- Generar políticas de acuerdo a cada plataforma y ambiente, no debe mezclar los ambientes productivos con los de test o desarrollo. Como se mencionó anteriormente al moverse un servidor la política no puede ser aplicada con normalidad, esto retrasa el proceso de backup, la revisión conlleva en todos los servidores que conforman el job.
- Establecer normativas específicas cuando se realice las actividades de puesta en producción del ambiente de FILE OVER y trate de ambientes donde esté constituido por contenedores.
- Mejorar y aumenta las capacidad de drive y tape en las librerías como también se sugiere mantener las cintas en óptimas condiciones.
- Mantener los licenciamientos de las herramientas de copias y restauración a buen recaudo y vigentes, al momento de solicitar soporte al proveedor en necesario tener toda la información sobre los productos licenciados y que se encuentren vigentes y dentro de un contrato de soporte especializado y dedicado durante un periodo negociado entre las partes (cliente – proveedor).

En el caso de la red SAN las recomendaciones son las siguientes:

- En el presente análisis se pudo evidenciar que existen alias y miembros que son parte de las configuraciones de las zonas que ya no existen, lo que ocasiona una saturación y sea difícil de administrar, no se lleva un orden, ni una secuencia en la asignación de los puertos.
- La topología entre los directores y switches que integran la red SAN tienen tarjetería distinta y negocian a velocidades diferentes, esto no es óptimo debido a que exista varios puntos de falla que ocasionaría cuellos de botella y retención de la información,
- lo que puede ocasionar una degradación en el rendimiento y aumento del delay y time out.

- Existen switches con velocidad de 8Gbps, en la mayoría de los switches, zonificados a un almacenamiento de contingencia, los cuales podrían ocasionar un cuello de botella en el momento que se active la contingencia y el FILE OVER.
- La topología actual con la que TCS está operando, es una combinación estrella-cascada, lo que ocasiona lo siguiente:
- Saltos entre dispositivos, zonas con demasiados miembros, más puntos de falla en cuanto a fibras entre switches y posible aumento en el delay de los paquetes.
- No hay redundancia de conexión entre los directores de FABRIC-1; en el FABRIC-2.
- En la topología no existen enlaces troncales, puesto que se carece de licenciamiento de TRUNKING para este propósito en los switches actuales.
- Las versiones de firmware de un director están desactualizadas y con errores en sus tarjetas de FO.
- Se observó que hay varios errores del tipo "ERROR" en varios puertos en ambos fabric, lo que implicaría que existirían problemas en los cables de fibra, en la HBA o en el transceiver involucrados.
- Se observó que los puertos de ISL no se encuentran en porcentajes de utilización críticos (70%), aun cuando las muestras corresponden a las horas pico, esto es, en la noche, cuando se corren los procesos batch.
- Se observa que las zonas tienen combinación de puertos, lo cual no es lo recomendado por las Mejores Prácticas del fabricante.

## 6. Conclusiones y Recomendaciones

### 6.1 Conclusiones

Al finalizar el presente caso de estudio se determina las conclusiones más distinguidas:

- Se logró identificar el comportamiento irregular de la red SAN, provocado por no realizar un mantenimiento y depuración en la configuración de los equipos SAN.
- Se encontró que existe dispositivos que forman parte de varias zonas y que no están siendo utilizados, lo que provoca el uso de recurso de memoria y procesamiento innecesario.
- La configuración de la topología asocia a varios equipos en distintos switches, se debería organizar la segmentación y depurar las wwn que ya no son utilizadas.
- La versión de un switch necesita una actualización urgente.
- No dispone de redundancia entre los directores, se debe ver la manera de generar un sistema de conexión alternativo para el caso de los directores.
- No existe licenciamiento con los puertos que forman la cascada entre los switch SAN.
- Los puertos negocian entre el 70-100% cuando se corren las backup, los cuales se realizan en el periodo nocturno.
- El análisis realizado identifico dos fallas de consideración, porque es necesario realizar una visita planificada del personal calificado y especializado en los equipos de SAN.
- Se identificó el encolamiento y retardo que se produce al momento de obtener el backup de seguridad por medio de la herramienta de Data Protector por falta de recursos en sus componentes principales como memoria y procesador.
- Con el análisis de Data Protector se logró identificar políticas mal aplicadas, se identificó el servidor que realiza mayor demanda de sistema de backup, el equipo requiere que se aumente procesador y memoria.
- Un mantenimiento planificado también resultaría gratificante.

### 6.2 Recomendaciones

Las recomendaciones, que serán un eje fundamental para dar a conocer a la empresa las posibles soluciones que servirán para mejorar y optimizar los tiempos de ejecución de las copias de seguridad y restauraciones, recomendaciones que serán presentadas a los departamentos regulatorios de la empresa para su evaluación y posterior aprobación. La empresa está en la potestad de decidir si las recomendaciones emitidas en el presente estudio son aplicables a sus requerimientos, necesidades y políticas institucionales.

- La segmentación de la red LAN para los ambientes de test - desarrollo y producción deben ser distintas, lo que representa el uso dedicado de la red y del canal.
- Depurar la configuración de los directores.
- Verificar los dispositivos que cumplieron con su vida útil e implementar con mejores dispositivos.
- En las tareas de zonificación se deba mantener el formato de mejores prácticas y las recomendaciones del fabricante.

- Todos los dispositivos deben mantener redundancia eléctrica, esta recomendación la debe garantizar el data center donde se encuentra la red SAN.
- Se debe pensar en mejorar las tarjetas HBA, para que aumente la velocidad de transmisión.
- Se debe pensar en un análisis sobre las librerías, su tarjetería también ocasiona retardos, considerar que el nivel de escritura de los tapes debe ir acorde a la velocidad de negociación de los demás equipos que conforman la red SAN.
- Aumentar más drives para que la información enviada desde la red SAN sea almacenada a velocidades mayores, mejorando el rendimiento de la red SAN.
- Depurar la configuración de las zonas en cada uno de los directores, la concurrencia debería ser balanceada entre todos los puertos de conexión.
- Mantener un inventario de los nuevos equipos que ingresan a formar parte de la red SAN.
- Generar un inventario codificado de las conexiones de fibra hacia las distintas HBA de los equipos que conforman la red SAN.
- Validar soporte extendido con el fabricante para recopilar las mejores implementaciones y analizar las sugerencias para el crecimiento y segmentación de la red SAN.
- Evitar que diferentes dominios convivan en una misma red SAN. Lo ideal es que solo uno gobierne toda la infraestructura, se debe separar las entidades que financieras que comparten los recursos del sistema de copias de seguridad y restauración.
- Mejorar el equipamiento de la red SAN, es necesario verificar en relación al coste de los equipos y no hay presupuesto se debe tener en consideración el tuning de los mismos, apegados siempre a las recomendaciones del fabricante y del soporte especializado que brindan las empresa como HPE e IBM.

## Bibliografía:

- [1] Bowker, M. (2012). <http://www.emc.com/>. Recuperado el Marzo de 2015, de <http://www.emc.com/collateral/analyst-reports/esg-emc-backup-recovery-large-scale-vmware-environments.pdf>
- [2] EMC Corporation. (7 de Julio de 2012). EMC Análisis Data Protector Administración Student Guide. Milford, Massachusetts, USA
- [3] Idc.com, *Worldwide Disk Storage Systems Report*, IDC
- [4] Kiosera.net, *SAN (Red de área de almacenamiento)*, Introducción a SAN, Recuperado de: <http://es.ccm.net/contents/638-SAN-red-de-area-de-almacenamiento>.
- [5] Mundo Cisco, *¿Qué es una Red SAN?*, Recuperado de: <http://www.mundocisco.com/2009/09/que-es-una-red-SAN.html>.
- [6] SAN for the Masses, *Computing Technology Industry Association*, recuperado de: <http://www.comptia.org/research/files/summaries/sansforthemassessummary1-02.pdf>
- [7] Symantec Corporation, *SAN (red de área de almacenamiento)*, 1995 - 2016, Recuperado de [https://www.symantec.com/es/mx/security\\_response/glossary/define.jsp?letter=s&word=SAN-storage-area-network](https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=s&word=SAN-storage-area-network)
- [8] Viveros, S. (Ed.). (2010). *Manual de publicaciones de la American Psychological Association*. México: Editorial El Manual Moderno para referencias bibliográficas.

Anexos:

SAN SUMMARY DETAILS FOR JC														Table Of Contents
SWITCHES IN SAN jc														
Fabric Name	Switch Name	Dom	IP Address	World Wide Name	Model	Spd	OS Ver	Status	Days Up	Pwr (W)	Serial Number	Ports (Total)	Unusd	UnLicnd
Director1	c7000-sw 7	1	10.151.16.70	10:00:00:05:1e:c6:17:cd	5480	8G	7.4.1c	Healthy	120	36	ALED0442E06B	24 (24)	17	0
Director1	c7000-sw 5	2	10.151.16.72	10:00:00:05:1e:c5:42:a4	5480	8G	7.4.1c	Healthy	120	36	ALED0442E06K	24 (24)	16	0
Director1	c7001-sw 5	3	10.151.16.92	10:00:00:05:33:43:bf:da	5480	8G	7.4.1c	Healthy	119	36	ALED0448F0F5	24 (24)	5	0
Director1	c7001-sw 7	4	10.151.16.95	10:00:00:05:33:4a:01:68	5480	8G	7.4.1c	Healthy	119	36	ALED0448F0F7	24 (24)	8	0
Director1	c7002-sw 5	7	10.151.16.100	10:00:00:05:33:49:f7:bd	5480	8G	7.4.1c	Healthy	119	36	ALED0448F0F4	24 (24)	15	0
Director1	c7002-sw 7	8	10.151.16.102	10:00:00:05:33:49:e9:a1	5480	8G	7.4.1c	Healthy	119	36	ALED0448F0ED	24 (24)	18	0
Director1	sansw_bp11	11	10.151.16.131	10:00:00:05:33:c0:f8:00	DCX-8510-4	16G	7.4.1c	Healthy	119	1104	ANN2502H01S	192 (256)	9	0
Director1	sansw_bp13	13	10.151.16.234	10:00:00:27:f8:60:29:68	5480	8G	7.4.1c	Healthy	120	36	ALED0408J010	24 (24)	5	14
Director1	sw 5:xp24000	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	5100	8G	7.0.1a	Healthy	284	84	ALMD640E02K	40 (40)	33	0
Director2	c7000-sw 8	1	10.151.16.73	10:00:00:05:1e:c8:1e:62	5480	8G	7.4.1c	Healthy	118	36	ALED0442E02S	24 (24)	16	0
Director2	c7000-sw 6	2	10.151.16.71	10:00:00:05:1e:c8:33:c0	5480	8G	7.4.1c	Healthy	118	36	ALED0442E040	24 (24)	17	0
Director2	c7001-sw 6	3	10.151.16.28	10:00:00:05:33:42:00:88	5480	8G	7.4.1c	Healthy	118	36	ALED0448F0E1	24 (24)	5	0
Director2	c7002-sw 6	7	10.151.16.101	10:00:00:06:33:49:f7:00	5480	8G	7.4.1c	Healthy	118	36	ALED0448F0F1	24 (24)	15	0
Director2	c7002-sw 8	8	10.151.16.103	10:00:00:06:33:49:fc:a8	5480	8G	7.4.1c	Healthy	118	36	ALED0448F0G7	24 (24)	18	0
Director2	sansw_bp12	12	10.151.16.134	10:00:00:05:33:81:9e:00	DCX-8510-4	16G	7.4.1c	Healthy	118	1104	ANN2528G02S	192 (256)	8	0
Director2	sansw_bp14	14	10.151.16.235	10:00:00:27:f8:60:0a:dc	5480	8G	7.4.1c	Healthy	118	36	ALED0408J023	24 (24)	5	14
Director2	c7001-sw 8	48	10.151.16.28	10:00:00:05:33:49:fa:14	5480	8G	7.4.1c	Healthy	118	36	ALED0448F0GB	24 (24)	8	0

Figura 43 Summary Red SAN

SUMMARY FOR 17 SWITCHES WITH 760 PORTS ( LICENSED PORTS - 732) THAT ARE 70 % UTILIZED																			
Fabric Name	Switch Count							Port Count							Port Use Metrics				
	2G	4G	8G	10G	16G	32G	Total	2G	4G	8G	10G	16G	32G	Total	ISL Ports	Device Ports	Devices	Unused	Utilization
Director1	0	0	8	0	1	0	9	2	84	300	0	0	0	400	22	252	602	126	67 %
Director2	0	0	7	0	1	0	8	2	47	297	0	0	0	360	20	248	597	92	73 %
TOTALS	0	0	15	0	2	0	17	4	131	597	0	0	0	760	42	500	1199	218	70 %

DEVICE COUNT FOR ALL FABRICS 1199 (Including all NPIV and Loop Devices)					
Device Description	Count	Device Description	Count	Device Description	Count
3PAR Data	42	Emulex HBA	110	Emulex HBA (HP-LUX)	1
HP HBA (Qlogic)	23	HP Library	49	HP Storage (Hitachi)	12
HP Virtual Connect	4	IBM Disk	8	IBM SAN Volume Controller	12
IBM TotalStorage DS8000	4	IBM Ultrium	4	IBM Ultrium (ADIC)	6
NON-STANDARDS COMPLIANT WWN	7	NPIV Host	727	Qlogic HBA	190

PORT USE																					
Fabric Name	Port Counts			Attached Device Types				Inter Switch Links				Fan Out Ratios			Long Distance Modes						
	Total	Unusd	Unlicd	Disk	Tape	Host	Appliance	Gateway	ISLs	IFLs	Trnk Mstr	Trnk Sw	Host:Disk	Non-ISL:ISL	ISL Device:ISL	10km	25km	50km	100k	300k	Auto
Director1	400	126	14	34	11	495	6	56	22	0	0	0	14.56:1	17.18:1	27.36:1	400	0	0	0	0	0
Director2	360	92	14	35	11	490	6	55	20	0	0	0	14:1	17:1	29.85:1	360	0	0	0	0	0
TOTALS	760	218	28	69	22	985	12	111	42	0	0	0				760	0	0	0	0	0

LICENSE SUMMARY										
Fabric Name	License Name	Count	License Name	Count	License Name	Count	License Name	Count	License Name	Count
Director1	8GigFC	8	EnhancedManagement	8	FullFabric	8	No Active Licenses	1	POD12	6
Director2	8GigFC	7	EnhancedManagement	7	FullFabric	7	No Active Licenses	1	POD12	6

BANDWIDTH UTILIZATION STATISTICS																										
Fabric Name	Device Bandwidth Utilization (per port)						ISL Bandwidth Utilization (per port)						IFL Bandwidth Utilization (per port)													
	Devic	0 - 25%		26 - 75%		76 - 100%		0 - 25%		26 - 75%		76 - 100%		IFL		0 - 25%		26 - 75%		76 - 100%		Avg		Peak		
Director1	602	602	438	0	163	0	1	18.1	2496	22	22	14	0	7	0	1	27.5	855	0	0	0	0	0	0	0	0
Director2	597	596	432	1	165	0	0	20.4	1783	20	20	14	0	6	0	0	29.4	788	0	0	0	0	0	0	0	0
TOTALS	1199	1198	870	1	328	0	1	19.2		42	42	28	0	13	0	1	28.4		0	0	0	0	0	0	0	0

Figura 44 Summary de Licencias – puertos.

ZONING METRICS													
Fabric Name	Zone Database Use	Aliases Statistics				Zone Statistics				Config Statistics			
		Aliases	Avg Mem	Max Mem	Hang Mem	Zones	Avg Mem	Max Mem	Hang Mem	Configs	Avg Mem	Max Mem	Hang Mem
Director1	14.7%of1046274B	766	1.01	2	266	922	2.72	11	349	1	857	857	259
Director2	14.4%of1046274B	735	1	2	240	914	2.74	11	362	1	841	841	253
TOTALS		1501	1	2	506	1836	2.7	11	711	2	849	857	512

Figura 45 Zonas de la red SAN.

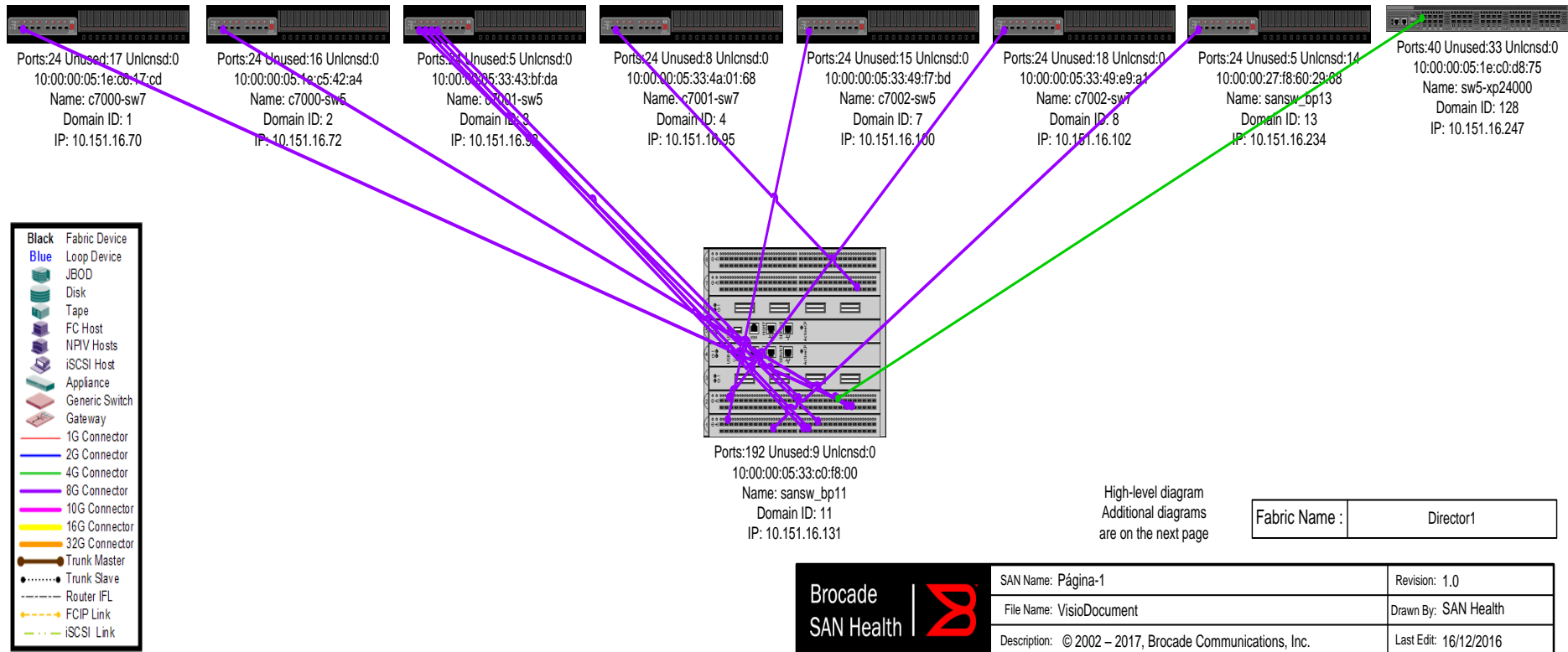


Figura 46 Topología Director 1

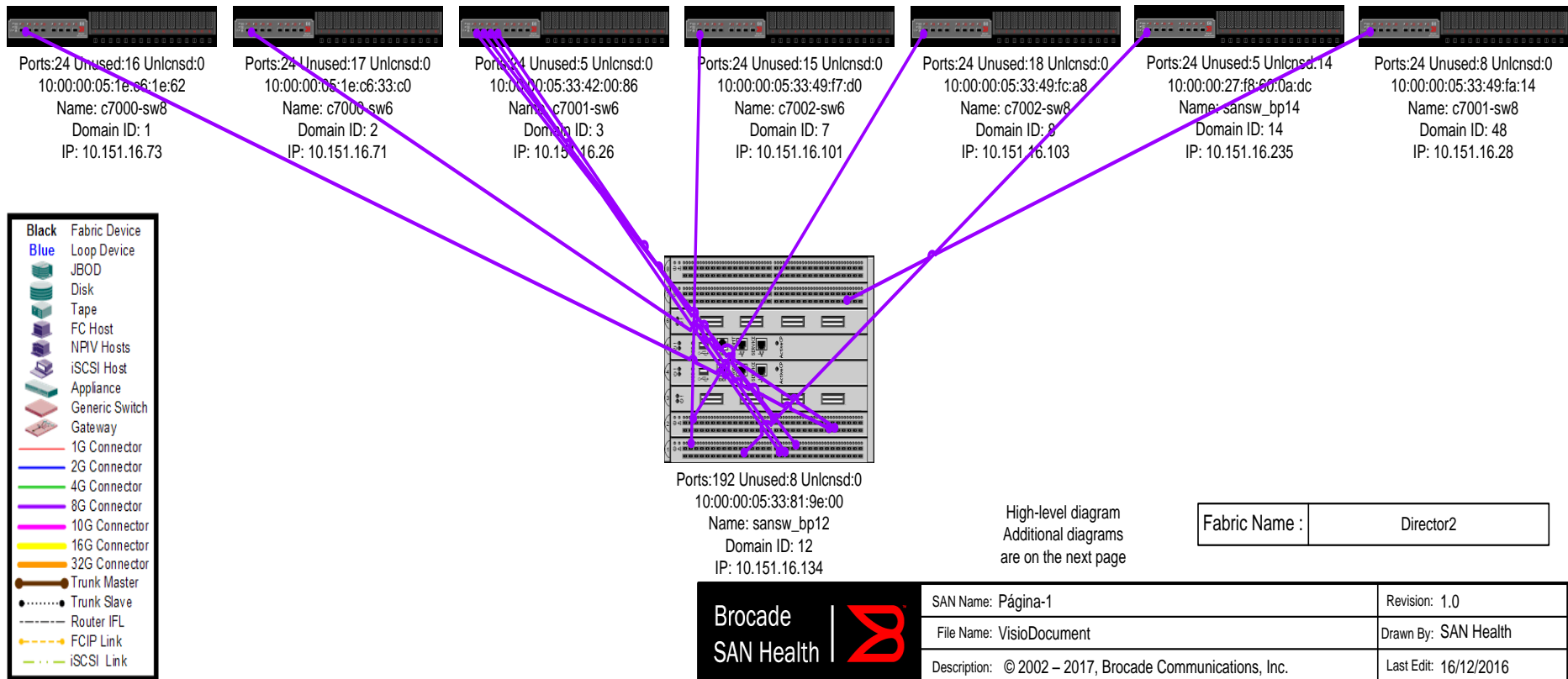


Figura 47 Topología Director 2



Survey Of SAN  
jc  
Completed For  
TCS  
On  
Mon Dec 12 2016

SAN Health Client Version : 4.0.7  
Reporter Builder Version : 4.0.7

*Figura 48 Análisis de la red SAN*

**SAN SUMMARY DETAILS FOR JC**

[Table Of Contents](#)

SWITCHES IN SAN jc														
Fabric Name	Switch Name	Dom	IP Address	World Wide Name	Model	Spd	OSVer	Status	DaysUp	Fwrv	Serial Number	Ports (Total)	Unused	UnLicnd
Director1	c7000-sw7	1	10.151.16.70	10:00:00:05:1e:c6:17:cd	5480	8G	7.4.1c	Healthv	120	36	ALE0442E06B	24 (24)	17	0
Director1	c7000-sw5	2	10.151.16.72	10:00:00:05:1e:c5:42:e4	5480	8G	7.4.1c	Healthv	120	36	ALE0442E06K	24 (24)	16	0
Director1	c7001-sw5	3	10.151.16.92	10:00:00:05:33:43:bf:da	5480	8G	7.4.1c	Healthv	119	36	ALE0448F0F5	24 (24)	5	0
Director1	c7001-sw7	4	10.151.16.95	10:00:00:05:33:4a:01:68	5480	8G	7.4.1c	Healthv	119	36	ALE0448F0F7	24 (24)	8	0
Director1	c7002-sw5	7	10.151.16.100	10:00:00:05:33:49:17:bd	5480	8G	7.4.1c	Healthv	119	36	ALE0448F0F4	24 (24)	15	0
Director1	c7002-sw7	8	10.151.16.102	10:00:00:05:33:49:e9:e1	5480	8G	7.4.1c	Healthv	119	36	ALE0448F0ED	24 (24)	18	0
Director1	sansw_bp11	11	10.151.16.131	10:00:00:05:33:c0:f9:00	DCX-8510-4	16G	7.4.1c	Healthv	119	1104	ANN2502H01S	192 (256)	9	0
Director1	sansw_bp13	13	10.151.16.234	10:00:00:27:18:60:29:68	5480	8G	7.4.1c	Healthv	120	36	ALE0408J010	24 (24)	5	14
Director1	sw5-xp24000	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	5100	8G	7.0.1a	Healthv	284	84	ALM0640E02K	40 (40)	33	0
Director2	c7000-sw8	1	10.151.16.73	10:00:00:05:1e:c6:1e:62	5480	8G	7.4.1c	Healthv	118	36	ALE0442E02S	24 (24)	16	0
Director2	c7000-sw6	2	10.151.16.71	10:00:00:05:1e:c6:33:c0	5480	8G	7.4.1c	Healthv	118	36	ALE0442E040	24 (24)	17	0
Director2	c7001-sw6	3	10.151.16.26	10:00:00:05:33:42:00:86	5480	8G	7.4.1c	Healthv	118	36	ALE0448F0ET	24 (24)	5	0
Director2	c7002-sw6	7	10.151.16.101	10:00:00:05:33:49:1f:d0	5480	8G	7.4.1c	Healthv	118	36	ALE0448F0F1	24 (24)	15	0
Director2	c7002-sw8	8	10.151.16.103	10:00:00:05:33:49:1c:a8	5480	8G	7.4.1c	Healthv	118	36	ALE0448F0G7	24 (24)	18	0
Director2	sansw_bp12	12	10.151.16.134	10:00:00:05:33:81:9e:00	DCX-8510-4	16G	7.4.1c	Healthv	118	1104	ANN2528G02S	192 (256)	8	0
Director2	sansw_bp14	14	10.151.16.235	10:00:00:27:18:60:0a:dc	5480	8G	7.4.1c	Healthv	118	36	ALE0408J023	24 (24)	5	14
Director2	c7001-sw8	48	10.151.16.28	10:00:00:05:33:49:1e:14	5480	8G	7.4.1c	Healthv	118	36	ALE0448F0GB	24 (24)	8	0

SUMMARY FOR 17 SWITCHES WITH 760 PORTS (LICENSED PORTS - 732) THAT ARE 70 % UTILIZED																			
Fabric Name	Switch Count						Port Count						Port Use Metrics						
	2G	4G	8G	10G	16G	32G	Total	2G	4G	8G	10G	16G	32G	Total	ISL Ports	Device Ports	Devices	Unused	Utilization
Director1	0	0	8	0	1	0	9	2	84	300	0	0	0	400	22	252	602	126	67 %
Director2	0	0	7	0	1	0	8	2	47	297	0	0	0	360	20	248	597	92	73 %
TOTALS	0	0	15	0	2	0	17	4	131	597	0	0	0	760	42	500	1199	218	70 %

DEVICE COUNT FOR ALL FABRICS 1199 (Including all NPV and Loop Devices)			
Device Description	Count	Device Description	Count
3PAR Data	42	Emulex HBA	110
HP HBA (Qlogic)	23	HP Library	49
HP Virtual Connect	4	IBM Disk	8
IBM TotalStorage DS8000	4	IBM SAN Volume Controller	12
NON-STANDARDS COMPLIANT WWN	7	IBM Ultrium	4
		NPV Host	727
		Qlogic HBA	190

PORT USE																							
Fabric Name	Port Counts		Attached Device Types				Inter Switch Links				Fan Out Ratios		Long Distance Modes										
	Total	rUnused (Unlicd)	Disk	Tape	Host	Appliance	Gateway	ISLs	IFLs	Trnk Mstr	Trnk Slv	Host/Disk	Non-ISL/ISL (Device/ISL)	10km	25km	50km	100k	300k	Auto				
Director1	400	126	14	34	11	495	6	56	22	0	0	1	14.56:1	17	18:1	27	36:1	400	0	0	0	0	0
Director2	360	92	14	35	11	490	6	55	20	0	0	0	14.1	17:1	29.85:1	360	0	0	0	0	0	0	0
TOTALS	760	218	28	69	22	985	12	111	42	0	0	0				760	0	0	0	0	0	0	0

LICENSE SUMMARY										
Fabric Name	License Name	Count	License Name	Count	License Name	Count	License Name	Count	License Name	Count
Director1	8GigFC	8	EnhancedManagement	8	FullFabric	8	No Active Licenses	1		
	POD16	1	POD8	1					POD12	6
Director2	8GigFC	7	EnhancedManagement	7	FullFabric	7	No Active Licenses	1		
									POD12	6

BANDWIDTH UTILIZATION STATISTICS																								
Fabric Name	Device Bandwidth Utilization (per port)					ISL Bandwidth Utilization (per port)					IFL Bandwidth Utilization (per port)													
	Dev#	0 - 25%	26 - 75%	76 - 100%	Avg Peak	ISL	0 - 25%	26 - 75%	76 - 100%	Avg Peak	IFL	0 - 25%	26 - 75%	76 - 100%	Avg Peak									
Director1	602	602	438	0	163	0	1	18.1	2496	22	22	14	0	7	0	1	27.5	855	0	0	0	0	0	0
Director2	597	596	432	1	165	0	0	20.4	1783	20	20	14	0	6	0	0	29.4	788	0	0	0	0	0	0
TOTALS	1199	1198	870	1	328	0	1	19.2		42	42	28	0	13	0	1	28.4		0	0	0	0	0	0

ZONING METRICS														
Fabric Name	Zone Database Use		Aliases Statistics				Zone Statistics				Config Statistics			
	14.7% of 1045274B	766	Avg Mems	Max Mems	Hang Mems	Zones	Avg Mems	Max Mems	Hang Mems	Configs	Avg Mems	Max Mems	Hang Mems	
Director1	14.7% of 1045274B	766	1.01	2	2	266	922	2.72	11	349	1	857	857	259
Director2	14.4% of 1045274B	735	1	2	2	240	914	2.74	11	362	1	841	841	253
TOTALS		1501	1	2	2	506	1836	2.7	11	711	2	849	857	512

Figura 49 Detalle Resumido de la red SAN.

**ALERTS**

[Table Of Contents](#)

UNDESIRABLE FIRMWARE LEVELS IN USE



**Old Firmware Levels**

A non-ideal version of firmware is in use on one or more switches. It is strongly recommended that you migrate to a designated Target Path release.

**Understanding "Target Path"**

Target Path is a set of guidelines for use when trying to determine the ideal firmware version to implement. A target path release is a version of firmware that was created primarily for stability and reliability, and not for the introduction of new features. This version of firmware may contain RAS (Reliability, Availability, and Serviceability) improvements and enhancements, but it typically will not contain any new software features or support for new hardware. The specified code level (or an earlier patch at the same release level) must be deployed in a sufficient number of end-user production environments for a period of at least three months and must have no known critical issues or defect. The Target Path release recommendations should be used in conjunction with advice and guidance from your support provider, as well as any special requirements and needs of your particular environment. Always refer to the Brocade FOS Release Notes documentation and carefully review the "Important Notes and Known Defects" information prior to selecting and installing any version of FOS on a switch.

SWITCHES THAT ARE NOT ON TARGET PATH RELEASES

Fabric Name	Switch Name	Domain	IP Address	World Wide Name	Model	Current OS Ver	Target Path OS Version	FICON in use
Director1	sw5-xp24000	128	10.151.16.247	10:00:00:05:1e:c0:d8:75	5100	7.0.1a	7.2.0d.7.1.0c	

Figura 50 Erres de la red SAN.

FABRIC SUMMARY FOR DIRECTOR1

Table Of Contents

SUMMARY FOR Director1 (9 SWITCHES IN FABRIC)																										
Switch Name	Dom	IP Address	World Wide Name	Model	Spd	OSVer	Status	DevUp	FWr(W)	Mode	Serial Number	Ports(Total ports)	Unused	Unlicnsd												
c7000-sw7	1	10.151.16.70	10.00.00.051e.c6.17.cd	5480	8G	7.4.1c	Health	120	36	Netive	ALE0442E06B	24 (24)	17	0												
c7000-sw5	2	10.151.16.72	10.00.00.051e.c5.42.e4d	5480	8G	7.4.1c	Health	120	36	Netive	ALE0442E06K	24 (24)	16	0												
c7001-sw5	3	10.151.16.92	10.00.00.0533.43.bf.da	5480	8G	7.4.1c	Health	119	36	Netive	ALE0448F0F5	24 (24)	5	0												
c7001-sw7	4	10.151.16.95	10.00.00.0533.4a.01.68	5480	8G	7.4.1c	Health	119	36	Netive	ALE0448F0F7	24 (24)	8	0												
c7002-sw5	7	10.151.16.100	10.00.00.0533.49.f7.bd	5480	8G	7.4.1c	Health	119	36	Netive	ALE0448F0F4	24 (24)	15	0												
c7002-sw7	8	10.151.16.102	10.00.00.0533.49.e9.a1	5480	8G	7.4.1c	Health	119	36	Netive	ALE0448F0ED	24 (24)	18	0												
sansw_bp11	11	10.151.16.131	10.00.00.0533.c0.18.00	DCX-8510-4	16G	7.4.1c	Health	119	1104	Netive	ANN2502H01S	192 (256)	9	0												
sansw_bp13	13	10.151.16.234	10.00.00.27.f8.60.29.68	5480	8G	7.4.1c	Health	120	36	Netive	ALE0408J010	24 (24)	5	14												
sw5-xp24000	128	10.151.16.247	10.00.00.051e.c0.d8.75	5100	8G	7.0.1a	Health	284	84	Netive	ALM0640E02K	40 (40)	33	0												
ATTACHED DEVICE COUNT 602 (Including all NPV and Loop Devices)																										
Device Description	Count	Device Description	Count	Device Description	Count																					
3PAR Data	21	Emulex HBA	58	HP HBA (Ologic)	11																					
HP Library	25	HP Storage (Hitachi)	7	HP Virtual Connect	2																					
IBM Disk	4	IBM SAN Volume Controller	6	IBM TotalStorage DS9000	2																					
IBM Ultrium	2	IBM Ultrium (ADIC)	3	NON-STANDARDS COMPLIANT WWN	2																					
NPV Host	364	Ologic HBA	95																							
PORT USE																										
Switch Name	Port Counts		Attached Device Types		Inter Switch Links			Fan Out Ratios			Port Speeds					Long Distance Modes										
	Total	Unused (Unlck)	Disk	Tap	Host	Applc	GTWY	ISL	TrkMet	TrkSlv	Hst Trq (Dvc)	ISL	2G	4G	8G	16G	32G	1GE	10GE	10km	25km	50km	100k	300k	Auto	
c7000-sw7	24	17	0	0	0	6	0	0	1	0	0	6.0	6.1	0	4	20	0	0	0	0	24	0	0	0	0	0
c7000-sw5	24	16	0	0	0	7	0	1	1	0	0	7.1	8.1	0	4	20	0	0	0	0	24	0	0	0	0	0
c7001-sw5	24	5	0	0	0	15	0	0	4	0	0	15.0	3.75:1	0	1	23	0	0	0	0	24	0	0	0	0	0
c7001-sw7	24	8	0	0	0	15	0	0	1	0	0	15.0	15:1	0	0	24	0	0	0	0	24	0	0	0	0	0
c7002-sw5	24	15	0	0	0	8	0	0	1	0	0	8.0	8:1	0	3	21	0	0	0	0	24	0	0	0	0	0
c7002-sw7	24	18	0	0	0	5	0	0	1	0	0	5.0	5:1	0	3	21	0	0	0	0	24	0	0	0	0	0
sansw_bp11	192	9	0	34	11	429	6	55	11	0	0	4.05:1	48.64:1	2	29	161	0	0	0	0	192	0	0	0	0	0
sansw_bp13	24	5	14	0	0	4	0	0	1	0	0	4.0	4:1	0	0	10	0	0	0	0	24	0	0	0	0	0
sw5-xp24000	40	33	0	0	0	6	0	0	1	0	0	6.0	6:1	0	40	0	0	0	0	0	40	0	0	0	0	0
TOTALS	400	126	14	34	11	495	6	56	22	0	0	2	84	300	0	0	0	0	0	0	400	0	0	0	0	0
SWITCH COMPONENTS																										
Switch Name	Component	Location	Status	Serial Number	Part Number	Uptime	Error Code	Power Used																		
c7000-sw7	WWN Unit	Unit1		ALE0442E06B	40-1000127-10	118days																				
c7000-sw5	WWN Unit	Unit1		ALE0442E06K	40-1000127-10	118days																				
c7001-sw5	WWN Unit	Unit1		ALE0448F0F5	40-1000127-10	118days																				
c7001-sw7	WWN Unit	Unit1		ALE0448F0F7	40-1000127-10	118days																				
c7002-sw5	WWN Unit	Unit1		ALE0448F0F4	40-1000127-10	118days																				
c7002-sw7	WWN Unit	Unit1		ALE0448F0ED	40-1000127-10	118days																				
sansw_bp11	FC8-64	Slot1	ENABLED	BAH0417H01P	60-0000071-12	118days		115																		
sansw_bp11	FC8-64	Slot2	ENABLED	BAH0418H02H	60-0000071-12	118days		115																		
sansw_bp11	CP8 Control Processor Blade	Slot4	ENABLED	AHJ0449G06M	60-1000376-08	118days		40																		
sansw_bp11	CP8 Control Processor Blade	Slot5	ENABLED	AHJ0451G02B	60-1000376-08	118days		40																		
sansw_bp11	CORE BLADE Version 2	Slot3	ENABLED	BOD0444G01P	60-1002055-13	118days																				
sansw_bp11	CORE BLADE Version 2	Slot6	ENABLED	BOD0449G03E	60-1002055-13	118days																				
sansw_bp11	FC8-64	Slot7	ENABLED	BAH0434J00D	60-0000071-13	118days		115																		
sansw_bp11	Power Supply Version 2	PS1	OK	AGC031G7H7	23-0000067-01	42days																				
sansw_bp11	Power Supply Version 2	PS2	OK	AGC031G7GG	23-0000067-01	43days																				
sansw_bp11	Fan Version 2	Fan1	OK	AGB2551G0D2	60-1000384-12	118days																				
sansw_bp11	Fan Version 2	Fan2	OK	AGB1911F023	60-1000384-12	118days																				
sansw_bp11	WWN Unit	Unit1		ANN2502H01S	60-1000888-05	118days																				
sansw_bp11	WWN Unit	Unit2		ANQ0448G0G4	60-1000888-05	118days																				
sansw_bp13	WWN Unit	Unit1		ALE0408J010	40-1000127-13	118days																				
sw5-xp24000	Fan	Fan1	OK			281days																				
sw5-xp24000	Fan	Fan2	OK			281days																				
sw5-xp24000	Power Supply	PS1	OK			43days																				
sw5-xp24000	Power Supply	PS2	OK			42days																				
sw5-xp24000	WWN Unit	Unit1		ALM0640E02K	40-1000133-12	281days																				
LICENSE SUMMARY																										
Switch Name	License Name	License Key	License Name	License Key	License Name	License Key																				
c7000-sw7	POD12	RdSPbR99d9SuXSd0	FullFabric	QMtPaYzTr7M73gTS14agGKGoG	EnhancedManagement	QMtPaYzTr7M73gTS14agGKGoG																				
c7000-sw5	8GioFC	GMiPaYzTr7M73gTS14agGKGoG	FullFabric	NrnL3tY44fQ13RAMSKBJBEWt	EnhancedManagement	NrnL3tY44fQ13RAMSKBJBEWt																				
c7001-sw5	8GioFC	NrnL3tY44fQ13RAMSKBJBEWt	POD12	zb9PRdPRRe0sESSk	EnhancedManagement	74XMLXaQEXOARBaMdmSWHt																				
c7001-sw7	8GioFC	3GMFRCTYLPWJ07gGJEEZY2	POD12	SdcReRcbSbTuhStE	EnhancedManagement	JS7FTRZKwrmDZHKPHA4X723X																				
c7002-sw5	8GioFC	byO9h0cSOsczRacT	POD12	SdbedyycbTufce0	EnhancedManagement	A3Gts3GEZLYG94EQMJNWNQ																				
c7002-sw7	8GioFC	3ONZBGtTKg7x4XfagmKDRaF	POD12	RebdddSvdsRSvqeeD	EnhancedManagement	q4HKEFDJSAXYJEWLaT7DP3tE																				
sansw_bp11	No Active Licenses																									
sansw_bp13	FullFabric	bcSzdydRccdt0E0	EnhancedManagement	WREGa3P9EAHCtHmPRLKwaf	8GioFC	NagHFxa7NBWtH39WDZDBWtH																				
sw5-xp24000	FullFabric	bey9PR99cQctzASO	POD8	Sd0eb9bSRRTuVtch	POD16	Sd0eb9bSRRTuVtch																				
	EnhancedManagement	W7e4ft379YJTt9EaWraEaNCMA	8GioFC	CJfENSMEAN3ASH0mtGY174E																						

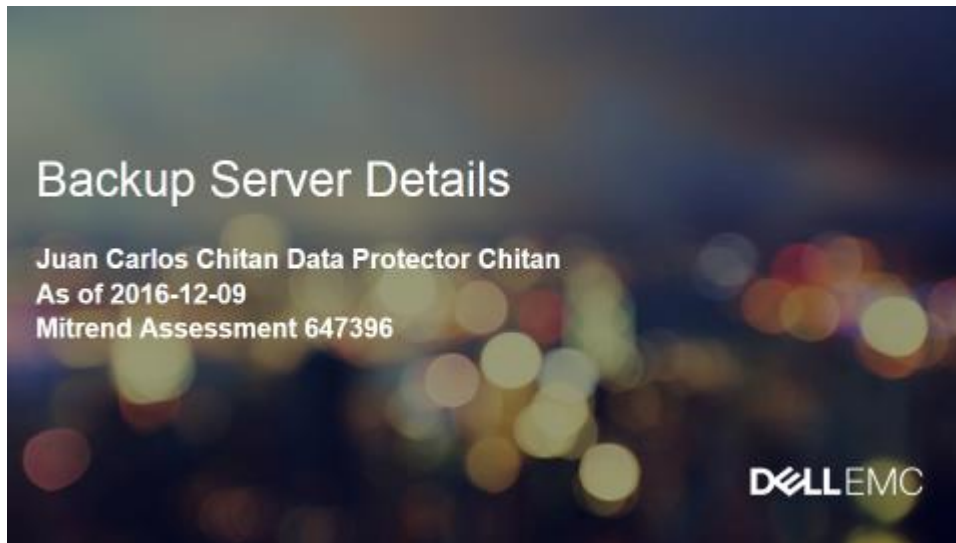
Figura 51 Resumen de la configuración del Director 1

FABRIC SUMMARY FOR DIRECTOR2

SUMMARY FOR Director2 (8 SWITCHES IN FABRIC)																										
Switch Name	Dom	IP Address	World Wide Name	Model	Spd	OSVer	Status	DaysUp	Prv(W)	Mode	Serial Number	Ports(Total parts)	Unused	Unlicnsd												
c7000-sw8	1	10.151.16.73	10.00.00.05.1e.c6.1e.62	5480	8G	7.4.1c	Health	118	36	Netive	ALE0442E02S	24 (24)	16	0												
c7000-sw6	2	10.151.16.71	10.00.00.05.1e.c6.33.c0	5480	8G	7.4.1c	Health	118	36	Netive	ALE0442E040	24 (24)	17	0												
c7001-sw6	3	10.151.16.26	10.00.00.05.33.42.00.86	5480	8G	7.4.1c	Health	118	36	Netive	ALE0448F0ET	24 (24)	5	0												
c7002-sw6	7	10.151.16.101	10.00.00.05.33.49.1f.a0	5480	8G	7.4.1c	Health	118	36	Netive	ALE0448F0F1	24 (24)	15	0												
c7002-sw6	8	10.151.16.103	10.00.00.05.33.49.1f.c8	5480	8G	7.4.1c	Health	118	36	Netive	ALE0448F0G7	24 (24)	18	0												
sansw_bp12	12	10.151.16.134	10.00.00.05.33.81.9e.00	DCX-8510-4	16G	7.4.1c	Health	118	1104	Netive	ANN2528G02S	192 (256)	8	0												
sansw_bp14	14	10.151.16.235	10.00.00.27.18.60.0a.cd	5480	8G	7.4.1c	Health	118	36	Netive	ALE0408J023	24 (24)	5	14												
c7001-sw8	48	10.151.16.28	10.00.00.05.33.49.1a.14	5480	8G	7.4.1c	Health	118	36	Netive	ALE0448F0GB	24 (24)	8	0												
ATTACHED DEVICE COUNT597 (Including all NPV and Loop Devices)																										
Device Description	Count	Device Description	Count	Device Description	Count																					
3PAR Data	21	Emulex HBA	52	Emulex HBA (HP-UX)	1																					
HP HBA (Glogic)	12	HP Library	24	HP Storage (Hitachi)	5																					
HP Virtual Connect	2	IBM Disk	4	IBM SAN Volume Controller	6																					
IBM TotalStorage DS8000	2	IBM Ultrium	2	IBM Ultrium (ADIC)	3																					
NON-STANDARDS COMPLIANT WWN	5	NPV Host	363	Glogic HBA	95																					
PORT USE																										
Switch Name	Total	Unusd (Unlicd)	Disk	Tape	Host	Applc	Gateway	Inter Switch Links	ISL TrkMst	TrkSlv	Fan Out Ratios	ISL Trk Trq (Dvc)ISL	2G	4G	8G	16G	32G	1GE	10GE	10km	25km	50km	100k	300k	Auto	
c7000-sw8	24	16	0	0	0	7	0	0	1	0	0	7.0	7.1	0	4	20	0	0	0	0	24	0	0	0	0	0
c7000-sw6	24	17	0	0	0	6	0	0	1	0	0	6.1	7.1	0	4	20	0	0	0	0	24	0	0	0	0	0
c7001-sw6	24	5	0	0	0	15	0	0	4	0	0	15.0	3.75	1	23	0	0	0	0	0	24	0	0	0	0	0
c7002-sw6	24	15	0	0	0	8	0	0	1	0	0	8.0	8.1	0	3	21	0	0	0	0	24	0	0	0	0	0
c7002-sw8	24	18	0	0	0	5	0	0	1	0	0	5.0	5.1	0	3	21	0	0	0	0	24	0	0	0	0	0
sansw_bp12	192	8	0	35	11	430	6	54	10	0	0	4.06	153.6	2	32	158	0	0	0	0	192	0	0	0	0	0
sansw_bp14	24	5	14	0	0	4	0	0	1	0	0	4.0	4.1	0	0	10	0	0	0	0	24	0	0	0	0	0
c7001-sw8	24	8	0	0	0	15	0	0	1	0	0	15.0	15.1	0	0	24	0	0	0	0	24	0	0	0	0	0
TOTALS	360	92	14	35	11	490	6	55	20	0	0	2	47	297	0	0	0	0	0	0	360	0	0	0	0	0
SWITCH COMPONENTS																										
Switch Name	Component	Location	Status	Serial Number	Part Number	Uptime	Error Code	Power Used																		
c7000-sw8	WWN Unit	Unit 1		ALE0442E02S	40-1000127-10	117days																				
c7000-sw6	WWN Unit	Unit 1		ALE0442E040	40-1000127-10	117days																				
c7001-sw6	WWN Unit	Unit 1		ALE0448F0ET	40-1000127-10	117days																				
c7002-sw6	WWN Unit	Unit 1		ALE0448F0F1	40-1000127-10	117days																				
c7002-sw8	WWN Unit	Unit 1		ALE0448F0G7	40-1000127-10	117days																				
sansw_bp12	FC8-64	Slot 1	ENABLED	BAH0417H029	60-0000071-12	117days		115																		
sansw_bp12	FC8-64	Slot 2	ENABLED	BAH0425F00H	60-0000071-12	117days		115																		
sansw_bp12	CP9 Control Processor Blade	Slot 4	ENABLED	AHJ0419G08D	60-1000376-08	117days		40																		
sansw_bp12	CP9 Control Processor Blade	Slot 5	ENABLED	AHJ0421G0F1	60-1000376-08	117days		40																		
sansw_bp12	CORE BLADE Version 2	Slot 3	ENABLED	B0D0422G021	60-1002055-13	117days																				
sansw_bp12	CORE BLADE Version 2	Slot 6	ENABLED	B0D0421G002	60-1002055-13	117days																				
sansw_bp12	FC8-64	Slot 7	ENABLED	BAH0434J00W	60-0000071-13	117days		115																		
sansw_bp12	Power Supply Version 2	PS 1	OK	AGC2M07G3E7	23-0000067-01	43days																				
sansw_bp12	Power Supply Version 2	PS 2	OK	AGC2M07G3E6	23-0000067-01	42days																				
sansw_bp12	Fan Version 2	Fan 1	Ok	AGB2548G03V	60-1000384-12	117days																				
sansw_bp12	Fan Version 2	Fan 2	Ok	AGB2539K00J	60-1000384-12	117days																				
sansw_bp12	WWN Unit	Unit 1		ANN2528G02S	60-1000888-05	117days																				
sansw_bp12	WWN Unit	Unit 2		ANN0419G02A	60-1000888-05	117days																				
sansw_bp14	WWN Unit	Unit 1		ALE0408J023	40-1000127-13	117days																				
c7001-sw8	WWN Unit	Unit 1		ALE0448F0GB	40-1000127-10	117days																				
LICENSE SUMMARY																										
Switch Name	License Name	License Key	License Name	License Key	License Name	License Key																				
c7000-sw8	POD12	S9dORSyec9TOiR5O	FullFabric	JG7W9QLmfIERC4SGKGSGCP	EnhancedManagement	JG7W9QLmfIERC4SGKGSGCPV																				
c7000-sw6	8GigFC	JG7W9QLmfIERC4SGKGSGCP	FullFabric	aQZq7PYFaEBmCE7YMHaYYP0	EnhancedManagement	aQZq7PYFaEBmCE7YMHaYYP0																				
c7001-sw6	8GigFC	aQZq7PYFaEBmCE7YMHaYYP0	POD12	bScQcSSbdSghPdN	EnhancedManagement	BYTaNJHrWGXE793YPRtYCY4																				
c7002-sw6	8GigFC	fZCKAK4rTRMYPJ4HPRZWWF2	POD12	RdQzyceSdbSvU0zD	EnhancedManagement	S4RjYDYBFHGKSRBBBQNPXKJ																				
c7002-sw8	8GigFC	fRiDADAJbaP7R3BPiPAyKTi7N	POD12	zySzSdFyb0FX0Ti	EnhancedManagement	QHRRJIB4qQRHq7PmQJ9tm3rKz																				
sansw_bp12	No Active Licenses																									
sansw_bp14	FullFabric	RSR99eSeOdStSAa6	EnhancedManagement	tAIR4LPae4Y4MmeBMM3F3CC	8GigFC	TF40MHMwWXGD7TYRPFCSGb																				
c7001-sw8	FullFabric	bPdyCQecSScSec9d9	POD12	R3tce9e9bS04dfY	EnhancedManagement	i9BPJrK54JEMBLDQEA9Ftmf																				
c7001-sw8	8GigFC	EXNTAHWNtPaG7gHKNPDKJ3																								
ISL / TRUNK SUMMARY																										
From Switch	Dom	Area	Slot/Port	To Switch	Dom	Area	Slot/Port	ISL or Trunk Type	FSFP	Farthest Pnt (Hops)	Dynamic or Static	Speed	BW (Average)	Available Bandwidth	Utilization (Peak)	[% Use (Peak)										
c7000-sw8	1	17	17	sansw_bp12	12	122	2/56	Normal ISL	500	2	D	8 Gbps	8	135.3 MB/s	9%	787.5 MB/s	43%									
c7000-sw6	2	17	17	sansw_bp12	12	123	2/59	Normal ISL	500	2	D	8 Gbps	8	110.4 MB/s	7%	756 MB/s	47%									
c7001-sw6	3	17	17	sansw_bp12	12	20	1/20	Normal ISL	500	2	D	8 Gbps	8	84.8 MB/s	5%	290.6 MB/s	18%									
c7001-sw6	3	18	18	sansw_bp12	12	80	2/16	Normal ISL	500	2	D	8 Gbps	8	84.3 MB/s	5%	289.4 MB/s	18%									
c7001-sw6	3	19	19	sansw_bp12	12	49	1/49	Normal ISL	500	2	D	8 Gbps	8	85 MB/s	5%	288 MB/s	18%									
c7001-sw6	3	20	20	sansw_bp12	12	50	1/50	Normal ISL	500	2	D	8 Gbps	8	84.6 MB/s	5%	298.9 MB/s	19%									
c7002-sw6	7	17	17	sansw_bp12	12	1	1/1	Normal ISL	500	2	D	8 Gbps	8	123.2 MB/s	8%	572.1 MB/s	36%									
c7002-sw8	8	17	17	sansw_bp12	12	65	2/1	Normal ISL	500	2	D	8 Gbps	8	16.6 MB/s	1%	136.9 MB/s	9%									
sansw_bp14	14	42	1/42	sansw_bp14	14	17	1/17	Normal ISL	500	1	D	8 Gbps	8	5.4 MB/s	0%	58.5 MB/s	4%									
sansw_bp12	12	188	7/80	c7001-sw8	48	17	1/17	Normal ISL	500	1	D	8 Gbps	8	37.9 MB/s	2%	254.1 MB/s	16%									
BANDWIDTH UTILIZATION STATISTICS																										
Switch Name	All Active Ports	% BW used	All ISL Ports	% BW used	All Host Ports	% BW used	All Target Ports	% BW used																		
c7000-sw8	8	33.8	788	3	5	0	1	135.3																		
c7000-sw6	8	27.7	756	4	4	0	1	110.4																		
c7001-sw6	19	35.7	878	15	4	0	4	84.7																		
c7002-sw6	9	27.4	572	6	3	0	1	123.2																		
c7002-sw8	6	5.5	137	6	0	0	1	16.8																		
sansw_bp12	546	29.6	1200	391	155	0	10	77.8																		
sansw_bp14	5	2.4	63	5	0	0	1	6.1																		
c7001-sw8	16	4.3	230	16	0	0	1	34																		
TOTALS	617	20.8	446	171	0	0	20	73.5																		

Figura 52 Resumen de la configuración del Director 2.

# Análisis de la red SAN por DELLEMC Data Protector.



## Backup Scan Summary

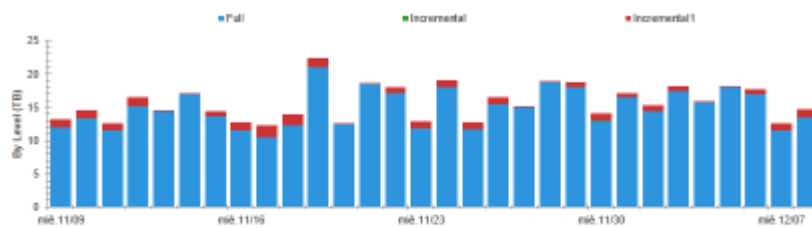
Start and End Date is the period of collected data. Report Start and End Date is the period of time analyzed in this report.

Server	Start Date	End Date	Report Start	Report End
edp9hcb2.uso.bpichircha.com	2016-11-07 20:00	2016-12-09 19:00	2016-11-09	2016-12-09

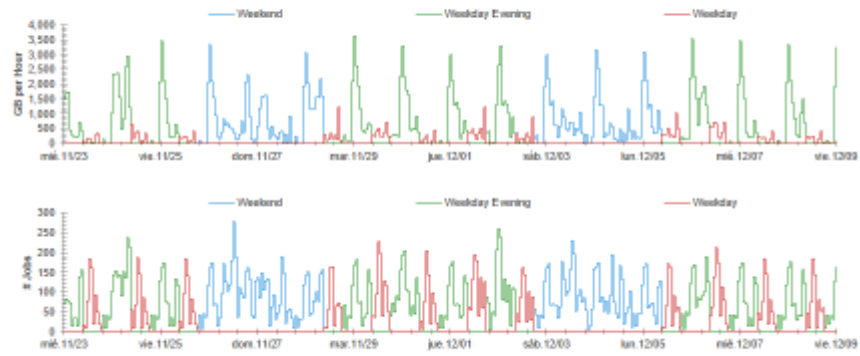
## Servers

Full backups typically have large amounts of duplicate data; great fit for deduplication.

Server	Software	Version	# Clients w/ Images	Backed Up (TB)	Last Backup
edp9hcb2.uso.bpichircha.com	Data Protector		20	470.01	2016-12-09



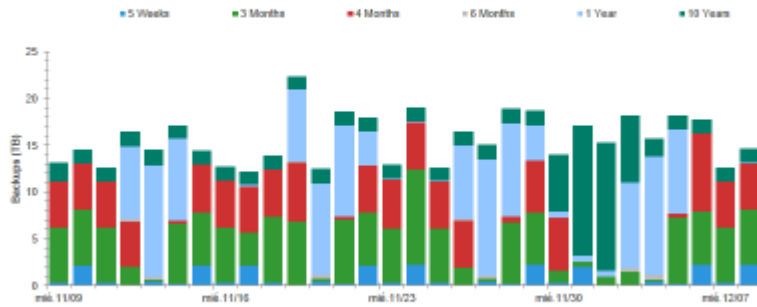
## Daily Window



© Copyright 2016 Dell EMC

Dell EMC

## Backup Data Retention

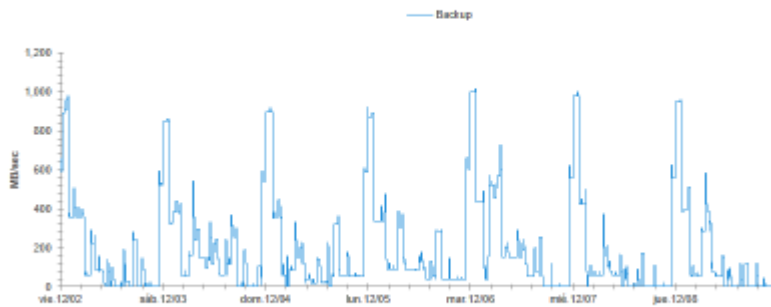


© Copyright 2016 Dell EMC

Dell EMC

## Activities

Overlap between backups and other activities, such as reclamations and migrations, often indicates insufficient tape drives.



© Copyright 2016 Dell EMC

Dell EMC

## Backup Job Summary

Long backups are a sign of unhealthy and overloaded backup servers

Server	ectbphb2.uio.tpicincha.com
Clients	28
# Jobs	37,992
# Clients > 8 Hours	6
# Clients > 12 Hours	5
# Clients > 24 Hours	3
Backed Up (TB)	479.61
# Files	124,647,868

## Recommended Assessments

- [Data Domain](#): Utilization trends, performance and client data change rates
- [VMware](#): VM to Backup Relationships
- [Oracle RMAN](#): Directly measure client size, backup duration, and change rates
- [SAN Health](#): Understand how the SAN impacts backups

# Protected Data

DELL EMC

## Top Client - Sizing Summary

Host	Operating System	Policy Type	# Policies	Single Peak Daily (GB)	Peak Daily by Policy Type (GB)	Peak Daily Maxima plus Peak by Policy Stream
precphcd0.us.tpchincha.com	ibm m6600 aix-7.1	FileSystem, Oracle8	17	10,085	10,779	4,703
eculo197602.us.tpchincha.com	microsoft amd64 vHNT-6.8-S	WinFS	1	3,769	3,769	3,769
ecbphcd02.us.tpchincha.com	hp ia64 hp-ux-11.31	FileSystem	8	1,311	1,311	2,197
ecbphcp2.us.tpchincha.com	hp s800 hp-ux-11.11	FileSystem, Oracle8	21	10,317	10,856	2,068
ecbphcp1.bgr.com	hp ia64 hp-ux-11.31	FileSystem	2	2,064	2,064	1,337
ecbphcp1.bgr.com	hp s800 hp-ux-11.11	FileSystem	4	1,530	1,530	1,182
ecbphcpa.us.tpchincha.com	hp s800 hp-ux-11.11	FileSystem, Oracle8	11	2,332	2,334	554
eculo197601.us.tpchincha.com	microsoft i386 vHNT-5.0-S	WinFS	1	476	476	476
ecbphcop.us.tpchincha.com	hp ia64 hp-ux-11.31	FileSystem, Oracle8	15	248	249	297
ecbphq1	ggl x86_64 linux-2.6.18-164.el5	FileSystem	2	570	578	268
ecbphcp.us.tpchincha.com	hp ia64 hp-ux-11.31	FileSystem, Oracle8	11	152	203	197
ecbphcb2.us.tpchincha.com	hp ia64 hp-ux-11.31	FileSystem, IDB	2	462	463	183
ecbphcb2.us.tpchincha.com	hp s800 hp-ux-11.11	FileSystem	3	896	896	147
ecbphcm.us.tpchincha.com	hp ia64 hp-ux-11.31	FileSystem	3	110	110	136
ecbphsm1.us.tpchincha.com	ggl x86_64 linux-2.6.32-594.el6.x86_64	FileSystem	2	104	104	95

10 © Copyright 2016 Dell EMC

DELL EMC

## Policy Types Peak Summary

Server	Operating System	Policy Type	# Clients	Peak Daily (GB)
ecbphcb2.us.tpchincha.com	ggl x86_64 linux-2.6.18-164.el5	FileSystem	1	570
ecbphcb2.us.tpchincha.com	ggl x86_64 linux-2.6.32-594.el6.x86_64	FileSystem	4	166
ecbphcb2.us.tpchincha.com	ggl x86_64 linux-2.6.32-594.el6.x86_64	Oracle8	2	129
ecbphcb2.us.tpchincha.com	ggl x86_64 linux-2.6.32-573.7.1.el6.x86_64	FileSystem	2	35
ecbphcb2.us.tpchincha.com	ggl x86_64 linux-2.6.32-573.7.1.el6.x86_64	Oracle8	1	22
ecbphcb2.us.tpchincha.com	hp ia64 hp-ux-11.31	FileSystem	8	4,092
ecbphcb2.us.tpchincha.com	hp ia64 hp-ux-11.31	IDB	1	154
ecbphcb2.us.tpchincha.com	hp ia64 hp-ux-11.31	Oracle8	2	175
ecbphcb2.us.tpchincha.com	hp s800 hp-ux-11.11	FileSystem	5	3,022
ecbphcb2.us.tpchincha.com	hp s800 hp-ux-11.11	Oracle8	2	11,723
ecbphcb2.us.tpchincha.com	ibm m6600 aix-7.1	FileSystem	1	695
ecbphcb2.us.tpchincha.com	ibm m6600 aix-7.1	Oracle8	1	10,085
ecbphcb2.us.tpchincha.com	microsoft amd64 vHNT-6.8-S	WinFS	1	3,769
ecbphcb2.us.tpchincha.com	microsoft i386 vHNT-5.0-S	WinFS	1	476
ecbphcb2.us.tpchincha.com	microsoft i386 vHNT-5.2-S	WinFS	4	89
ecbphcb2.us.tpchincha.com	sun sparc solaris-5.10	Oracle8	1	92
				36,193

11 © Copyright 2016 Dell EMC

DELL EMC

## NetWorker Capacity Licensing Metrics - Type

All sizes are after any client-side compression, including RMAN compression.

Operating System	Policy Type	Peak Daily - App (GB)	Peak Daily - Unique or Manual Filesystem (GB)	Total Largest Fulls - Filesystems (GB)	Capacity Estimate (GB)
ggl x86_64 linux-2.6.18-164.el5	FileSystem	0	0	570	570
ggl x86_64 linux-2.6.32-584.el5 x86_64	FileSystem	0	0	166	166
ggl x86_64 linux-2.6.32-584.el5 x86_64	Oracle8	129	0	0	129
ggl x86_64 linux-2.6.32-573.7.1.el5 x86_64	FileSystem	0	0	35	35
ggl x86_64 linux-2.6.32-573.7.1.el5 x86_64	Oracle8	22	0	0	22
hp ia64 hp-ux-11.31	FileSystem	0	0	5,651	5,651
hp ia64 hp-ux-11.31	IDB	154	0	0	154
hp ia64 hp-ux-11.31	Oracle8	191	0	0	191
hp s800 hp-ux-11.11	FileSystem	0	0	3,845	3,845
hp s800 hp-ux-11.11	Oracle8	11,723	0	0	11,723
ibm rs6000 aix-7.1	FileSystem	0	0	695	695
ibm rs6000 aix-7.1	Oracle8	10,065	0	0	10,065
microsoft amd64 win7-6.0-5	WinFS	0	0	3,789	3,789
microsoft i386 win7-5.0-5	WinFS	0	0	476	476
microsoft i386 win7-5.2-5	WinFS	0	0	89	89
sun sparc solaris-5.10	Oracle8	92	0	0	92

12 © Copyright 2016 Dell EMC

Dell EMC

## NetWorker Capacity Licensing Metrics - Type (Cont.)

Operating System	Policy Type	Peak Daily - App (GB)	Peak Daily - Unique or Manual Filesystem (GB)	Total Largest Fulls - Filesystems (GB)	Capacity Estimate (GB)
		22,395	0	15,296	37,691

13 © Copyright 2016 Dell EMC

Dell EMC

## NetWorker Capacity Metrics

Server	Version	Total Largest Fulls - Filesystems (GB)	Peak Daily - App (GB)	Peak Daily - Unique or Manual Filesystem (GB)	Capacity Estimate (GB)
ectp062.uko.bpichircha.com		15,296.17	22,395.16	0.00	37,691.33

14 © Copyright 2016 Dell EMC

Dell EMC

## Database Directory Backups (estimated)

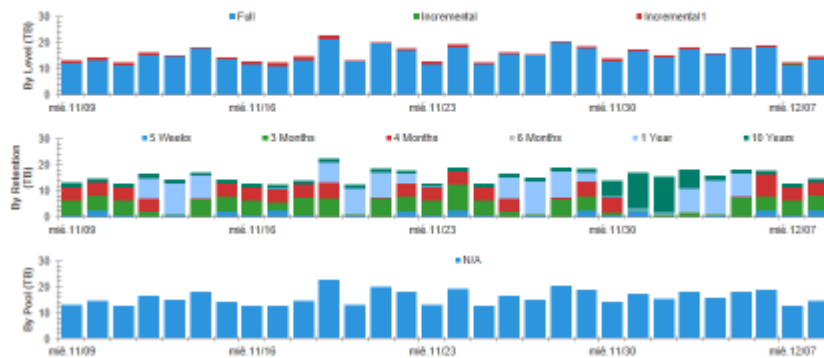
List UNIX filesystems that are named with common database directory names, such as /ora1 or /dbdata1.

Category	# Job Names	# Hosts
DELETED	2	4
Oracle	38	5
	40	9

# Capacity

## Daily Capacity by Type Backup

Use fewer pools to improve drive and tape utilization, and to simplify media management.



# Long Term Retention

D&L EMC

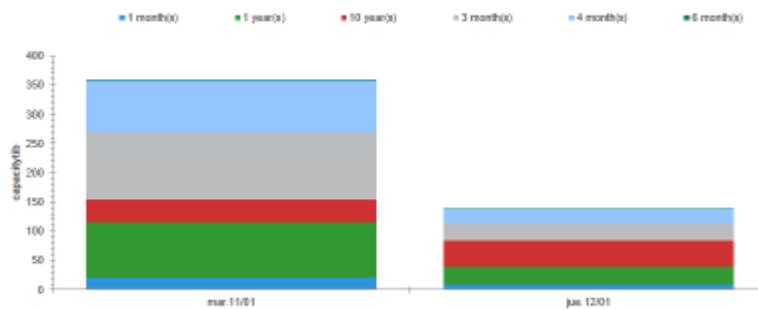
## Long Term Retention Summary

Server	# Policies	Retention (Months)	# Clients	Capacity (TiB)	Past Month (TiB)
ec2pfc2.uso.bpichircha.com	26	3 month(s)	14	144	135,700
ec2pfc2.uso.bpichircha.com	5	4 month(s)	3	113	165,094
ec2pfc2.uso.bpichircha.com	3	6 month(s)	9	3	2,772
ec2pfc2.uso.bpichircha.com	30	1 year(s)	24	127	129,661
ec2pfc2.uso.bpichircha.com	25	10 year(s)	9	64	83,027

19 © Copyright 2016 Dell EMC

D&L EMC

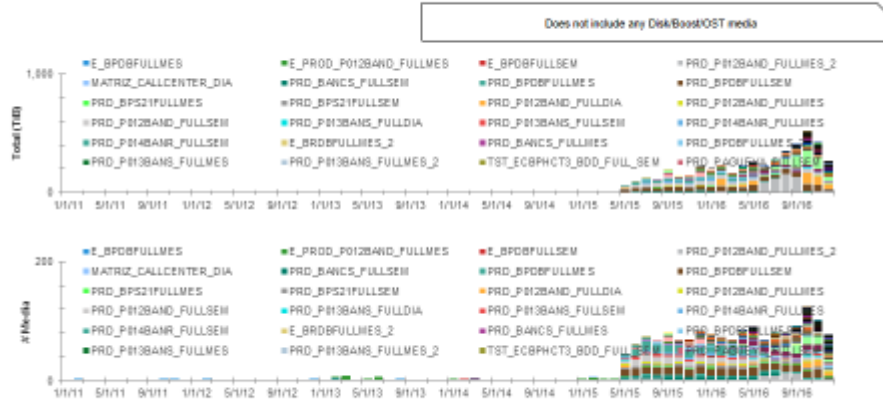
## Monthly Data Protection



21 © Copyright 2016 Dell EMC

D&L EMC

# Media Consumption by Month



## Media Pool Summary

Under-utilized 'Full' Media may indicate compression or media write errors.

Server	Pool	Type	# Media	# Full	Written (TB)	Avg Full Media Util (GB)
ecp9hc2.usa.bplchircha.com	EXPIRADAS	LTO-Ultium	54		72	
ecp9hc2.usa.bplchircha.com	E_SPD8FULLMES	LTO-Ultium	34		1	
ecp9hc2.usa.bplchircha.com	E_SPD8FULLSEM	LTO-Ultium	5		8	
ecp9hc2.usa.bplchircha.com	E_SPD8FULLMES_2	LTO-Ultium	7		2	
ecp9hc2.usa.bplchircha.com	E_PROD_P9125AND_FULLMES	LTO-Ultium	45		8	
ecp9hc2.usa.bplchircha.com	MATRIZ_CALLCENTER_DIA	LTO-Ultium	1		1	
ecp9hc2.usa.bplchircha.com	MATRIZ_HOMEFOLDER_MES	LTO-Ultium	81		189	
ecp9hc2.usa.bplchircha.com	MATRIZ_PROD_IVR	LTO-Ultium	3		8	
ecp9hc2.usa.bplchircha.com	PROD_BANCOS_FULLMES	LTO-Ultium	58		24	
ecp9hc2.usa.bplchircha.com	PROD_BANCOS_FULLSEM	LTO-Ultium	57		35	
ecp9hc2.usa.bplchircha.com	PROD_BANCOS_FULL_MIG_ANTES	LTO-Ultium	2		2	
ecp9hc2.usa.bplchircha.com	PROD_BDCONTROLM_DIA	LTO-Ultium	2		8	
ecp9hc2.usa.bplchircha.com	PROD_BDCONTROLM_MES	LTO-Ultium	2		9	
ecp9hc2.usa.bplchircha.com	PROD_BDCONTROLM_SEM	LTO-Ultium	1		6	
ecp9hc2.usa.bplchircha.com	PROD_BDOVO_FULLDIA	LTO-Ultium	4		25	
ecp9hc2.usa.bplchircha.com	PROD_BDOVO_FULLMES	LTO-Ultium	3		13	
ecp9hc2.usa.bplchircha.com	PROD_BDOVO_FULLSEM	LTO-Ultium	2		18	

## Media Pool Summary (Cont.)

Server	Pool	Type	# Media	# Full	Written (TB)	Avg Full Media Util (GB)
ecp9hc2.usa.bplchircha.com	PROD_BP8PMFULLDIA	LTO-Ultium	4		24	
ecp9hc2.usa.bplchircha.com	PROD_BP8PMFULLMES	LTO-Ultium	2		9	
ecp9hc2.usa.bplchircha.com	PROD_BP8PMFULLSEM	LTO-Ultium	3		19	
ecp9hc2.usa.bplchircha.com	PROD_BP8PFULLDIA	LTO-Ultium	61		432	
ecp9hc2.usa.bplchircha.com	PROD_BP8PFULLMES	LTO-Ultium	59		86	
ecp9hc2.usa.bplchircha.com	PROD_BP8PFULLMES_2	LTO-Ultium	58		162	
ecp9hc2.usa.bplchircha.com	PROD_BP8PFULLSEM	LTO-Ultium	240		664	
ecp9hc2.usa.bplchircha.com	PROD_BP8PFULLSEM_8	LTO-Ultium	5		5	
ecp9hc2.usa.bplchircha.com	PROD_BP8PFULLDIA	LTO-Ultium	13		42	
ecp9hc2.usa.bplchircha.com	PROD_BP8VFD_FULLDIA	LTO-Ultium	2		12	
ecp9hc2.usa.bplchircha.com	PROD_BP8VFD_FULLMES	LTO-Ultium	1		4	
ecp9hc2.usa.bplchircha.com	PROD_BP8VFD_FULLSEM	LTO-Ultium	1		6	
ecp9hc2.usa.bplchircha.com	PROD_BP8S21FULLDIA	LTO-Ultium	4		57	
ecp9hc2.usa.bplchircha.com	PROD_BP8S21FULLMES	LTO-Ultium	20		26	
ecp9hc2.usa.bplchircha.com	PROD_BP8S21FULLSEM	LTO-Ultium	77		49	
ecp9hc2.usa.bplchircha.com	PROD_BP8S1FULLDIA	LTO-Ultium	3		39	
ecp9hc2.usa.bplchircha.com	PROD_BP8S1FULLSEM	LTO-Ultium	4		21	

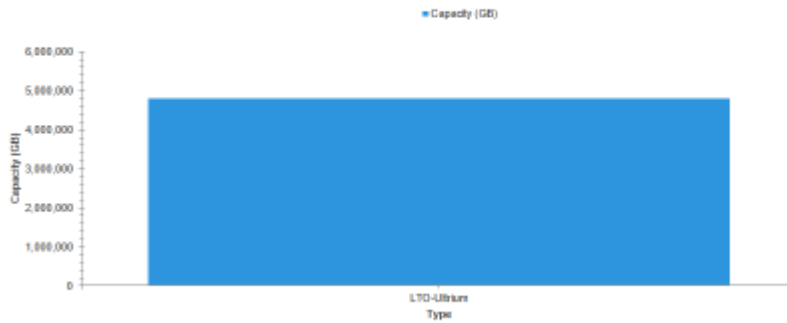
## Media Pool Summary (Cont.)

Server	Pool	Type	# Media	# Full	Written (TB)	Avg Full Media Util (GB)
ecp9hc2.uis.bpichircha.com	PRD_P613BAHS_FULLMES	LTO-Ultrium	15		1	
ecp9hc2.uis.bpichircha.com	PRD_P613BAHS_FULLMES_2	LTO-Ultrium	20		3	
ecp9hc2.uis.bpichircha.com	PRD_P613BAHS_FULLSEM	LTO-Ultrium	58		5	
ecp9hc2.uis.bpichircha.com	PRD_P613BAHS_MIGANTES	LTO-Ultrium	1		0	
ecp9hc2.uis.bpichircha.com	PRD_P614BAHR_FULLDIA	LTO-Ultrium	3		12	
ecp9hc2.uis.bpichircha.com	PRD_P614BAHR_FULLMES	LTO-Ultrium	39		186	
ecp9hc2.uis.bpichircha.com	PRD_P614BAHR_FULLSEM	LTO-Ultrium	141		187	
ecp9hc2.uis.bpichircha.com	PRD_P614BAHR_MIGANTES	LTO-Ultrium	2		4	
ecp9hc2.uis.bpichircha.com	PRD_P616BAHR_MIGANTES	LTO-Ultrium	1		4	
ecp9hc2.uis.bpichircha.com	PRD_P6GUEYA_FULLDIA	LTO-Ultrium	3		3	
ecp9hc2.uis.bpichircha.com	PRD_P6GUEYA_FULLSEM	LTO-Ultrium	12		22	
ecp9hc2.uis.bpichircha.com	TST_4048_BS_JgalaServer	LTO-Ultrium	2		1	
ecp9hc2.uis.bpichircha.com	TST_4048_DESA_BRDBFULLSEM	LTO-Ultrium	15		44	
ecp9hc2.uis.bpichircha.com	TST_4048_DESA_BRDBFULLSEM	LTO-Ultrium	2		1	
ecp9hc2.uis.bpichircha.com	TST_4048_EC8PHC02_FULLDIA	LTO-Ultrium	1		2	
ecp9hc2.uis.bpichircha.com	TST_4048_EC8PHC02_FULLSEM	LTO-Ultrium	2		5	
ecp9hc2.uis.bpichircha.com	TST_4048_EC8PHC01_FULLDIA	LTO-Ultrium	1		1	

© Copyright 2016 Dell EMC

Dell EMC

## Media Capacity By Type



© Copyright 2016 Dell EMC

Dell EMC

## Drive Allocation Summary (Cont.)

Media Server	"MSL3420_2D_LTO6" LTO-Ultrium # Drive IDs	"MSL4040_2D_LTO4" LTO-Ultrium # Drive IDs	"MSL6480_16D_LTO6" LTO-Ultrium # Drive IDs	"MSL6480_4D_LTO4" LTO-Ultrium # Drive IDs	"MSL6696_4D_LTO4" LTO-Ultrium # Drive IDs
cam			2		
cam			8	1	

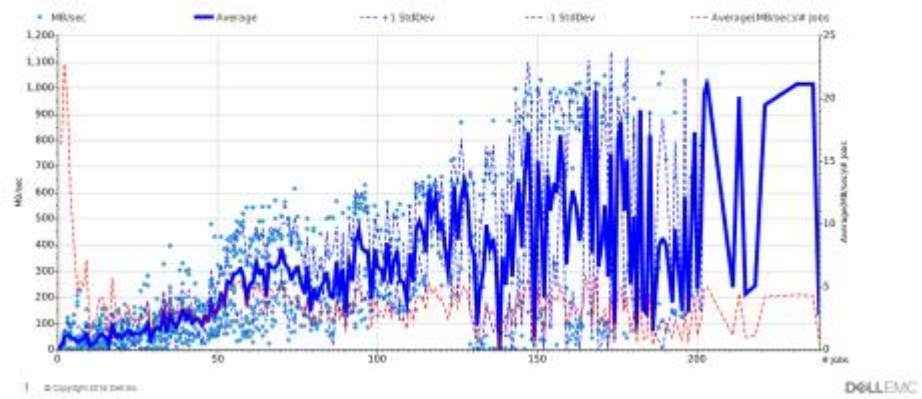
© Copyright 2016 Dell EMC

Dell EMC

# Performance

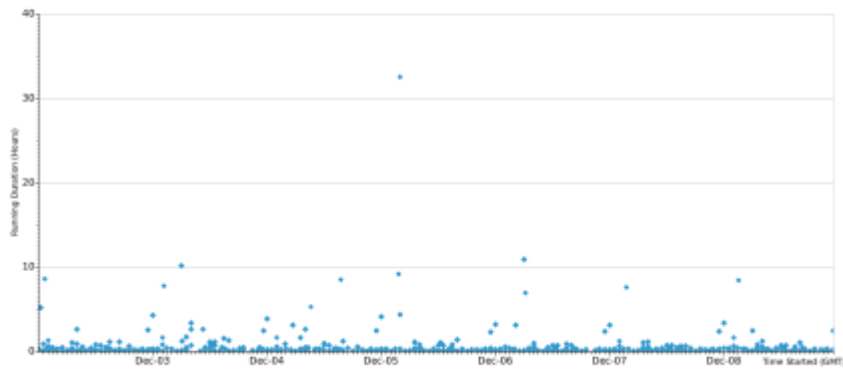
D&L EMC

## Backup Throughput



## Job Duration by Day

Long backups occur nearly every day, not just on weekends.

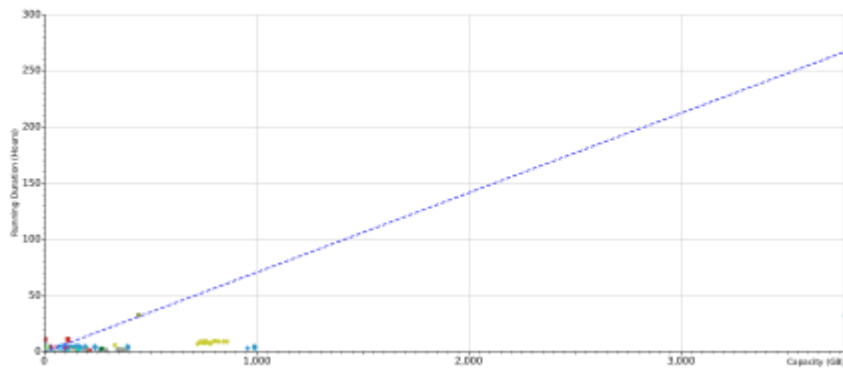


© Copyright 2016 Dell EMC

Dell EMC

## Job Capacity vs Duration

Long + small backups (top left), and large + fast backups (bottom right).

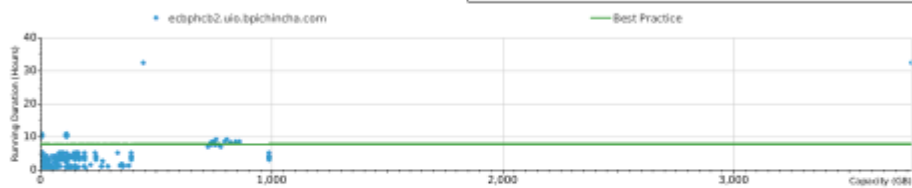


© Copyright 2016 Dell EMC

Dell EMC

## Job Performance

Each point is a single backup.  
Note long + small backups (top left), and large + fast backups (bottom right).



- Are jobs frequently exceeding 8, 12 or 24 hour durations?
- What time of day are the longest jobs occurring?
- Are network or server bottlenecks the problem?

© Copyright 2016 Dell EMC

Dell EMC

# Top Clients

Dell EMC

## Largest Clients (Top 15)

Server	Host	Operating System	Peak Daily (GB)	Avg GB/day
ecbphc2.uis.bpichincha.com	ecbphcp2.uis.bpichincha.com	hp s800 hp-ux-11.11	10,317	5,095
ecbphc2.uis.bpichincha.com	precbphcds.uis.bpichincha.com	ibm rs6900 aix-7.1	10,085	5,520
ecbphc2.uis.bpichincha.com	ecau197h02.uis.bpichincha.com	microsoft amd64 wNT-6.0-S	3,799	614
ecbphc2.uis.bpichincha.com	ecbphcpa.uis.bpichincha.com	hp s800 hp-ux-11.11	2,332	961
ecbphc2.uis.bpichincha.com	ecbphcp1.bgr.com	hp ia64 hp-ux-11.31	2,064	1,546
ecbphc2.uis.bpichincha.com	ecbphcp1.bgr.com	hp s800 hp-ux-11.11	1,530	238
ecbphc2.uis.bpichincha.com	ecbphcdp2.uis.bpichincha.com	hp ia64 hp-ux-11.31	1,311	639
ecbphc2.uis.bpichincha.com	ecbphcd2.uis.bpichincha.com	hp s800 hp-ux-11.11	896	133
ecbphc2.uis.bpichincha.com	ecbphcp1	gpl x86_64 linux-2.6.18-164.el5	570	88
ecbphc2.uis.bpichincha.com	ecau197h01.uis.bpichincha.com	microsoft i386 wNT-5.0-S	476	82
ecbphc2.uis.bpichincha.com	ecbphcd2.uis.bpichincha.com	hp ia64 hp-ux-11.31	462	104
ecbphc2.uis.bpichincha.com	ecbphcpop.uis.bpichincha.com	hp ia64 hp-ux-11.31	245	107
ecbphc2.uis.bpichincha.com	ecbphcomp.uis.bpichincha.com	hp ia64 hp-ux-11.31	152	91
ecbphc2.uis.bpichincha.com	ecbphcont.uis.bpichincha.com	hp ia64 hp-ux-11.31	110	55
ecbphc2.uis.bpichincha.com	ecbphmbf1.uis.bpichincha.com	gpl x86_64 linux-2.6.32-504.el6.x86_64	105	51

1 © copyright 2016 Dell EMC

Dell EMC

## Top Backup Window Consumers (Top 15)

Server	Host	Operating System	Percent of Total Backup Duration	Total Backed Up (GB)	# Jobs
ecbphc2.uis.bpichincha.com	ecbphcp2.uis.bpichincha.com	hp s800 hp-ux-11.11	49	174,723	16,848
ecbphc2.uis.bpichincha.com	precbphcds.uis.bpichincha.com	ibm rs6900 aix-7.1	21	164,305	7,109
ecbphc2.uis.bpichincha.com	ecbphcpa.uis.bpichincha.com	hp s800 hp-ux-11.11	13	26,839	1,766
ecbphc2.uis.bpichincha.com	ecbphcdp2.uis.bpichincha.com	hp ia64 hp-ux-11.31	3	19,157	1,360
ecbphc2.uis.bpichincha.com	ecbphcpop.uis.bpichincha.com	hp ia64 hp-ux-11.31	3	5,995	1,555
ecbphc2.uis.bpichincha.com	ecbphcp1.bgr.com	hp s800 hp-ux-11.11	2	5,727	728
ecbphc2.uis.bpichincha.com	ecbphcd2.uis.bpichincha.com	hp s800 hp-ux-11.11	1	3,983	476
ecbphc2.uis.bpichincha.com	ecbphcp3.bgr.com	hp ia64 hp-ux-11.31	1	45,393	62
ecbphc2.uis.bpichincha.com	ecbphmbf1.uis.bpichincha.com	gpl x86_64 linux-2.6.32-504.el6.x86_64	1	1,516	1,076
ecbphc2.uis.bpichincha.com	ecbphcpd.uis.bpichincha.com	sun sparc solaris-5.10	1	2,702	1,340
ecbphc2.uis.bpichincha.com	ecbphcomp.uis.bpichincha.com	hp ia64 hp-ux-11.31	1	2,727	1,323
ecbphc2.uis.bpichincha.com	ecbphcd2.uis.bpichincha.com	hp ia64 hp-ux-11.31	1	3,196	1,394
ecbphc2.uis.bpichincha.com	ecbphmbf2.uis.bpichincha.com	gpl x86_64 linux-2.6.32-504.el6.x86_64	1	757	772
ecbphc2.uis.bpichincha.com	ecau197h02.uis.bpichincha.com	microsoft amd64 wNT-6.0-S	0	15,901	27
ecbphc2.uis.bpichincha.com	ecau197h01.uis.bpichincha.com	microsoft i386 wNT-5.0-S	0	2,368	27

44 © copyright 2016 Dell EMC

Dell EMC

# Longest Backups

Backups are taking up to 33 hours. If large file servers, consider NAS+NDMP+Dedup. If large databases, consider 10GBE direct to Data Domain.

Host	Job Name	Job Level	Group Name	Capacity (GB)	# Files	Date Time	Hours
ecalo197h01.uis.bpichecha.com	IE...	Full	MATRIZ_HOMEFOLDER_MES	475	345,762	2016-11-14	33
ecalo197h02.uis.bpichecha.com	IE...	Full	MATRIZ_HOMEFOLDER_MES	3,022	2,601,174	2016-11-14	33
ecalo197h01.uis.bpichecha.com	IE...	Full	MATRIZ_HOMEFOLDER_MES	442	326,802	2016-12-05	33
ecalo197h02.uis.bpichecha.com	IE...	Full	MATRIZ_HOMEFOLDER_MES	3,709	2,732,945	2016-12-05	33
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	7	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	0	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	7	0	2016-11-29	25
ecbphoqa.uis.bpichecha.com	TST_DTST_FULLDIA_EC B...	Full	Oracle8 TST_DTST_FULLDIA_ECBPHOQA	109	0	2016-11-29	25

DRILL/C