ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO Y DESPLIEGUE DE UNA ARQUITECTURA MULTITENANT HYPERCONVERGENTE PARA ALOJAR CARGAS DE CÓMPUTO BASADAS EN UN MODELO CLOUD IAAS"

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

KEVIN EDWIN INTRIAGO NARVAEZ

GUAYAQUIL- ECUADOR
2020

AGRADECIMIENTO

A Dios, por haberme permitido concluir un ciclo más de mi formación académica, a mis padres por su motivación y apoyo constante durante este proceso, a mis hermanos Luis, Andreina, Génesis y José, por estar en momentos cruciales cuando requerí de su ayuda.

DEDICATORIA

Dedico este trabajo a Narcisa Narvaez y Victor Intriago, por su amor y apoyo incondicional durante todo mi proceso académico, que a pesar de las distintas adversidades que les tocó enfrentar, nunca escatimaron sus esfuerzos para brindarme una educación digna de alto nivel.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenín Freire Cobo

COORDINADOR MSIG

MSIG. Juan García Plúa

PROFESOR MSIG

RESUMEN

El diseño y despliegue propuesto, tiene como objetivo principal disponibilizar un ambiente multitenant hyperconvergente para alojar cargas de cómputo basadas en un modelo Cloud IaaS, con el fin de garantizar la disponibilidad y seguridad de los servicios tecnológicos, que permita responder de forma ágil y dinámica al negocio, así como mantener la operación con altos niveles de redundancia, un respaldo apropiado de la información en casos emergentes y además, que los clientes paguen por lo que realmente consumen.

Posterior al despliegue de un ambiente Cloud Iaas, los clientes tendrán la posibilidad de tener completa visibilidad de la infraestructura de cómputo desde un panel de administración, además, la gestión en la configuración de los servidores virtuales será autónoma, debido a que se podrán reiniciar, pausar, detener, tomar snapshots y agregar discos de almacenamiento en tiempo real, sin afectar la continuidad de negocio.

La arquitectura de cómputo desplegada contará con un nivel de disponibilidad del 99.98%, además, el despliegue de la instancia de Firewall tendrá funcionalidades de filtrado de paquetes IP, NAT, Source NAT y Destination NAT, VPN, cifrado IPSEC/L2TP, IPS, AMP, PAM, UTP, IPAM, Web Filtering, AS, Security Rating, Antispam, proporcionando una capa de seguridad adicional a nivel del VDC.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AMP	Advanced Malware Protection.
CPU	Central Processing Unit.
GCP	Google Cloud Platform
IAAS	Infrastructure as a service.
IPS	Intrusion Prevention System.
IPSEC	Internet Protocol Security.
L2TP	Layer Two Tunneling Protocol.
MSIG	Magíster en Sistemas de Información Gerencial.
NAT	Network Address Translation
PAM	Privileged Access Management
RAM	Random Access Memory
SDN	Software Defined Network
TI	Tecnologías de Información
UTP	Unified Threat Protection
VPN	Virtual Private Network
VPC	Virtual Private Network.
VPC	Virtual Private Cloud.
VDC	Virtual Datacenter.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En el presente documento se detalla las actividades realizadas para solventar una problemática relacionada a la disponibilización de recursos de cómputo bajo consumo, y a su vez se analiza la evaluación de los resultados obtenidos posterior al despliegue integral de la solución.

A continuación, se resumen los apartados del documento.

En el capítulo 1 – Generalidades, se describe el problema y se propone una solución que permite solventarlo.

En el capítulo 2 – Metodología para el Desarrollo de la solución, se detalla el levantamiento de información, el dimensionamiento de hardware y software requerido, además, el plan de acción a seguir, finalizando con el despliegue de la solución, la cual está dividida en tres fases, en primera instancia la implantación de los nodos hyperconvergentes, posteriormente el despliegue de la seguridad lógica y finalmente la integración de todos los componentes con la arquitectura Cloud IaaS.

En el capítulo 3 – Evaluación de Resultados, se realiza el monitoreo de la solución integral, adicionalmente se ejecutan el despliegue de servidores virtuales, posteriormente se genera un informe comparativo y finalmente se listan los beneficios de la solución.

El documento finaliza con conclusiones y recomendaciones.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

La empresa de Telecomunicaciones sujeta al análisis estaba en busca de una solución que le permitiera innovar a través de nuevas tendencias en el despliegue de infraestructuras de cómputo, para hospedar cargas de trabajo de misión crítica. Además, que le permita contribuir al logro y cumplimiento de los objetivos y exigencias del mercado en relación a los servicios que estos demandan.

La empresa contaba con nodos de cómputo convergentes, los cuales funcionan de forma independiente a nivel de procesamiento, almacenamiento y conectividad, además, el despliegue de la seguridad

lógica y servidores virtualizados, se administraban en portales diferentes, haciendo que la experiencia de usuario no sea tan amigable.

No existía una solución que permita garantizar compatibilidad entre hypervisores VMware, Hyper V y KVM, además no se contaba con replicación entre sitio principal y alterno, que asegure la continuidad al negocio y respaldo apropiado de la información.

Finalmente, el cobro por el servicio de infraestructura de cómputo se realizaba mediante tarifa plana y no por consumo de recursos, tales como memoria RAM y vCPU.

1.2 SOLUCIÓN PROPUESTA

Debido a la problemática identificada, al no disponer infraestructura integral de aprovisionamiento automatizado y con mayor rendimiento, compatibilidad de hypervisores y un portal de autogestión que le permita al usuario administrar desde una sola interfaz las diferentes funcionalidades a nivel de cómputo, almacenamiento y seguridad, se propone el “Diseño y Despliegue de una arquitectura multitenant hyperconvergente para alojar cargas de cómputo basadas en un modelo Cloud IaaS.”. La solución propuesta permitirá que los clientes tengan

acceso directo al tenant creado en la plataforma de gestión basada en Openstack, donde podrán contar con funcionalidades que le permitan acceder a nuevos casos de uso como:

1. Creación de aplicaciones empresariales basadas en arquitecturas de microservicios.
2. Selección de la zona de disponibilidad para el despliegue de servicios con menor latencia.
3. Crear reglas de conectividad entre servidores o aplicaciones y bases de datos.
4. Asignar direccionamiento IP (IPV4 o IPv6) homologado o público dinámicamente, en dual stack.
5. Desplegar grupos de aplicaciones multinivel que permitan generar soluciones verticales dirigidas a segmentos de mercado específicos.

Para el despliegue de la infraestructura se contará con el siguiente equipamiento.

1. Cuatro (4) nodos VxRail S570 con las siguientes capacidades por servidor.
    - 512 vCPU
    - 1.536 GB de Memoria RAM

- 25 TB de Almacenamiento

2. Dos (2) firewalls Fortigate 300E.
3. Cuatro (4) switches Isilon X210 - Mellanox 8 puertos QDR.
4. Dos (2) switches SAN 8 puertos de 16 Gbps.

El desarrollo de este modelo permitirá crear servicios de manera rápida, acorde a las necesidades del mercado, con el fin de garantizar la disponibilidad y seguridad de los servicios tecnológicos, basados en una solución integral que responda de forma ágil y dinámica al negocio, así como mantener la operación con altos niveles de disponibilidad, cumpliendo con la normativa legal vigente y proporcionando a los clientes un respaldo apropiado de la información en casos emergentes.

A continuación, se describen las funcionalidades del servicio:

1. El usuario podrá seleccionar el sistema operativo Windows o Linux que requiera de acuerdo con su distribución, con o sin base de datos.
2. El usuario tendrá acceso a un panel de autogestión que le facilitará la administración del servidor virtual y le proporcionará información general como: Tipo de subscripción, número de servidores virtuales, características (memoria RAM, vCPU, Almacenamiento, Sistema Operativo), arquitectura del equipo Host (características

físicas como procesador, velocidad en GHz, I/O, etc) y capacidades generales de uso, nombre del equipo, usuarios (alta, baja y cambio).

3. El usuario podrá acceder a diferentes opciones dentro del panel de control, que le permitirá agregar o contratar nuevas funcionalidades o servicios, como son: servidores virtuales adicionales, configuración de políticas de seguridad, registro de DNS, contratación de almacenamiento adicional, Licenciamiento, Servicios administrados, adicionales o monitoreo.
4. Para consumir cada uno de los servicios, el usuario accederá a través del panel, interface SSH (Linux) o Escritorio remoto (Windows), para realizar actividades de administración y configuración de los servicios e Instalar, desplegar y ejecutar aplicaciones.

Algunos de los motivos para el uso de Arquitecturas Cloud son:

1. Modernización de los procesos de negocio.
2. Evitar gastos de capital.
3. Flexibilidad y escalabilidad.
4. Aumento de la capacidad informática y del rendimiento.
5. Diversificación de los sistemas.
6. Optimización de la infraestructura TI.

7. Continuidad de negocio y capacidad de recuperación ante desastres.
8. Evaluación de la viabilidad y rentabilidad de nuevos servicios.
9. Controlar los costes y beneficios marginales

CAPÍTULO 2

METODOLOGÍA PARA EL DESARROLLO DE LA SOLUCIÓN

2.1 LEVANTAMIENTO DE LA INFORMACIÓN

El servicio a desplegar debe contener funciones de administración que facilite la creación, comunicación, y asociación de grupos de seguridad y gestión de los componentes de cómputo, además de contar con las siguientes características de conectividad:

1. Conectividad Pública: Internet, VPN Ipsec (L2L o Cliente Servidor)
2. Conectividad Privada: RPV (MPLS)

A continuación, se describen las funcionalidades requeridas en el servicio:

1. El cliente podrá seleccionar alguna de las ofertas de servidores virtuales preestablecidos dentro de la familia.
2. El usuario podrá seleccionar el sistema operativo Windows o Linux que requiera.
3. Una vez contratado el servicio el usuario tendrá acceso a un panel de control que facilitará la administración del servidor virtual contratado, donse deberá poder visualizar la información general, tales como, tipo de subscripción, detalles generales de uso, nombre del equipo, cantidad de servidores virtuales contratados, capacidad de cómputo y almacenamiento.
4. El usuario tendrá acceso a diferentes opciones dentro del panel de control, entre las cuales le permitirá agregar o contratar nuevas funcionalidades o servicios, como servidores virtuales adicionales, configuración de políticas de seguridad, registro de DNS, contratación de almacenamiento adicional, Servicios administrados o de monitoreo.
5. Para consumir los servicios el usuario deberá acceder directamente a través del panel de control o en su defecto por medio de una interface SSH en el caso que el sistema operativo sea Linux o por escritorio remoto en sistemas Windows, con el objetivo de realizar actividades de administración y configuración

de los servicios, ya sea estos de Instalación o despliegue de aplicaciones.

6. El usuario podrá realizar actividades de administración sobre su máquina virtual desde el panel de control; entre las cuales se encuentran las siguientes:
   - Gestionar snapshot (eliminar, crear, restaurar y cancelar Snapshots a un su servidor virtual).
   - Realizar Backup del servidor (backup básico, incremental, seleccionar políticas de respaldo ya definida).
   - Funciones de control de acceso (Registrar una cuenta, dar de alta, dar de baja, borrar y/o asignar usuario a un grupo vía consola de administración de usuario).
   - Funciones de gestión de máquinas virtuales como: Crear, Iniciar, Detener, Re-iniciar, Borrar, Preparar imágenes y snapshopts.
   - Borrar y/o Renombrar instancias de imágenes.
   - Clonar instancias.
   - Asignación, Carga y Almacenamiento de llaves públicas SSH a instancias de Linux.
   - Funciones de red como: creación de ruteo, permisos de direccionamiento y grupos de seguridad, VPN (IPSec), Nat gateway, IP elástica.

- Aplicar reglas de autoscaling horizontal o vertical
- Crecer o decrecer las capacidades de RAM o vCPU de su máquina virtual
- Agregar más discos
- Crear templates de la configuración de su servidor virtual

2.1.1 REQUERIMIENTOS FUNCIONALES

Posterior al levantamiento de información se consideraron los requerimientos mínimos a cumplir para cada funcionalidad del servicio.

Tabla 1 Requerimientos Funcionales de la solución

Categoría	Funcionalidad	Descripción
Red	Virtual Private Cloud (VPC)	Nube Privada Virtual o VPC, proporciona un entorno virtual aislado de forma lógica donde el cliente puede construir sus servicios basados en una red definida por software.
	Red virtual	Permite crear subnets con acceso público o privado dentro de un VPC.
	Ruteo	Permite la interconectar de máquinas virtuales entre sí, a través de diferentes segmentos de red
	Firewall	Permite aplicar políticas de seguridad Norte-Sur entre servidores y el cliente,

Categoría	Funcionalidad	Descripción
		es decir controla el tráfico desde internet o alguna aplicación al servidor
	Conectividad Pública: VPN IPSec (L2L o Cliente Servidor)	Permite establecer comunicación de manera segura con los servicios en Cloud mediante una comunicación de tipo cliente-servidor IPSec
Cómputo	Servidor Virtual -	Proporciona infraestructura bajo de manda con diversidad de plantillas de Sistemas Operativos, con capacidad de CPU, RAM y Disco local estándar.
	Snapshot	Permite capturar el estado actual de la configuración de su servidor virtual y preservarlo para regresarlo a ese estado si así lo desea.
	Incrementar o decrementar RAM	Puede incrementar o decrementar los recursos de memoria RAM de un servidor virtual a través del panel de control
	Incrementar o decrementar CPU	Puede incrementar o decrementar los vCPU de un servidor virtual a través del panel de control
	Agregar discos	Permite agregar o eliminar un disco adicional en un servidor virtual
	Crecer disco	Permite crecer el disco principal de un servidor virtual
	Respaldos	Permite definir políticas de respaldos dentro del servicio (diario, semanal, mensual)

Categoría	Funcionalidad	Descripción
	Pago por uso	Permite desglosar costos de recursos de computo por hora usada

Fuente: Elaborado por el autor

La VPC deberá contar con las siguientes funcionalidades, las cuales se deberán gestionar directamente desde la consola de administración.

2.1.2 INFRAESTRUCTURA DE CÓMPUTO COMO SERVICIO

El servicio describe funcionalidades de Auto aprovisionamiento y abastecimiento automatizado de las instancias de servidores virtuales bajo demanda, flexible, escalable, confiable y seguro.

Tabla 2 Funcionalidades de Servidores Virtuales

Componente	Descripción
Servidor virtual	Proporciona infraestructura bajo de manda con diferentes plantillas de Sistemas Operativos (Windows, RedHat, Centos).
Autoscaling	El cliente podrá crecer y decrecer de manera automática sus recursos de cómputo, para atender

Componente	Descripción
	grandes cargas de trabajo que se presentan de manera esporádica o por temporadas.
Snapshot	El cliente podrá capturar el estado actual de la configuración de su servidor virtual y preservarlo para regresarlo a ese estado si así lo desea.
Incrementar o decrementar RAM	El cliente podrá incrementar o decrementar los recursos de memoria RAM de su servidor virtual si así lo requiere.
Incrementar o decrementar CPU	El cliente podrá incrementar o decrementar los recursos de vCPU de su servidor virtual si así lo requiere.
Agregar discos	El cliente podrá agregar un disco adicional a una Máquina virtual si así lo desea. También podrá asociar o desasociar el disco adicional aprovisionado a la máquina virtual.

Fuente: Elaborado por el autor

En la siguiente tabla se ilustra las configuraciones disponibles de vCPU y vRAM, para el despliegue de las máquinas virtuales.

Tabla 3 Combinación de vCPU y vRAM

VCPU \ RAM (GB)	1	2	4	6	8	10	12	16	24	32	48	64	72	96	112	128
1	◉	◉	◉	◉	◉											
2	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉						
4		◉	◉	◉	◉	◉	◉	◉	◉	◉						
6			◉	◉	◉	◉	◉	◉	◉	◉	◉	◉				
8			◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉		
10							◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
12							◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
16								◉	◉	◉	◉	◉	◉	◉	◉	◉
32										◉	◉	◉	◉	◉	◉	◉

Fuente: Elaborado por el autor

2.1.3 CARACTERÍSTICAS NO FUNCIONALES

A continuación, se detallan las características no funcionales de la solución.

1. Interface de gestión vía internet, VPN o SSH.
2. Soporte para IPv4 e IPv6, en dual stack.
3. Capacidad de retener VMs apagadas y cobrar solo el almacenamiento.

4. Crear y administrar sub-redes, mapear y borrar direcciones IP hacia o desde máquinas virtuales.
5. Segmentación de tráfico: administración, backup, storage, producción.
6. Publicación y acceso a internet desde equipo virtual con la conectividad Cloud.

2.2 DIMENSIONAMIENTO SOFTWARE Y HARWARE

2.2.1 DIMENSIONAMIENTO DE SOFTWARE

El despliegue de la solución requiere ciertos componentes de licenciamiento, los cuales se detallan en la Tabla 4 – Licencias de la Infraestructura.

Tabla 4 Licencias de la Infraestructura

Cantidad	Descripción
4	VxRail Software 4.7.300 Factory Install
4	Red Hat Enterprise Linux Operating System
2	FortiGuard IPS Service
2	FortiGuard Security Rating Service
2	FortiGuard Web Filtering Service

Fuente: Elaborado por el autor

Los paquetes a considerar para el funcionamiento de la solución serán los siguientes.

Tabla 5 Componentes de la solución Cloud

Nombre	Función
Horizon	Permite que los usuarios puedan visualizar el Portal de Administración, también conocido por FrontEnd.
Keystone	Encargado de gestionar la autenticación.
Magnum	Es el encargado de orquestar las imágenes de Sistemas Operativos.
Nova	Proporciona mecanismos de autogestión que permite el aprovisionamiento de las máquinas virtuales.
Neutron	Permite aprovisionar a las máquinas virtuales redes basadas en software, también conocidas como SDN.
Swift	Almacena datos no estructurados, los cuales son escalables y garantizan confiabilidad y seguridad.
Manila	Proporciona acceso a sistemas de archivos compartidos o distribuidos.
Ceilometer	Permite monitorear los recursos de cómputo y alarmas, por cada uno de los componentes de la arquitectura.

Fuente: Elaborado por el autor

2.2.2 DIMENSIONAMIENTO DEL HARWARE

Para la implementación del Clúster Hyperconvergente se requiere:

1. Cuatro (4) nodos VxRail S570 con las siguientes capacidades por servidor.
   - 512 vCPU
   - 1.536 GB de Memoria RAM
   - 25 TB de Almacenamiento
2. Dos (2) firewalls Fortigate 300E.
3. Cuatro (4) switches Isilon X210 - Mellanox 8 puertos QDR.
4. Dos (2) switches SAN 8 puertos de 16 Gbps.

Para implementar el Proxy se requerirá un servidor HP DL140 G4. El detalle de las características del Hardware requerido se encuentra en la tabla 2.

Tabla 6 Características del Hardware Requerido

Tipo	Modelo	Procesador	Core	RAM	Disco Duro
Nodo de Cómputo 1	VxRail S570	Intel Xeon Gold 5218R	40	384 GB	20 TB
Nodo de Cómputo 2	VxRail S570	Intel Xeon Gold 5218R	40	384 GB	20 TB
Nodo de Cómputo 3	VxRail S570	Intel Xeon Gold 5218R	40	384 GB	20 TB
Nodo de Cómputo 4	VxRail S570	Intel Xeon Gold 5218R	40	384 GB	20 TB

Tipo	Modelo	Procesador	Core	RAM	Disco Duro
Firewall Principal	Fortigate 301E	NP6 and CP9	-	-	132 GB
Firewall Secundario	Fortigate 301E	NP6 and CP9	-	-	240 GB
Switch Principal	CTX DS-6610B 8P/	-	-	-	-
Switch Secundario	CTX DS-6610B 8P/	-	-	-	-
Infiniband Nodo 1	IB QDR 8	-	-	-	-
Infiniband Nodo 2	IB QDR 8	-	-	-	-
Infiniband Nodo 3	IB QDR 8	-	-	-	-
Infiniband Nodo 4	IB QDR 8	-	-	-	-

Fuente: Elaborado por el autor

2.3 GENERACIÓN DEL PLAN DE ACCIÓN

Para la ejecución del proyecto se requieren un total de 60 días, tal como se muestra en la figura 2.1, el cual está divido en tres fases, la adquisición del equipamiento que tomará 35 días, posteriormente se ejecutará la fase de implementación de la solución, la cual requiere de 20 días y finalmente las pruebas funcionales con su respectiva documentación, la misma que durará un tiempo de 5 días.

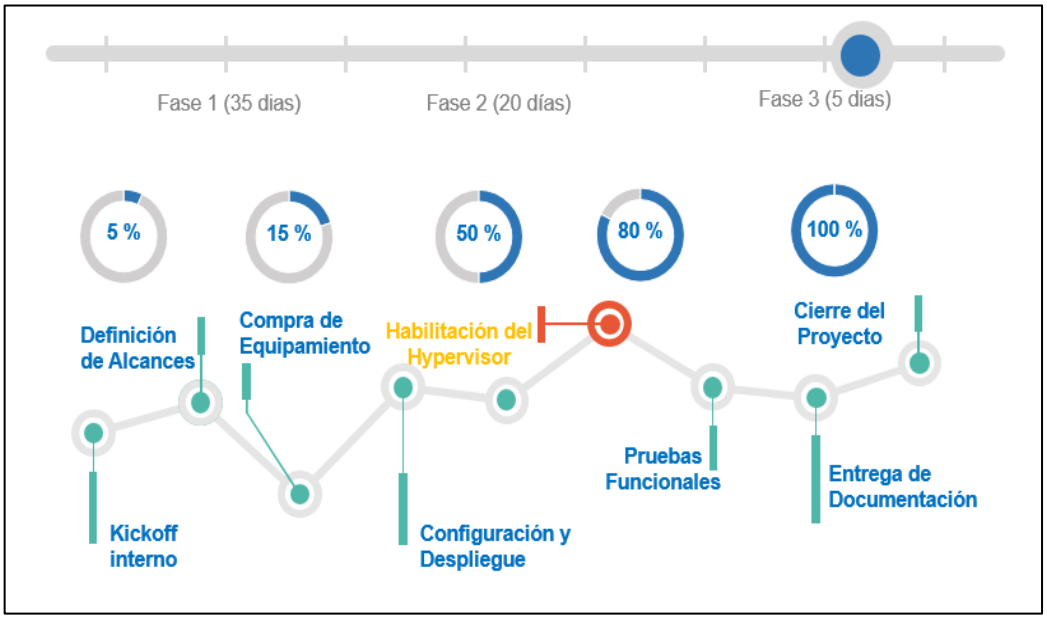


Figura 2.1 Cronograma de despliegue de la solución

Fuente: Elaborado por el autor

La adquisición de la infraestructura es una de las actividades que mayor impacto tienen sobre el tiempo de puesta en marcha de la solución, sin embargo, se trabajará en paralelo para disponibilizar el componente de housing, lugar donde se alojará todo el equipamiento de hardware que se utilizará para el despliegue integral de solución.

A continuación, se detallan cada una las actividades que se realizarán en las diferentes fases.

Fase 1. Compra de equipamiento

1. Socialización del proyecto con las áreas involucradas.
2. Asignación de presupuesto.
3. Liberación de términos de referencia.
4. Evaluación de proveedores.
5. Negociación con proveedores.
6. Elección de Proveedor de Hardware.
7. Importación de Equipamiento.

Fase 2. Despliegue de la Solución

1. Puesta en marcha de los servidores hyperconvergentes.
2. Configuración del Hypervisor.
3. Ejecución de Hardening.
4. Habilitación de Nube Privada Virtual.
5. Despliegue del componente de Infraestructura de cómputo como servicio.
6. Despliegue del Firewall Virtual.
7. Habilitación de enrutamiento.
8. Habilitación de zonas DNS.
9. Habilitación de Balanceo de Carga.

10. Acondicionamiento de plantillas de sistema operativo.
11. Configuración de herramienta de pago por consumo.
12. Despliegue de Conectividad.

Fase 3. Pruebas Funcionales

1. Plan de pruebas de instalación, firmware y funcionamiento del equipamiento.
2. Pruebas de Alta Disponibilidad.
3. Pruebas de Servicios de Balanceo.
4. Pruebas de Conectividad.
5. Pruebas de despliegue de servidores virtuales.

2.4. DESPLIEGUE DE LA SOLUCIÓN

2.4.1 CONFIGURACIÓN DE NODOS HYPERCONVERGENTES

Se procedió a realizar la habilitación del Rack, donde se ejecutaron las siguientes actividades.

1. Instalación de Rack (anclaje y etiquetamiento)
2. Instalación de 2 puntos eléctricos (cableado desde el Rack hasta las PDUs)
3. Instalación de 2 rPDUs (para redundancia eléctrica)
4. Instalación de 2 puntos de datos para el monitoreo de las rPDUs

Posteriormente se ejecutó el anclaje de los equipos y finalmente setup de configuración, detallado a continuación.

1. Habilitación de Redes y VxRail Manager
2. Asignación de VLAN de reserva y configuración de DNS
3. Reservación de tres o más direcciones IP contiguas y una máscara de subred para vSAN.
4. Asignación de un nombre de host y una dirección IP para VxRail Manager

5. Configuración de Zona horaria y nombre de host del servidor NTP.
6. Configuración del switch de interconexión
7. Configuración Puertos físicos no asignados
8. Finalmente se estableció la confirmación de la configuración y el acceso de red.

2.4.2 PRUEBAS DE NODOS HYPERCONVERGENTES

Se realizó un plan de pruebas respecto a la instalación y funcionamiento de la arquitectura física de cómputo.

Tabla 7 Firmware de los nodos de cómputo

Criterios de Aceptación	Detalle de la Prueba	Cumple	
		SI	NO
Los 4 nodos VxRail deben contar con la versión de firmware 4.0.0-5396804	Equipos con la última versión de firmware instalado, funcional y sin errores.	X	
OBJETIVO: El objetivo de la prueba, es validar que los nodos hyperconvergentes cuenten con las últimas actualizaciones recomendadas por el fabricante.			
RESULTADO: Se visualiza que los 4 equipos VxRail 560 se encuentran con la versión actualizada.			

Fuente: Elaborado por el autor

Tabla 8 Pruebas de Apagado y Encendido de los nodos

Criterios de Aceptación	Detalle de la Prueba	Cumple	
		SI	NO
Correcto apagado y encendido de los 4 nodos VxRail, el cual debe subir sin errores.	Se verificará el correcto apagado y encendido de los equipos sin presentar novedades y errores	X	
OBJETIVO: El objetivo de esta prueba, es validar que los nodos hyperconvergentes se apaguen y enciendan de manera normal, sin ningún error de Software.			
RESULTADO: Los equipos se apagaron y encendieron sin ningún problema.			

Fuente: Elaborado por el autor

2.4.3 IMPLEMENTACIÓN DE SEGURIDAD LÓGICA

Se realizó el despliegue del cluster FG 300E, donde en primera instancia se lo rackeó y posteriormente se establecieron los diferentes canales de comunicación con el ambiente privado y público, tal como se muestra en la figura 2.2.

A continuación, se detallan una serie de actividades ejecutadas previo al despliegue integral de la arquitectura cloud.

1. Se validó que esté instalada la última versión de firmware liberada por el fabricante, además, se validó que el soporte con el fabricante esté activo.

2. Se configuraron DNS y el servicio de NTP.
3. Se realizó segregación de redes para la segmentación de los servidores
4. Se aseguraron las redes internas, incluida la DMZ y se establecieron doble factor de autenticación para todo el acceso remoto incluido los de sitio a sitio y VPN personal

2.4.4 PRUEBAS DE FUNCIONAMIENTO SEGURIDAD LÓGICA

Se realizaron diferentes pruebas de funcionamiento y validación de mejores prácticas aplicadas al componente de seguridad lógica, logrando los siguientes resultados.

Tabla 9 Versión de Firmware de los Firewalls

Criterios de Aceptación	Detalle de la Prueba	Cumple	
		SI	NO
Los 2 equipos de seguridad deben contar con la versión de firmware 6.2	Equipos con la última versión de firmware instalado, funcional y sin errores.	X	
OBJETIVO: Verificar que los equipos cuenten con las últimas actualizaciones recomendadas por el fabricante.			
RESULTADO: Se visualiza que los 2 equipos FG 300E se encuentran con la versión actualizada.			

Fuente: Elaborado por el autor

Tabla 10 Apagado y Encendido de los Firewalls

Criterios de Aceptación	Detalle de la Prueba	Cumple	
		SI	NO
Correcto apagado y encendido de los 2 equipos FG 300E, el cual debe subir sin errores.	Se verificará el correcto apagado y encendido de los equipos sin presentar novedades y errores	X	
OBJETIVO: El objetivo de esta prueba, es verificar que los FG 300E se apaguen y enciendan de manera normal, sin ningún error de Software.			
RESULTADO: Los equipos se apagaron y encendieron sin problemas.			

Fuente: Elaborado por el autor

Se realizará el siguiente plan de pruebas con la finalidad de que los equipos solamente realicen la conmutación de Activo/Standby y Standby/Activo cuando uno de los dos este apagado. Cuando todo se restablezca los equipos deben de volver a su estado inicial automáticamente.

Tabla 11 Alta Disponibilidad Firewall Principal

Criterios de Aceptación	Detalle de la Prueba	Cumple	
		SI	NO
Correcto Funcionamiento del equipo principal el cual se va a encontrar en estado Activo, una vez apagado el equipo	Se verificará que, al momento de apagar el equipo principal, el equipo secundario toma el rol de Activo.	X	

principal el equipo secundario tomara el rol de Activo. Encendido del equipo Principal, una vez operativo el equipo principal, automáticamente en 40 segundos volverá a tomar el rol de Activo.	Se verificará que, al momento de encender el equipo principal, automáticamente tome el rol de activo en 40 segundos.		
OBJETIVO: El objetivo de esta prueba, es observar el cambio de Activo/Standby de la alta disponibilidad, al momento de apagar y encender el equipo principal.			
RESULTADO: El proceso de conmutación de Activo a Standby y luego a Activo para el equipo principal, se dio sin ningún problema.			

Fuente: Elaborado por el autor

Tabla 12 Alta Disponibilidad Firewall Secundario

Criterios de Aceptación	Detalle de la Prueba	Cumple	
		SI	NO
Correcto funcionamiento del equipo secundario el cual se va a encontrar en estado Activo, una vez apagado el equipo secundario, el equipo principal tomará el rol de Activo. Encendido del equipo Secundario, una vez	Se verificará que, al momento de apagar el equipo secundario, el equipo principal toma el rol de Activo. Se verificará que, al momento de encender el equipo secundario, automáticamente tome el rol de standby en	X	

operativo el equipo secundario, automáticamente en 40 segundos volverá a tomar el rol de Standby.	aproximadamente en 40 segundos.		
OBJETIVO: El objetivo de esta prueba, es observar el cambio de Activo/Standby de la alta disponibilidad, al momento de apagar y encender el equipo principal.			
RESULTADO: El proceso de conmutación de Standby a Activo y luego a Standby para el equipo principal, se dio sin ningún problema.			
OBSERVACIONES:			

Fuente: Elaborado por el autor

2.4.5 DESPLIEGUE DEL AMBIENTE CLOUD

Para el despliegue de la solución se utilizará una plataforma de software gratuita y de código abierto llamada openstack, la cual proporciona ambientes IaaS para nubes públicas y privadas. [10]

La plataforma OpenStack consta de varios proyectos interrelacionados que controlan el hardware, el almacenamiento y los recursos de red de un centro de datos, como: Computación, Servicio de imágenes, Almacenamiento, Servicio de identidad, Redes, Almacenamiento de objetos, Orquestación y Base de datos. [11]

La administración de esos componentes se puede gestionar a través de la interfaz basada en web o con la ayuda de la línea de comandos de OpenStack.

La Arquitectura de despliegue a considerar será la siguiente.

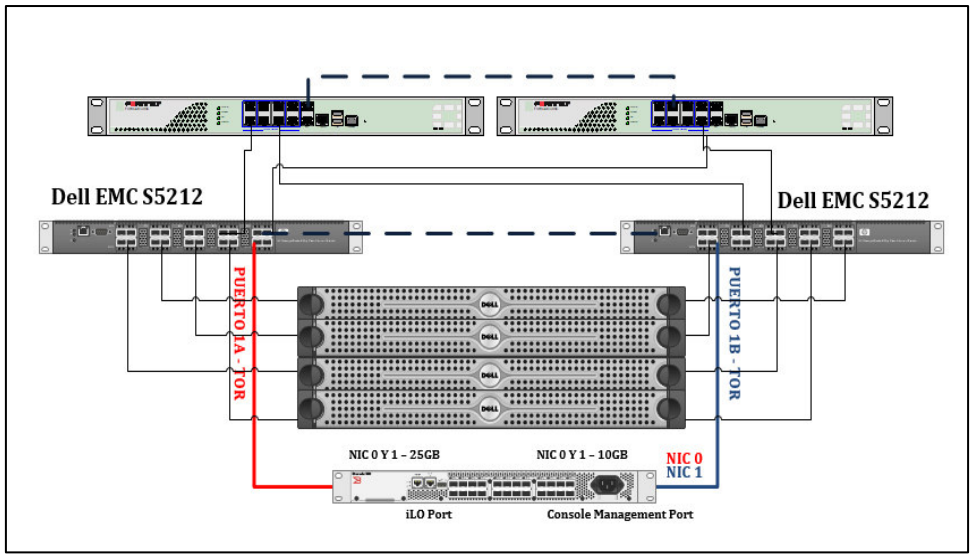


Figura 2.2 Diagrama de la Arquitectura Cloud

Fuente: Elaborado por el autor

Los elementos de Cómputo, Seguridad y Conectividad, estarán alojados en un Rack que posee las siguientes características.

1. Dimensiones del Rack: 80 cm de Ancho y 120 cm de Profundidad.
2. 42 U (Unidades de Rack) Totales.

3. 3 U (Unidades de Rack) Utilizadas/Consumidas en accesorios preinstalados.
4. 39 U (Unidades de Rack) Disponibles/Utilizables.
5. 3 KVA nominales, consumo al 67% 4,69 KW.
6. Incremento de consumo soportado hasta 7 KVA nominales. (Facturables bajo demanda).
7. Seguridad física del Rack mediante cerraduras en cada compuerta (frontal y posterior).
8. 2 PDUs verticales monitoreables, marca APC. (conectadas a diferentes UPS).
9. 1 Organizador horizontal de 2U para cableado.
10. 2 Puntos de Red más cableado UTP categoría 6A.

Las ubicaciones de los equipos quedaron establecidas tal como se muestra en la figura 2.3.

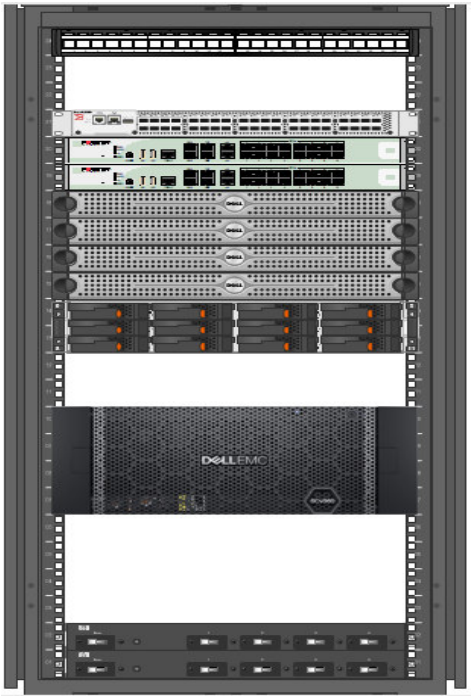


Figura 2.3 Distribución del Hardware en 1 Full Rack

Fuente: Elaborado por el autor

En la arquitectura de cómputo existirá un nodo controlador y tres nodos de cómputo, tal como se muestra la figura 2.4.

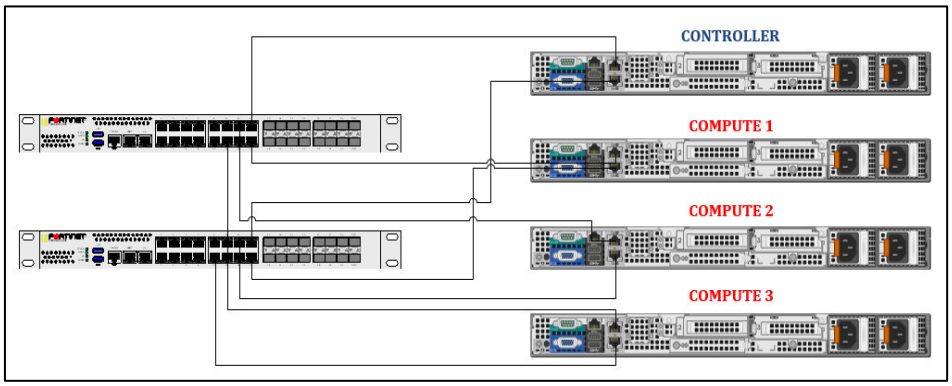


Figura 2.4 Arquitectura del ambiente Cloud

Fuente: Elaborado por el autor

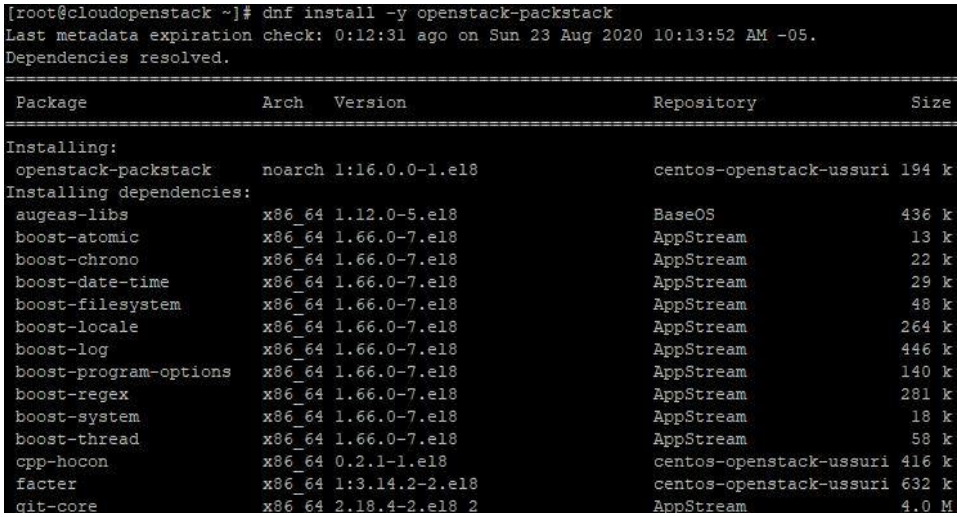
El entorno utilizado cumplirá con las siguientes características.

1. Red pública (red IP flotante): 192.168.100.8/24
2. Red interna: solo conexión física (eth1)
3. IP del controlador público: 192.168.50.2 (eth0)
4. IP de cómputo público: 192.168.50.3 (eth0)

En primera instancia se accedió con el usuario root para realizar la actualización del sistema operativo. Posteriormente se aplicó Hardening a los servidores, tal como se muestra en el Anexo 5.

Posteriormente se habilitó los repositorios rdo usando el comando yum install https://www.rdoproject.org/repos/rdo-release.rpm.

Se procedió a instalar el paquete PackStack a nivel del controlador, el cual representa una utilidad que facilita la implementación en múltiples nodos para diferentes componentes de OpenStack a través de conexiones SSH y módulos Puppet.

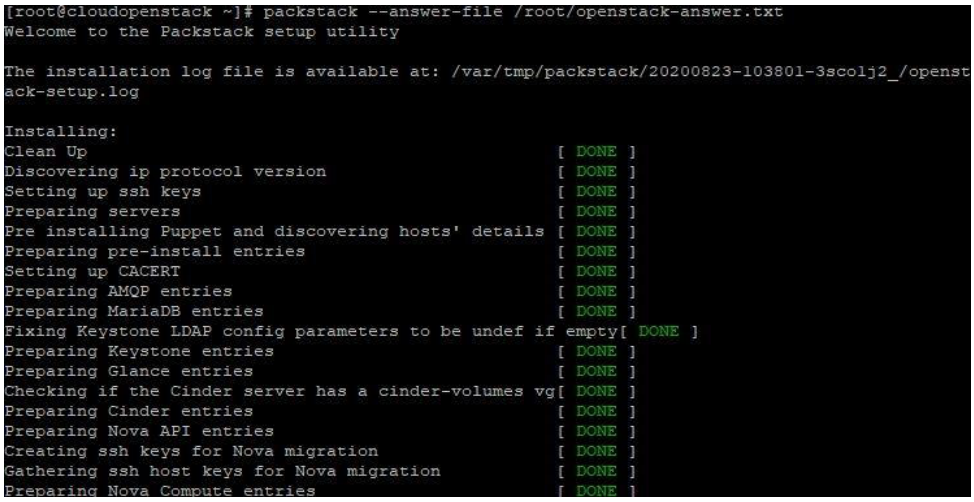


```
[root@cloudopenstack ~]# dnf install -y openstack-packstack
Last metadata expiration check: 0:12:31 ago on Sun 23 Aug 2020 10:13:52 AM -05.
Dependencies resolved.
================================================================================
 Package                Arch   Version                     Repository          Size
================================================================================
Installing:
 openstack-packstack    noarch 1:16.0.0-1.el8              centos-openstack-ussuri 194 k
Installing dependencies:
 augeas-libs            x86_64 1.12.0-5.el8                BaseOS              436 k
 boost-atomic           x86_64 1.66.0-7.el8                AppStream            13 k
 boost-chrono           x86_64 1.66.0-7.el8                AppStream            22 k
 boost-date-time        x86_64 1.66.0-7.el8                AppStream            29 k
 boost-filesystem       x86_64 1.66.0-7.el8                AppStream            48 k
 boost-locale           x86_64 1.66.0-7.el8                AppStream           264 k
 boost-log              x86_64 1.66.0-7.el8                AppStream           446 k
 boost-program-options  x86_64 1.66.0-7.el8                AppStream           140 k
 boost-regex            x86_64 1.66.0-7.el8                AppStream           281 k
 boost-system           x86_64 1.66.0-7.el8                AppStream            18 k
 boost-thread           x86_64 1.66.0-7.el8                AppStream            58 k
 cpp-hocon              x86_64 0.2.1-1.el8                 centos-openstack-ussuri 416 k
 facter                 x86_64 1:3.14.2-2.el8              centos-openstack-ussuri 632 k
 git-core               x86_64 2.18.4-2.el8_2              AppStream           4.0 M
```

Figura 2.5 Instalación del paquete packstack

Fuente: Elaborado por el autor

Posteriormente se procedió a generar un archivo de respuesta para la instalación automatizada de packstack a nivel del nodo del controlador.

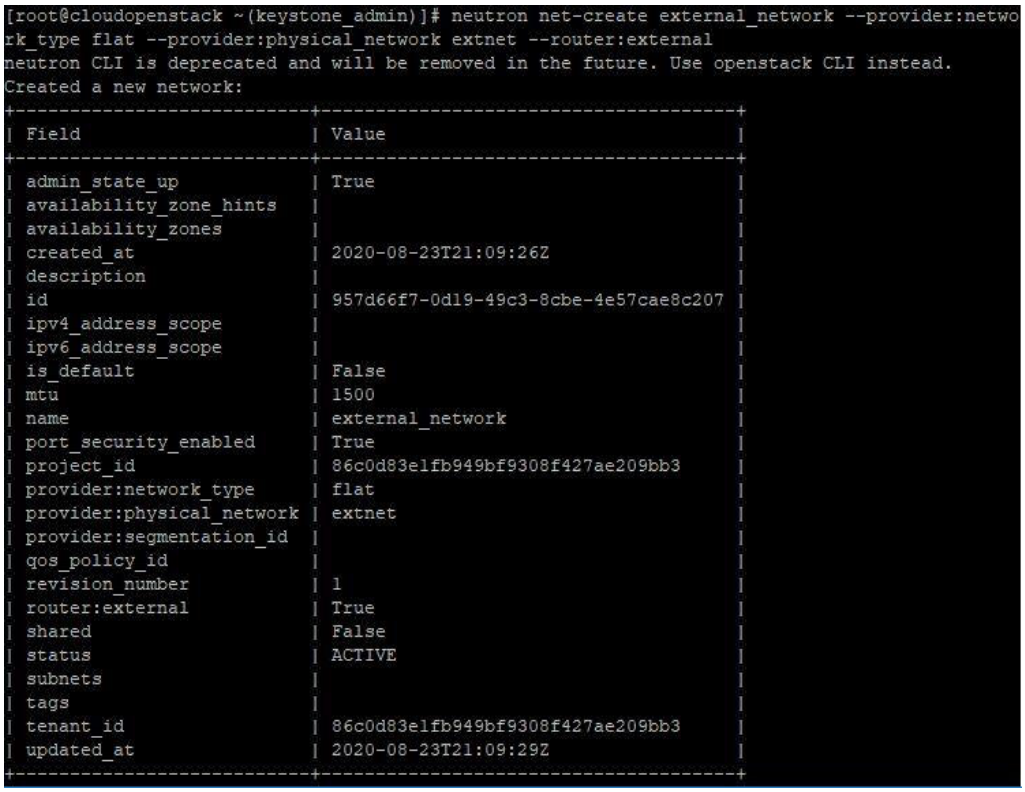


```
[root@cloudopenstack ~]# packstack --answer-file /root/openstack-answer.txt
Welcome to the Packstack setup utility

The installation log file is available at: /var/tmp/packstack/20200823-103801-3scolj2_/openst
ack-setup.log

Installing:
Clean Up                                             [ DONE ]
Discovering ip protocol version                      [ DONE ]
Setting up ssh keys                                  [ DONE ]
Preparing servers                                    [ DONE ]
Pre installing Puppet and discovering hosts' details [ DONE ]
Preparing pre-install entries                        [ DONE ]
Setting up CACERT                                    [ DONE ]
Preparing AMQP entries                               [ DONE ]
Preparing MariaDB entries                            [ DONE ]
Fixing Keystone LDAP config parameters to be undef if empty[ DONE ]
Preparing Keystone entries                           [ DONE ]
Preparing Glance entries                             [ DONE ]
Checking if the Cinder server has a cinder-volumes vg[ DONE ]
Preparing Cinder entries                             [ DONE ]
Preparing Nova API entries                           [ DONE ]
Creating ssh keys for Nova migration                 [ DONE ]
Gathering ssh host keys for Nova migration           [ DONE ]
Preparing Nova Compute entries                       [ DONE ]
```

Figura 2.6 Generación de archivo packstack

Fuente: Elaborado por el autor

Posterior a la instalación de Openstack se procedió a crear las redes y las diferentes interfaces a nivel del nodo controlador, tal como se muestra en la figura 2.7.



```
[root@cloudopenstack ~(keystone_admin)]# neutron net-create external_network --provider:netwo
rk_type flat --provider:physical_network extnet --router:external
neutron CLI is deprecated and will be removed in the future. Use openstack CLI instead.
Created a new network:
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | True                                 |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2020-08-23T21:09:26Z                 |
| description               |                                      |
| id                        | 957d66f7-0d19-49c3-8cbe-4e57cae8c207 |
| ipv4_address_scope        |                                      |
| ipv6_address_scope        |                                      |
| is_default                | False                                |
| mtu                       | 1500                                 |
| name                      | external_network                     |
| port_security_enabled     | True                                 |
| project_id                | 86c0d83e1fb949bf9308f427ae209bb3     |
| provider:network_type     | flat                                 |
| provider:physical_network | extnet                               |
| provider:segmentation_id  |                                      |
| qos_policy_id             |                                      |
| revision_number           | 1                                    |
| router:external           | True                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   |                                      |
| tags                      |                                      |
| tenant_id                 | 86c0d83e1fb949bf9308f427ae209bb3     |
| updated_at                | 2020-08-23T21:09:29Z                 |
+---------------------------+--------------------------------------+
```

Figura 2.7 Creación de Interfaces de Redes

Fuente: Elaborado por el autor

Finalmente se deberá acceder al portal de administración, donde se deberá iniciar sesión en el Panel de OpenStack, para el posterior despliegue de las máquinas virtuales.

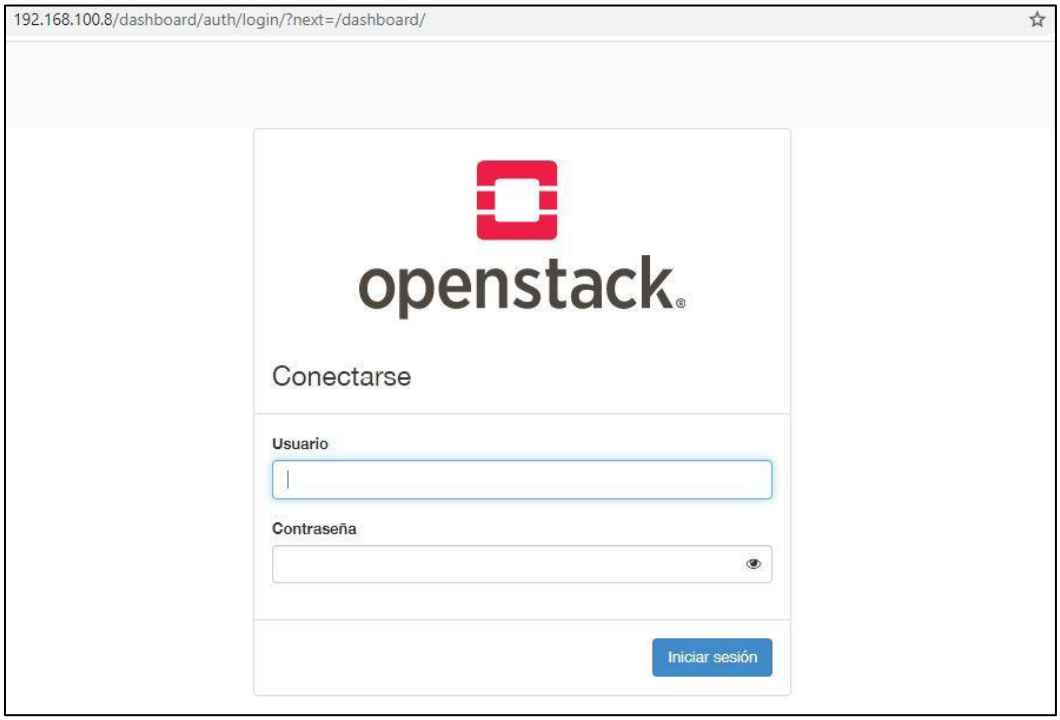


Figura 2.8 Creación de Llaves de Seguridad

Fuente: Elaborado por el autor

2.4.6 CREACIÓN DE MÁQUINA VIRTUALES

En primera instancia se deberá ingresar al portal, dirigirse hacia el menú superior Ir a Console > Computing > Elastic Cloud Server, posterior se le deberá un clic en Apply for ECS y elegir el tipo de sistema operativo requerido para el despliegue del servidor, tal como se muestra en la figura 2.9.

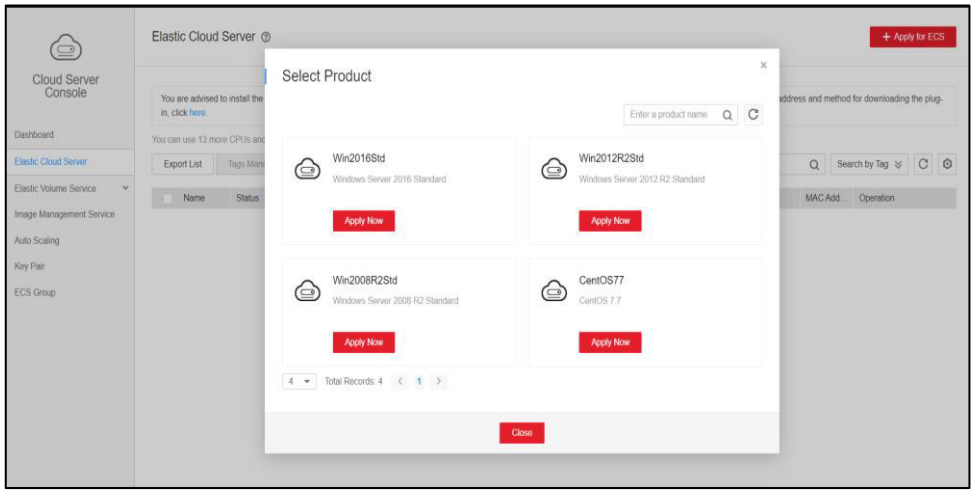


Figura 2.9 Elección de Sistema Operativo

Fuente: Elaborado por el autor

Posteriormente, se deberá ingresar la información básica necesaria, tal como la especificación del vCPUs, Memory RAM, capacidad de almacenamiento, configuración de red y finalmente el tipo de seguridad, tal como se muestran en la figura 2.10 y 2.11 respectivamente.

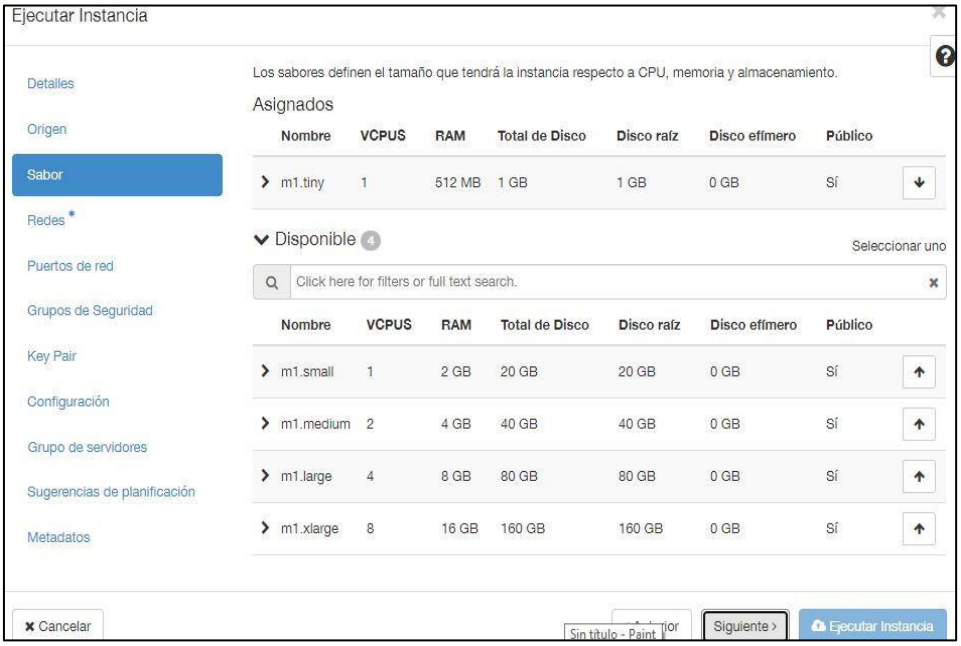


Figura 2.10 Elección de capacidad de cómputo

Fuente: Elaborado por el autor

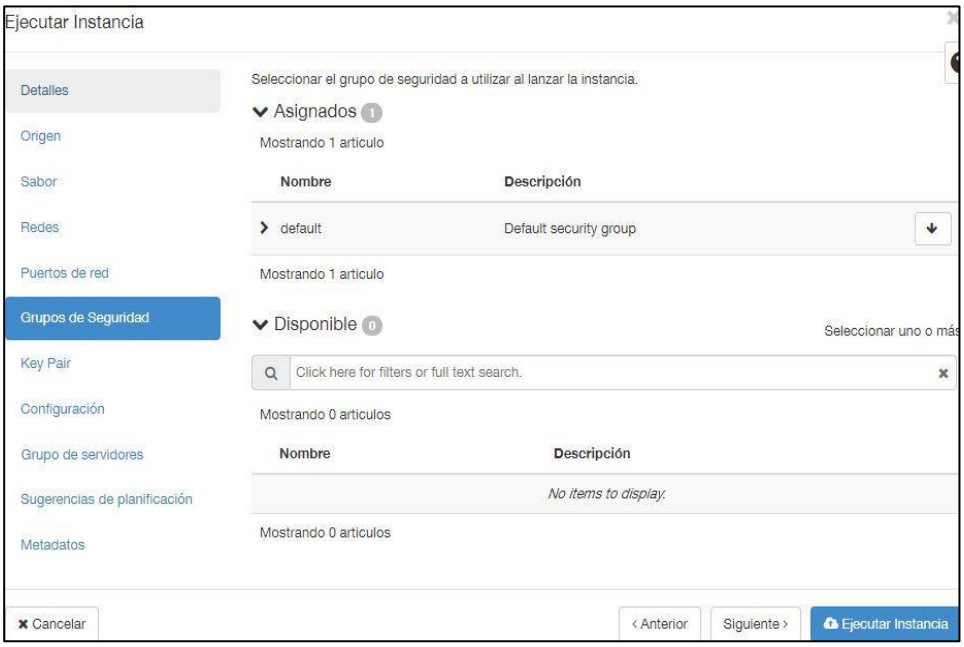


Figura 2.11 Creación de Politicas de Seguridad

Fuente: Elaborado por el autor

El paso final previo a la creación del servidor, será la generación de la llave pública y privada para el acceso al servidor, mediante escritorio remoto o consola ssh.

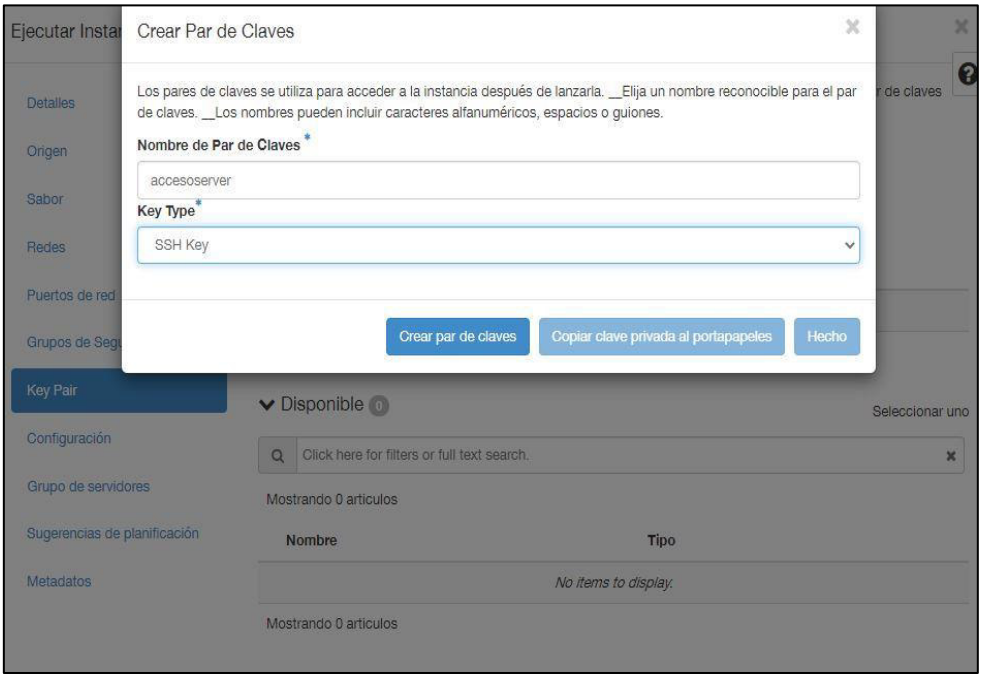


Figura 2.12 Creación de Llaves de Seguridad

Fuente: Elaborado por el autor

2.5 ESTABILIZACIÓN DE LA SOLUCIÓN

El área de Datacenter & Cloud monitorearon los servicios durante 48 horas posterior al despliegue de la arquitectura multitenant, los cuales no presentaron novedades en el rendimiento funcional.

Durante la semana de estabilización, el standby de Datacenter & Cloud asistió dos horas antes del ingreso a su jornada laboral, esto con el objetivo

de solventar inconvenientes que pudieran presentarse sobre la plataforma, mismos que no hubo en ningún elemento de la arquitectura.

2.6 DOCUMENTACIÓN

El servicio desplegado es de mucha criticidad debido a que alojará ambientes productivos, por lo cual, se creó la siguiente documentación para socializarla con las áreas complementarias.

1. Guía de Planeación e Instalación de la solución (hardware y software) describiendo todas las especificaciones y requerimientos necesarios usados en la implementación.
2. Análisis de Riesgos detectados.
3. Inventario detallado (descripciones y datos de identificación) de componentes necesarios para la solución Hardware, software, licencias y lista de materiales.
4. Actualizaciones de software y firmware a la última versión disponible soportada, compatible y estable.
5. Manuales de referencia, operación y administración de los productos.
6. Anexos con los seriales e identificadores los componentes bajo contrato, que sean necesarios para reportar eventualidades,

tramitar licencias, registrar y acceder a todos los sistemas de consulta del proveedor disponibles para sus clientes.

7. Plan de crecimiento.
8. Manuales de entrenamiento en formato electrónico.
9. Sesiones de transferencia de conocimiento.

CAPÍTULO 3

EVALUACIÓN DE RESULTADOS

3.1 MONITOREO DE LA ARQUITECTURA CLOUD IAAS

Posterior a la implementación del ambiente Cloud IaaS, se validó que los recursos de cómputo y almacenamiento se encuentren disponibles para la asignación, en los nuevos despliegues de máquinas virtuales, tal como se muestra la figura 3.1. Adicionalmente, se monitoreó cada uno de los componentes que forman parten integral del proyecto.

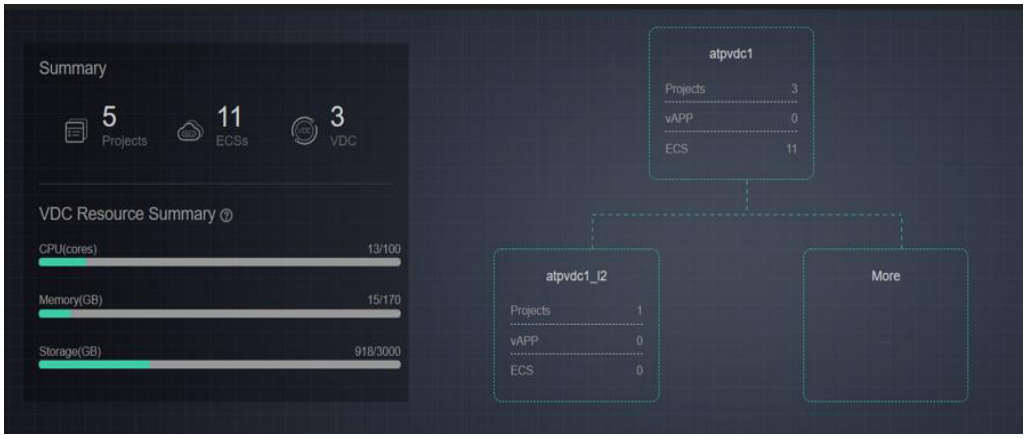


Figura 3.1 Recursos de cómputo y almacenamiento

Fuente: Elaborado por el autor

Los monitoreos se ejecutaron con frecuencia y por cada nuevo cliente se enviaba un mail a las áreas de preventa, indicando la capacidad disponible y utilizada, con el objetivo puedan hacer estimaciones de cómputo y almacenamiento, en base a la capacidad existente, tal como se pueden observar en la figura 3.2 y 3.3 respectivamente.

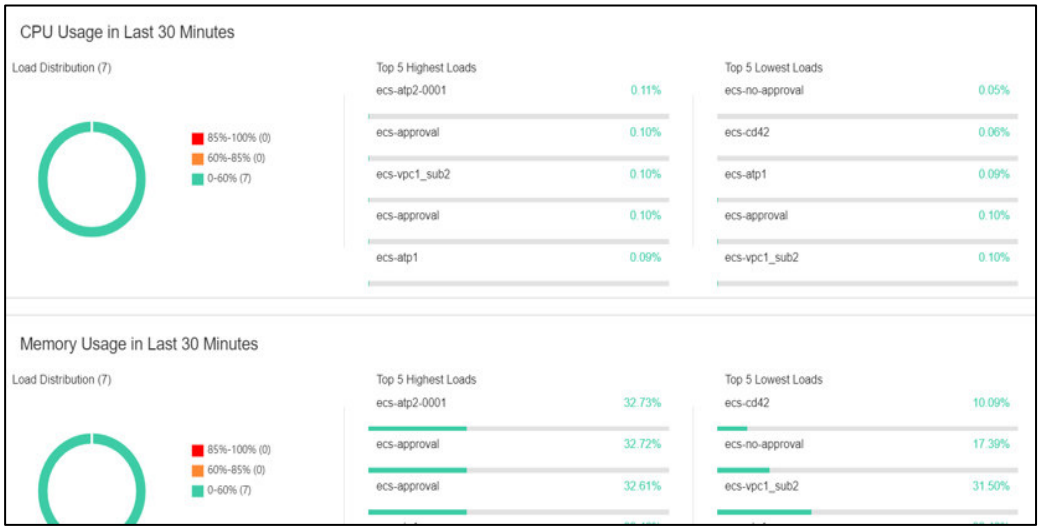


Figura 3.3 Disponibilidad de Cómputo

Fuente: Elaborado por el autor

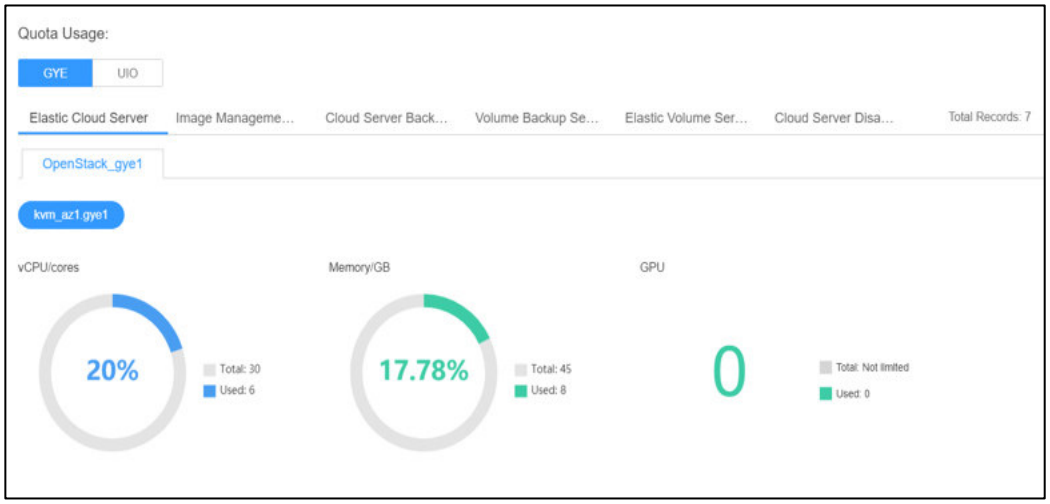


Figura 3.4 Utilización de procesamiento

Fuente: Elaborado por el autor

En paralelo también se revisó el estado del cluster de seguridad lógica, los cuales no sufrieron ninguna indisponibilidad del servicio, las interfaces de red quedaron habilitadas durante todo el despliegue, manteniendo la disponibilidad del servicio. Adicionalmente, se verificó los niveles de procesamiento posterior al despliegue de la solución, tal como se muestran en la figura 3.4 y 3.5 respectivamente.

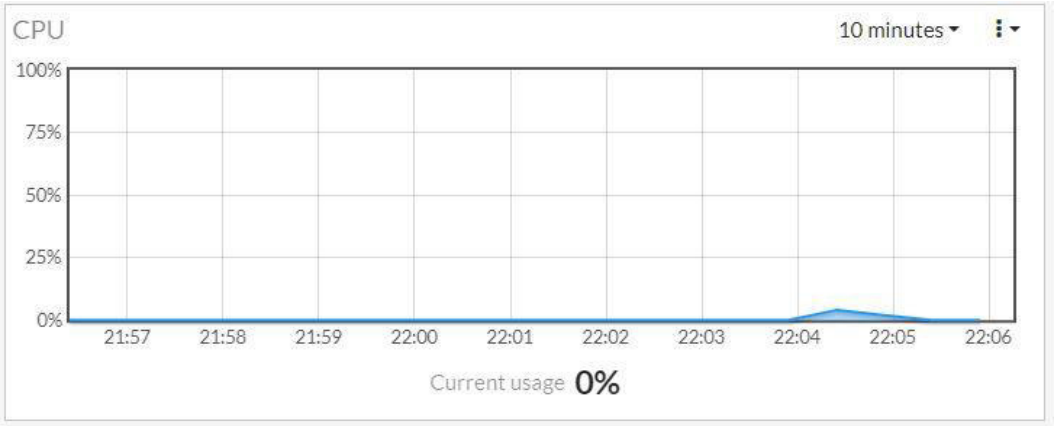


Figura 3.4 Utilización de CPU FG 300E

Fuente: Elaborado por el autor

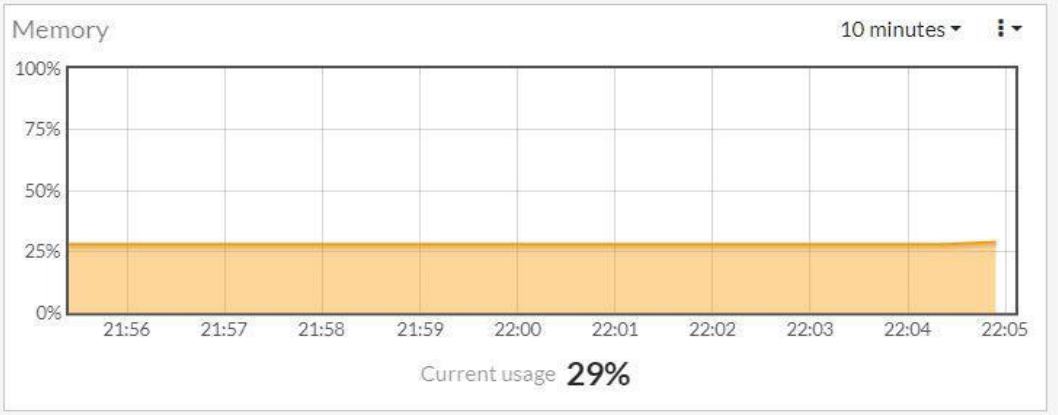


Figura 3.5 Utilización de memoria RAM FG 300E

Fuente: Elaborado por el autor

Desde el portal de administración del elemento de seguridad se monitoreó el nivel de tráfico, los paquetes permitidos y descartados, esto con el objetivo de comprobar accesos no autorizados a la arquitectura Cloud IaaS.

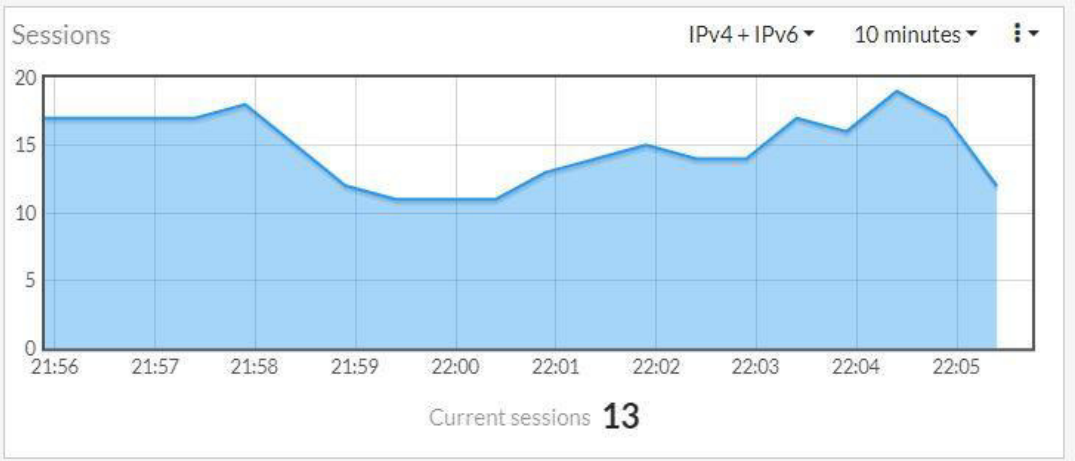


Figura 3.6 Sesiones Concurrentes FG 300E

Fuente: Elaborado por el autor

Finalmente se aplicó una tarea programada para ejecutar un respaldo semanal de la configuración del Firewall. Cabe mencionar que el respaldo es diferencial e incluye los logs de todos los eventos capturados por el Firewall.

3.2 BENEFICIOS DE LA SOLUCIÓN

El despliegue de la solución Cloud IaaS proporcionaron los siguientes beneficios para los clientes corporativos.

1. Agregación de servidores virtuales, modificación dinámica en la configuración de CPU virtuales, Memoria RAM y almacenamiento.
2. Ahorro de costos, debido que los clientes sólo pagarán por los recursos que utilizan.
3. Otorga al cliente absoluto control y autonomía en el despliegue y gestión de su infraestructura virtualizada
4. Gestión autónoma en la configuración de los Servidores Virtuales, debido a que se los puedes reiniciar, pausar, detener, tomar snapshots y agregar discos de almacenamiento.
5. Asistencia de especialistas en la nube las 24 horas, los 365 días del año.
6. Programa de respaldos automatizado, el cual permite realizar tareas administrativas en cualquier momento.

Posterior a la implementación del ambiente Cloud, la empresa obtuvo beneficios tales como.

1. Aumento de ingresos en soluciones bajo la modalidad de Cloud IaaS.
2. Reducción de espacio en la instalación de equipamiento físico.
3. Disminución de Capex.
4. Optimización en la administración de la plataforma.
5. Mayor eficiencia en el Delivery o entrega del servicio.

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones y recomendaciones son el resultado del despliegue realizado, con proyecciones a garantizar la estabilidad y escalabilidad de la arquitectura.

CONCLUSIONES

1. Se realizó el diseño de una infraestructura basada en nodos hyperconvergentes para el despliegue de una arquitectura Cloud IaaS, la cual generó entrega de servicios en la nube más eficientes y competitivos, apostando por la innovación y la generación de ofertas orientadas al desarrollo de nuevas soluciones bajo modelos de cloud computing.

2. Se obtuvo mayores ingresos por el despliegue de la solución, debido al aumento de clientes, quienes argumentaron que este tipo de solución les permitió disminuir su grado de riesgo ante eventos no deseados, garantizando la continuidad del negocio y asegurando la disponibilidad de los activos de información tecnológica, además redujeron costos de capex.

3. La implementación de la Arquitectura Cloud IaaS fue exitosa, y tuvo un impacto positivo dentro de la organización, logrando así, que se ejecute un proyecto transversal, que permita migrar al menos un 60% de las cargas de trabajo alojadas en servidores físicos, hacia ambientes virtuales.

RECOMENDACIONES

1. Desarrollar APIs de comunicación que se integren con servicios de nubles públicas, tales como AWS, Azure y GCP.
2. Habilitar mecanismos de conectividad que permitan a los clientes corporativos, usar conexiones de tipo LAN extendida.
3. Implementar mecanismos de balanceo de carga a nivel aplicacional y conectividad.
4. Desplegar una arquitectura con similares prestaciones en un sitio alterno, con el objetivo de proveer un servicio de recuperación ante desastres.
5. Incluir a los nodos de cómputo, hardware certificado por SAP para alojar cargas de base de datos Hana.
6. Permitir migración de cargas de trabajo entre ambientes onpremise.
7. Implementar mecanismos para poder importar instancias virtuales basadas en formatos OVA, VMDK o VHD.
8. Permitir al usuario configurar nombres de dominios tales como, .com.ec, .com, .net, .org, .info, .biz, .website, .club y .me.
9. Permitir el despliegue de contenedores de aplicación para aplicaciones empresariales.

BIBLIOGRAFÍA

[1] VMware, Suite de Soluciones, Definición de VMware, https://www.vmware.com/solutions/virtualization.html, fecha de consulta: septiembre de 2020

[2] KVM, Virtualización, Definición de KVM, https://www.redhat.com/en/topics/virtualization/what-is-KVM, fecha de consulta: septiembre de 2020

[3] HyperV, Tecnología de Virtualización, Definición de HyperV https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview, fecha de consulta: septiembre de 2020

[4] Networkworld, Infraestructura Hyperconvergente, Definición de Hyperconvergencia, https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview, fecha de consulta: septiembre de 2020

[5] zdnet, Importancia y Funcionamiento Hyperconvergente, Definición de Hyperconvergencia, https://www.zdnet.com/article/what-hyperconvergence-is-how-it-works-and-why-it-matters/, fecha de consulta: septiembre de 2020.

[6] Techtarget, Cloud Computing, Definición de IaaS, https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS, fecha de consulta: septiembre de 2020

[7] Azure, Infrastructure as a service, Definición de IaaS, https://azure.microsoft.com/en-us/overview/what-is-iaas/, fecha de consulta: septiembre de 2020

[8] Techopedia, Seguridad, Definición de Antispam, https://www.techopedia.com/definition/1629/anti-spam, fecha de consulta: septiembre de 2020

[9] Todmephis, Hardening Centos 7, https://gist.github.com/todmephis/9160c693b115dca4b6be73fd2b176458, fecha de consulta: septiembre de 2020

[10] Openstack, Software, https://www.openstack.org/software/, fecha de consulta: octubre de 2020

[11] Openstack, Software, https://www.openstack.org/software/project-navigator/openstack-components#openstack-services, fecha de consulta: octubre de 2020

[12] Online Solutions Configurator, Solution Configurator, https://www.delltechnologies.com/partner/es-ec/auth/sales/solution-configurator.htm, fecha de consulta: octubre de 2020

[13] Deals Register, Solution Configurator, https://www.dell.com/solutions/configurator/EC/EN/g_20/LA/osc/your-solutions, fecha de consulta: octubre de 2020

[14] Center for Internet Security, CIS Benchmarks Hardening Red Hat 7, https://www.cisecurity.org/cis-benchmarks/, fecha de consulta: octubre de 2020

[15] Security Through System Integrity, CIS Benchmarks Hardening Red Hat 7, https://www.newnettechnologies.com/, fecha de consulta: octubre de 2020

GLOSARIO

VMware es un hipervisor que se ejecuta en arquitecturas x86 de los sistemas operativos Windows y Linux, el cual permite a los usuarios desplegar máquinas virtuales (VM) sobre una sola máquina física. [1]

KVM es una tecnología de virtualización de código abierto integrada en Linux, que permite que una máquina física ejecute múltiples entornos virtuales aislados llamados máquinas virtuales (VM). [2]

HyperV es el producto de virtualización de hardware de Microsoft, el cual permite crear y ejecutar una versión de software de una computadora, llamada máquina virtual. [3]

Hypercongencia combina computación, almacenamiento y redes en un solo hardware. [4], [5]

IaaS proporciona recursos de cómputo y almacenamiento virtualizados, los cuales son aprovisionados y administrados a través de Internet o un enlace de comunicación de datos. [6], [7]

Antispam es un servicio que bloquea y mitigar los efectos de correos electrónicos ilegales, o spam, en los usuarios de correo electrónico. [8]

ANEXOS

ANEXO 1: LISTA DE MATERIALES NODOS DE CÓMPUTO

Descripción	Número de Parte	Cantidad
VxRail S570, 14x3.5"	210-APXN	4
S570 Branding	325-BCVX	4
PSNT Info	329-BDWH	4
Dell Hardware Limited Warranty Initial Year	819-0973	4
ProSupport Mission Critical 4-Hour 7X24 On-Site Service 60 Months	819-11XX	4
ProSupport Mission Critical: 7X24 HW Tech Support and Assistance, 60 Months	819-1149	4
ProSupport Mission Critical 4H 7X24 On-Site Service, 60 Months Extended	819-11XX	4
Thank you choosing Dell ProSupport. For tech support, visit //support.dell.com/ProSupport	911-6619	4
Dell Limited Hardware Warranty Extended	975-3461	4
US Order	332-1286	4
HCI System Software as part of VxRail	379-BDYQ	4
ProDeploy Plus Training Credits 200 Redeem at education.dellemc.com Expires 1Yr from Order Date	812-4548	4
ProDeploy Plus Dell EMC VxRail Deployment	819-2554	4
ProDeploy Plus Dell EMC VxRail Deployment Verfication	819-2555	4
ProSupport Mission Critical, vSAN, Standard, 1 Processor, 39 Months	823-4440	8
VxRail VMware, vSAN Standard, 3 Years	634-BSJR	8
VxRail VMware vSphere Standard for 1 processor, 5 Years	634-BRIP	8
60 Months, ProSupport With Mission Critical, Software Support	819-1439	4
VxRail Hyper Converged OS, Capacity Drive 4.0TB HDD	634-BSKU	20
VxRail HCI System Software Hybrid, S	634-BSQI	8
LKEY,SW,EMC,RES,5YR	634-BSKK	4

Descripción	Número de Parte	Cantidad
ProSupport Mission Critical, vSphere Standard, 1 processor (no vRAM limitation for EOEM use), 60 Months	819-7468	8
VxRail S570 Shipping	340-BYVW	4
PowerEdge R740 CE, CCC, BIS Marking	389-DSWP	4
Riser Config 1, 4 x8 slots	330-BBKE	4
Intel X710 Quad Port 10GbE SFP+, rNDC	555-BCKP	4
iDRAC9,Enterprise	385-BBKT	4
Chassis with up to 12 x 3.5" HDDs on BP, 4 x 3.5" HDDs on MP and 2 x 3.5" HDDs Flexbay, 1 and 2CPU Configuration	321-BCPV	4
6 Performance Fans forR740/740XD	384-BBPZ	4
VxRail P/V/S 570 Bezel	350-BBNR	4
Performance BIOS Settings	384-BBBL	4
No Energy Star	387-BBEY	4
UEFI BIOS Boot Mode with GPT Partition	800-BBDM	4
VxRail S570 Luggage Tag	350-BBNX	4
PowerEdge R740/R740XD Motherboard	329-BEIK	4
No RAID for S570	780-BCJB	4
HBA330 Controller, 12Gbps Mini card	405-AANV	4
IDSDM and Combo Card Reader	385-BBLE	4
Intel Xeon Gold 5218R 2.1G, 20C/40T, 10.4GT/s, 27.5 M Cache, Turbo, HT (125W) DDR4-2666	338-BVKJ	4
Intel Xeon Gold 5218R 2.1G, 20C/40T, 10.4GT/s, 27.5 M Cache, Turbo, HT (125W) DDR4-2666	338-BVKJ	4
Additional Processor Selected	379-BDCO	4
32GB RDIMM, 3200MT/s, Dual Rank	370-AEVN	48
3200MT/s RDIMMs	370-AEVR	4
Performance Optimized	370-AAIP	4
4TB 7.2K 12Gbps 512n 3.5in Hot-plug Hard Drive	400-ASHY	20
1.6TB SSD SAS Mix Use 12Gbps 512 2.5in Flex Bay AG Drive,3.5 HYB CARR, 3 DWPD, 8760 TBW	400-AZQW	4
No Trusted Platform Module	461-AADZ	4
VxRail Small Form Factor Pluggable Cable Kit	470-ACPE	4

Descripción	Número de Parte	Cantidad
No Systems Documentation, No OpenManage DVD Kit	631-AACK	4
ReadyRails Sliding Rails With Cable Management Arm	770-BBBR	4
Dual, Hot-plug, Redundant Power Supply (1+1), 1100W	450-ADWM	4
Power Cord - C13, 3M, 125V, 15A (North America, Guam, North Marianas, Philippines, Samoa, Vietnam)	450-AALV	8
C13 to C14, PDU Style, 12 AMP, 6.5 Feet (2m) Power Cord, North America	492-BBDI	8
Dell EMC PowerEdge SFP+ SR Optic 10GbE 850nm	407-BCBE	8
Redundant SD Cards Enabled	385-BBCF	4
64GB microSDHC/SDXC Card	385-BBKI	4
64GB microSDHC/SDXC Card	385-BBKI	4
VxRail E/P/V/S Hardware Component Firmware Lock	384-BCIM	4
VxRail Software 4.7.300 Factory Install	634-BUWB	4
HCIA RecoverPoint for VMWare for 1 node	634-BRLY	4
DHCP with Zero Touch Configuration	379-BCRB	4
PowerEdge R740 Shipping Material	343-BBFG	4
iDRAC Group Manager, Disabled	379-BCQY	4
iDRAC,Legacy Password	379-BCRF	4
No Quick Sync	350-BBJV	4
BOSS controller card + with 2 M.2 Sticks 240G (RAID 1) LP	403-BBRU	4
DIMM Blanks for System with 2 Processors	370-ABWE	4
1U Pipe Low Profile Heatsink	412-AAIP	4
1U Pipe Low Profile Heatsink	412-AAIP	4

ANEXO 2: LISTA DE MATERIALES SEGURIDAD LÓGICA

Descripción	Número de Parte	Cantidad
18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 16 x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2x 240GB onboard SSD storage.	FG-301E	2
Hardware plus ASE FortiCare and FortiGuard 360 Protection	FG-301E-BDL-817-36	2
Hardware plus 24x7 FortiCare and FortiGuard Enterprise Protection	FG-301E-BDL-811-36	2
Hardware plus 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	FG-301E-BDL-950-36	2
360 Protection (ASE FortiCare plus App Ctrl, IPS, AMP, Web Filtering, AS, Security Rating, IoT Detection, SD-WAN Orchestrator/Cloud Monitoring/Overlay Ctrl VPN, FMG/FAZ/IPAM Cloud, Industrial Security and FortiConverter Svc)	FC-10-00307-817-02-36	2
Enterprise Protection (24x7 FortiCare plus Application Control, IPS, AMP, Web Filtering, Antispam, IoT Detection, Industrial Security, Security Rating, and FortiConverter Svc)	FC-10-00307-811-02-35	2
Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AMP, Web Filtering and Antispam Service)	FC-10-00307-950-02-36	2
Advanced Threat Protection (24x7 FortiCare plus Application Control, IPS and AMP Service)	FC-10-00307-928-02-36	2
FortiGate Cloud Management, Analysis and 1 Year Log Retention	FC-10-00307-131-02-36	2
FortiGuard Advanced Malware Protection (AMP) including Antivirus, Mobile Malware and FortiGate Cloud Sandbox Service	FC-10-00307-100-02-36	2
FortiGuard IPS Service	FC-10-00307-108-02-36	2
FortiGuard Web Filtering Service	FC-10-00307-112-02-36	2

Descripción	Número de Parte	Cantidad
FortiGuard Industrial Security Service	FC-10-00307-159-02-36	2
FortiGuard Security Rating Service	FC-10-00307-175-02-36	2
IoT Detection Service	FC-10-00307-231-02-36	2
FortiIPAM Cloud Service	FC-10-00307-233-02-36	2
SD-WAN Cloud Assisted Monitoring: Cloud-based SD-WAN Bandwidth & Quality Monitoring Service	FC-10-00307-288-02-36	2
SD-WAN Overlay Controller VPN Service: Cloud-based SD-WAN VPN Overlay Service & Portal	FC-10-00307-289-02-36	2
SD-WAN Orchestrator Entitlement License	FC-10-00307-319-02-36	2
FortiManager Cloud: Cloud-based Central Management & Orchestration Service	FC-10-00307-179-02-36	2
FortiAnalyzer Cloud: Cloud-based Events and Security Log Monitoring including IOC Service	FC-10-00307-188-02-36	2
FortiConverter Service for one time configuration conversion service	FC-10-00307-189-02-36	2
24x7 FortiCare Contract	FC-10-00307-247-02-36	2
ASE FortiCare (24x7 plus Advanced Services Ticket Handling)	FC-10-00307-284-02-36	2
Next Day Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-00307-210-02-36	2
4-Hour Hardware Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-00307-211-02-36	2
4-Hour Hardware and Onsite Engineer Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-00307-212-02-36	2
Secure RMA Service	FC-10-00307-301-02-36	2

ANEXO 3: LISTA DE MATERIALES SWITCHES SAN

Descripción	Número de Parte	Cantidad
CTX DS-6610B 8P/24P switch w/rear to front airflow (Includes 8x16Gb SFPs + rack kit)	210-ASSS	2
Dell Hardware Warranty Initial Year	825-2364	2
ProSupport Mission Critical: 4-Hours 7X24 On-Site Service with Emergency Dispatch, 30 Months	825-2369	2
ProSupport Mission Critical: 4-Hours 7X24 On-Site Service with Emergency Dispatch, 60 Months Ext	825-2373	2
ProSupport Mission Critical: 7X24 HW/SW Technical Support and Assistance, 60 Months	825-2396	2
Thank you choosing Dell Pro Support	911-6619	2
Dell Limited Hardware Warranty Extended Year(s)	975-3461	2
ProDeploy Plus Training Credits 300 Redeem at education.dellemc.com Expires 1Yr from Order Date	812-4549	2
ProDeploy Plus Connectrix Fibre Channel Switch Deployment (up to 4 new hosts)-LA	825-3439	2
ProDeploy Plus Connectrix Fibre Channel Switch Deployment Verification (up to 4 new hosts)-LA	825-3440	2
C13 to C14, PDU Style, 10 AMP, 13 Feet (4m) Power Cord, Argentina	450-ACSO	4

ANEXO 4: LISTA DE MATERIALES SWITCHES INFINIBAND

Descripción	Número de Parte	Cantidad
Switch IB QDR 8 Port 1PS 1U-half width	210-AVYW	4
PWRCRD,2,IEC320 C14-C13,208V UNIVERSAL	450-AJMB	4
5 Years ProSupport and Mission Critical 4Hr Onsite Service-LA	8037, 836-8091	4

ANEXO 5: HARDENING APLICADO A NODOS DE CÓMPUTO

```
#!/bin/bash
#Kevin Intriago
MODPROBEFILE="/etc/modprobe.d/CIS.conf"
MODPROBEFILE2="/etc/modprobe.d/usb_storage.conf"
ANSWER=0

#1.1 Filesystem Configuration
analyze_part () {
        if [ "$#" != "1" ]; then
                options="$(echo $@ | awk 'BEGIN{FS="[()]"}{print $2}')"
        echo "[+]$@"
        apply_part_rule $1usb

        else
                echo "[-]\"$1\" not in separated partition. Check section \"1.1
Filesystem Configuration\" in CIS Benchmark."
        fi
}

apply_part_rule (){
        if [ "$1" == "/tmp" ]; then
                suggested="nodev nosuid noexec"
                echo "Suggested rule: $suggested"
                prompt "Do you want to apply suggested rule?"
                if [ "$ANSWER" == "1" ]; then
                        cat                >                /etc/systemd/system/local-
fs.target.wants/tmp.mount << "EOF"
                        [Mount]
                        Options=mode=1777,strictatime,noexec,nodev,nosuid
EOF
                        mount -o remount,nodev,nosuid,noexec /tmp
                        mount | grep /tmp | awk '{print $6}'
                        echo "[+]Rule applied"
                elif [ "$1" == "-1" ]; then
                        echo "[-]No rule applied"
                fi
        elif [ "$1" == "/var/tmp" ]; then
                suggested="nodev nosuid noexec"
                echo "Suggested rule: $suggested"
                prompt "Do you want to apply suggested rule?"
                if [ "$ANSWER" == "1" ]; then
```

```
                        echo YES
                elif [ "$1" == "-1"]; then
                        echo NO
                fi
        elif [ "$1" == "/dev/shm" ]; then
                suggested="nodev nosuid noexec"
                echo "Suggested rule: $suggested"
                prompt "Do you want to apply suggested rule?"
                if [ "$ANSWER" == "1" ]; then
                        echo YES
                elif [ "$1" == "-1" ]; then
                        echo NO
                fi
        elif [ "$1" == "/home" ]; then
                suggested="nodev"
                echo "Suggested rule: $suggested"
                prompt "Do you want to apply suggested rule?"
                if [ "$ANSWER" == "1" ]; then
                        echo YES
                elif [ "$1" == "-1" ]; then
                        echo NO
                fi
        fi
}

prompt (){
        while true; do
           read -p "$1 [Y/n] " input
           case $input in
              [Yy]* ) ANSWER=1; break;;
              [Nn]* ) ANSWER=-1; break;;
              * ) echo "Invalid input...";;
           esac
        done
}
prompt "Do you want to update system before continuing?"
if [ "$ANSWER" == "1" ]; then
        yum update
        echo "[+]Done"
fi
echo -e "\n[1]Initial Setup\n"
echo "Disable unused filesystems:"
cat > $MODPROBEFILE << "EOF"
install udf /bin/true
```

```
install vfat /bin/true
install cramfs /bin/true
install freevxfs /bin/true
install jffs2 /bin/true
install hfs /bin/true
install hfsplus /bin/true
install squahfs /bin/true
EOF

cat > $MODPROBEFILE2 << "EOF"
install usb-storage /bin/true
EOF

echo Following rules has been added to $MODPROBEFILE
echo Following rules has been added to $MODPROBEFILE2
cat $MODPROBEFILE
cat $MODPROBEFILE2
echo "[+]Done"

echo "Partition Check:"
particiones=(/tmp /var /var/tmp /var/log /var/log/audit /home /dev/shm)
for particion in ${particiones[*]}; do
        out="$(mount | grep $particion)"
        analyze_part $particion $out
done

#1.2 Configure Software Updates
out="$(df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type
d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null)"
if [ -z "$out"  ]; then
        echo "[+]Pass"
else
        echo "[-]Error"
                echo "[+]Done"
        fi
fi
echo "Automounting disabled?"
out="$(systemctl is-enabled autofs)"
if [ "$out" == "disabled" ]; then
        echo "[+]Pass"
else
        echo "[-]Error"
        prompt "What to fix it?"
        if [ "$ANSWER" == "1" ]; then
```

```
                systemctl disable autofs
                echo "[+]Done"
        fi
fi
prompt "Show repo list?"
if [ "$ANSWER" == "1" ]; then
        yum repolist
        echo "[+]Done"
fi
echo "GPG Keys are configured"
out="$(rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} -->
%{summary}\n')"
if [ "$out" == "package gpg-pubkey is not installed" ]; then
        echo "[-]Error"
else
        echo "[+]Pass"
fi

echo "Gpgcheck \"yum.conf\""
out="$(grep ^gpgcheck /etc/yum.conf)"
if [ "$out" == "gpgcheck=1" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: Please edit \"/etc/yum.conf\" and set 'gpgcheck=1'."
fi

echo " Está activado Gpgcheck?"
out="$(grep ^gpgcheck /etc/yum.repos.d/* | grep =0)"
if [ -z "$out" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: Edit any failing files in \"/etc/yum.repos.d/*\" and set all
instances of gpgcheck to '1'."
fi

#1.3 Configure sudo
echo "Sudo está activado globalmente?"
out="$(rpm -q sudo)"
if [ "$out" == "sudo-1.8.23-9.el7.x86_64" ]; then
        echo "[+]Pass"
else
        yum -y install sudo -v
        echo "[+]Done"
fi
```

```
#[14]
# 1.4 Filesystem Integrity Checking
echo "AIDE está instalado?"
out="$(rpm -q aide)"
if [ "$out" == "package aide is not installed" ]; then
        echo "[-]Error: $out"
        prompt "Want to install it?"
        if [ "$ANSWER" == "1" ]; then
        yum -y install aide -v
        echo "[+]Done: Configure AIDE es apropiado para su ambiente."
        fi
else
        echo "[+]Pass"
fi
prompt "Want to initialize AIDE?"
if [ "$ANSWER" == "1" ]; then
        aide --init -v
        mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
        echo "[+]Done"
fi

#[14]
echo "Filesystem integrity is regularly checked"
out="$(crontab -u root -l | grep aide)"
if [[ $out = *"aide"* ]]; then
        echo "[+]Pass"
else
        echo "[-]Error"
        prompt "Want to add aide to cron job?"
        if [ "$ANSWER" == "1" ]; then
        (crontab -l 2>/dev/null; echo "0 5 * * * /usr/sbin/aide --check") | crontab
-
        crontab -l
        echo "[+]Done"
        fi
fi

#1.5 Secure Boot Settings
echo "Permissions on bootloader config"
echo "[*]Setting permissions"
chown root:root /boot/grub2/grub.cfg
chmod og-rwx /boot/grub2/grub.cfg
echo "[+]Done"
```

```
echo "Bootloader password"
out="$(grep "^GRUB2_PASSWORD" /boot/grub2/grub.cfg)"
if [ -z "$out" ]; then
        prompt "[-]No password set, do you want to set it up now?"
        if [ "$ANSWER" == 1 ]; then
                grub2-setpassword
                echo "[+]Done"
        fi
else
        echo "[+]Pass"
fi
out="$(grep /sbin/sulogin /usr/lib/systemd/system/rescue.service)"
rule="ExecStart=-/bin/sh -c \"/usr/sbin/sulogin; /usr/bin/systemctl --fail --no-block default\""
if [ "$out" == "$rule" ]; then
        out="$(grep                                                    /sbin/sulogin /usr/lib/systemd/system/emergency.service)"
        if [ "$out" == "$rule" ]; then
                echo "[+] Pass"
        fi
else
        echo "[-] Error: Check section \"1.5 Secure Boot Settings\" in CIS Benchmark."
fi

#1.6 Additional Process Hardening
echo "Setting core dump security limits"
echo '* hard core 0' > /etc/security/limits.conf
echo "[+]Done"

echo "XD/NX support"
dmesg | grep NX | awk 'FNR==1 {print FILENAME, $0}'
echo "[+]Done"

echo "Address space layout randomization (ASLR)"
grep -qxF "kernel.randomize_va_space = 2" /etc/sysctl.conf || echo "kernel.randomize_va_space = 2" >> /etc/sysctl.conf
sysctl -w kernel.randomize_va_space=2
sysctl kernel.randomize_va_space
echo "[+]Done"

echo "Prelink is disabled?"
out="$(rpm -q prelink)"
```

```
if [ "$out" == "package prelink is not installed" ]; then
        echo "[+]Pass"
else
        prompt "[-]Prelink is installed, want to uninstall it?"
        if [ "$ANSWER" == "1" ]; then
        prelink -ua
        yum remove prelink
        echo "[+]Done"
        fi
fi

#[14]
#1.7 Mandatory Access Control
prompt "You want to configure the Mandatory Access Control?"
if [ "$ANSWER" == "1" ]; then
yum install libselinux
yum remove setroubleshoot
yum remove mcstrans
echo "SELINUX=permissive" >> /etc/selinux/config
echo "SELINUXTYPE=targeted" >> /etc/selinux/config
setenforce 0
sed "6,7d"  /etc/default/grub
echo "[+]Done"
fi

#1.8 Warning Banners
prompt "You want to configure the Banner?"
if [ "$ANSWER" == "1" ]; then
chown root:root /etc/motd
chmod u-x,go-wx /etc/motd
yum remove gdm

grep -qxF "Banner /etc/issue" /etc/ssh/sshd_config || echo "Banner
/etc/issue" >> /etc/ssh/sshd_config

echo    "**************************************************************************"    >>
/etc/issue
echo    "**************************************************************************"    >>
/etc/issue
echo "*                    A T E N C I O N                          *" >> /etc/issue
echo "*                                                             *" >> /etc/issue
echo "* Este es un Sistema Privado operado por LA TELCO             *" >>
/etc/issue
```

```
echo "* Es requerida autorizacion por parte de la Gerencia de *" >>
/etc/issue
echo "* Sistemas para el acceso y uso de este sistema. *" >>
/etc/issue
echo "* *" >> /etc/issue
echo "* El Acceso no autorizado a sistemas de computacion y
comunicaciones *" >> /etc/issue
echo "* infringe las normas y politicas de seguridad informatica internas *"
>> /etc/issue
echo "* establecidas por la TELCO y será penalizado segun los reglamentos
*" >> /etc/issue
echo "* internos y leyes locales vigentes. *" >> /etc/issue
echo "* *" >> /etc/issue
echo "**************************************************************************" >>
/etc/issue
echo "**************************************************************************" >>
/etc/issue
systemctl restart sshd.service
echo "[+]Done"
fi

#2.1 Ensure xinetd is not installed
yum -y remove xinetd
#2.2 Special Purpose Services

echo "Disabling \"chargen\" services"
chkconfig chargen-dgram off
chkconfig chargen-stream off
echo "[+]Done"

echo "Disabling \"daytime\" services"
chkconfig daytime-dgram off
chkconfig daytime-stream off
echo "[+]Done"

echo "Disabling \"discard\" services"
chkconfig discard-dgram off
chkconfig discard-stream off
echo "[+]Done"

echo "Disabling \"echo\" services"
chkconfig echo-dgram off
chkconfig echo-stream off
echo "[+]Done"
```

```
echo "Disabling \"time\" services"
chkconfig time-dgram off
chkconfig time-stream off
echo "[+]Done"

echo "Disabling \"xinetd\""
systemctl disable xinetd
echo "[+]Done"

echo "Time synchronization"
out="$(rpm -q ntp)"
if [ "$out" == "package ntp is not installed" ]; then
        echo "[*]$out. Installing..."
        yum -y install ntp
        echo "[+]Done"
fi

#[14]
echo "Setting ntp configuration..."
cat >> /etc/ntp.conf << "EOF"
restrict -4 default kod nomodify notrap nopeer noquery
EOF
cat >> c << "EOF"
OPTIONS="-u ntp:ntp"
EOF
echo "[+]Done"

echo "X Window System not installed"
out="$(rpm -qa xorg-x11*)"
if [ -z "$out" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: $out. Uninstalling..."
        yum remove xorg-x11*
fi

echo "[*]Disabling Avahi Server..."
systemctl disable avahi-daemon

echo "[*]Disabling CUPS..."
systemctl disable cups

echo "[*]Disabling DHCP Server..."
```

```
systemctl disable dhcpd

echo "[*]Disabling LDAP Server..."
systemctl disable slapd

echo "[*]Disabling NFS and RPC..."
systemctl disable nfs
systemctl disable nfs-server
systemctl disable rpcbind

echo "[*]Disabling DNS Server..."
systemctl disable named

echo "[*]Disabling FTP Server..."
systemctl disable vsftpd

echo "[*]Disabling HTTP Server..."
systemctl disable httpd

echo "[*]Disabling IMAP and POP3..."
systemctl disable dovecot

echo "[*]Disabling SAMBA..."
systemctl disable smb

echo "[*]Disabling HTTP Proxy..."
systemctl disable squid

echo "[*]Disabling SNMP..."
systemctl disable snmpd

echo "MTA local-only"
out="$(netstat -an | grep LIST | grep ":25[[:space:]]")"
if [ -z "$out" ]; then
        echo "[-]Error: Check section \"2.2.15 CIS Benchmark for remediation"
else
        echo "[+]Pass"
fi

echo "[*]Disabling NIS Server..."
systemctl disable ypserv

echo "[*]Disabling RSH Server..."
systemctl disable rsh.socket
```

```
systemctl disable rlogin.socket
systemctl disable rexec.socket

echo "[*]Disabling Telnet Server..."
systemctl disable telnet.socket

echo "[*]Disabling TFTP Server..."
systemctl disable tftp.socket

echo "[*]Disabling rsync service..."
systemctl disable rsyncd

echo "[*]Disabling talk Server..."
systemctl disable ntalk

echo "¿Está instalado el cliente NIS?”
out="$(rpm -q ypbind)"
if [ "$out" == "package ypbind is not installed" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: $out. Uninstalling..."
        yum remove ypbind
fi

echo "¿Está instalado el cliente RSH?"
out="$(rpm -q rsh)"
if [ "$out" == "package rsh is not installed" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: $out. Uninstalling..."
        yum remove rsh
fi

echo "¿Está instalado el cliente Talk?"
out="$(rpm -q talk)"
if [ "$out" == "package talk is not installed" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: $out. Uninstalling..."
        yum remove talk
fi

echo "¿Está instalado el cliente Telnet?"
out="$(rpm -q telnet)"
```

```
if [ "$out" == "package telnet is not installed" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: $out. Uninstalling..."
        yum remove telnet
fi

echo "¿Está instalado el cliente LDAP?"
out="$(rpm -q openldap-clients)"
if [ "$out" == "package openldap-clients is not installed" ]; then
        echo "[+]Pass"
else
        echo "[-]Error: $out. Uninstalling..."
        yum remove openldap-clients
fi

##3Network Configuration
grep -Els "^\s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri "s/^\s*(net\.ipv4\.ip_forward\s*)(=)(\s*\S+\b).*$/# *REMOVED* \1/" $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1

grep -Els "^\s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri "s/^\s*(net\.ipv6\.conf\.all\.forwarding\s*)(=)(\s*\S+\b).*$/# *REMOVED* \1/" $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1

grep -qxF "net.ipv4.conf.all.send_redirects = 0" /etc/sysctl.conf || echo "net.ipv4.conf.all.send_redirects = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.default.send_redirects = 0" /etc/sysctl.conf || echo "net.ipv4.conf.default.send_redirects = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.all.accept_source_route = 0" /etc/sysctl.conf || echo "net.ipv4.conf.all.accept_source_route = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.default.accept_source_route = 0" /etc/sysctl.conf || echo "net.ipv4.conf.default.accept_source_route = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv6.conf.all.accept_source_route = 0" /etc/sysctl.conf || echo "net.ipv6.conf.all.accept_source_route = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv6.conf.default.accept_source_route = 0" /etc/sysctl.conf || echo "net.ipv6.conf.default.accept_source_route = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.all.accept_redirects = 0" /etc/sysctl.conf || echo "net.ipv4.conf.all.accept_redirects = 0" >> /etc/sysctl.conf
```

```
grep -qxF "net.ipv4.conf.default.accept_redirects = 0" /etc/sysctl.conf || echo "net.ipv4.conf.default.accept_redirects = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv6.conf.all.accept_redirects = 0" /etc/sysctl.conf || echo "net.ipv6.conf.all.accept_redirects = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv6.conf.default.accept_redirects = 0" /etc/sysctl.conf || echo "net.ipv6.conf.default.accept_redirects = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.all.log_martians = 1" /etc/sysctl.conf || echo "net.ipv4.conf.all.log_martians = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.default.log_martians = 1" /etc/sysctl.conf || echo "net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv4.icmp_echo_ignore_broadcasts = 1" /etc/sysctl.conf || echo "net.ipv4.icmp_echo_ignore_broadcasts = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv4.icmp_ignore_bogus_error_responses = 1" /etc/sysctl.conf || echo "net.ipv4.icmp_ignore_bogus_error_responses = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.all.rp_filter = 1" /etc/sysctl.conf || echo "net.ipv4.conf.all.rp_filter = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv4.conf.default.rp_filter = 1" /etc/sysctl.conf || echo "net.ipv4.conf.default.rp_filter = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv4.tcp_syncookies = 1" /etc/sysctl.conf || echo "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.conf
grep -qxF "net.ipv6.conf.all.accept_ra = 0" /etc/sysctl.conf || echo "net.ipv6.conf.all.accept_ra = 0" >> /etc/sysctl.conf
grep -qxF "net.ipv6.conf.default.accept_ra = 0" /etc/sysctl.conf || echo "net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.conf
sysctl -w net.ipv4.conf.all.send_redirects=0
sysctl -w net.ipv4.conf.default.send_redirects=0
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv4.conf.all.accept_source_route=0
sysctl -w net.ipv4.conf.default.accept_source_route=0
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.default.accept_redirects=0
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv6.conf.all.accept_redirects=0
sysctl -w net.ipv6.conf.default.accept_redirects=0
sysctl -w net.ipv6.route.flush=1
sysctl -w net.ipv4.conf.all.log_martians=1
sysctl -w net.ipv4.conf.default.log_martians=1
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv4.conf.all.rp_filter=1
sysctl -w net.ipv4.conf.default.rp_filter=1
```

```
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv4.tcp_syncookies=1
sysctl -w net.ipv4.route.flush=1
sysctl -w net.ipv6.conf.all.accept_ra=0
sysctl -w net.ipv6.conf.default.accept_ra=0
sysctl -w net.ipv6.route.flush=1

grep -qxF "install dccp /bin/true" /etc/modprobe.d/dccp.conf || echo "install dccp /bin/true" >> /etc/modprobe.d/dccp.conf
grep -qxF "install sctp /bin/true" /etc/modprobe.d/dccp.conf || echo "install sctp /bin/true" >> /etc/modprobe.d/dccp.conf


#bonustrack
systemctl mask ctrl-alt-del.target

#3.5.1 Configure firewalld
prompt "You want to configure the Firewall Policy?"
if [ "$ANSWER" == "1" ]; then
systemctl stop iptables
systemctl stop ip6tables
yum remove iptables-services
yum remove nftables
systemctl --now enable firewalld
firewall-cmd --set-default-zone=public
firewall-cmd --zone=customezone --change-interface=enp0s3
firewall-cmd --remove-port=25/tcp
firewall-cmd --permanent --zone=public --add-port=80/tcp
firewall-cmd --zone=public --add-service=443
firewall-cmd --permanent --zone=dmz --add-service=http
firewall-cmd --permanent --zone=dmz --add-service=https
firewall-cmd --reload
echo "[+]Done"
fi
iptables -F

#4 Logging and Auditing
echo "Audit is installed"
out="$(rpm -q audit)"
if [ "$out" == "package audit is not installed" ]; then
        yum install audit
else
        echo "[+]Pass"
fi
```

```
echo "Audit-libs is installed"
out="$(rpm -q audit-libs)"
if [ "$out" == "package audit-libs is not installed" ]; then
        yum install audit-libs
        systemctl --now enable auditd
else
        echo "[+]Pass"
fi

grep -qxF "GRUB_CMDLINE_LINUX="audit=1"" /etc/default/grub || echo "GRUB_CMDLINE_LINUX="audit=1"" >> /etc/default/grub
grep -qxF "max_log_file = 100" /etc/audit/auditd.conf || echo "max_log_file = 200" >> /etc/audit/auditd.conf
grep -qxF "max_log_file_action = keep_logs" /etc/audit/auditd.conf || echo "max_log_file_action = keep_logs" >> /etc/audit/auditd.conf
grep -qxF "space_left_action = email" /etc/audit/auditd.conf || echo "space_left_action = email" >> /etc/audit/auditd.conf
grep -qxF "action_mail_acct = root" /etc/audit/auditd.conf || echo "action_mail_acct = root" >> /etc/audit/auditd.conf
grep -qxF "admin_space_left_action = halt" /etc/audit/auditd.conf || echo "admin_space_left_action = halt" >> /etc/audit/auditd.conf
grep -qxF "GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"" /etc/audit/auditd.conf || echo "GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"" >> /etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
echo "[+]Done"
echo "Reglas locales del sistema configuradas"


prompt "Quieres configurar las reglas de las sesiones?"
if [ "$ANSWER" == "1" ]; then
touch /etc/audit/rules.d/session.rules
grep -qxF "\-w /var/run/utmp -p wa -k session" /etc/audit/rules.d/session.rules || echo "-w /var/run/utmp -p wa -k session" >> /etc/audit/rules.d/session.rules
grep -qxF "\-w /var/log/wtmp -p wa -k logins" /etc/audit/rules.d/session.rules || echo "-w /var/log/wtmp -p wa -k logins" >> /etc/audit/rules.d/session.rules
grep -qxF "\-w /var/log/btmp -p wa -k logins" /etc/audit/rules.d/session.rules || echo "-w /var/log/btmp -p wa -k logins" >> /etc/audit/rules.d/session.rules
echo "[+]Done"
fi
echo " Reglas de sesiones configuradas"
```

```
prompt "Desea garantizar cambios en el alcance de la administración del sistema (sudoers)?"
if [ "$ANSWER" == "1" ]; then
echo "-w /etc/sudoers -p wa -k scope" >> etc/audit/rules.d/scope.rules
echo "-w /etc/sudoers.d/ -p wa -k scope" >> etc/audit/rules.d/scope.rules
echo "[+]Done"
fi
echo "Cambios en el ámbito de administración del sistema (sudoers) configurados"


prompt " ¿Quiere garantizar las acciones del administrador del sistema (sudolog)?”
if [ "$ANSWER" == "1" ]; then
echo "-w /var/log/sudo.log -p wa -k actions" >> /etc/audit/rules.d/actions.rules
echo "[+]Done"
fi
echo "Acciones del administrador del sistema (sudolog) estén configuradas"


prompt "¿Quiere asegurarse de que la configuración de auditoría sea inmutable?"
if [ "$ANSWER" == "1" ]; then
echo "-e 2" >> /etc/audit/rules.d/99-finalize.rules
echo "[+]Done"
fi
echo "Configuración de auditoría inmutable configurada"


#4.2 Configure Logging
echo "rsyslog is installed"
out="$(rpm -q rsyslog)"
if [ "$out" == "package rsyslog is not installed" ]; then
        yum install rsyslog -y
        systemctl --now enable rsyslog
else
        echo "[+]Pass"
fi
echo "rsyslog is installed"

grep -qxF "\$FileCreateMode 0640" /etc/rsyslog.d/*.conf || echo "\$FileCreateMode 0640" >> /etc/rsyslog.d/*.conf
grep -qxF "\$FileCreateMode 0640" /etc/rsyslog.conf || echo "\$FileCreateMode 0640" >> /etc/rsyslog.conf
```

```
echo "$FileCreateMode is 0640 conigured in /etc/rsyslog.conf"
echo "[+]Done"

prompt "You want to add configuration for Rsyslog?"
if [ "$ANSWER" == "1" ]; then
grep -qxF "news.crit "\ " "\ " "\ " -/var/log/news/news.crit" /etc/rsyslog.conf ||
echo "news.crit "\ " "\ " "\ " -/var/log/news/news.crit" >> /etc/rsyslog.conf
grep -qxF "news.err "\ " "\ " "\ " -/var/log/news/news.err" /etc/rsyslog.conf ||
echo "news.err "\ " "\ " "\ " -/var/log/news/news.err" >> /etc/rsyslog.conf
grep -qxF "news.notice "\ " "\ " "\ " -/var/log/news/news.notice"
/etc/rsyslog.conf || echo "news.notice "\ " "\ " "\ " -/var/log/news/news.notice"
>> /etc/rsyslog.conf
grep -qxF "*.=warning;*.=err "\ " "\ " "\ " -/var/log/warn" /etc/rsyslog.conf ||
echo "*.=warning;*.=err "\ " "\ " "\ " -/var/log/warn" >> /etc/rsyslog.conf
grep -qxF "*.crit "\ " "\ " "\ " /var/log/warn" /etc/rsyslog.conf || echo "*.crit "\ " "\
" "\ " /var/log/warn" >> /etc/rsyslog.conf
systemctl restart rsyslog
echo "[+]Done"
fi
echo "Ensure logging is configured"

prompt "You want to add configuration for Rsyslog?"
if [ "$ANSWER" == "1" ]; then
echo "*.* @@ipserver" >> /etc/rsyslog.conf
echo "[+]Done"
echo "Open /etc/rsyslog.conf and verify or modify ipserver"
fi
echo "Rsyslog is configured"

grep -qxF "\$ModLoad imtcp" /etc/rsyslog.conf || echo "\$ModLoad imtcp" >>
/etc/rsyslog.conf
grep -qxF "\$InputTCPServerRun 514" /etc/rsyslog.conf || echo
"\$InputTCPServerRun 514" >> /etc/rsyslog.conf
systemctl restart rsyslog

#4.2.2 Configure journald
grep -qxF "ForwardToSyslog=yes" /etc/systemd/journald.conf || echo
"ForwardToSyslog=yes" >> /etc/systemd/journald.conf
grep -qxF "Compress=yes" /etc/systemd/journald.conf || echo
"Compress=yes" >> /etc/systemd/journald.conf
grep -qxF "Storage=persistent" /etc/systemd/journald.conf || echo
"Storage=persistent" >> /etc/systemd/journald.conf
echo "Journald is configured"
echo "[+]Done"
```

```
find /var/log -type f -exec chmod g-wx,o-rwx "{}" + -o -type d -exec chmod g-wx,o-rwx "{}" +

#5 Access, Authentication and Authorization
systemctl --now enable crond
chown root:root /etc/crontab
chmod u-x,og-rwx /etc/crontab
chown root:root /etc/cron.hourly/
chmod og-rwx /etc/cron.hourly/
chown root:root /etc/cron.daily
chmod og-rwx /etc/cron.daily
chown root:root /etc/cron.weekly/
chmod og-rwx /etc/cron.weekly/
chown root:root /etc/cron.monthly
chmod og-rwx /etc/cron.monthly
chown root:root /etc/cron.d
chmod og-rwx /etc/cron.d
touch /etc/cron.allow
chown root:root /etc/cron.allow
chmod u-x,og-rwx /etc/cron.allow
touch /etc/at.allow
chown root:root /etc/at.allow
chmod u-x,og-rwx /etc/at.allow
chown root:root /etc/ssh/sshd_config
chmod og-rwx /etc/ssh/sshd_config
find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod u-x,g-wx,o-rwx {} \;
find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:ssh_keys {} \;
find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod u-x,go-wx {} \;
find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root {} \;


prompt "You want to configure SSH Service?"
if [ "$ANSWER" == "1" ]; then
grep -qxF "LogLevel VERBOSE" /etc/ssh/sshd_config || echo "LogLevel VERBOSE" >> /etc/ssh/sshd_config
grep -qxF "X11Forwarding no" /etc/ssh/sshd_config || echo "X11Forwarding no" >> /etc/ssh/sshd_config
grep -qxF "LMaxAuthTries 4" /etc/ssh/sshd_config || echo "MaxAuthTries 4" >> /etc/ssh/sshd_config
```

```
grep -qxF "IgnoreRhosts yes" /etc/ssh/sshd_config || echo "IgnoreRhosts yes" >> /etc/ssh/sshd_config
grep -qxF "HostbasedAuthentication no" /etc/ssh/sshd_config || echo "HostbasedAuthentication no" >> /etc/ssh/sshd_config
grep -qxF "PermitRootLogin no" /etc/ssh/sshd_config || echo "PermitRootLogin no" >> /etc/ssh/sshd_config
grep -qxF "PermitEmptyPasswords no" /etc/ssh/sshd_config || echo "PermitEmptyPasswords no" >> /etc/ssh/sshd_config
grep -qxF "LogLevel VERBOSE" /etc/ssh/sshd_config || echo "PermitUserEnvironment no" >> /etc/ssh/sshd_config
grep -qxF "ClientAliveInterval 300" /etc/ssh/sshd_config || echo "ClientAliveInterval 300" >> /etc/ssh/sshd_config
grep -qxF "ClientAliveCountMax 3" /etc/ssh/sshd_config || echo "ClientAliveCountMax 3" >> /etc/ssh/sshd_config
grep -qxF "LoginGraceTime 60" /etc/ssh/sshd_config || echo "LoginGraceTime 60" >> /etc/ssh/sshd_config
grep -qxF "UsePAM yes" /etc/ssh/sshd_config || echo "UsePAM yes" >> /etc/ssh/sshd_config
grep -qxF "AllowTcpForwarding no" /etc/ssh/sshd_config || echo "AllowTcpForwarding no" >> /etc/ssh/sshd_config
grep -qxF "maxstartups 10:30:60" /etc/ssh/sshd_config || echo "maxstartups 10:30:60" >> /etc/ssh/sshd_config
grep -qxF "MaxSessions 10" /etc/ssh/sshd_config || echo "MaxSessions 10" >> /etc/ssh/sshd_config

grep -qxF "Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr" /etc/ssh/sshd_config || echo "Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr" >> /etc/ssh/sshd_config

grep -qxF "MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256" /etc/ssh/sshd_config || echo "MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256" >> /etc/ssh/sshd_config

grep -qxF "KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256" /etc/ssh/sshd_config || echo "KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-
```

```
sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-
sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-
hellman-group-exchange-sha256" >> /etc/ssh/sshd_config


fi
echo "SSH Service is configured"
echo "[+]Done"

#5.3 Configure PAM
prompt "You want to configure PAM (Pluggable Authentication Modules)?"
if [ "$ANSWER" == "1" ]; then
grep -qxF "minlen = 14" /etc/security/pwquality.conf || echo "minlen = 14" >>
/etc/security/pwquality.conf
grep -qxF "minclass = 4" /etc/security/pwquality.conf || echo "minclass = 4"
>> /etc/security/pwquality.conf
grep -qxF "password "\ ""\ " requisite "\ ""\ ""\ " pam_pwquality.so
try_first_pass retry=3" /etc/pam.d/password-auth || echo "password "\ ""\ "
requisite "\ ""\ ""\ " pam_pwquality.so try_first_pass retry=3" >>
/etc/pam.d/password-auth
grep -qxF "password "\ ""\ " requisite "\ ""\ ""\ " pam_pwquality.so
try_first_pass retry=3" /etc/pam.d/system-auth || echo "password "\ ""\ "
requisite "\ ""\ ""\ " pam_pwquality.so try_first_pass retry=3" >>
/etc/pam.d/system-auth
grep -qxF "auth "\ ""\ ""\ ""\ ""\ ""\ " required "\ ""\ ""\ ""\ " pam_faillock.so
preauth silent audit deny=5 unlock_time=900" /etc/pam.d/system-auth ||
echo "auth "\ ""\ ""\ ""\ ""\ ""\ " required "\ ""\ ""\ ""\ " pam_faillock.so preauth
silent audit deny=5 unlock_time=900" >> /etc/pam.d/system-auth
grep -qxF "auth "\ ""\ ""\ ""\ ""\ ""\ " [default=die] pam_faillock.so authfail audit
deny=5 unlock_time=900" /etc/pam.d/password-auth || echo "auth "\ ""\ ""\ ""\
""\ ""\ " [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900"
>> /etc/pam.d/password-auth
grep -qxF "password "\ ""\ " sufficient "\ ""\ " pam_unix.so sha512"
/etc/pam.d/password-auth || echo "password "\ ""\ " sufficient "\ ""\ "
pam_unix.so sha512" >> /etc/pam.d/password-auth
grep -qxF "password "\ ""\ " sufficient "\ ""\ " pam_unix.so sha512"
/etc/pam.d/system-auth || echo "password "\ ""\ " sufficient "\ ""\ "
pam_unix.so sha512" >> /etc/pam.d/system-auth
grep -qxF "password "\ ""\ " required "\ ""\ ""\ ""\ " password pam_pwhistory.so
remember=5" /etc/pam.d/system-auth || echo "password "\ ""\ " required "\ ""\
""\ ""\ " password  pam_pwhistory.so remember=5" >> /etc/pam.d/system-
auth
grep -qxF "password "\ ""\ " required "\ ""\ ""\ ""\ " password pam_pwhistory.so
remember=5" /etc/pam.d/password-auth || echo "password "\ ""\ " required "\
```

```
""\ ""\ ""\ " password pam_pwhistory.so remember=5" >> /etc/pam.d/password-auth
fi
echo "PAM is configured"


#5.4 User Accounts and Environment
prompt "You want to configure User Accounts and Environment?"
if [ "$ANSWER" == "1" ]; then
echo "Please edit Manually \"/etc/login.defs\" and set 'PASS_MAX_DAYS 365'."
echo "Please edit Manually \"/etc/login.defs\" and set 'PASS_MIN_DAYS 1'."
echo "Please edit Manually \"/etc/login.defs\" and set 'PASS_WARN_AGE 7'."
usermod -g 0 root

grep -qxF "readonly TMOUT=900 ; export TMOUT" /etc/profile || echo "readonly TMOUT=900 ; export TMOUT" >> /etc/profile
grep -qxF "readonly TMOUT=900 ; export TMOUT" /etc/bashrc || echo "readonly TMOUT=900 ; export TMOUT" >> /etc/bashrc
grep -qxF "readonly TMOUT=900 ; export TMOUT" /etc/profile.d/256term.sh || echo "readonly TMOUT=900 ; export TMOUT" >> /etc/profile.d/256term.sh
grep -qxF "readonly TMOUT=900 ; export TMOUT" /etc/profile.d/colorgrep.sh || echo "readonly TMOUT=900 ; export TMOUT" >> /etc/profile.d/colorgrep.sh
grep -qxF "readonly TMOUT=900 ; export TMOUT" /etc/profile.d/less.sh || echo "readonly TMOUT=900 ; export TMOUT" >> /etc/profile.d/less.sh
grep -qxF "readonly TMOUT=900 ; export TMOUT" /etc/profile.d/which2.sh || echo "readonly TMOUT=900 ; export TMOUT" >> /etc/profile.d/which2.sh
grep -qxF "umask 027" /etc/profile || echo "umask 027" >> /etc/profile
grep -qxF "umask 027" /etc/bashrc || echo "umask 027" >> /etc/bashrc
grep -qxF "umask 027" /etc/profile.d/256term.sh || echo "umask 027" >> /etc/profile.d/256term.sh
grep -qxF "umask 027" /etc/profile.d/colorgrep.sh || echo "umask 027" >> /etc/profile.d/colorgrep.sh
grep -qxF "umask 027" /etc/profile.d/less.sh || echo "umask 027" >> /etc/profile.d/less.sh
grep -qxF "umask 027" /etc/profile.d/which2.sh || echo "umask 027" >> /etc/profile.d/which2.sh

fi
echo "User Accounts and Environment is configured"
echo "[+]Done"
```

```
#6 System Maintenance
prompt "You want to configure System Maintenance?"
if [ "$ANSWER" == "1" ]; then
chown root:root /etc/passwd
chmod u-x,g-wx,o-wx /etc/passwd
chown root:root /etc/shadow
chmod 0000 /etc/shadow
chown root:root /etc/gshadow # chmod 0000 /etc/gshadow
chown root:root /etc/passwd- # chmod u-x,go-wx /etc/passwd-
chown root:root /etc/shadow- # chmod 0000 /etc/shadow-
chown root:root /etc/gshadow- # chmod 0000 /etc/gshadow-

sed -e 's/^\([a-zA-Z0-9_]*\):[^:]*:/\1:x:/' -i /etc/passwd
awk -F: '($3 == 0) { print $1 }' /etc/passwd
echo "No results"
echo "[+]Done"
grep ^shadow:[^:]*:[^:]*:[^:]+ /etc/group
awk -F: '($4 == "<shadow-gid>") { print }' /etc/passwd
echo "No results"
echo "[+]Done"
fi
echo "System Maintenance is configured"
echo "[+]Done"

echo "The server is Hardned"
echo "End to Script"
```