



■ Openshift Container Platform
100% digital

■ Memoria Técnica

■ Autor: Edson Ruben Angel Nuñez

eangel@actiglobal.com

■ Mayo, 2018

Contenido

1	Objetivo del documento.....	3
1.1	Propósito	3
1.2	Audiencia	3
1.3	Alcance del documento	3
2	Plataforma de nube: MS Azure	4
2.1	Suscripción y gestión de recursos	4
2.2	Almacenamiento	6
2.3	Redes y conexiones híbridas	11
2.4	Servidores virtuales y alta disponibilidad	15
3	Plataforma de contenedores: RedHat Openshift.....	23
3.1	Arquitectura.....	24
3.2	Instalación de Cluster	26
3.3	Configuración de registros de imágenes	36
3.4	Configuración de router.....	38
3.5	Configuración de autenticación	40
3.6	Integración con Microsoft Azure	41
3.7	Configuración de almacenamiento persistente	42
3.8	Configuración de métricas.....	44
4	Plataforma DevOps: Azure DevOps.....	46
5	Diagrama de infraestructura	47
6	Aceptación	48

1 Objetivo del documento

1.1 Propósito

Este documento se presenta como marco de referencia sobre la implementación de la plataforma de contenedores Redhat Openshift en Claro Colombia, dando detalle de las configuraciones realizadas y validadas por el cliente; el propósito del documento es que éste le sirva como línea base en caso de cualquier eventualidad que surja derivada de la integración a futuro de nuevos servicios, actualizaciones de la plataforma de sistema operativo y/u Openshift Container Platform.

1.2 Audiencia

La audiencia de éste documento son todas aquellas personas con conocimiento de nivel bajo-intermedio del producto Redhat Openshift Container Platform, así como de conocimientos de nivel medio alto de arquitecturas y funcionalidad para ambientes y/o desarrollo de microservicios; éstos temas son necesarios debido a que el contenido de éste documento maneja detalles técnicos de Plataforma de nube, Sistema Operativo, plataforma de contenedores, Publicación de Servicios, comunicaciones, etc.

1.3 Alcance del documento

Este documento se debe utilizar para determinar el estado de la configuración de la plataforma de contenedores Openshift que se encuentra instalado en MS Azure público de Claro Colombia, considerando los cambios aplicados por cuestiones administrativas de la plataforma, lo que permitirá ofrecer y mantener la operación en un estado saludable y fuera de riesgos que impliquen un impacto al área de negocios del cliente.

2 Plataforma de nube: MS Azure

Los siguientes puntos forman parte de los aspectos considerados al implementar cada uno de los roles y funcionalidades de la plataforma de contenedores Openshift, mismos que permiten la gestión de cada uno de los elementos que integran la solución y que son los que permiten identificar algún riesgo y/o configuración inapropiada en la plataforma:

- Suscripción y gestión de recursos
- Almacenamiento
- Redes y conexiones híbridas
- Servidores virtuales y alta disponibilidad

Con base a los puntos mencionados se realizaron las configuraciones correspondientes de cada uno de ellos cumpliendo los requerimientos del proyecto “100% digital”, mismos que fueron solicitados por Claro Colombia y que están expresados en la Orden de Trabajo.

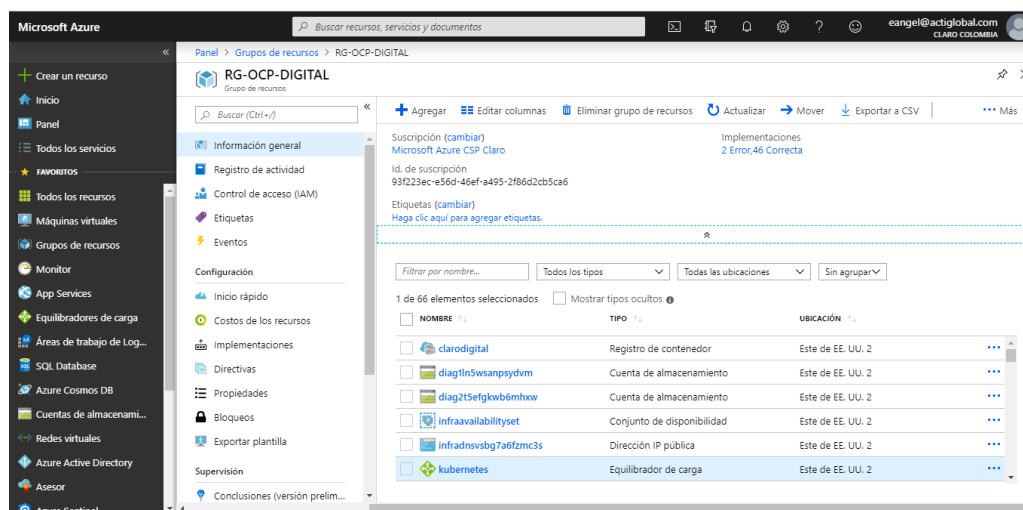
2.1 Suscripción y gestión de recursos

Las actividades de configuración de la plataforma de nube MS Azure consistieron en crear un conjunto de recursos virtuales de almacenamiento, redes y procesamiento para generar un ambiente de alta disponibilidad en IaaS para OCP (Openshift Container Platform). A continuación se mostraran las configuraciones que se realizaron a nivel de MS Azure:

Para el despliegue de esta solución y la infraestructura virtual relacionada se utiliza una suscripción de tipos CSP propiedad de claro con los siguientes datos:

Datos de suscripción de Azure	
Nombre	Microsoft Azure CSP Claro
ID	93f223ec-e56d-46ef-a495-2f86d2cb5ca6
Oferta	CSP
Tenant/ID	Claro Colombia/bc21c6c5-b0ee-414b-9a51-352b288d6b45

La gestión de los recursos a nivel plataforma se realiza por medio de Azure Resource Manager, el cual utiliza los grupos de recursos para poder organizar y gestionar la infraestructura desplegada en Azure. Con el fin de tener una buena práctica en la administración de Azure, se creó un grupo de recursos llamado "RG-OCP-DIGITAL". Este grupo de recursos y todos los recursos que contiene se crearon en la ubicación "Este de EE. UU. 2"



Para finalizar las configuraciones de gestión de plataforma de nube se creó un SP dentro del tenant Claro Colombia que tiene la función de orquestar la creación de nuevos recursos de plataforma de nube desde el ambiente de Openshift. A continuación, se muestra la configuración del SP "OCP-DIGITAL-AAD":

Nombre	openshiftcloudprovider
ID de aplicacion	6b57c83c-d603-454f-ad86-ae2452591cf5
Secret	+T;>[@n6kQ2*\$a#rr}yD}0!

Claro Colombia - App registrations

Azure Active Directory

Buscar (Ctrl+J)

[+ Nuevo registro](#)
[Puntos de conexión](#)
[X Solución de problemas](#)
[Got feedback?](#)





















Le damos la bienvenida a los registros de aplicaciones nuevos y mejorados (ahora disponibles de forma general). Vea las novedades. →

ER	Excel Reader	e858ee30-31f8-4835-811f-5e8390fe3290	27/3/2019	Current
OP	openshiftcloudprovider	6b57c83c-d603-454f-ad86-ae2452591cf5	1/11/2018	Current
OC	OCP-DIGITAL-AAD	d6bbc3ad-054c-420f-93f8-3f69fcc0683c	20/4/2019	Current

2.2 Almacenamiento

El servicio de almacenamiento en Azure es brindado por un recurso llamado "Storage Account"; las cuentas de almacenamiento brindan diferentes servicios de almacenamiento como son: blobs, files, tablas y colas. Para poder facilitar la escalabilidad vertical como horizontal de Openshift se desplegaron máquinas virtuales con discos administrados; los discos administrados son discos virtuales tanto de sistema operativo y de datos que son gestionados por el fabric de Azure el cual se encarga de aprovisionarlos en cuentas de

almacenamiento con la suficiente capacidad para soportar cualquier volumen de escrito y lectura hacia disco. Los discos virtuales administrados que se crearon se muestran a continuación:

NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓
 kubernetes-dynamic-pvc-004e74d2-6537-11e9-a5be-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-2cf24993-71a8-11e9-b515-000d3a00a005	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-79ec42cc-636d-11e9-b59e-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-8eb290c1-6555-11e9-a5be-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-90a127a2-6698-11e9-987e-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-accd5461-636e-11e9-b59e-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-eb66e89d-63dc-11e9-bd6a-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-f9ed551b-6536-11e9-a5be-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-fc0a513e-6536-11e9-a5be-000d3a00a470	Disco	Este de EE. UU. 2
 kubernetes-dynamic-pvc-fe3d3fbb-6536-11e9-a5be-000d3a00a470	Disco	Este de EE. UU. 2
 ocp-digital-infra-0-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-infra-0-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-infra-1-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-infra-1-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-infra-2-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-infra-2-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-master-0-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-master-0-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-master-1-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-master-1-osdisk	Disco	Este de EE. UU. 2

 ocp-digital-master-2-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-master-2-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-node-0-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-node-0-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-node-1-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-node-1-osdisk	Disco	Este de EE. UU. 2
 ocp-digital-node-2-docker-pool	Disco	Este de EE. UU. 2
 ocp-digital-node-2-osdisk	Disco	Este de EE. UU. 2

Como se puede observar y se mencionó anteriormente, se crearon 2 disco administrados por máquina virtual, uno para el sistema operativo y otro como disco adicional para los datos de cada máquina virtual. Cada uno de los discos de sistema operativo se crearon con las siguientes características:



Discos para Sistema Operativo	
Tipo	Administrado
Tier	SSD Premium
Capacidad	64 GiB
Rendimiento estimado (E/S x seg)	240
Capacidad de proceso	50 MB/s

Los discos de datos se utilizarán para generar un Cluster de almacenamiento llamado GLUSTER el cual servirá como servicio de almacenamiento para los pods desplegados por diferentes proyectos; a continuación, se muestran las especificaciones cada disco de datos:

Discos para Datos de Pods	
Tipo	Administrado
Tier	SSD Premium
Capacidad	1024 GiB
Rendimiento estimado (E/S x seg)	5000
Capacidad de proceso	200 MB/s


Las máquinas virtuales tienen la capacidad de generar información de diagnósticos y las cuales pueden ayudar a resolver problemas de encendido, acceso y/o comunicaciones, estos datos de diagnóstico se almacenan en cuentas de almacenamiento con las siguientes características:

Nombre	Rendimiento	Replicación	Tipo	Uso
diag1ln5wsanpsydvms	Estandar	LRS	General v1	Logs de diagnóstico de MV
diag2t5efgkwb6mhxw	Estandar	LRS	General v1	Logs de diagnóstico de MV

NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓
 diag1ln5wsanpsydvms	Cuenta de almacenamiento	Este de EE. UU. 2
 diag2t5efgkwb6mhxw	Cuenta de almacenamiento	Este de EE. UU. 2


Además de estas 2 cuentas de almacenamiento se crearon otras 2 con diferentes propósitos; la primera su propósito principal es el generar el registro de los metadatos de proyectos creados en Openshift. A continuación, se muestran las características y configuraciones de esta cuenta de almacenamiento:

Nombre	Rendimiento	Replicación	Tipo	Uso
registrykweqmefgouzrg	Estandar	LRS	General v1	Registro de metada de proyectos

NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓
 registrykweqmefgouzrg	Cuenta de almacenamiento	Este de EE. UU. 2

La otra cuenta de almacenamiento que se creó su principal funcionalidad es de servidor como almacenamiento persisten para cualquier proyecto y/o aplicación que se despliegue en Openshift, brindado la capacidad de almacenar hasta 2 PB de datos, 20000 solicitudes por segundo y 5 GBps de entrada de datos, 50 Gbps de salida de datos, estas especificaciones están sujetas a las diferentes configuraciones y limitantes de acceso compartido ya que el tipo de almacenamiento presentado hacia Openshift es Azure Files. Las características y configuraciones de esta cuenta de almacenamiento son:

Nombre	Rendimiento	Replicación	Tipo	Uso
odcdigitalpv	Estándar/Hot	GRS	General v2	Almacenamiento persistente para Cluster Openshift

NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓
 odcdigitalpv	Cuenta de almacenamiento	Oeste de EE. UU. 2

2.3 Redes y conexiones híbridas

Para poder tener comunicación entre máquinas virtuales y por lo tanto aplicativos montados en ellas, Azure ofrece un recurso llamado Azure virtual Network o vNet el cual tiene las funcionalidades de cualquier switch físico capa 3 con un ancho de banda entre máquinas virtuales de hasta 30 Gbps. Para el despliegue de la infraestructura de este proyecto se reutilizo una vNet llamada **"openshiftvnet"** que pertenece a otro grupo de recursos llamado **"RG-OPENSIFT-PROD"**. Debido a los requerimientos de conectividad y utilización de conexiones VPN ya existentes se optó por esta vNet, aprovechando sus configuraciones, las cuales se detallan a continuación:

Nombre de vNet	openshiftvnet
Espacio de direcciones	10.0.0.0/8 172.0.0.0/8
DNS	Proporcionado por Azure
Subred para servidores maestros	mastersubnet
Subred para servidores de infraestructura	mastersubnet
Subred para servidores de contenedores/aplicaciones	nodesubnet

A continuación, se muestra el listado de las interfaces de red y su IP, las cuales pertenecen a cada una de las máquinas virtuales del ambiente de Openshift y su distribución en cada subred:






DISPOSITIVO	TIPO	DIRECCIÓN IP	SUBRED
ocp-digital:infra-0-nic	Interfaz de red	10.1.0.16	mastersubnet
ocp-digital:infra-2-nic	Interfaz de red	10.1.0.17	mastersubnet
ocp-digital:infra-1-nic	Interfaz de red	10.1.0.18	mastersubnet
ocp-digital:master-2-nic	Interfaz de red	10.1.0.19	mastersubnet
ocp-digital:master-1-nic	Interfaz de red	10.1.0.20	mastersubnet
ocp-digital:master-0-nic	Interfaz de red	10.1.0.21	mastersubnet
ocp-digital:node-0-nic	Interfaz de red	10.2.0.15	nodesubnet
ocp-digital:node-1-nic	Interfaz de red	10.2.0.16	nodesubnet
ocp-digital:node-2-nic	Interfaz de red	10.2.0.17	nodesubnet

Para poder lograr la comunicación de las aplicaciones hospedadas en OpenShift y los servicios legado de Claro Colombia se realiza por medio de 3 conexiones de tipo VPN, una para la red fija y otra para la red móvil de la infraestructura de Claro Colombia. Estas conexiones VPN ya se encontraban generadas y administradas por un appliance virtual Fortigate, solo se añadieron los siguientes destinos de red a las configuraciones de fase 2 de VPN y políticas ruteo y acceso en el firewall Fortigate; la siguiente imagen muestra los requerimientos principales de conectividad hacia los servicios legados:


Nombre de la Máquina	Dirección IP	Dirección NAT	Numero de Puerto	Tipo Protocolo	Servicio de Red
SAP QA	172.19.139.35	null	3300 3600 3200	TCP	http
SAP DEV	172.19.141.34	null	3300 3600 3200	TCP	http
COMHP44	132.147.170.95	null	1450 1810 1521	TCP	http
LNXSQA02	172.22.85.117	null	7045 8013 9999 7044	TCP	http

Las siguientes imágenes muestran los dominios de encriptacion dados de alta, los objetos y grupos de objetos y las reglas de seguridad y Nateo aplicadas:















Phase 2 Selectors		
VPN_Claro_7	10.60.242.104	132.147.170.95
VPN_Claro_8	10.60.242.104	100.126.64.0/255.255.255.0
VPN_Claro_9	10.60.242.104	100.126.65.0/255.255.255.0
VPN_Claro_10	10.60.242.126	166.210.224.0/255.255.255.0
VPN_Claro_11	10.60.242.126	132.147.170.0/255.255.255.0
VPN_Claro_12	10.60.242.125	10.244.140.25
VPN_Claro_13	10.60.242.104	172.19.139.35
VPN_Claro_14	10.60.242.104	172.19.141.34
VPN_Claro_5	10.60.242.104	172.22.0.0/255.255.0.0

 ClaroM_VPN_13	Subnet	172.19.139.35/32
 ClaroM_VPN_14	Subnet	172.19.141.34/32
 ClaroM_VPN_5	Subnet	172.22.0.0/16
 ClaroM_VPN_6	Subnet	172.24.0.0/16
 ClaroM_VPN_7	Subnet	132.147.170.95/32

Group Name

Color 

Members

	ClaroM_VPN_1	X
	ClaroM_VPN_10	X
	ClaroM_VPN_11	X
	ClaroM_VPN_12	X
	ClaroM_VPN_13	X
	ClaroM_VPN_14	X
	ClaroM_VPN_2	X
	ClaroM_VPN_3	X
	ClaroM_VPN_4	X
	ClaroM_VPN_5	X
	ClaroM_VPN_6	X
	ClaroM_VPN_7	X
	ClaroM_VPN_8	X
	ClaroM_VPN_9	X
		+

Show in Address List ☒

Static Route Configuration ☐

2.4 Servidores virtuales y alta disponibilidad




Actiglobal, al no tener una volumetría de conexiones aproximada por Claro Colombia para el proyecto de E-Commerce, el cual fue la punta de lanza de este proyecto, se desplego un ambiente base para entornos de producción de la plataforma de contenedores de Openshift. Este ambiente base consta de 9 máquinas virtuales divididas en 3 roles (Master, Infra y Aplicación), cada rol forma parte de un Cluster para determinadas funcionalidades de la plataforma.

NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓	GRUPO DE RECURSOS ↑↓
 ocp-digital-infra-0	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-infra-1	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-infra-2	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-master-0	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-master-1	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-master-2	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-node-0	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-node-1	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-node-2	Máquina virtual	Este de EE. UU. 2	RG-OCP-DIGITAL

A continuación, se detallan las especificaciones de cada una de las máquinas virtuales desplegadas:

Servidor	Azure VM	Sistema Operativo	vCPU	RAM (GiB)	Disco SSD OS (GiB)	Disco SSD Datos (GiB)
OCP-DIGITAL-MASTER-0	E4s v3	RHEL 7.4	4	32	64	1024
OCP-DIGITAL-MASTER-1	E4s v3	RHEL 7.4	4	32	64	1024
OCP-DIGITAL-MASTER-2	E4s v3	RHEL 7.4	4	32	64	1024
OCP-DIGITAL-INFRA-0	E8s v3	RHEL 7.4	8	64	64	1024
OCP-DIGITAL-INFRA-1	E8s v3	RHEL 7.4	8	64	64	1024
OCP-DIGITAL-INFRA-2	E8s v3	RHEL 7.4	8	64	64	1024
OCP-DIGITAL-NODE-0	E8s v3	RHEL 7.4	8	64	64	1024
OCP-DIGITAL-NODE-1	E8s v3	RHEL 7.4	8	64	64	1024
OCP-DIGITAL-NODE-2	E8s v3	RHEL 7.4	8	64	64	1024

Para ofrecer alta disponibilidad a nivel de aplicación y se generaron 3 conjuntos de disponibilidad en Azure los cuales se mapean con cada rol de la plataforma de OpenShift y así poder formar un Cluster de rol. Los conjuntos de disponibilidad brindan la capacidad de garantizar la disponibilidad de la aplicación hosteada en esas máquinas virtuales por medio de dominios de error y dominios de actualización. Los dominios de error definen un grupo de máquinas virtuales que comparten un origen de alimentación y un interruptor de red y aseguran que cada máquina este en un dominio diferente; los dominios de actualización definen grupos de máquinas virtuales en el hardware físico subyacente que se pueden reiniciar junto con el HW físico sin afectar la disponibilidad de las otras máquinas virtuales miembro del dominio de actualización. A continuación, se detalla las propiedades, miembros y configuración de cada conjunto de disponibilidad:



NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓	GRUPO DE RECURSOS ↑↓
 infraavailabilityset	Conjunto de disponibilidad	Este de EE. UU. 2	RG-OCP-DIGITAL
 masteravailabilityset	Conjunto de disponibilidad	Este de EE. UU. 2	RG-OCP-DIGITAL
 nodeavailabilityset	Conjunto de disponibilidad	Este de EE. UU. 2	RG-OCP-DIGITAL

Nombre	masteravailabilityset
Grupo de recursos	RG-OCP-DIGITAL
Ubicación	Este de EE. UU. 2
Miembros	OCP-DIGITAL-MASTER-0 OCP-DIGITAL-MASTER-1 OCP-DIGITAL-MASTER-2
Dominios de error	2
Dominios de actualización	5

Nombre	infraavailabilityset
Grupo de recursos	RG-OCP-DIGITAL
Ubicación	Este de EE. UU. 2
Miembros	OCP-DIGITAL-INFRA-0 OCP-DIGITAL-INFRA-1 OCP-DIGITAL-INFRA-2
Dominios de error	2
Dominios de actualización	5

Nombre	nodeavailabilityset
Grupo de recursos	RG-OCP-DIGITAL
Ubicación	Este de EE. UU. 2
Miembros	OCP-DIGITAL-NODE-0 OCP-DIGITAL-NODE-1 OCP-DIGITAL-NODE-2
Dominios de error	2
Dominios de actualización	5

Otra configuración que se realizó para brindar alta disponibilidad en el Cluster de Openshift, fue generar balanceadores de carga en Azure los cuales se expusieron hacia internet para realizar la tarea de un Fron-End de los servicios de gestión y operación de Openshift. A continuación, se muestra la configuración de los balanceadores de carga de Azure:




 ocp-digital-infralb	RG-OCP-DIGITAL	Este de EE. UU. 2	Microsoft Azure CSP Claro
 ocp-digital-masterlb	RG-OCP-DIGITAL	Este de EE. UU. 2	Microsoft Azure CSP Claro

ALB ocp-digital-infralb

Backend	OCP-DIGITAL-INFRA-0 OCP-DIGITAL-INFRA-1 OCP-DIGITAL-INFRA-2
IP-Front	137.116.47.4
Sondeos de estado	TCP-80 TCP-443
Reglas de equilibrio de carga	OpenShiftRouterHTTP TCP-80→(TCP/443) OpenShiftRouterHTTPS TCP-443→(TCP/443)

ALB ocp-digital-masterlb	
Backend	OCP-DIGITAL-MASTER-0 OCP-DIGITAL-MASTER-1 OCP-DIGITAL-MASTER-2
IP-Front	137.116.55.75
Sondeos de estado	TCP-443
Reglas de equilibrio de carga	OpenShiftAdminConsole-TCP-443→(TCP/443)
Reglas NAT de entrada	SSH-ocp-digital-master0 137.116.55.75:2200→10.1.0.21:22

La configuración de infraestructura finaliza con el despliegue de la capa de seguridad por medio de grupos de seguridad que se encuentran asociados a las interfaces de red de cada maquina virtual miembro del Cluster de OpenShift. Se crearon 3 grupos de seguridad los cuales cada uno de ellos esta mapeado a cada rol del Cluster de OpenShift. A continuación, se muestra los 3 grupos de seguridad creados:

NOMBRE ↑↓	TIPO ↑↓	UBICACIÓN ↑↓	GRUPO DE RECURSOS ↑↓
 ocp-digital-infra-nsg	Grupo de seguridad de red	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-master-nsg	Grupo de seguridad de red	Este de EE. UU. 2	RG-OCP-DIGITAL
 ocp-digital-node-nsg	Grupo de seguridad de red	Este de EE. UU. 2	RG-OCP-DIGITAL

En las siguientes tablas se muestra la configuración de las reglas de acceso de entrada/salida y las interfaces asociadas de cada uno de los grupos de seguridad:

ocp-digital-infra-nsg - Reglas de seguridad de entrada					
Nombre	Puerto	Protocolo	Origen	Destino	Acción
allowSSHIn_all	22	tcp	Any	Any	Permitir
allowHTTPSIn_all	443	tcp	Any	Any	Permitir
allowHTTPIn_all	80	tcp	Any	Any	Permitir
AllowVnetInBound	Any	tcp	VirtualNetwork	VirtualNetwork	Permitir

ocp-digital-infra-nsg - Reglas de seguridad de salida					
Nombre	Puerto	Protocolo	Origen	Destino	Acción
AllowVnetOutBound	Any	tcp	VirtualNetwork	VirtualNetwork	Permitir
AllowInternetOutBound	Any	tcp	Any	Any	Permitir

ocp-digital-infra-nsg - Interfaces de red		
Nombre	Dirección IP Privada	Máquina virtual
ocp-digital-infra-0-nic	10.1.0.16	ocp-digital-master-0
ocp-digital-infra-1-nic	10.1.0.18	ocp-digital-master-1
ocp-digital-infra-2-nic	10.1.0.17	ocp-digital-master-2

ocp-digital-master-nsg - Reglas de seguridad de entrada

Nombre	Puerto	Protocolo	Origen	Destino	Acción
allowSSHin_all	22	tcp	Any	Any	Permitir
allowHTTPSIn_all	443	tcp	Any	Any	Permitir
AllowVnetInBound	Any	tcp	VirtualNetwork	VirtualNetwork	Permitir

ocp-digital-master-nsg - Reglas de seguridad de salida

Nombre	Puerto	Protocolo	Origen	Destino	Acción
AllowVnetOutBound	Any	tcp	VirtualNetwork	VirtualNetwork	Permitir
AllowInternetOutBound	Any	tcp	Any	Any	Permitir

ocp-digital-master-nsg - Interfaces de red

Nombre	Dirección IP Privada	Máquina virtual
ocp-digital-master-0-nic	10.1.0.21	ocp-digital-master-0
ocp-digital-master-1-nic	10.1.0.20	ocp-digital-master-1
ocp-digital-master-2-nic	10.1.0.19	ocp-digital-master-2

ocp-digital-node-nsg - Reglas de seguridad de entrada

Nombre	Puerto	Protocolo	Origen	Destino	Acción
allowSSHin_all	22	tcp	Any	Any	Permitir
allowHTTPSIn_all	443	tcp	Any	Any	Permitir
allowHTTPIn_all	80	tcp	Any	Any	Permitir
AllowVnetInBound	Any	tcp	VirtualNetwork	VirtualNetwork	Permitir

ocp-digital-node-nsg - Reglas de seguridad de salida

Nombre	Puerto	Protocolo	Origen	Destino	Acción
AllowVnetOutBound	Any	tcp	VirtualNetwork	VirtualNetwork	Permitir
AllowInternetOutBound	Any	tcp	Any	Any	Permitir

ocp-digital-master-nsg - Interfaces de red

Nombre	Dirección IP Privada	Máquina virtual
ocp-digital-node-0-nic	10.2.0.15	ocp-digital-master-0
ocp-digital-node-1-nic	10.2.0.16	ocp-digital-master-1
ocp-digital-node-2-nic	10.2.0.17	ocp-digital-master-2

3 Plataforma de contenedores: RedHat Openshift

RedHat Openshift es una plataforma de contenedores Kubernetes empresarial con operaciones automatizadas integrales para gestionar implementaciones de nube híbrida y multicloud. OpenShift está optimizada para mejorar la productividad de los desarrolladores y promover la innovación. Hay muchas opciones en lo que respecta a las soluciones de Kubernetes, OpenShift se destaca como líder con una plataforma Kubernetes compatible centrada en la seguridad.

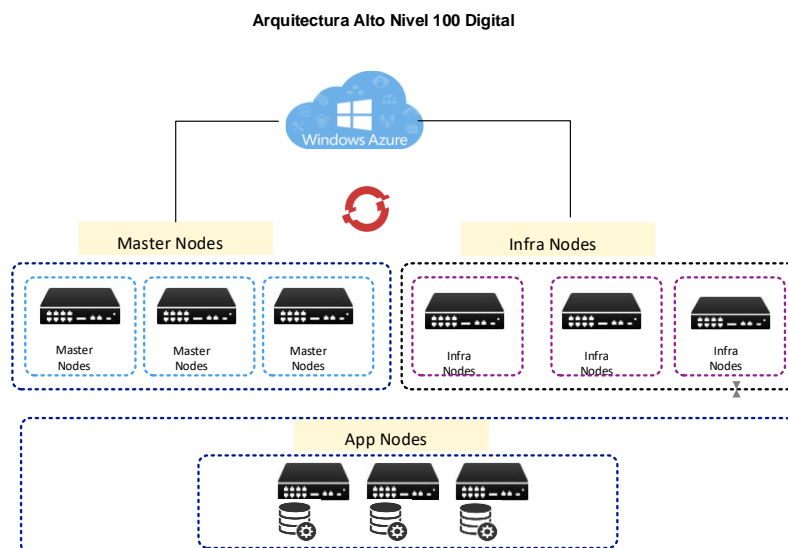
A continuación, se detalla la configuración realizada del ambiente Openshift, mismas que permiten la gestión de cada uno de los elementos que integran la solución y que son los que permiten identificar algún riesgo y/o configuración inapropiada en la plataforma:

- Arquitectura
- Instalación de Cluster
- Configuración de Registros de imágenes
- Configuración de Router
- Configuración de autenticación
- Integración con MS Azure
- Configuración de almacenamiento persistente
- Configuración de métricas

3.1 Arquitectura

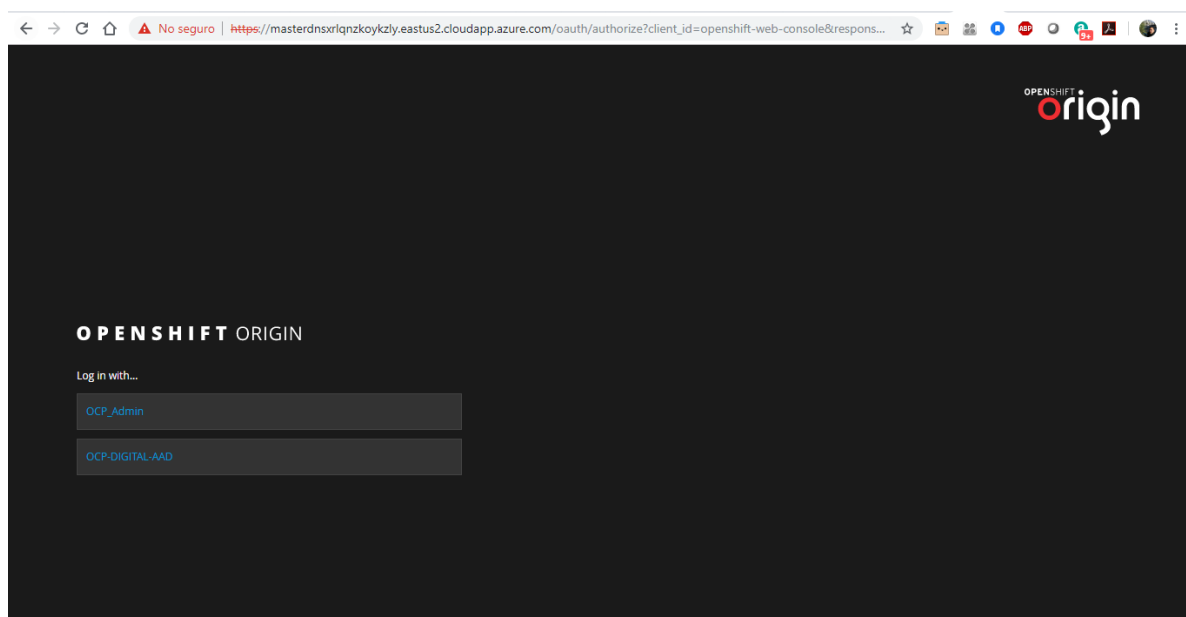
La siguiente imagen muestra la arquitectura del Cluster Openshift propuesto por Actiglobal, el cual se basa en una solución escalable y flexible tomando las ventajas de las plataformas MS Azure y Redhat Openshift. Los principales componentes de infraestructura son:

- **Nodos Maestros:** contienen los componentes maestros, incluido el servidor de API, el servidor del administrador del controlador y etcd. Los maestros administran los nodos en el clúster Openshift y programa los pods para que se ejecuten en los nodos.
- **Nodos Infraestructura:** un nodo de infraestructura proporciona los entornos para los componentes de servicio y monitoreo de la infraestructura como son los routers y métricas.
- **Nodos Aplicaciones:** Un nodo de aplicación proporciona los entornos de tiempo de ejecución para contenedores, cada nodo de aplicación en un clúster Openshift tiene los servicios requeridos para ser administrados por los nodos maestro. Los nodos de aplicación también tienen los servicios necesarios para ejecutar pods que forman parte de los proyectos de aplicaciones.



Un componente muy importante en la arquitectura OpenShift es el registro de contenedores y/o imágenes; Openshift puede utilizar cualquier servidor que implemente la API de registro de Docker como fuente de imágenes, incluido Docker Hub, registros privados ejecutados por terceros y el registro OpenShift integrado. Por requerimientos del negocio se implementara el servicio Azure Container Registry para aprovisionar imágenes customizadas por el equipo de desarrollo de Claro Colombia.

Finalmente, el componente de gestión es la consola web Openshift es una interfaz de usuario accesible desde un navegador web, los desarrolladores pueden usar la consola web para visualizar, explorar y administrar el contenido de los proyectos.



3.2 Instalación de Cluster

La instalación de paquetes de software necesarios en el sistema operativo para ejecutar el ambiente de contenedores se realizó por medio de un script generado por la plantilla de MS Azure, esto se realizó en todos los nodos que componen el Cluster de Openshift:

```
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep net-tools
net-tools.x86_64                2.0-0.24.20131004git.el7       @base
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep bind-utils
bind-utils.x86_64              32:9.9.4-73.el7_6             @updates
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep yum-utils
yum-utils.noarch               1.1.31-50.el7                 @base
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep iptables-services
iptables-services.x86_64       1.4.21-28.el7                 @base
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep bridge-utils
bridge-utils.x86_64            1.5-9.el7                     @anaconda
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep bash-completion
bash-completion.noarch         1:2.1-6.el7                   @anaconda
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep kexec-tools
kexec-tools.x86_64             2.0.15-21.el7                 @base
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep sos
sos.noarch                     3.6-16.el7.centos             @updates
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep psacct
psacct.x86_64                  6.6.1-13.el7                  @anaconda
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep atomic
atomic-registries.x86_64       1:1.22.1-26.gitb507039.el7.centos @extras
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep epel
epel-release.noarch            7-11                           installed
python2-passlib.noarch         1.7.1-1.el7                   @epel
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep ansible
ansible.noarch                 2.6.2-1.el7.ans               installed
clusteradmin@ocp-digital-master-0:~$ sudo yum list installed | grep pyOpenSSL
pyOpenSSL.x86_64               0.13.1-4.el7                  @base
```

```
clusteradmin@ocp-digital-master-0:~$ sudo rpm -V docker-1.13.1
S.5....T. c /etc/sysconfig/docker-network
S.5....T. c /etc/sysconfig/docker-storage
clusteradmin@ocp-digital-master-0:~$ sudo docker version
Client:
 Version:           1.13.1
 API version:       1.26
 Package version:   docker-1.13.1-94.gitb2f74b2.el7.centos.x86_64
 Go version:        gol.10.3
 Git commit:        b2f74b2/1.13.1
 Built:             Tue Mar 12 10:27:24 2019
 OS/Arch:           linux/amd64

Server:
 Version:           1.13.1
 API version:       1.26 (minimum version 1.12)
 Package version:   docker-1.13.1-94.gitb2f74b2.el7.centos.x86_64
 Go version:        gol.10.3
 Git commit:        b2f74b2/1.13.1
 Built:             Tue Mar 12 10:27:24 2019
 OS/Arch:           linux/amd64
 Experimental:      false
clusteradmin@ocp-digital-master-0:~$
```

Para realizar la instalación y configuración masiva de Openshift se utiliza Ansible como software de instalación multi-nodo y administrador de configuraciones. En las siguientes imágenes se muestra secciones básicas del archivo de inventario que se configuro para las tareas de configuración de Openshift:

```
[OSEv3:children]
masters
nodes
etcd
master0
new_nodes

# Set variables common for all OSEv3 hosts
[OSEv3:vars]
ansible_ssh_user=clusteradmin
ansible_become=yes
openshift_install_examples=true
openshift_deployment_type=origin
openshift_release=v3.9
docker_udev_workaround=True
openshift_use_dnsmasq=True
openshift_master_default_subdomain=137.116.47.4.nip.io
openshift_override_hostname_check=true
os_sdn_network_plugin_name='redhat/openshift-ovs-multitenant'
openshift_master_api_port=443
openshift_master_console_port=443
osm_default_node_selector='region=app'
openshift_disable_check=disk_availability,memory_availability,docker_image_availability
openshift_cloudprovider_kind=azure
osm_controller_args='["cloud-provider": ["azure"], "cloud-config": ["/etc/origin/cloudprovider/azure.conf]]'
osm_api_server_args='["cloud-provider": ["azure"], "cloud-config": ["/etc/origin/cloudprovider/azure.conf]]'
openshift_node_kubelet_args='["cloud-provider": ["azure"], "cloud-config": ["/etc/origin/cloudprovider/azure.conf"], "enable-controller-attach-detach": ["true"]]
```

```
# default selectors for router and registry services
openshift_router_selector='region=infra'
openshift_registry_selector='region=infra'

openshift_master_cluster_method=native
openshift_master_cluster_hostname=masterdnxrlqnskykzly.eastus2.cloudapp.azure.com
openshift_master_cluster_public_hostname=masterdnxrlqnskykzly.eastus2.cloudapp.azure.com
openshift_master_cluster_public_vip=137.116.55.75

# Enable HTPasswdPasswordIdentityProvider
openshift_master_identity_providers=[{"name": 'htpasswd_auth', 'login': 'true', 'challenge': 'true', 'kind': 'HTPasswdPasswordIdentityProvider', 'filename': '/etc/origin/master/htpasswd'}]
openshift_master_identity_providers=[{"name": 'OCP_Admin', 'login': 'true', 'challenge': 'true', 'kind': 'HTPasswdPasswordIdentityProvider', 'filename': '/etc/origin/master/htpasswdadmins'}]
```

```
# host group for nodes
[nodes]

ocp-digital-master-0 openshift_node_labels="{ 'region': 'master', 'zone': 'default' }" openshift_hostname=ocp-digital-master-0
ocp-digital-master-1 openshift_node_labels="{ 'region': 'master', 'zone': 'default' }" openshift_hostname=ocp-digital-master-1
ocp-digital-master-2 openshift_node_labels="{ 'region': 'master', 'zone': 'default' }" openshift_hostname=ocp-digital-master-2

ocp-digital-infra-0 openshift_node_labels="{ 'region': 'infra', 'zone': 'default' }" openshift_hostname=ocp-digital-infra-0
ocp-digital-infra-1 openshift_node_labels="{ 'region': 'infra', 'zone': 'default' }" openshift_hostname=ocp-digital-infra-1
ocp-digital-infra-2 openshift_node_labels="{ 'region': 'infra', 'zone': 'default' }" openshift_hostname=ocp-digital-infra-2

ocp-digital-node-0 openshift_node_labels="{ 'region': 'app', 'zone': 'default' }" openshift_hostname=ocp-digital-node-0
ocp-digital-node-1 openshift_node_labels="{ 'region': 'app', 'zone': 'default' }" openshift_hostname=ocp-digital-node-1
ocp-digital-node-2 openshift_node_labels="{ 'region': 'app', 'zone': 'default' }" openshift_hostname=ocp-digital-node-2
```

Las imágenes anteriores mapean la configuración de la siguiente tabla y las cuales van a dictaminar el rol de cada nodo dentro del Cluster de Openshift:

Hostname	Componente de infraestructura instalado
ocp-digital-master-0	Master, etcd y nodo de aplicaciones
ocp-digital-master-1	
ocp-digital-master-2	
ocp-digital-infra-0	Nodo con etiqueta de "infra"
ocp-digital-infra-1	
ocp-digital-infra-2	
ocp-digital-node-0	Nodos de aplicaciones
ocp-digital-node-1	
ocp-digital-node-2	

Una vez instalado el software de Openshift correspondiente en cada nodo, podemos ver los nodos desde la línea de comandos de la herramienta:

```
[clusteradmin@ocp-digital-master-0 ~]$ oc get node
NAME                                STATUS    ROLES    AGE     VERSION
ocp-digital-infra-0                 Ready    <none>    37d     v1.9.1+a0celbc657
ocp-digital-infra-1                 Ready    <none>    37d     v1.9.1+a0celbc657
ocp-digital-infra-2                 Ready    <none>    37d     v1.9.1+a0celbc657
ocp-digital-master-0                Ready    master    37d     v1.9.1+a0celbc657
ocp-digital-master-1                Ready    master    37d     v1.9.1+a0celbc657
ocp-digital-master-2                Ready    master    37d     v1.9.1+a0celbc657
ocp-digital-node-0                  Ready    compute   37d     v1.9.1+a0celbc657
ocp-digital-node-1                  Ready    compute   37d     v1.9.1+a0celbc657
ocp-digital-node-2                  Ready    compute   37d     v1.9.1+a0celbc657
```

A continuación, se muestra el estado de cada nodo:

OCP-DIGITAL-MASTER-0:

```
[clusteradmin@ocp-digital-master-0 ~]$ oc describe node ocp-digital-master-0
Name:          ocp-digital-master-0
Roles:         master
Labels:        beta.kubernetes.io/arch=amd64
               beta.kubernetes.io/instance-type=Standard_E4s_v3
               beta.kubernetes.io/os=linux
               failure-domain.beta.kubernetes.io/region=eastus2
               failure-domain.beta.kubernetes.io/zone=0
               kubernetes.io/hostname=ocp-digital-master-0
               logging=true
               logging-infra-fluentd=true
               node-role.kubernetes.io/master=true
               openshift-infra=apiserver
               region=master
               zone=default
Annotations:   volumes.kubernetes.io/controller-managed-attach-detach=true
Taints:        <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:40 -0500
Conditions:
  Type            Status  LastHeartbeatTime             LastTransitionTime            Reason                       Message
  ----            -
  OutOfDisk       False   Mon, 27 May 2019 13:53:01 -0500 Sun, 26 May 2019 23:37:06 -0500 KubeletHasSufficientDisk    kubelet has sufficient disk space available
  MemoryPressure  False   Mon, 27 May 2019 13:53:01 -0500 Sun, 26 May 2019 23:37:06 -0500 KubeletHasSufficientMemory  kubelet has sufficient memory available
  DiskPressure    False   Mon, 27 May 2019 13:53:01 -0500 Sun, 26 May 2019 23:37:06 -0500 KubeletHasNoDiskPressure    kubelet has no disk pressure
  Ready          True    Mon, 27 May 2019 13:53:01 -0500 Sun, 26 May 2019 23:37:06 -0500 KubeletReady                 kubelet is posting ready status

Addresses:
  InternalIP:  10.1.0.21
  Hostname:    ocp-digital-master-0
Capacity:
  cpu:    4
  memory: 32927876Ki
  pods:   40
Allocatable:
  cpu:    4
  memory: 32825476Ki
  pods:   40
```

OCP-DIGITAL-MASTER-1:

```
Name:          ocp-digital-master-1
Roles:         master
Labels:        beta.kubernetes.io/arch=amd64
               beta.kubernetes.io/instance-type=Standard_E4s_v3
               beta.kubernetes.io/os=linux
               failure-domain.beta.kubernetes.io/region=eastus2
               failure-domain.beta.kubernetes.io/zone=1
               kubernetes.io/hostname=ocp-digital-master-1
               logging=true
               logging-infra-fluentd=true
               node-role.kubernetes.io/master=true
               region=master
               zone=default
Annotations:   volumes.kubernetes.io/controller-managed-attach-detach=true
Taints:        <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:39 -0500
Conditions:
  Type            Status  LastHeartbeatTime             LastTransitionTime            Reason                       Message
  ----            -
  OutOfDisk       False   Mon, 27 May 2019 13:56:56 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientDisk    kubelet has sufficient disk space available
  MemoryPressure  False   Mon, 27 May 2019 13:56:56 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientMemory  kubelet has sufficient memory available
  DiskPressure    False   Mon, 27 May 2019 13:56:56 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasNoDiskPressure    kubelet has no disk pressure
  Ready          True    Mon, 27 May 2019 13:56:56 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletReady                 kubelet is posting ready status

Addresses:
  InternalIP:  10.1.0.20
  Hostname:    ocp-digital-master-1
Capacity:
  cpu:    4
  memory: 32927876Ki
  pods:   40
Allocatable:
  cpu:    4
  memory: 32825476Ki
  pods:   40
```

OCP-DIGITAL-MASTER-2:

```

Name: ocp-digital-master-2
Roles: master
Labels: beta.kubernetes.io/arch=amd64
        beta.kubernetes.io/instance-type=Standard_F4s_v3
        beta.kubernetes.io/os=linux
        failure-domain.beta.kubernetes.io/region=eastus2
        failure-domain.beta.kubernetes.io/zone=0
        kubernetes.io/hostname=ocp-digital-master-2
        logging=true
        logging-infra-fluentd=true
        node-role.kubernetes.io/master=true
        region=master
        zone=default
Annotations: volumes.kubernetes.io/controller-managed-attach-detach=true
Taints: <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:39 -0500
Conditions:
  Type             Status  LastHeartbeatTime             LastTransitionTime             Reason                        Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 13:59:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientDisk     kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 13:59:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientMemory   kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 13:59:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasNoDiskPressure     kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 13:59:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletReady                  kubelet is posting ready status

Addresses:
  InternalIP: 10.1.0.19
  Hostname: ocp-digital-master-2
Capacity:
  cpu: 4
  memory: 32927876Ki
  pods: 40
Allocatable:
  cpu: 4
  memory: 32825476Ki
  pods: 40

```

OCP-DIGITAL-INFRA-0:

```

Name: ocp-digital-infra-0
Roles: <none>
Labels: beta.kubernetes.io/arch=amd64
        beta.kubernetes.io/instance-type=Standard_E8s_v3
        beta.kubernetes.io/os=linux
        failure-domain.beta.kubernetes.io/region=eastus2
        failure-domain.beta.kubernetes.io/zone=0
        kubernetes.io/hostname=ocp-digital-infra-0
        logging=true
        logging-infra-fluentd=true
        region=infra
        zone=default
Annotations: volumes.kubernetes.io/controller-managed-attach-detach=true
Taints: <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:40 -0500
Conditions:
  Type             Status  LastHeartbeatTime             LastTransitionTime             Reason                        Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 14:01:00 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientDisk     kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 14:01:00 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientMemory   kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 14:01:00 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasNoDiskPressure     kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 14:01:00 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletReady                  kubelet is posting ready status

Addresses:
  InternalIP: 10.1.0.16
  Hostname: ocp-digital-infra-0
Capacity:
  cpu: 8
  memory: 65857996Ki
  pods: 80
Allocatable:
  cpu: 8
  memory: 65855596Ki
  pods: 80

```

OCP-DIGITAL-INFRA-1:

```

Name: ocp-digital-infra-1
Roles: <none>
Labels: beta.kubernetes.io/arch=amd64
        beta.kubernetes.io/instance-type=Standard_E8s_v3
        beta.kubernetes.io/os=linux
        failure-domain.beta.kubernetes.io/region=eastus2
        failure-domain.beta.kubernetes.io/zone=1
        kubernetes.io/hostname=ocp-digital-infra-1
        logging=true
        logging-infra-fluentd=true
        region=infra
        zone=default
Annotations: volumes.kubernetes.io/controller-managed-attach-detach=true
Taints: <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:39 -0500
Conditions:
  Type             Status  LastHeartbeatTime           LastTransitionTime        Reason                    Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 14:02:22 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletHasSufficientDisk   kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 14:02:22 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletHasSufficientMemory  kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 14:02:22 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletHasNoDiskPressure    kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 14:02:22 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletReady                kubelet is posting ready status
Addresses:
  InternalIP: 10.1.0.18
  Hostname: ocp-digital-infra-1
Capacity:
  cpu: 8
  memory: 65957996Ki
  pods: 80
Allocatable:
  cpu: 8
  memory: 65855596Ki
  pods: 80

```

OCP-DIGITAL-INFRA-2:

```

[clusteradmin@ocp-digital-master-0 ~]$ oc describe node ocp-digital-infra-2
Name: ocp-digital-infra-2
Roles: <none>
Labels: beta.kubernetes.io/arch=amd64
        beta.kubernetes.io/instance-type=Standard_E8s_v3
        beta.kubernetes.io/os=linux
        failure-domain.beta.kubernetes.io/region=eastus2
        failure-domain.beta.kubernetes.io/zone=0
        kubernetes.io/hostname=ocp-digital-infra-2
        logging=true
        logging-infra-fluentd=true
        region=infra
        zone=default
Annotations: volumes.kubernetes.io/controller-managed-attach-detach=true
Taints: <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:40 -0500
Conditions:
  Type             Status  LastHeartbeatTime           LastTransitionTime        Reason                    Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 14:03:03 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletHasSufficientDisk   kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 14:03:03 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletHasSufficientMemory  kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 14:03:03 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletHasNoDiskPressure    kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 14:03:03 -0500   Sat, 25 May 2019 06:32:21 -0500   KubeletReady                kubelet is posting ready status
Addresses:
  InternalIP: 10.1.0.17
  Hostname: ocp-digital-infra-2
Capacity:
  cpu: 8
  memory: 65957996Ki
  pods: 80
Allocatable:
  cpu: 8
  memory: 65855596Ki
  pods: 80

```

OCP-DIGITAL-NODE-0:

```

Name: ocp-digital-node-0
Roles: compute
Labels: beta.kubernetes.io/arch=amd64
       beta.kubernetes.io/instance-type=Standard_E8s_v3
       beta.kubernetes.io/os=linux
       failure-domain.beta.kubernetes.io/region=eastus2
       failure-domain.beta.kubernetes.io/zone=0
       kubernetes.io/hostname=ocp-digital-node-0
       logging=true
       logging-infra-fluentd=true
       node-role.kubernetes.io/compute=true
       region=app
       zone=default
Annotations: volumes.kubernetes.io/controller-managed-attach-detach=true
Taints: <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:40 -0500
Conditions:
  Type             Status  LastHeartbeatTime             LastTransitionTime             Reason                       Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 14:04:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientDisk    kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 14:04:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientMemory  kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 14:04:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasNoDiskPressure    kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 14:04:26 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletReady                 kubelet is posting ready status

Addresses:
  InternalIP: 10.2.0.15
  Hostname: ocp-digital-node-0
Capacity:
  cpu: 8
  memory: 65957996Ki
  pods: 80
Allocatable:
  cpu: 8
  memory: 65855596Ki
  pods: 80

```

OCP-DIGITAL-NODE-1:

```

Name: ocp-digital-node-1
Roles: compute
Labels: beta.kubernetes.io/arch=amd64
       beta.kubernetes.io/instance-type=Standard_E8s_v3
       beta.kubernetes.io/os=linux
       failure-domain.beta.kubernetes.io/region=eastus2
       failure-domain.beta.kubernetes.io/zone=1
       kubernetes.io/hostname=ocp-digital-node-1
       logging=true
       logging-infra-fluentd=true
       node-role.kubernetes.io/compute=true
       region=app
       zone=default
Annotations: volumes.kubernetes.io/controller-managed-attach-detach=true
Taints: <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:40 -0500
Conditions:
  Type             Status  LastHeartbeatTime             LastTransitionTime             Reason                       Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 14:05:53 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientDisk    kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 14:05:53 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasSufficientMemory  kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 14:05:53 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletHasNoDiskPressure    kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 14:05:53 -0500 Sat, 25 May 2019 06:32:21 -0500 KubeletReady                 kubelet is posting ready status

Addresses:
  InternalIP: 10.2.0.16
  Hostname: ocp-digital-node-1
Capacity:
  cpu: 8
  memory: 65957996Ki
  pods: 80
Allocatable:
  cpu: 8
  memory: 65855596Ki
  pods: 80

```


OCP-DIGITAL-NODE-2:

```

Name: ocp-digital-node-2
Roles: compute
Labels:
  beta.kubernetes.io/arch=amd64
  beta.kubernetes.io/instance-type=Standard_E8s_v3
  beta.kubernetes.io/os=linux
  failure-domain.beta.kubernetes.io/region=eastus2
  failure-domain.beta.kubernetes.io/zone=0
  kubernetes.io/hostname=ocp-digital-node-2
  logging=true
  logging-infra-fluentd=true
  node-role.kubernetes.io/compute=true
  region=app
  zone=default
Annotations:
  volumes.kubernetes.io/controller-managed-attach-detach=true
Taints:
  <none>
CreationTimestamp: Sat, 20 Apr 2019 07:55:40 -0500
Conditions:
  Type             Status  LastHeartbeatTime             LastTransitionTime             Reason                           Message
  ----             -
  OutOfDisk         False   Mon, 27 May 2019 14:07:08 -0500 Sun, 26 May 2019 23:37:08 -0500 KubeletHasSufficientDisk         kubelet has sufficient disk space available
  MemoryPressure    False   Mon, 27 May 2019 14:07:08 -0500 Sun, 26 May 2019 23:37:08 -0500 KubeletHasSufficientMemory       kubelet has sufficient memory available
  DiskPressure      False   Mon, 27 May 2019 14:07:08 -0500 Sun, 26 May 2019 23:37:08 -0500 KubeletHasNoDiskPressure         kubelet has no disk pressure
  Ready             True    Mon, 27 May 2019 14:07:08 -0500 Sun, 26 May 2019 23:37:08 -0500 KubeletReady                     kubelet is posting ready status
Addresses:
  InternalIP: 10.2.0.17
  Hostname: ocp-digital-node-2
Capacity:
  cpu: 8
  memory: 6595800Ki
  pods: 80
Allocatable:
  cpu: 8
  memory: 65855600Ki
  pods: 80

```

Finalmente se muestran las opciones de configuración de los archivos de nodos maestros y nodos de aplicación. Openshift instala su propio servidor de nombres en los nodos maestros para poder realizar llamados por FQDN desde cualquier servidor en el clúster. La imagen de abajo muestra la configuración del servidor de nombres:

```

dnsConfig:
  bindAddress: 0.0.0.0:8053
  bindNetwork: tcp4
etcdClientInfo:
  ca: master.etcd-ca.crt
  certFile: master.etcd-client.crt
  keyFile: master.etcd-client.key
  urls:
  - https://ocp-digital-master-0:2379
  - https://ocp-digital-master-1:2379
  - https://ocp-digital-master-2:2379
etcdStorageConfig:
  kubernetesStoragePrefix: kubernetes.io
  kubernetesStorageVersion: v1
  openShiftStoragePrefix: openshift.io
  openShiftStorageVersion: v1

```

En la siguiente imagen se muestran las configuraciones de llaves para los llamados de dockers por medio de comunicación segura. Otra configuración importante es la ruta del archivo de configuración del proveedor de nube que en este caso es Azure.

```
kind: MasterConfig
kubeletClientInfo:
  ca: ca-bundle.crt
  certFile: master.kubelet-client.crt
  keyFile: master.kubelet-client.key
  port: 10250
kubernetesMasterConfig:
  apiServerArguments:
    cloud-config:
      - /etc/origin/cloudprovider/azure.conf
    cloud-provider:
      - azure
    runtime-config:
      - apis/settings.k8s.io/v1alpha1=true
    storage-backend:
      - etcd3
    storage-media-type:
      - application/vnd.kubernetes.protobuf
    feature-gates:
      - PVCProtection=true
  controllerArguments:
    cloud-config:
      - /etc/origin/cloudprovider/azure.conf
    cloud-provider:
      - azure
    feature-gates:
      - PVCProtection=true
  masterCount: 3
  masterIP: 10.1.0.21
  podEvictionTimeout: null
  proxyClientInfo:
    certFile: master.proxy-client.crt
    keyFile: master.proxy-client.key
  schedulerArguments: null
  schedulerConfigFile: /etc/origin/master/scheduler.json
  servicesNodePortRange: ''
  servicesSubnet: 172.30.0.0/16
  staticNodeNames: []
```

Por ultimo se muestran la configuración de redes de contenedores y los métodos de autenticación de usuarios hacia la plataforma de Openshift:

```
networkConfig:
  clusterNetworkCIDR: 10.128.0.0/14
  clusterNetworks:
  - cidr: 10.128.0.0/14
    hostSubnetLength: 9
  externalIPNetworkCIDRs:
  - 0.0.0.0/0
  hostSubnetLength: 9
  networkPluginName: redhat/openshift-ovs-subnet
  serviceNetworkCIDR: 172.30.0.0/16
oauthConfig:
  assetPublicURL: https://masterdnsxrlqzkykzly.eastus2.cloudapp.azure.com/console/
  grantConfig:
    method: auto
  identityProviders:
  - challenge: true
    login: true
    mappingMethod: claim
    name: OCP_Admin
    provider:
      apiVersion: v1
      file: /etc/origin/master/htpasswdadmins
      kind: HTTPasswdPasswordIdentityProvider
  - name: OCP-DIGITAL-AAD
    challenge: false
    login: true
    mappingMethod: claim
    provider:
      apiVersion: v1
      kind: OpenIDIdentityProvider
      clientID: d6bbc3ad-054c-420f-93f8-3f69fcc0683c
      clientSecret: Cl4r04dmln2019!
    claims:
      id:
      - sub
      preferredUsername:
      - unique_name
      name:
      - name
      email:
      - email
    urls:
      authorize: https://login.microsoftonline.com/bc21c6c5-b0ee-414b-9a51-352b288d6b45/oauth2/authorize
      token: https://login.microsoftonline.com/bc21c6c5-b0ee-414b-9a51-352b288d6b45/oauth2/token
```

3.3 Configuración de registros de imágenes

Openshift por default consume imágenes de contenedores publicas hospedadas en DockerHub, por lo tanto, las imágenes que se pudiesen desplegar en los diferentes proyectos sobre la plataforma Openshift pudiesen corromperse al tener acceso publico y debido a este problema de seguridad se planteo utilizar el servicio Azure Container Registry para hospedar imágenes creadas por el equipo de desarrollo y que posteriormente se utilizaran para el despliegue de aplicaciones en Openshift.

Se realizo el despliegue y configuración del servicio de Azure Container Registry llamado **clarodigital.azurecr.io** con las siguientes configuraciones:

Grupo de recursos ([cambiar](#))
RG-OCP-DIGITAL

Ubicación
Este de EE. UU. 2

Suscripción ([cambiar](#))
Microsoft Azure CSP Claro

Id. de suscripción
93f223ec-e56d-46ef-a495-2f86d2cb5ca6

Servidor de inicio de sesión
clarodigital.azurecr.io

Fecha de creación
25/4/2019 17:59 GMT-5

SKU
Prémium

Estado de aprovisionamiento
Correcto

Además, se agregó la dirección de ACR en el archivo de configuración de repositorios de Docker en todos los nodos del clúster de Openshift:

```
# This is a system-wide configuration file used to
# keep track of registries for various container backends.
# It adheres to TOML format and does not support recursive
# lists of registries.

# The default location for this configuration file is /etc/containers/registries.conf.

# The only valid categories are: 'registries.search', 'registries.insecure',
# and 'registries.block'.

[registries.search]
registries = ['registry.access.redhat.com', 'clarodigital.azurecr.io', 'docker.io', 'registry.fedoraproject.org', 'quay.io', 'registry.centos.org']

# If you need to access insecure registries, add the registry's fully-qualified name.
# An insecure registry is one that does not have a valid SSL certificate or only does HTTP.
[registries.insecure]
registries = []

# If you need to block pull access from a registry, uncomment the section below
# and add the registries fully-qualified name.
#
```

NOTA: Hasta el momento de la creación de este documento se decidió dejar los demás repositorios de imágenes para pruebas del equipo de desarrollo, posteriormente se eliminarán y solo se quedará el repositorio de Azure.

3.4 Configuración de router

Para gestionar el tráfico externo destinado a los servicios dentro del clúster de Openshift, se utiliza un ruteador interno o también conocido como HAProxy, este servicio se despliega por medio de imágenes en contenedores; para poder ofrecer un esquema de alta disponibilidad de este servicio se instaló 1 contenedor de HA Proxy por cada nodo de infraestructura que existe en el clúster de Openshift, a continuación, se muestra la distribución de HAProxy en el clúster:

<p>Status</p> <p>Status: Running</p> <p>Deployment: router, #1</p> <p>IP: 10.1.0.18</p> <p>Node: ocp-digital-infra-1 (10.1.0.18)</p> <p>Restart Policy: Always</p> <p>Container router</p> <p>State: Running since May 29, 2019 12:35:53 AM</p> <p>Ready: true</p> <p>Restart Count: 0</p>	<p>Template</p> <p>Containers</p> <p>router</p> <p> Image: openshift/origin-haproxy-router:v3.9.0</p> <p> Ports: 80/TCP → 80, 443/TCP → 443, 1936/TCP (stats) → 1936</p> <p> Mount: server-certificate → /etc/pki/tls/private read-only</p> <p> Mount: router-token-chkxm → /var/run/secrets/kubernetes.io/serviceaccount read-only</p> <p> CPU: 100 millicores requested</p> <p> Memory: 256 MiB requested</p> <p> Readiness Probe: GET /healthz on port 1936 (HTTP) 10s delay, 1s timeout</p> <p> Liveness Probe: GET /healthz on port 1936 (HTTP) 10s delay, 1s timeout</p>
<p>Status</p> <p>Status: Running</p> <p>Deployment: router, #1</p> <p>IP: 10.1.0.16</p> <p>Node: ocp-digital-infra-0 (10.1.0.16)</p> <p>Restart Policy: Always</p> <p>Container router</p> <p>State: Running since Apr 30, 2019 6:50:39 AM</p> <p>Ready: true</p> <p>Restart Count: 0</p>	<p>Template</p> <p>Containers</p> <p>router</p> <p> Image: openshift/origin-haproxy-router:v3.9.0</p> <p> Ports: 80/TCP → 80, 443/TCP → 443, 1936/TCP (stats) → 1936</p> <p> Mount: server-certificate → /etc/pki/tls/private read-only</p> <p> Mount: router-token-chkxm → /var/run/secrets/kubernetes.io/serviceaccount read-only</p> <p> CPU: 100 millicores requested</p> <p> Memory: 256 MiB requested</p> <p> Readiness Probe: GET /healthz on port 1936 (HTTP) 10s delay, 1s timeout</p> <p> Liveness Probe: GET /healthz on port 1936 (HTTP) 10s delay, 1s timeout</p>
<p>Status</p> <p>Status: Running</p> <p>Deployment: router, #1</p> <p>IP: 10.1.0.17</p> <p>Node: ocp-digital-infra-2 (10.1.0.17)</p> <p>Restart Policy: Always</p> <p>Container router</p> <p>State: Running since Apr 30, 2019 7:01:13 AM</p> <p>Ready: true</p> <p>Restart Count: 0</p>	<p>Template</p> <p>Containers</p> <p>router</p> <p> Image: openshift/origin-haproxy-router:v3.9.0</p> <p> Ports: 80/TCP → 80, 443/TCP → 443, 1936/TCP (stats) → 1936</p> <p> Mount: server-certificate → /etc/pki/tls/private read-only</p> <p> Mount: router-token-chkxm → /var/run/secrets/kubernetes.io/serviceaccount read-only</p> <p> CPU: 100 millicores requested</p> <p> Memory: 256 MiB requested</p> <p> Readiness Probe: GET /healthz on port 1936 (HTTP) 10s delay, 1s timeout</p> <p> Liveness Probe: GET /healthz on port 1936 (HTTP) 10s delay, 1s timeout</p>

A continuación, se muestra la configuración de los servicios de HAProxy a nivel del clúster, se puede observar que esta configurado para utilizar balanceo por "roundrobin" y que tiene capacidad de 240000 conexiones por segundo:

```
Name: router
Namespace: default
Created: 5 weeks ago
Labels: router=router
Annotations: <none>
Latest Version: 4
Selector: router=router
Replicas: 3
Triggers: Config
Strategy: Rolling
Template:
Pod Template:
  Labels: router=router
  Service Account: router
  Containers:
    router:
      Image: openshift/origin-haproxy-router:v3.9.0
      Ports: 80/TCP, 443/TCP, 1936/TCP
      Requests:
        cpu: 100m
        memory: 256Mi
      Liveness: http-get http://localhost:1936/healthz delay=10s timeout=1s period=10s #success=1 #failure=3
      Readiness: http-get http://localhost:1936/healthz delay=10s timeout=1s period=10s #success=1 #failure=3
      Environment:
        DEFAULT_CERTIFICATE_DIR: /etc/pki/tls/private
        DEFAULT_CERTIFICATE_PATH: /etc/pki/tls/private/tls.crt
        ROUTER_CIPHERS:
        ROUTER_EXTERNAL_HOST_HOSTNAME:
        ROUTER_EXTERNAL_HOST_HTTPS_VSERVER:
        ROUTER_EXTERNAL_HOST_HTTP_VSERVER:
        ROUTER_EXTERNAL_HOST_INSECURE: false
        ROUTER_EXTERNAL_HOST_INTERNAL_ADDRESS:
        ROUTER_EXTERNAL_HOST_PARTITION_PATH:
        ROUTER_EXTERNAL_HOST_PASSWORD:
        ROUTER_EXTERNAL_HOST_PRIVKEY: /etc/secret-volume/router.pem
        ROUTER_EXTERNAL_HOST_USERNAME:
        ROUTER_EXTERNAL_HOST_VXLAN_GW_CIDR:
        ROUTER_LISTEN_ADDR: 0.0.0.0:1936
        ROUTER_METRICS_TYPE: haproxy
        ROUTER_SERVICE_HTTPS_PORT: 443
        ROUTER_SERVICE_HTTP_PORT: 80
        ROUTER_SERVICE_NAME: router
        ROUTER_SERVICE_NAMESPACE: default
        ROUTER_SUBDOMAIN:
        STATS_PASSWORD: JWCuFRQ8I4
        STATS_PORT: 1936
        STATS_USERNAME: admin
        ROUTER_MAX_CONNECTIONS: 240000
        ROUTER_TCP_BALANCE_SCHEME: roundrobin
        ROUTER_LOAD_BALANCE_ALGORITHM: roundrobin
      Mounts:
        /etc/pki/tls/private from server-certificate (ro)
  Volumes:
    server-certificate:
      Type: Secret (a volume populated by a Secret)
      SecretName: router-certs
      Optional: false
```

3.5 Configuración de autenticación

Por default Openshift instala "HTPasswd Authentication" como proveedor de identidades para el clúster. A modo de entregar un ambiente más seguro se añadió otro método de autenticación utilizando Azure Active Directory como proveedor de identidades, restringiendo el acceso por medio de HTPasswd para usuarios administrativos del clúster y dejando el acceso de usuarios comunes (desarrolladores, tester, etc) por medio Azure AD y poder tener un control de usuarios y contraseñas más robusto.

A continuación, se muestran las configuraciones hechas con el servicio de identidades; la primera imagen nos muestra los 2 proveedores de identidades configurados:

Métodos de autenticación	
Nombre	Proveedor de identidad
OCP_Admin	HTPaswd
OCP-DIGITAL-AAD	Azure Active Directory

```

oauthConfig:
  assetPublicURL: https://masterdnsxrlqzkykzly.eastus2.cloudapp.azure.com/console/
  grantConfig:
    method: auto
  identityProviders:
  - challenge: true
    login: true
    mappingMethod: claim
    name: OCP_Admin
    provider:
      apiVersion: v1
      file: /etc/origin/master/htpasswdadmins
      kind: HTPasswdPasswordIdentityProvider
    name: OCP-DIGITAL-AAD
    challenge: false
    login: true
    mappingMethod: claim
    provider:
      apiVersion: v1
      kind: OpenIDIdentityProvider
      clientID: d6bbc3ad-054c-420f-93f8-3f69fcc0683c
      clientSecret: C14r04dmln2019!
    claims:
      id:
      - sub
      preferredUsername:
      - unique_name
      name:
      - name
      email:
      - email
    urls:
      authorize: https://login.microsoftonline.com/bc21c6c5-b0ee-414b-9a51-352b288d6b45/oauth2/authorize
      token: https://login.microsoftonline.com/bc21c6c5-b0ee-414b-9a51-352b288d6b45/oauth2/token

```


3.6 Integración con Microsoft Azure

Openshift se puede configurar para acceder a la infraestructura de Microsoft Azure, incluido el uso del disco de Azure o Azure Files como almacenamiento persistente para los datos de la aplicación.

Se realizaron las configuraciones necesarias en el archivo llamado “azure.conf” que se encuentra en cada uno de los nodos miembros del clúster de Openshift:

```
("aadClientSecret": "={0}/{1}/{2}*({3}:+)AM(d)=", "securityGroupName": "", "vmName": "", "aadClientId": "6b57c83c-d603-454f-ad96-aa2452591cf5", "tenantId": "bc21c6c5-b0ee-414b-9a51-352b288d6b45", "resourceGroup": "RG-OCF-DIGITAL", "a
adTenantId": "bc21c6c5-b0ee-414b-9a51-352b288d6b45", "location": "eastus", "primaryAvailabilitySetName": "", "subscriptionId": "93f113ec-a36d-46ef-a495-2f86d2b5ca6", "cloud": "AzurePublicCloud")
```

También se añadieron las líneas en los archivos de configuración de los nodos Maestros, Infra y Aplicaciones; para los nodos Maestros se realizó la siguiente configuración:

```
kubernetesMasterConfig:
  apiServerArguments:
    cloud-config:
      - /etc/origin/cloudprovider/azure.conf
    cloud-provider:
      - azure
    runtime-config:
      - apis/settings.k8s.io/v1alpha1=true
    storage-backend:
      - etcd3
    storage-media-type:
      - application/vnd.kubernetes.protobuf
  controllerArguments:
    cloud-config:
      - /etc/origin/cloudprovider/azure.conf
    cloud-provider:
      - azure
```

En los nodos de infraestructura y los nodos primarios, cuentan con esta configuración:

```
kubeletArguments:
  cloud-config:
    - /etc/origin/cloudprovider/azure.conf
  cloud-provider:
    - azure
  enable-controller-attach-detach:
    - 'true'
  node-labels:
    - region=infra
    - zone=default
```

3.7 Configuración de almacenamiento persistente

El framework de Kubernetes permite aprovisionar un clúster de Openshift con almacenamiento persistente mediante almacenamiento en red disponible en el entorno. Esto se realizó después de completar la instalación del clúster añadiendo Azure Files como un tipo de almacenamiento persistente en el cual los usuarios tengan una forma de solicitar recursos sin tener conocimiento de la capacidad de la infraestructura subyacente.

Para poder ofrecer esta funcionalidad se creó una cuenta de almacenamiento dedicada a este servicio llamada **“odcdogotalpv”**, con las siguientes características:

Grupo de recursos ([cambiar](#))
RG-OCP-DIGITAL

Estado
Principal: Disponible, secundario: Disponible

Ubicación
Oeste de EE. UU. 2, Centro-oeste de EE. UU.

Suscripción ([cambiar](#))
Microsoft Azure CSP Claro

Id. de suscripción
93f223ec-e56d-46ef-a495-2f86d2cb5ca6

Rendimiento/Nivel de acceso
Estándar/Hot

Replicación
Almacenamiento con redundancia geográfica (GRS)

Tipo de cuenta
StorageV2 (uso general v2)

Como bien se sabe las cuentas de almacenamiento en Azure utilizan una llave para poder autenticarse y consumir el servicio, a nivel del clúster de Openshift se creó un recurso llamado "Secret":

NAME	TYPE	DATA	AGE
azure-storage-account-odcdigitalpv-secret	Opaque	2	38d

Las opciones de este recurso de clúster son:

```
Name:      azure-storage-account-odcdigitalpv-secret
Namespace: openshift-infra
Labels:    <none>
Annotations: <none>

Type: Opaque

Data
====
azurestorageaccountkey: 88 bytes
azurestorageaccountname: 12 bytes
```

NOTA: No se muestra el KEY de la cuenta de almacenamiento por seguridad, pero se puede obtener de las propiedades de esta misma desde el portal de Azure.

El siguiente paso fue registrar la nueva cuenta de almacenamiento como una clase de tipo "Azure Files" llamada "**azurefile**" dentro del clúster de Openshift:

NAME	PROVISIONER	AGE
azurefile (default)	kubernetes.io/azure-file	39d
generic	kubernetes.io/azure-disk	40d

Las propiedades de esta clase de almacenamiento se detallan a continuación:

```
Name:      azurefile
IsDefaultClass: Yes
Annotations: storageclass.kubernetes.io/is-default-class=true
Provisioner: kubernetes.io/azure-file
Parameters: location=eastus2,skuName=StandardRAGRS,storageAccount=odcdigitalpv
ReclaimPolicy: Delete
Events:    <none>
```

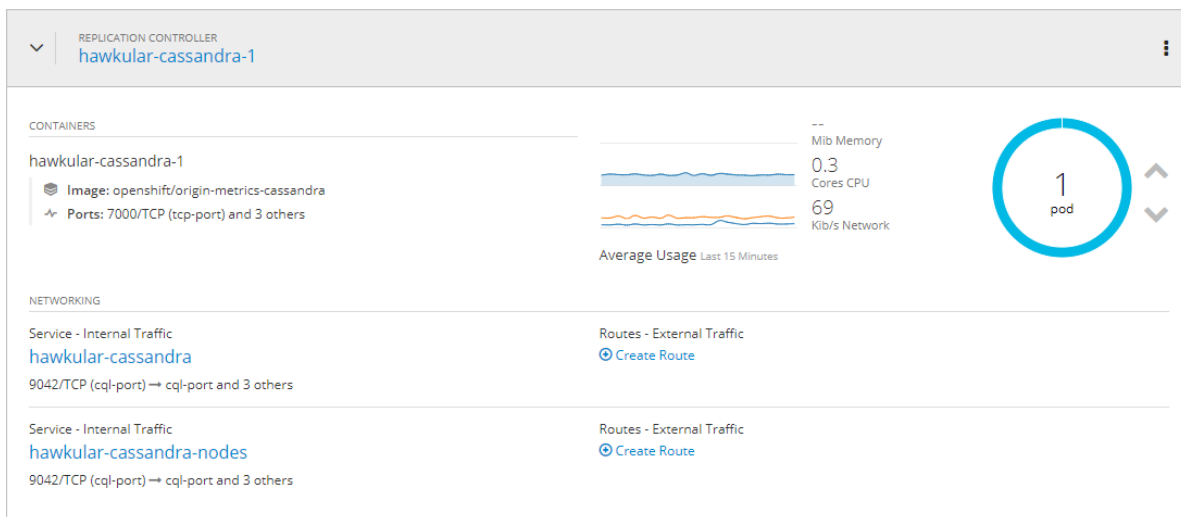
Con esta configuración el desarrollador puede solicitar recursos de almacenamiento por medio de los archivos de despliegue de imágenes y montarlos en ellas.

3.8 Configuración de métricas

Para concluir la configuración de la plataforma Openshift se activaron las métricas del clúster por medio de un proyecto llamado **"openshift-infra"** y en el cual los contenedores de este proyecto están hospedados en los nodos de infraestructura del clúster de openshift.

A continuación, se observa los 3 pods desplegados en el proyecto, cada pod tiene realiza una función diferente para el servicio de monitoreo de infraestructura; cassandra almacena las métricas, hawkular recolecta y procesa las métricas, heapster se encarga de recoger la información de los que hay en cada nodo del clúster y enviarlo a cassandra.

NAME	READY	STATUS	RESTARTS	AGE
hawkular-cassandra-1-tzg7j	1/1	Running	55	30d
hawkular-metrics-76hg6	1/1	Running	1	30d
heapster-qsnjm	1/1	Running	1	30d



▼
⋮

REPLICATION CONTROLLER
hawkular-metrics

CONTAINERS

hawkular-metrics

- Image: openshift/origin-metrics-hawkular-metrics
- Ports: 8080/TCP (http-endpoint) and 2 others

Average Usage Last 15 Minutes

Metric	Value
Mib Memory	0.06
Cores CPU	110
Kib/s Network	-

1

pod

NETWORKING

Service - Internal Traffic

hawkular-metrics

443/TCP → https-endpoint

Routes - External Traffic

<https://hawkular-metrics.137.116.47.4.nip.io>

Route [hawkular-metrics](#)

▼
REPLICATION CONTROLLER
heapster
⋮

CONTAINERS

heapster

- Image: openshift/origin-metrics-heapster
- Ports: 8082/TCP (http-endpoint)

Average Usage Last 15 Minutes

--	Mib Memory
0.01	Cores CPU
55	Kib/s Network

1
pod

⌵
⌶

NETWORKING

Service - Internal Traffic

heapster

80/TCP ⇒ http-endpoint

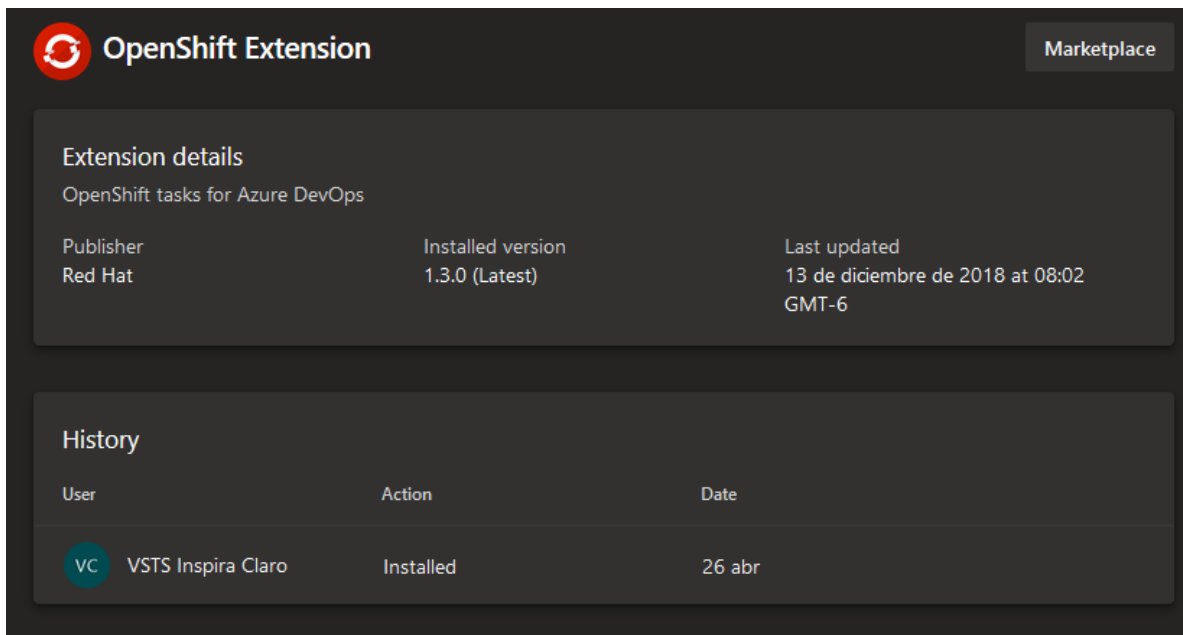
Routes - External Traffic

[➕ Create Route](#)

4 Plataforma DevOps: Azure DevOps

Azure DevOps proporciona servicios para desarrolladores y ayudar a los equipos a planificar el trabajo, colaborar en el desarrollo de código y crear e implementar aplicaciones. Los desarrolladores pueden trabajar en la nube con los Servicios de DevOps de Azure. El ambiente de Azure DevOps es independiente al portal de Azure y su configuración es independiente; las configuraciones que se realizaron fueron las siguientes:

Se añadió la extensión de Openshift, esta extensión proporciona un método de conexión hacia el clúster de Openshift.



OpenShift Extension Marketplace

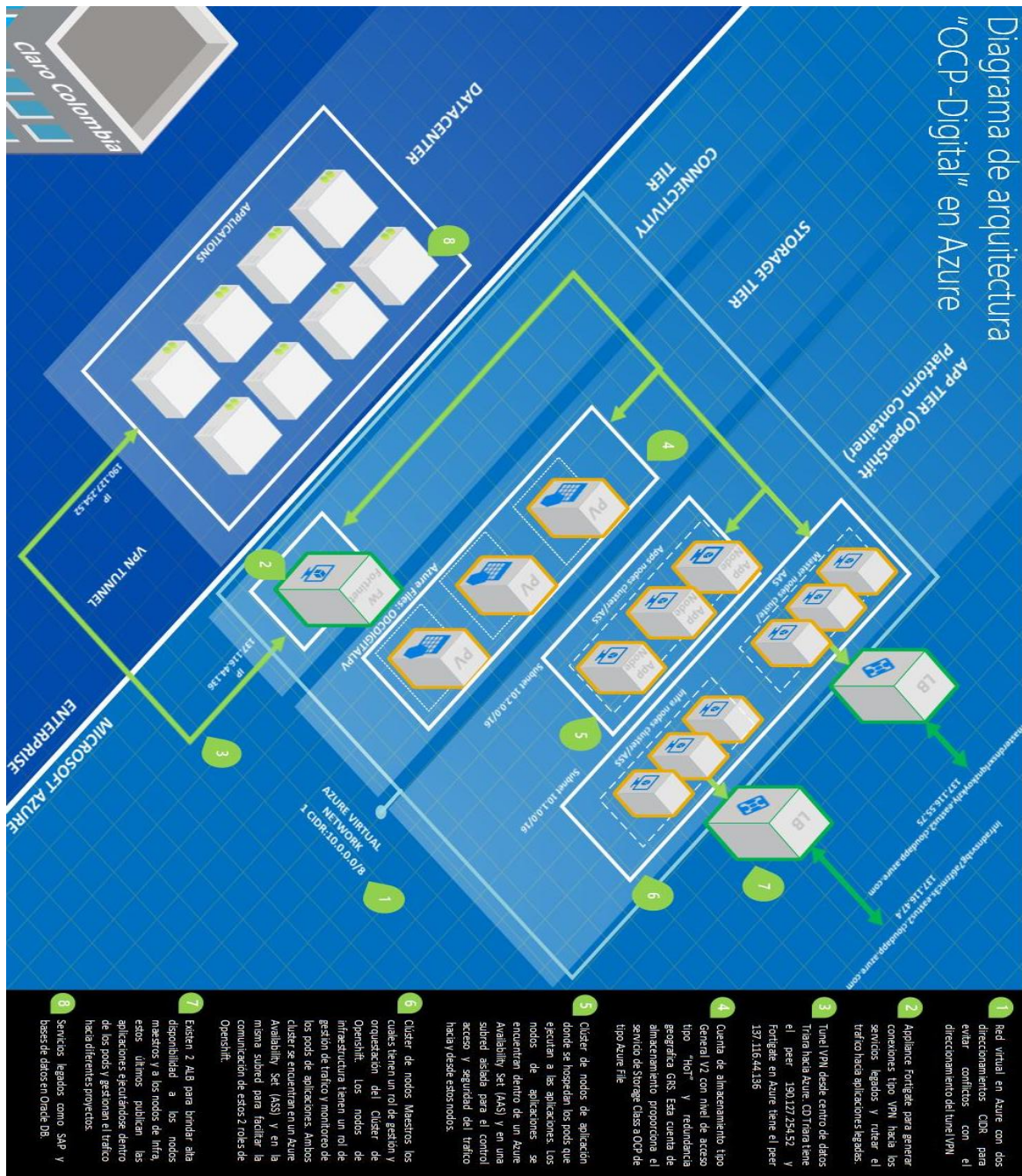
Extension details
OpenShift tasks for Azure DevOps

Publisher	Installed version	Last updated
Red Hat	1.3.0 (Latest)	13 de diciembre de 2018 at 08:02 GMT-6

History

User	Action	Date
VC VSTS Inspira Claro	Installed	26 abr

5 Diagrama de infraestructura



6 Aceptación

El siguiente apartado del documento tiene como objetivo presentar la conformidad de las partes que se consideran como claves dentro de la toma de decisiones del proyecto en curso. Una vez firmado este documento se dará como aprobado el enfoque, estrategia, visión y alcances definidos por el equipo de consultoría de Actiglobal.

Actiglobal

Claro Colombia