



Citrix ADC CPX 13.1

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Citrix solo tiene traducción automática. Citrix no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Citrix se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Citrix, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Citrix no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Acerca de Citrix ADC CPX	3
Arquitectura y flujo de tráfico	5
Licencias de Citrix ADC CPX	8
Implementación de una instancia CPX de Citrix ADC en Docker	17
Agregar instancias CPX de Citrix ADC a Citrix ADM	25
Agregador de licencias Citrix ADC CPX	29
Configuración de Citrix ADC CPX	35
Configuración de AppFlow en una instancia de Citrix ADC CPX	39
Configuración de Citrix ADC CPX mediante un archivo de configuración	42
Compatibilidad con redirección dinámica en Citrix ADC CPX	44
Configuración de alta disponibilidad para Citrix ADC CPX	47
Configuración de controladores de registro de Docker	53
Actualización de una instancia CPX de Citrix ADC	54
Uso de servidores virtuales comodín en la instancia de Citrix ADC CPX	56
Implementar Citrix ADC CPX como proxy para habilitar el flujo de tráfico de este a oeste	57
Implementar Citrix ADC CPX en una red de host único	61
Implementar Citrix ADC CPX en una red multihost	62
Implementar Citrix ADC CPX con acceso directo a la red	68
Configurar Citrix ADC CPX en Kubernetes mediante ConfigMaps	69
Implementar CPX de Citrix ADC como cachés DNS locales para nodos de Kubernetes	72
Implementar el proxy CPX de Citrix ADC en Google Compute Engine	77
Solución de problemas de Citrix ADC CPX	100

Acerca de Citrix ADC CPX

February 19, 2022

Citrix ADC CPX es un controlador de entrega de aplicaciones basado en contenedores que se puede aprovisionar en un host Docker. Citrix ADC CPX permite a los clientes aprovechar las capacidades del motor de Docker y utilizar las funciones de equilibrio de carga y administración de tráfico de Citrix ADC para aplicaciones basadas en contenedores. Puede implementar una o más instancias de Citrix ADC CPX como instancias independientes en un host de Docker.

Una instancia de Citrix ADC CPX proporciona un rendimiento de hasta 1 Gbps.

Como factor de forma en contenedores de Citrix ADC, Citrix ADC CPX se integra bien en el entorno de Kubernetes y forma parte integral de la solución nativa de la nube de Citrix. La solución nativa de Citrix Cloud le ayuda a crear y entregar aplicaciones de software con velocidad, agilidad y eficiencia en un entorno Kubernetes. Con la solución nativa de la nube de Citrix, puede garantizar la fiabilidad y la seguridad de nivel empresarial para su entorno de Kubernetes.

Para obtener más información, consulte [Solución nativa de la nube de Citrix](#).

En este documento se asume que está familiarizado con Docker y su funcionamiento. Para obtener información sobre Docker, consulte la documentación de Docker en <https://docs.docker.com>.

Funciones disponibles

Citrix ADC CPX admite las siguientes funciones:

- Disponibilidad de aplicaciones
 - Equilibrio de carga L4 y conmutación de contenido L7
 - Descarga de SSL
 - Traducción de protocolos IPv6
 - Equilibrio de carga de Microsoft MySQL,
 - Controles de tarifas de AppExpert
 - Dirección de tráfico consciente del suscriptor
 - Protección contra sobretensiones y colas prioritarias
 - Protocolos de redirección dinámica
- aceleración de aplicaciones
 - Optimizaciones de TCP de clientes y servidores
 - Redirección de memoria caché
 - AppCompress
 - AppCache
- Seguridad de las aplicaciones
 - Reescritura y respuesta de L7

- Defensas DoS L4
- Defensas DoS L7
- Firewall de aplicaciones web (WAF). Citrix ADC CPX admite todas las funciones WAF que se admiten en otros factores de forma de Citrix ADC. Para obtener información sobre las funciones WAF compatibles, consulte [Citrix Web Application Firewall](#).
- Autenticación, autorización y auditoría (AAA) para el tráfico de aplicaciones
- Optimización del protocolo TCP
 - TCP de rutas múltiples
 - Control de la congestión de aumento binario (BIC) y TCP
- Capacidad de administración sencilla
 - Registro web
 - AppFlow
 - Citrix Application Delivery Management
 - Análisis de acciones
- Optimización de aplicaciones
 - Almacenamiento en caché integrado
- Redirección BGP e inyección de estado de ruta (RHI)
- Alta disponibilidad (tanto de capa 2 como de capa 3)

Nota:

Las funciones de interfaz como Rx, Tx, GRO, GSO y LRO están inhabilitadas para las interfaces (host Linux) asignadas al dispositivo Citrix ADC CPX. Estas funciones permanecen en estado inhabilitado incluso después de que se detiene el dispositivo Citrix ADC CPX. Además, la MTU se cambia a 1500 bytes para dichas interfaces.

Plataformas compatibles

Citrix ADC CPX se admite en las siguientes plataformas:

- Kubernetes
- Red Hat OpenShift
- Nubes públicas
 - Servicio Amazon Elastic Kubernetes (EKS)
 - Servicio Azure Kubernetes (AKS)
 - Motor de Google Kubernetes (GKE)
- Ranchero
- Servicio de contenedores pivotaes (PKS)
- Docker versión 1.12 y superior

Arquitectura y flujo de tráfico

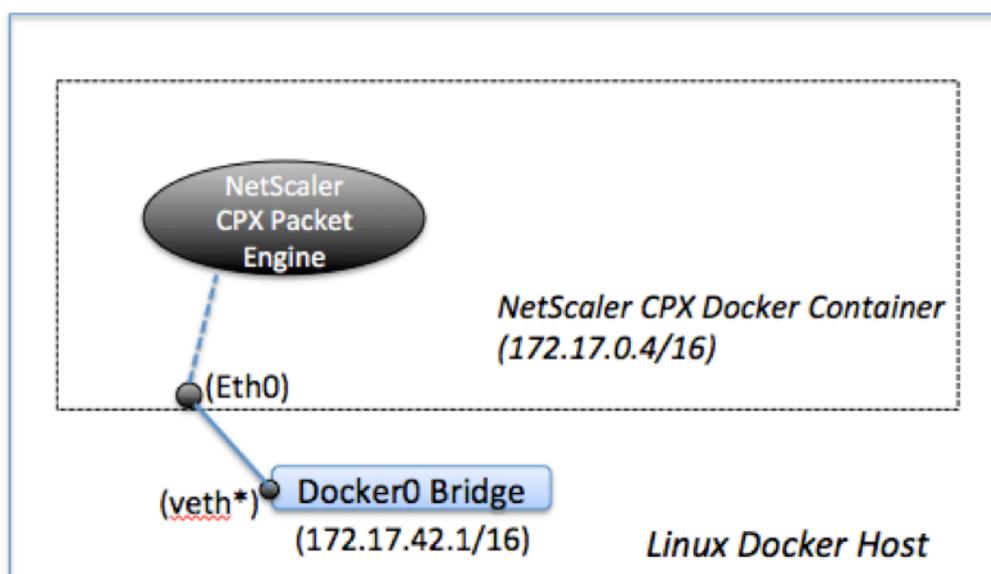
February 19, 2022

En esta sección se describe la arquitectura del modo puente CPX de Citrix ADC y el flujo de tráfico. Citrix ADC CPX también se puede implementar en modo host.

Cuando aprovisiona una instancia CPX de Citrix ADC en un host de Docker, el motor de Docker crea una interfaz virtual, eth0, en la instancia CPX. Esta interfaz eth0 está conectada directamente a una interfaz virtual (veth*) en el puente docker0. El motor de Docker también asigna una dirección IP a la instancia de Citrix ADC CPX en la red 172.17.0.0/16.

La puerta de enlace predeterminada para la instancia CPX es la dirección IP del puente docker0, lo que significa que cualquier comunicación con la instancia CPX de Citrix ADC se realiza a través de la red Docker. Todo el tráfico entrante recibido desde el puente docker0 lo recibe la interfaz eth0 en la instancia Citrix ADC CPX y el motor de paquetes Citrix ADC CPX lo procesa.

Esta ilustración ilustra la arquitectura de una instancia de Citrix ADC CPX en un host Docker.



Cómo funciona una dirección IP única en Citrix ADC CPX

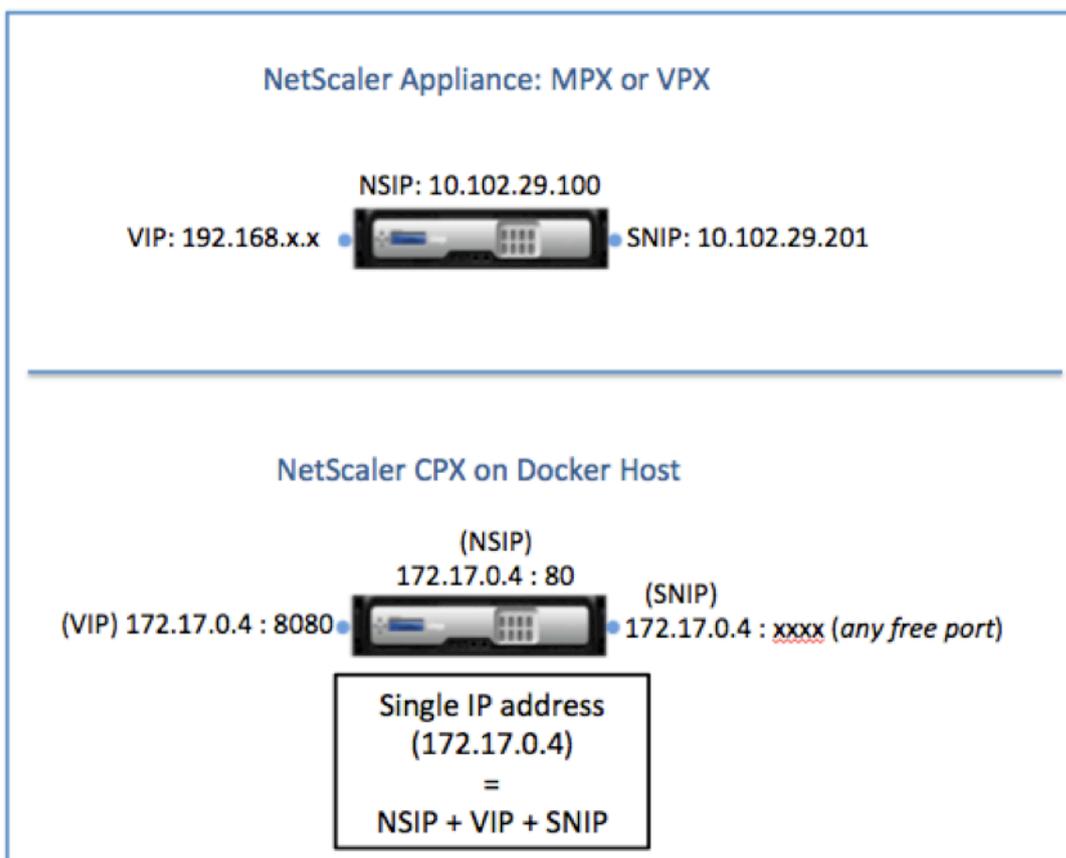
Un dispositivo Citrix ADC MPX o VPX normal requiere al menos tres direcciones IP para funcionar:

- Dirección IP de administración denominada dirección IP de Citrix ADC (NSIP)
- Dirección IP de subred (SNIP) para comunicarse con el conjunto de servidores
- Direcciones IP (VIP) del servidor virtual para aceptar solicitudes de clientes

Una instancia de Citrix ADC CPX funciona con una sola dirección IP que se utiliza tanto para la administración como para el tráfico de datos.

Durante el aprovisionamiento, el motor de Docker solo asigna una dirección IP privada (dirección IP única) a una instancia de Citrix ADC CPX. Las tres funciones IP de una instancia de Citrix ADC se multiplexan en una dirección IP. Esta única dirección IP utiliza diferentes números de puerto para funcionar como NSIP, SNIP y VIP (s).

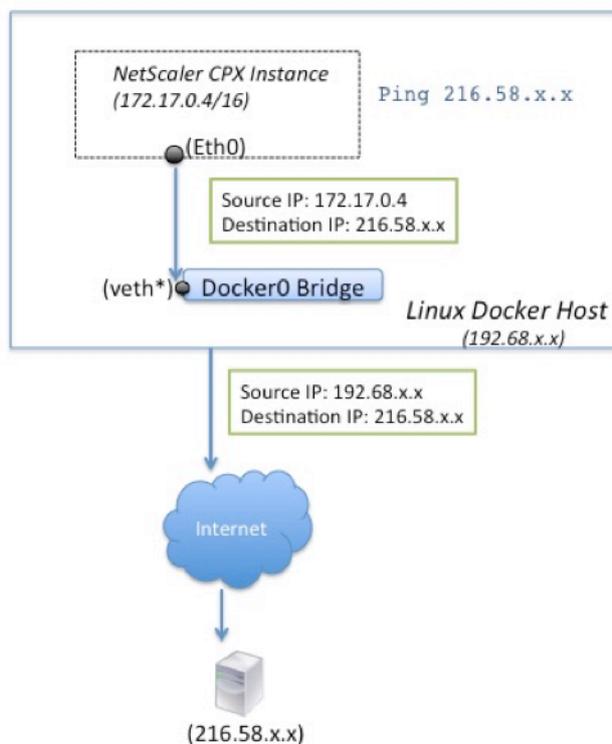
La siguiente imagen ilustra cómo se usa una sola dirección IP para realizar las funciones de NSIP, SNIP y VIP (s).



Flujo de tráfico para solicitudes que se originan en la instancia CPX de Citrix ADC

Docker configura implícitamente tablas IP y una regla NAT para dirigir el tráfico que se origina en la instancia CPX de Citrix ADC a la dirección IP de docker0.

Esta ilustración ilustra cómo una solicitud ping que se origina en una instancia de Citrix ADC CPX llega al destino.



En este ejemplo, el motor de paquetes envía la solicitud ping en la interfaz eth0 con la dirección IP de origen como la dirección IP CPX de Citrix ADC (172.17.0.4). A continuación, el host de Docker realiza la traducción de direcciones de red (NAT) para agregar la dirección IP del host (192.68.x.x) como dirección IP de origen y envía la solicitud al destino (216.58.x.x). La respuesta de la dirección IP de destino sigue la misma ruta a la inversa. El host Docker realiza NAT en la respuesta y reenvía la respuesta a la instancia de Citrix ADC CPX en la interfaz eth0.

Flujo de tráfico para solicitudes que se originan en la red externa

Para habilitar la comunicación externa, al aprovisionar Citrix ADC CPX, debe establecer parámetros de modo que Docker exponga ciertos puertos, como 80, 22 y cualquier otro puerto que desee. Si no ha configurado ningún puerto para que esté expuesto durante el aprovisionamiento, debe configurar reglas NAT en el host de Docker para que estos puertos estén disponibles.

La solicitud del cliente que se origina en Internet es recibida por el host de Docker, que luego realiza la traducción de direcciones de puerto (PAT) para asignar la dirección IP pública y el puerto a la dirección IP y el puerto únicos de la instancia de Citrix ADC CPX, y reenvía el tráfico a la instancia.

Esta ilustración muestra cómo el host Docker realiza la traducción de direcciones de puerto para dirigir el tráfico a la dirección IP única y al puerto Citrix ADC CPX.

sobre el servicio Citrix ADM, consulte el [servicio Citrix ADM](#).

Tipos de licencias de Citrix ADC CPX

Citrix ADC CPX admite licencias de ancho de banda y grupos de CPU virtual (núcleo) para implementaciones locales y basadas en la nube.

Grupo de ancho de banda: las licencias de Citrix ADC CPX se pueden asignar en función del consumo de ancho de banda de las instancias. Puede utilizar las licencias agrupadas para maximizar la utilización del ancho de banda al garantizar la asignación de ancho de banda necesaria a una instancia y no más de lo que se requiere. Actualmente, Citrix ADC CPX solo admite licencias de grupos de ancho de banda premium.

Grupo de vCPU: en las licencias virtuales basadas en el uso de CPU, la licencia especifica el número de CPU a las que tiene derecho una instancia de Citrix ADC CPX en particular. Por lo tanto, Citrix ADC CPX puede extraer licencias solo para la cantidad de CPU virtuales del servidor de licencias. Citrix ADC CPX desprotege las licencias en función del número de CPU que se ejecutan en el sistema. Para obtener más información sobre el grupo de vCPU, consulte [Licencias de CPU virtuales de Citrix ADC](#).

Capacidad agrupada admitida para instancias Citrix ADC CPX

Producto	Ancho de banda máximo	Ancho de banda mínimo	Instancias mínimas	Número máximo de instancias	Unidad mínima de ancho de banda
Citrix ADC CPX	40000 Nota: Depende de la frecuencia de la CPU, la generación, etc.	20 Mbps	1	16	10 Mbps

Nota: Citrix está trabajando actualmente en un modelo de licencias basado en el consumo de Citrix ADC CPX o basado en el pago a medida que crece para ofertas públicas basadas en la nube. Una vez listo, estará disponible en el mercado de la nube pública para su consumo.

¿Cómo funcionan las licencias de Citrix ADC CPX?

Capacidad agrupada de Citrix ADC CPX: un grupo de licencias común desde el que la instancia de Citrix ADC CPX puede extraer una licencia de instancia y solo el ancho de banda que necesite. Cuando

la instancia ya no requiere estos recursos, los vuelve a registrar en el grupo común, lo que hace que los recursos estén disponibles para otras instancias que necesitan estas licencias.

Licencias de registro y salida de Citrix ADC CPX: Citrix ADM asigna licencias de instancias Citrix ADC CPX a pedido. Una instancia de Citrix ADC CPX puede retirar la licencia de Citrix ADM cuando se aprovisiona una instancia de Citrix ADC CPX y volver a registrar su licencia en Citrix ADM cuando se destruye una instancia.

Comportamiento de Citrix ADC CPX: una sola instancia de Citrix ADC CPX que desprotege un rendimiento de hasta 1 Gbps, solo se desprotege del grupo de instancias y no del grupo de licencias de ancho de banda. Citrix ADC CPX funciona de esta manera hasta 1 Gbps de utilización de ancho de banda. Por ejemplo, si una instancia CPX consume un ancho de banda de 200 Mbps, utiliza el grupo de instancias de licencia, en lugar del conjunto de ancho de banda. Sin embargo, si una instancia de Citrix ADC CPX consume 1200 Mbps de rendimiento, los primeros 1000 Mbps se utilizan del grupo de instancias y los 200 Mbps restantes se consumen del grupo de ancho de banda.

Citrix ADC CPX Express

Citrix ADC CPX Express es una edición de software gratuita para implementaciones locales y en la nube. Cuando descarga la instancia CPX de Citrix ADC del repositorio de [Quay](#), esta es la capacidad predeterminada disponible para los POC que no requieren un archivo de licencia y viene con estas funciones:

- Ancho de banda 20 Mbps
- Máximo 250 sesiones SSL
- Rendimiento SSL de 20 Mbps

Debe obtener una licencia de su instancia de Citrix ADC CPX para realizar la actualización y lograr un mejor rendimiento y implementaciones de producción.

Modelos de licencia de Citrix ADC CPX

Citrix ofrece una gama de modelos de licencias de productos para que Citrix ADC CPX cumpla con los requisitos de su organización. Puede seleccionar opciones como vCPU o ancho de banda y local o en la nube.

Según sus requisitos, puede elegir cualquiera de los siguientes modelos:

- Licencias basadas en ancho de banda para Citrix ADC CPX desde el servicio ADM
- Licencias basadas en vCPU para Citrix ADC CPX desde el servicio ADM
- Licencias basadas en ancho de banda para Citrix ADC CPX desde ADM local
- Licencias basadas en vCPU para Citrix ADC CPX desde ADM local

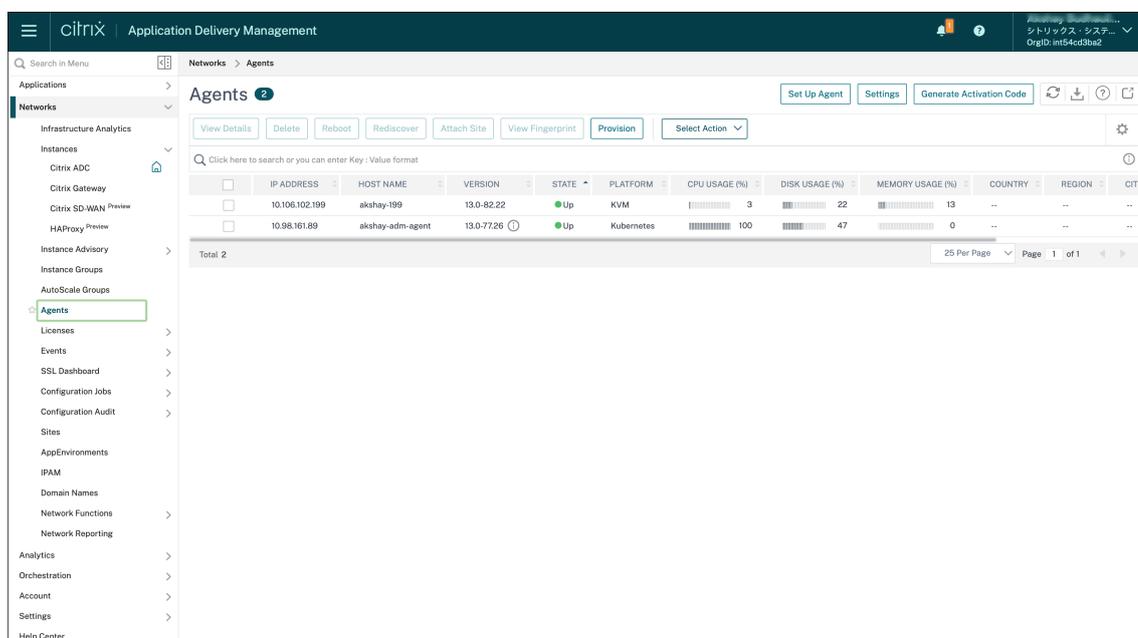
Aprovisionar licencias basadas en ancho de banda y basadas en CPU virtuales desde el servicio Citrix ADM para Citrix ADC CPX

Realice los siguientes pasos para aprovisionar licencias basadas en ancho de banda y licencias basadas en CPU virtuales para Citrix ADC CPX desde el servicio Citrix ADM.

1. Configure Citrix ADM.

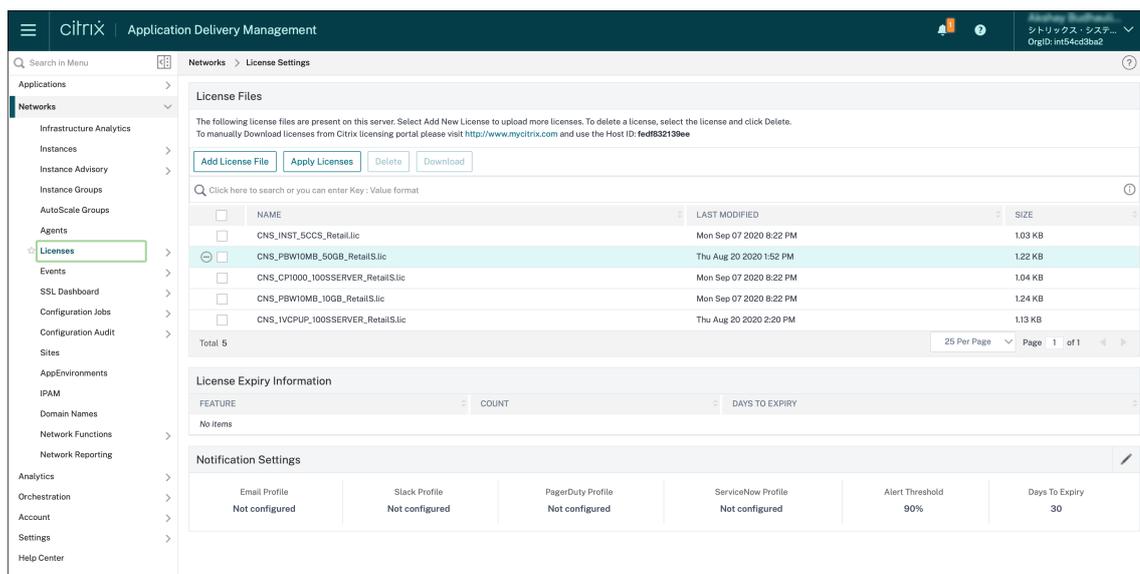
Asegúrese de que la configuración del servicio Citrix ADM funcione con el agente Citrix ADM. Debe tener un servicio Citrix ADM y una cuenta de agente Citrix ADM para que las licencias de Citrix ADC CPX funcionen. Para obtener información sobre cómo configurar el servicio Citrix ADM y el agente Citrix ADM, consulte el [servicio Citrix ADM](#).

Nota: En este procedimiento, se utiliza una configuración de agente Citrix ADM de hipervisor (local). En la siguiente imagen, 10.106.102.199 se muestra el agente local que se utiliza para obtener licencias de Citrix ADC CPX.



2. Agregue el grupo de licencias de instancias de Citrix ADC al servicio Citrix ADM.

Se supone que tiene un conjunto de licencias de ancho de banda disponibles para el servicio ADM. Para obtener información sobre cómo cargar un archivo de licencia en Citrix ADM, consulte [Configurar la capacidad agrupada](#). En la siguiente imagen, CNS_INST_200CC_Retail.lic se usa como el ancho de banda y el grupo de licencias de instancias.



3. Implemente la instancia CPX de Citrix ADC en el clúster de Kubernetes. Asegúrese de que las siguientes variables de entorno se agreguen al archivo YAML de Citrix ADC CPX para licenciar la instancia de Citrix ADC CPX.

Para las licencias basadas en ancho de banda del servicio Citrix ADM, especifique las siguientes variables de entorno en el archivo YAML:

- nombre: "LS_IP"
valor: "10.105.158.166" //IP del agente ADM como se mencionó en el paso 1
- nombre: "LS_PORT"
valor: "27000" // Puerto que escucha el servidor de licencias ADM
- nombre: "BANDWIDTH"
valor: "3000" //Capacidad en Mbps que quiere asignar a CPX
- nombre: "EDITION"
valor: "Standard" o "Enterprise" //para elegir una edición de licencia en particular que incluya Standard, Platinum y Enterprise. De forma predeterminada, se selecciona Platinum.

Para las licencias basadas en CPU virtuales del servicio Citrix ADM, especifique las siguientes variables de entorno en el archivo YAML:

- nombre: "LS_IP"
valor: "10.102.216.173" //IP del agente ADM como se mencionó en el paso 1
- nombre: "LS_PORT"
valor: "27000" // Puerto que escucha el servidor de licencias ADM
- nombre: "CPX_CORES"
valor: "4" // Cantidad de núcleos que quiere asignar
- nombre: "PLATFORM"
valor: "CP1000" // Cantidad de núcleos. El recuento de desprotección es igual al número

de núcleos.

4. Descargue el archivo `cpx-bandwidth-license-adm-service.yaml` con el siguiente comando:

```
1 kubectl create namespace bandwidth
2 wget https://raw.githubusercontent.com/citrix/cloud-native-getting-started/master/cpx-licensing/manifest/cpx-bandwidth-license-adm-service.yaml
```

5. Implemente el YAML modificado en el clúster de Kubernetes con el siguiente comando:

```
1 kubectl create -f cpx-bandwidth-license-adm-service.yaml -n bandwidth
```

6. Inicie sesión en Citrix ADC CPX para verificar la información de instancias mediante el siguiente comando:

```
1 kubectl exec -it 'cpx-pod-ip-name' bash -n bandwidth
```

7. Para ver la información de licencias de la instancia de Citrix ADC CPX determinada, ejecute los siguientes comandos:

```
1 cli_script.sh "show licenseserver"
2 cli_script.sh "show capacity"
```

Puede realizar un seguimiento del ancho de banda asignado y la capacidad de vCPU en el portal de servicios ADM.

Aprovisionar licencias basadas en ancho de banda y licencias basadas en vCPU para Citrix ADC CPX desde Citrix ADM local

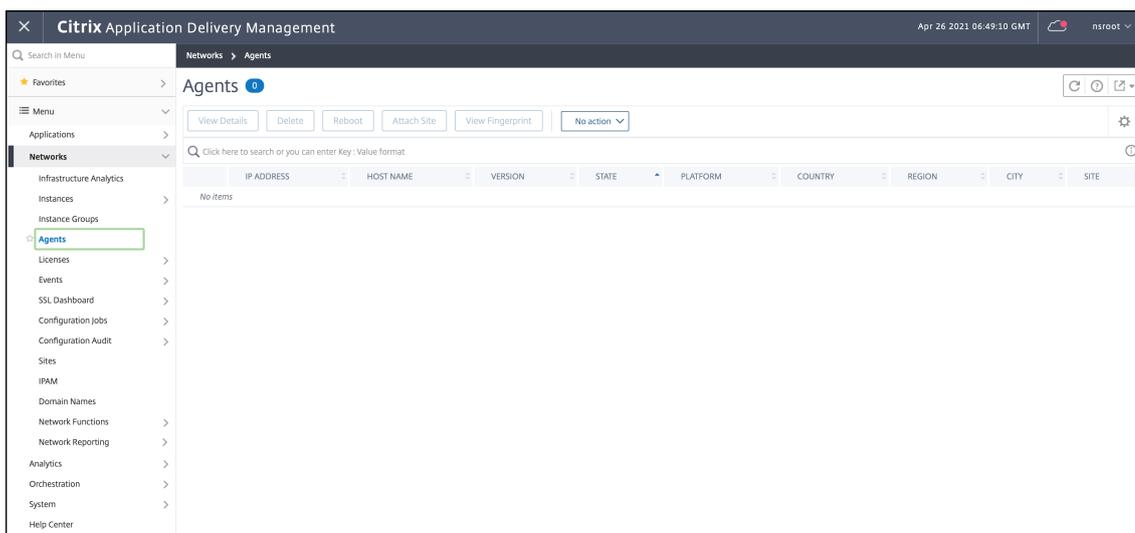
Realice los siguientes pasos para aprovisionar en función del ancho de banda y de la CPU virtual en Citrix ADC CPX desde Citrix ADM local.

1. Configure Citrix ADM.

Asegúrese de que la configuración local de ADM esté lista. Asegúrese de que Citrix ADM local con o sin la implementación del agente ADM para las licencias de Citrix ADC CPX esté funcionando.

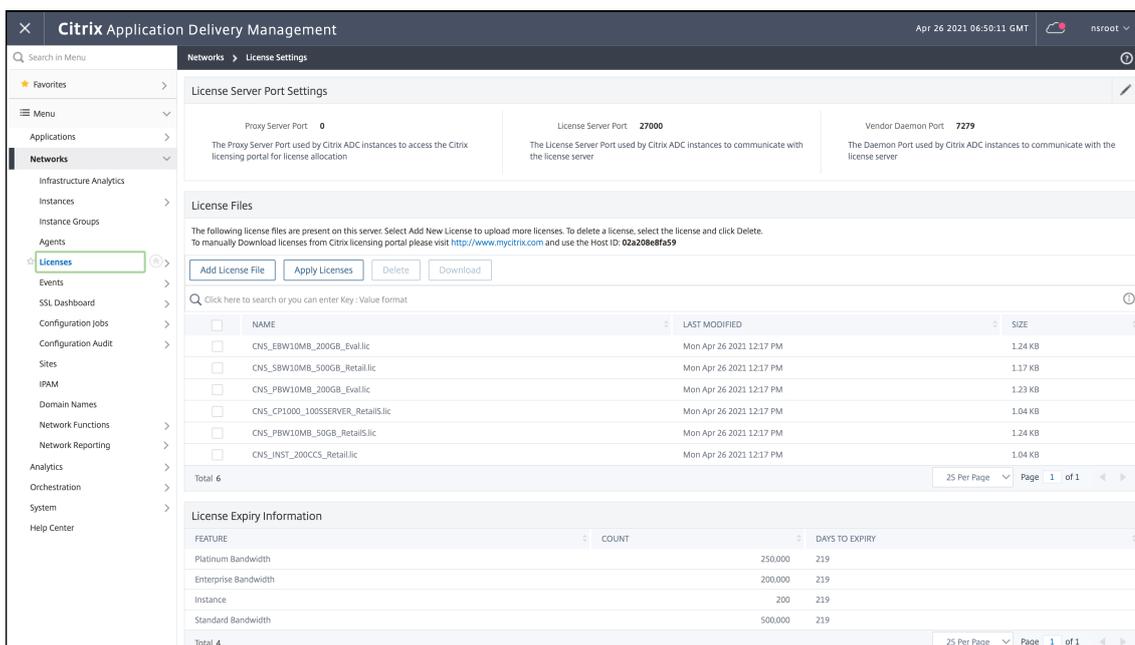
Para obtener información sobre cómo configurar Citrix ADM local y el agente Citrix ADM, consulte el [servicio Citrix ADM](#).

Nota: En este ejemplo, se utiliza un agente ADM integrado con ADM local. En la siguiente imagen, puede ver que no hay ningún agente implementado.



2. Agregue el grupo de licencias de instancias de Citrix ADC a ADM local.

Se supone que tiene un conjunto de licencias de ancho de banda disponible para ADM local. Para obtener información sobre cómo cargar un archivo de licencia en Citrix ADM, consulte [Licencias](#). En la siguiente imagen, `CNS_INST_200CC_Retail.lic` se usa como el ancho de banda y el grupo de licencias de instancias.



En la siguiente imagen, CP1000 se usa como el grupo de licencias de vCPU.

License Server Port Settings

Proxy Server Port	0	The Proxy Server Port used by Citrix ADC instances to access the Citrix licensing portal for license allocation
License Server Port	27000	The License Server Port used by Citrix ADC instances to communicate with the license server
Vendor Daemon Port	7279	The Daemon Port used by Citrix ADC instances to communicate with the license server

License Files

The following license files are present on this server. Select Add New License to upload more licenses. To delete a license, select the license and click Delete. To manually Download licenses from Citrix licensing portal please visit <http://www.myCitrix.com> and use the Host ID: **02a208e8159**

Buttons: Add License File, Apply Licenses, Delete, Download

Search: Click here to search or you can enter Key: Value format

NAME	LAST MODIFIED	SIZE
<input type="checkbox"/> CNS_EBW10MB_200GB_Eval.lic	Mon Apr 26 2021 12:29 PM	1.24 KB
<input type="checkbox"/> CNS_SBW10MB_500GB_Retail.lic	Mon Apr 26 2021 12:29 PM	1.17 KB
<input type="checkbox"/> CNS_FBW10MB_200GB_Eval.lic	Mon Apr 26 2021 12:29 PM	1.23 KB
<input type="checkbox"/> CNS_CP1000_100SSERVER_Retail.lic	Mon Apr 26 2021 12:29 PM	1.04 KB
<input type="checkbox"/> CNS_TVCPUP_100SSERVER_Retail.lic	Mon Apr 26 2021 12:29 PM	1.15 KB
<input type="checkbox"/> CNS_FBW10MB_50GB_Retail.lic	Mon Apr 26 2021 12:29 PM	1.24 KB
<input type="checkbox"/> CNS_INST_200CCS_Retail.lic	Mon Apr 26 2021 12:29 PM	1.04 KB

Total 7

License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Standard Bandwidth	500,000	219
Instance	200	219
Platinum Bandwidth	250,000	219
Enterprise Bandwidth	200,000	219

Total 4

3. Implemente la instancia CPX de Citrix ADC en el clúster de Kubernetes. Asegúrese de que las siguientes variables de entorno se agreguen al archivo YAML de Citrix ADC CPX para licenciar la instancia de Citrix ADC CPX.

Para las licencias basadas en ancho de banda de Citrix ADM local, especifique las siguientes variables de entorno en el archivo YAML:

- nombre: "LS_IP"
valor: "10.105.158.144" // IP de instancia local de ADM, si ha implementado el agente ADM, esta es la dirección IP de su agente como se describe en el paso 1
- nombre: "LS_PORT"
valor: "27000" // Puerto que escucha el servidor de licencias ADM
- nombre: "BANDWIDTH"
valor: "3000" // Capacidad en Mbps que quiere asignar a CPX

Para las licencias basadas en CPU virtuales de Citrix ADM local, especifique las siguientes variables de entorno en el archivo YAML:

- nombre: "LS_IP"
valor: "10.105.158.144" // IP de instancia local de ADM, si tiene implementación de agente ADM, esta será la IP de su agente como se describe en el paso 1
- nombre: "LS_PORT"
valor: "27000" // Puerto que escucha el servidor de licencias ADM
- nombre: "CPX_CORES"
valor: "4" // La cantidad de núcleos que quiere asignar
- nombre: "PLATFORM"

valor: "CP1000" // Cantidad de núcleos. El recuento de desprotección es igual al número de núcleos.

4. Descargue el archivo `cpx-bandwidth-license-adm-onprem.yaml` con el siguiente comando:

```
1 kubectl create namespace bandwidth
2 wget https://raw.githubusercontent.com/citrix/cloud-native-getting-started/master/cpx-licensing/manifest/cpx-bandwidth-license-adm-onprem.yaml
```

5. Implemente el YAML modificado en el clúster de Kubernetes con el siguiente comando:

```
1 kubectl create -f cpx-bandwidth-license-adm-onprem.yaml -n bandwidth
```

6. Inicie sesión en Citrix ADC CPX para verificar la información de instancias mediante el siguiente comando:

```
1 kubectl exec -it <cpx-pod-ip-name> bash -n bandwidth
```

7. Para ver la información de licencias de la instancia de Citrix ADC CPX, ejecute los siguientes comandos:

```
1 cli_script.sh "show licenseserver"
2 cli_script.sh "show capacity"
```

Puede realizar un seguimiento del ancho de banda asignado y la capacidad de vCPU en el portal local de ADM.

Comandos para limpiar las implementaciones

Puede usar los siguientes comandos para limpiar las distintas implementaciones de YAML:

```
1 kubectl delete -f cpx-bandwidth-license-adm-service.yaml -n bandwidth
2 kubectl delete -f cpx-core-license-adm-service.yaml -n core
3 kubectl delete -f cpx-bandwidth-license-adm-onprem.yaml -n bandwidth
4 kubectl delete -f cpx-core-license-adm-onprem.yaml -n core
5 kubectl delete namespace bandwidth
6 kubectl delete namespace core
```

Implementación de una instancia CPX de Citrix ADC en Docker

February 23, 2022

Las instancias CPX de Citrix ADC están disponibles como un archivo de imagen de Docker en el registro de contenedores de Quay. Para implementar una instancia, descargue la imagen de Citrix ADC CPX del registro de contenedores Quay y, a continuación, implemente la instancia mediante el comando `docker run` o la herramienta de redacción de Docker.

Requisitos previos

Asegúrese de que:

- El sistema host de Docker tiene al menos:
 - 1 CPU
 - 2 GB de RAM

Nota: Para un mejor rendimiento de Citrix ADC CPX, puede definir el número de motores de procesamiento que quiere que se inicie la instancia de Citrix ADC CPX. Para cada motor de procesamiento adicional que agregue, asegúrese de que el host de Docker contenga la cantidad equivalente de CPU virtuales y la cantidad de memoria en GB. Por ejemplo, si quiere agregar 4 motores de procesamiento, el host de Docker debe contener 4 vCPU y 4 GB de memoria.

- El sistema host Docker ejecuta Linux Ubuntu versión 14.04 o posterior.
- La versión 1.12 de Docker está instalada en el sistema host. Para obtener información sobre la instalación de Docker en Linux, consulte la [documentación de Docker](#).
- El host de Docker tiene conectividad a Internet.

Nota: Citrix ADC CPX tiene problemas cuando se ejecuta en ubuntu versión 16.04.5, kernel versión 4.4.0-131-generic. Por lo tanto, no se recomienda ejecutar Citrix ADC CPX en ubuntu versión 16.04.5 kernel versión 4.4.0-131-generic.

Nota: Las siguientes versiones de kubelet y kube-proxy tienen algunas vulnerabilidades de seguridad y no se recomienda usar Citrix ADC CPX con estas versiones:

- kubelet/kube-proxy v1.18.0-1.18.3
- kubelet/kube-proxy v1.17.0-1.17.6
- kubelet/kube-proxy <=1.16.10

Para obtener información sobre cómo mitigar esta vulnerabilidad, consulte [Mitigar esta vulnerabilidad](#).

Descarga de la imagen de Citrix ADC CPX desde Quay

Puede descargar la imagen de Citrix ADC CPX desde el registro de contenedores de Quay mediante el comando `docker pull` e implementarla en su entorno. Use el siguiente comando para descargar la imagen de Citrix ADC CPX del registro de contenedores de Quay:

```
1 docker pull quay.io/citrix/citrix-k8s-cpx-ingress:13.0-xx.xx
```

Por ejemplo, si quiere descargar la versión 13.0-64.35, utilice el siguiente comando:

```
1 docker pull quay.io/citrix/citrix-k8s-cpx-ingress:13.0-64.35
```

Use el siguiente comando para comprobar si la imagen de Citrix ADC CPX está instalada en imágenes de docker:

```
1 root@ubuntu:~# docker images | grep 'citrix-k8s-cpx-ingress'
2 quay.io/citrix/citrix-k8s-cpx-ingress          13.0-64.35
          952a04e73101          2 months ago          469 MB
```

Puede implementar la última imagen de Citrix ADC CPX desde el [registro de contenedores Quay](#).

Implementación de la instancia CPX de Citrix ADC mediante el comando docker run

En el host, puede instalar una instancia de Citrix ADC CPX en el contenedor de Docker mediante la imagen de Docker de Citrix ADC CPX que cargó en el host. Mediante el comando `docker run`, instale la instancia de Citrix ADC CPX con la configuración predeterminada de Citrix ADC CPX.

Importante:

Si ha descargado Citrix ADC CPX Express de [CPX Express](#), asegúrese de leer y entender el Contrato de licencia de usuario final (EULA) disponible en: [CPX Express](#) y de aceptar el EULA al implementar la instancia de Citrix ADC CPX.

Instale la instancia de Citrix ADC CPX en el contenedor de Docker mediante el siguiente comando **docker run**:

```
1 docker run -dt -P --privileged=true - net=host - e NS_NETMODE=" HOST"
   -e CPX_CORES=<number of cores> --name <container_name> --ulimit core
   =-1 -e CPX_NW_DEV='<INTERFACES>' -e CPX_CONFIG=' {
2   "YIELD" : " NO" }
3   ' -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> e PLATFORM=CP1000 -v
   <host_dir>:/cpx <REPOSITORY>:<TAG>
4 <!--NeedCopy-->
```

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -e
   CPX_NW_DEV='eth1 eth2' -e CPX_CORES=5 -e CPX_CONFIG='{
2   "YIELD":"No" }
3   ' -e LS_IP=10.102.38.134 -e PLATFORM=CP1000 -v /var/cpx:/cpx --name
   cpx_host cpx:13.0-x.x
4 <!--NeedCopy-->
```

En este ejemplo se crea un contenedor denominado `mycpx` función de la imagen de Docker de Citrix ADC CPX.

El `-p` parámetro es obligatorio. Indica a Docker que asigne los puertos expuestos en el contenedor por la imagen de Citrix ADC CPX Docker. Esto significa asignar los puertos 9080, 22, 9443 y 161/UDP a los puertos del host Docker que se seleccionan aleatoriamente del intervalo definido por el usuario. Este mapeo se hace para evitar conflictos. Si más tarde crea varios contenedores Citrix ADC CPX en el mismo host de Docker. Las asignaciones de puertos son dinámicas y se configuran cada vez que se inicia o se reinicia el contenedor. Los puertos se usan de la siguiente manera:

- 9080 se usa para HTTP
- 9443 se usa para HTTP
- 22 utilizados para SSH
- 161/UDP se utiliza para SNMP.

Si quiere asignaciones de puertos estáticas, use el parámetro `-p` para configurarlas manualmente.

La opción `--privileged=true` se usa para ejecutar el contenedor en modo privilegiado. Si ejecuta Citrix ADC CPX en modo Host de implementación, debe proporcionar todos los privilegios del sistema a Citrix ADC CPX. Si quiere ejecutar Citrix ADC CPX en modo puente con uno o varios núcleos, en lugar de esta opción, puede usar la opción `--cap-add=NET_ADMIN`. La `--cap-add=NET_ADMIN` opción le permite ejecutar el contenedor Citrix ADC CPX con todos los privilegios de red.

`**--net=host` Es una opción de comando de ejecución de docker estándar que especifica que el contenedor se ejecuta en la pila de red del host y tiene acceso a todos los dispositivos de red.

Nota

Ignore esta opción si ejecuta Citrix ADC CPX en una red puente o ninguna.

`-e NS_NETMODE="HOST"` es una variable de entorno específica de Citrix ADC CPX que le permite especificar que Citrix ADC CPX se inicie en modo host. Una vez que Citrix ADC CPX se inicia en modo host, configura 4 reglas iptables predeterminadas en una máquina host para el acceso de administración a Citrix ADC CPX. Utiliza los siguientes puertos:

- 9995 para HTTP
- 9996 para HTTPS
- 9997 para SSH
- 9998 para SNMP

Si quiere especificar puertos diferentes, puede usar las siguientes variables de entorno:

- -e NS_HTTP_PORT=
- -e NS_HTTPS_PORT=
- -e NS_SSH_PORT=
- -e NS_SNMP_PORT=

Nota

Ignore esta variable de entorno si ejecuta Citrix ADC CPX en una red puente o ninguna.

Se -e `CPX_CORES` trata de una variable de entorno opcional específica de Citrix ADC CPX. Puede usarlo para mejorar el rendimiento de la instancia de Citrix ADC CPX definiendo el número de motores de procesamiento que quiere que se inicie el contenedor de Citrix ADC CPX.

Nota: Citrix ADC CPX admite de 1 a 16 núcleos.

Nota

Por cada motor de procesamiento adicional que agregue, asegúrese de que el host de Docker contenga la cantidad equivalente de CPU virtuales y la cantidad de memoria en GB. Por ejemplo, si quiere agregar 4 motores de procesamiento, el host de Docker debe contener 4 vCPU y 4 GB de memoria.

-e `EULA = yes` Se trata de una variable de entorno específica de Citrix ADC CPX obligatoria, que se requiere para comprobar que ha leído y comprendido el Contrato de licencia de usuario final (EULA) disponible en: [CPX Express](#).

El -e `PLATFORM=CP1000` parámetro especifica el tipo de licencia de Citrix ADC CPX.

Si ejecuta Docker en una red host, puede asignar interfaces de red dedicadas al contenedor Citrix ADC CPX mediante la variable de entorno -e `CPX_NW_DEV`. Debe definir las interfaces de red separadas por un espacio en blanco. Las interfaces de red que defina se guardan en el contenedor Citrix ADC CPX hasta que desinstala el contenedor Citrix ADC CPX. Cuando se aprovisiona el contenedor Citrix ADC CPX, todas las interfaces de red asignadas se agregan al espacio de nombres de redes Citrix ADC.

Nota

Si ejecuta Citrix ADC CPX en una red puente, puede cambiar la red de contenedores, por ejemplo, configurar otra conexión de red al contenedor o eliminar una red existente. A continuación, asegúrese de reiniciar el contenedor Citrix ADC CPX para usar la red actualizada.

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -e
   EULA=yes -e CPX_NW_DEV='eth1 eth2' -e CPX_CORES=5 -e PLATFORM=CP1000
   --name cpx_host cpx:13.0-x.x
2 <!--NeedCopy-->
```

-e `CPX_CONFIG` es una variable de entorno específica de Citrix ADC CPX que le permite controlar el rendimiento de rendimiento del contenedor Citrix ADC CPX. Cuando Citrix ADC CPX no recibe ningún

tráfico entrante para procesar, produce la CPU durante este tiempo de inactividad, lo que resulta en un rendimiento bajo. Puede usar la variable de entorno `CPX_CONFIG` para controlar el rendimiento del rendimiento del contenedor Citrix ADC CPX en tales casos. Debe proporcionar los siguientes valores a la variable de entorno `CPX_CONFIG` en formato JSON:

- Si quiere que el contenedor Citrix ADC CPX genere CPU en casos inactivos, defina { `"YIELD" : "Yes" }`
- Si quiere que el contenedor Citrix ADC CPX evite producir la CPU en casos inactivos para que pueda obtener un rendimiento de alto rendimiento, defina { `"YIELD" : "No" }`

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -e
  EULA=yes -e CPX_CORES=5 -e CPX_CONFIG='{
2   "YIELD":"No" }
3   ' -e PLATFORM=CP1000 --name cpx_host cpx:13.0-x.x
4 <!--NeedCopy-->
```

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -e
  EULA=yes -e CPX_CORES=5 -e CPX_CONFIG='{
2   "YIELD":"Yes" }
3   ' -e PLATFORM=CP1000 --name cpx_host cpx:13.0-x.x
4 <!--NeedCopy-->
```

El `-v` parámetro es un parámetro opcional que especifica el punto de montaje del directorio de montaje de Citrix ADC CPX, `/cpx`. Un punto de montaje es un directorio en el host, en el que se monta el `/cpx` directorio. El `/cpx` directorio almacena los registros, los archivos de configuración, los certificados SSL y los archivos de volcado de memoria. En el ejemplo, el punto de montaje es `/var/cpx` y el directorio de montaje de Citrix ADC CPX es `/cpx`.

Si compró una licencia o tiene una licencia de evaluación, puede cargar la licencia en un servidor de licencias y especificar la ubicación del servidor de licencias con el comando `docker run`, mediante el `-e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT>` parámetro. En este caso, no necesita aceptar el EULA.

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -e
  CPX_CORES=5 -e CPX_CONFIG='{
2   "YIELD":"No" }
3   ' -e LS_IP=10.102.38.134 -e PLATFORM=CP1000 --name cpx_host cpx:13.0-x
  .x
4 <!--NeedCopy-->
```

Donde:

- `LS_IP_ADDRESS` es la dirección IP del servidor de licencias.
- `LS_PORT` es el puerto del servidor de licencias.

Puede ver las imágenes que se ejecutan en su sistema y los puertos asignados a los puertos estándar mediante el comando: `docker ps`

Implementación de una versión más ligera de Citrix ADC CPX mediante el comando `docker run`

Citrix proporciona una versión más ligera de Citrix ADC CPX que consume menos memoria en tiempo de ejecución. La versión más ligera de Citrix ADC CPX se puede implementar como un sidecar en implementaciones de malla de servicio.

La versión más ligera de Citrix ADC CPX admite las siguientes funciones:

- Disponibilidad de aplicaciones
 - Equilibrio de carga L4 y conmutación de contenido L7
 - Descarga SSL
 - Traducción de protocolos IPv6
- Seguridad de las aplicaciones
 - Reescritura y respuesta de L7
- Capacidad de administración sencilla
 - Registro web
 - AppFlow

Para crear una instancia de la versión más ligera de Citrix ADC CPX, establezca la variable de entorno `NS_CPX_LITE` mientras ejecuta el comando `Docker run`.

```
1 docker run -dt -P --privileged=true -e NS_CPX_LITE=1 -e EULA=yes --name
   <container_name> --ulimit core=-1 <REPOSITORY>:<TAG>
2 <!--NeedCopy-->
```

En el siguiente ejemplo, se crea un contenedor ligero basado en la imagen de Citrix ADC CPX.

```
1 docker run -dt -P --privileged=true -e NS_CPX_LITE=1 -e EULA=yes - -
   name lightweight --ulimit core=-1 cpx:latest
2 <!--NeedCopy-->
```

De forma predeterminada, el registro mediante `newnslog` está inhabilitado en la versión más ligera de Citrix ADC CPX. Para habilitarlo, debe establecer la variable de entorno `NS_ENABLE_NEWNSLOG` en 1 mientras abre la versión más ligera de Citrix ADC CPX.

El siguiente ejemplo muestra cómo habilitar el registro mediante `newnslog` al implementar la versión más ligera de Citrix ADC CPX.

```
1 docker run -dt --privileged=true --ulimit core=-1 -e EULA=yes -e
   NS_CPX_LITE=1 -e NS_ENABLE_NEWNSLOG=1 cpx:<tag>
2 <!--NeedCopy-->
```

Nota: La versión más ligera de CPX solo admite un solo núcleo (CPX_CORES=1).

Implementación de instancias CPX de Citrix ADC mediante Docker Compose

Puede usar la herramienta Redactar de Docker para aprovisionar una sola instancia de Citrix ADC CPX o varias instancias de Citrix ADC CPX. Para aprovisionar instancias CPX de Citrix ADC mediante Docker Compose, primero debe escribir un archivo de redacción. Este archivo especifica la imagen de Citrix ADC CPX, los puertos que quiere abrir para la instancia de Citrix ADC CPX y los privilegios de la instancia de Citrix ADC CPX.

Importante

Asegúrese de haber instalado la herramienta Docker Compose en el host.

Para aprovisionar varias instancias de Citrix ADC CPX:

1. Escribe un archivo de redacción, donde:
 - ****<service-name>**es el nombre del servicio que quieres aprovisionar.
 - **image::** <repository><tag>indica el repositorio y las versiones de la imagen de Citrix ADC CPX.
 - **privileged: true** proporciona todos los privilegios de root a la instancia de Citrix ADC CPX.
 - **cap_add** proporciona privilegios de red a la instancia de Citrix ADC CPX.
 - ****<host_directory_path>**indica el directorio en el host de la ventana acoplable que quiere montar para la instancia de Citrix ADC CPX.
 - ****<number_processing_engine>**es el número de motores de procesamiento que quiere que se inicie la instancia de Citrix ADC CPX. Para cada motor de procesamiento adicional, asegúrese de que el host de Docker contenga la cantidad equivalente de CPU virtuales y la cantidad de memoria en GB. Por ejemplo, si quiere agregar 4 motores de procesamiento, el host de Docker debe contener 4 vCPU y 4 GB de memoria.

El archivo de redacción suele tener un formato similar al siguiente:

```
1   <service-name>:
2   container_name:
3   image: <repository>:<tag>
4   ports:
5       - 22
6       - 9080
7       - 9443
8       - 161/udp
9       - 35021-35030
10  tty: true
11  cap_add:
12      - NET_ADMIN
13  ulimits:
```

```
14     core: -1
15     volumes:
16         - <host_directory_path>:/cpx
17     environment:
18         - EULA=yes
19         - CPX_CORES=<number_processing_engine>
20         - CPX_CONFIG='{
21     "YIELD":"Yes" }
22     '
23 <!--NeedCopy-->
```

```
1     CPX_0:
2     container_name: CPX_0
3     image: cpx:13.0-x.x
4     ports:
5         - 9443
6         - 22
7         - 9080
8         - 161/udp
9         - 35021-35030
10    tty: true
11    cap_add:
12        - NET_ADMIN
13    ulimits:
14        core: -1
15    volumes:
16        - /root/test:/cpx
17    environment:
18        - CPX_CORES=2
19        - EULA=yes
20 <!--NeedCopy-->
```

Si quiere aprovisionar una sola instancia de Citrix ADC CPX, debe agregar la siguiente línea al archivo de redacción: `container_name:<name_of_container>`

Ejecute el siguiente comando para aprovisionar varias instancias de Citrix ADC CPX:

```
docker-compose -f <compose_file_name> scale <service-name>=<number of
instances> up -d docker-compose -f docker-compose.yml scale cpxlb=3 up -d
```

Si quiere aprovisionar una sola instancia de Citrix ADC CPX, ejecute el siguiente comando: `docker-compose -f <compose_file_name> up -d`

Agregar instancias CPX de Citrix ADC a Citrix ADM

February 19, 2022

Debe agregar las instancias CPX de Citrix ADC instaladas en un host de Docker al software Citrix Application Delivery Management (ADM) si quiere administrar y supervisar estas instancias.

Puede agregar instancias al configurar ADM por primera vez o más tarde.

Para agregar instancias, debes crear un perfil de instancia y especificar el nombre de host o la dirección IP de cada instancia, o un intervalo de direcciones IP. Este perfil de instancia contiene el nombre de usuario y la contraseña de las instancias que quiere agregar a Citrix ADM. Para cada tipo de instancia, está disponible un perfil predeterminado. Por ejemplo, `ns-root-profile` es el perfil predeterminado para las instancias de Citrix ADC. Este perfil se define mediante las credenciales de administrador de ADC predeterminadas. Si ha cambiado las credenciales de administrador predeterminadas de las instancias, puede definir perfiles de instancia personalizados para esas instancias. Si cambia las credenciales de una instancia después de detectarse la instancia, debe modificar el perfil de instancia o crear un perfil y, a continuación, volver a descubrir la instancia.

Requisitos previos

Asegúrese de lo siguiente:

- Se instaló el software Citrix ADM en Citrix XenServer. Para obtener más información, consulte la [documentación de Citrix ADM](#).
- Se instalaron las instancias CPX de Citrix ADC en un host de Docker.

Para agregar instancias de Citrix ADC CPX a ADM:

1. En un explorador web, escriba la dirección IP de **Citrix Application Delivery Management** (por ejemplo, `http://192.168.100.1`).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador. Las credenciales de administrador predeterminadas son **nsroot** y **nsroot**.
3. Vaya a **Redes > Instancias > Citrix ADC** y haga clic en la ficha **CPX**.
4. Haga clic en **Agregar** para agregar nuevas instancias CPX en Citrix ADM.
5. Se abrirá la página **Add Citrix ADC CPX**. Introduzca los valores para los siguientes parámetros:
 - a) Puede agregar instancias CPX proporcionando la dirección IP accesible de la instancia CPX o la dirección IP del contenedor Docker donde está alojada la instancia CPX.
 - b) Seleccione el perfil de la instancia CPX.
 - c) Seleccione el sitio donde se van a implementar las instancias.

- d) Seleccione el agente.
- e) Como opción, puede introducir el par clave-valor en la instancia. La incorporación de un par clave-valor facilita la búsqueda de la instancia más adelante.

← Add Citrix ADC CPX

Enter Device IP Address Import from file

Enter one or more hostnames, IP addresses, and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

Routable IP/ Docker IP*

Profile Name*

Site*

Agent

Tags

6. Haga clic en **OK**.

Nota

Si quiere volver a descubrir una instancia, elija **Redes > Instancias > Citrix ADC > CPX**, seleccione la instancia que quiere redescubrir y, a continuación, en la lista desplegable **Seleccionar acción**, haga clic en **Redescubrir**.

Agregar instancias de Citrix ADC CPX a Citrix ADM mediante variables de entorno

También puede agregar las instancias CPX de Citrix ADC a Citrix ADM mediante variables de entorno. Para agregar instancias, debe configurar las siguientes variables de entorno para la instancia de Citrix ADC CPX.

- **NS_MGMT_SERVER** - Dirección IP ADM/FQDN
- **HOST** - Dirección IP del nodo
- **NS_HTTP_PORT** - Puerto HTTP asignado en el nodo
- **NS_HTTPS_PORT** - Puerto HTTPS asignado en el nodo
- **NS_SSH_PORT** - Puerto SSH mapeado en el nodo
- **NS_SNMP_PORT** - Puerto SNMP asignado en el nodo
- **NS_ROUTABLE** - (La dirección IP del pod de Citrix ADC CPX no se puede redirigir desde el exterior).

- `NS_MGMT_USER` — Nombre de usuario de ADM
- `NS_MGMT_PASS` — Contraseña ADM

A continuación, se muestra un comando `docker run` de ejemplo para agregar una instancia de Citrix ADC CPX a Citrix ADM.

```
1  docker run -dt --privileged=true -p 9080:9080 -p 9443:9443 -p 9022:22
   -p 9161:161 -e EULA=yes -e NS_MGMT_SERVER=abc-mgmt-server.com -e
   HOST=10.1.1.1 -e NS_HTTP_PORT=9080 -e NS_HTTPS_PORT=9443 -e
   NS_SSH_PORT=9022 -e NS_SNMP_PORT=9161 -e NS_ROUTABLE=0 --ulimit
   core=-1 - name test cpx:latest
2
3  <!--NeedCopy-->
```

Agregar instancias CPX de Citrix ADC a Citrix ADM mediante Kubernetes ConfigMaps

Citrix ADC CPX admite el registro en Citrix ADM mediante el uso de archivos montados en volumen a través de Kubernetes ConfigMaps. Para habilitar esta forma de registro, Citrix ADC CPX requiere algunas variables de entorno que se especificarán junto con algunos archivos montados en volúmenes a través de ConfigMaps y Secrets.

A continuación se muestran las variables de entorno requeridas y su descripción:

- `NS_HTTP_PORT` - Especifica el puerto HTTP asignado en el nodo.
- `NS_HTTPS_PORT` - Especifica el puerto HTTPS asignado en el nodo.
- `NS_SSH_PORT` - Especifica el puerto SSH asignado en el nodo.
- `NS_SNMP_PORT` - Especifica el puerto SNMP asignado en el nodo.

Además de las variables de entorno enumeradas, Citrix ADC CPX requiere información sobre el agente ADM con el que debe registrarse. Esta información contiene la dirección IP o los detalles y credenciales de FQDN del agente ADM. Citrix ADC CPX adquiere esta información de los archivos montados en el volumen. Un ConfigMap que contiene la dirección IP o el FQDN se monta como un archivo en el sistema de archivos de la instancia CPX de Citrix ADC. Un secreto de Kubernetes que contiene credenciales para el agente ADM también se monta como un archivo en el sistema de archivos de la instancia de Citrix ADC CPX. Con toda la información necesaria para el registro, Citrix ADC CPX intenta registrarse en el agente ADM.

A continuación se muestra un ejemplo de fragmento de archivo YAML de Citrix ADC CPX con ConfigMap y Secret montados como archivos:

```
1  ...
2  env:
3  - name: "EULA"
4  value: "yes"
```

```

5     - name: "NS_HTTP_PORT"
6       value: "9080"
7     - name: "NS_HTTPS_PORT"
8       value: "9443"
9     - name: "NS_SSH_PORT"
10      value: "22"
11    - name: "NS_SNMP_PORT"
12      value: "161"
13    - name: "KUBERNETES_TASK_ID"
14      value: ""
15    ...
16    volumeMounts:
17      ...
18      - mountPath: /var/adminfo/server/
19        name: adm-agent-config
20      - mountPath: /var/adminfo/credentials/
21        name: adm-agent-user
22      ...
23    volumes:
24      ...
25    - name: adm-agent-config
26      configMap:
27        name: adm-agent-config
28    - name: adm-agent-user
29      secret:
30        secretName: adm-secret

```

En el ejemplo anterior, se consumen un nombre ConfigMap `adm-agent-config` y un secreto `adm-agent-user`. A continuación se muestra un ejemplo para crear el ConfigMap y Secret necesarios.

ConfigMap: El ConfigMap se crea a partir de un archivo llamado `adm_reg_envs`. El archivo requiere la dirección IP o el FQDN del agente ADM en el siguiente formato:

```
1 NS_MGMT_SERVER=adm-agent
```

En el formato anterior, `adm-agent` es el FQDN del agente ADM en el que se debe registrar la instancia de Citrix ADC CPX.

Use el siguiente comando para crear un ConfigMap:

```
1 kubectl create configmap adm-agent-config --from-file=adm_reg_envs
```

Nota: El nombre del archivo debe tener la variable `adm_reg_envs` y debe montarse en la ruta: `/var/adminfo/server/`.

Secreto: usa el siguiente comando para crear un secreto de Kubernetes. En el siguiente comando, `user123` es el nombre de usuario del agente ADM y `pass123` es la contraseña.

```
1 kubectl create secret generic adm-secret --from-literal=NS_MGMT_USER=
   user123 --from-literal=NS_MGMT_PASS=pass123
```

Una instancia de Citrix ADC CPX se puede implementar en un clúster de Kubernetes con las variables de entorno y los archivos montados en volumen requeridos incluso antes de implementar el agente ADM en el clúster. Si implementa una instancia de Citrix ADC CPX antes de implementar el agente ADM, Citrix ADC CPX sigue intentando registrarse hasta que se implemente el agente ADM. Una vez que se implementa el agente ADM, la instancia de Citrix ADC CPX utiliza los datos de configuración proporcionados a través de las variables de entorno y los archivos montados en volumen para registrarse en el agente ADM. Le ayuda a evitar la reimplementación de Citrix ADC CPX con la información de configuración.

Una instancia de Citrix ADC CPX, que ya está registrada con un agente ADM, puede cambiar dinámicamente el registro a otro agente ADM después de un cambio en la configuración. Para ello, puede actualizar la información de configuración en ConfigMap y el secreto para el Citrix ADC CPX ya implementado. Debe actualizar el archivo desde el que se creó el ConfigMap con la dirección IP o el FQDN del nuevo agente ADM y eliminar el ConfigMap anterior y, a continuación, crear un nuevo ConfigMap. Del mismo modo, se debe eliminar el secreto existente y se debe crear un nuevo secreto con las credenciales del nuevo agente de ADM.

Agregador de licencias Citrix ADC CPX

November 8, 2022

Actualmente, los CPX de Citrix ADC obtienen licencias del servidor Citrix ADM. En un entorno de Kubernetes, los CPX de Citrix ADC pueden subir o bajar dinámicamente. Si un Citrix ADC CPX deja de funcionar inesperadamente, el servidor Citrix ADM tarda unos minutos en reclamar la licencia. El servidor Citrix ADM debe poder recuperar dichas licencias inmediatamente cuando los CPX de Citrix ADC dejen de funcionar, de modo que se pueda asignar la misma licencia a otro Citrix ADC CPX próximo. Además, si no se puede acceder al servidor Citrix ADM por algún motivo, no puede obtener licencias de los nuevos CPX de Citrix ADC en el clúster.

Citrix ADC CPX License Aggregator es un servicio de Kubernetes proporcionado por Citrix. Este servicio actúa como proveedor local de licencias de Citrix ADC CPX dentro de un clúster de Kubernetes. El servicio Citrix ADC CPX License Aggregator implementado en un clúster de Kubernetes puede actuar como intermediario entre los CPX de Citrix ADC y el servidor de licencias de ADM y realizar un seguimiento de los CPX de Citrix ADC y las licencias asignadas. Con el servicio Citrix ADC CPX License

Aggregator, el servidor Citrix ADM puede reclamar licencias inmediatamente cuando Citrix ADC CPXS deja de funcionar.

En un clúster de Kubernetes, el servicio Citrix ADC CPX License Aggregator admite Citrix ADC CPX como sidecar e implementaciones independientes.

Nota:

Para obtener licencias mediante el agregador de licencias CPX de Citrix ADC se requiere Citrix ADC CPX 13.1-30.x o una versión posterior. Citrix ADC CPX License Aggregator no admite la licencia de las versiones anteriores de Citrix ADC CPX.

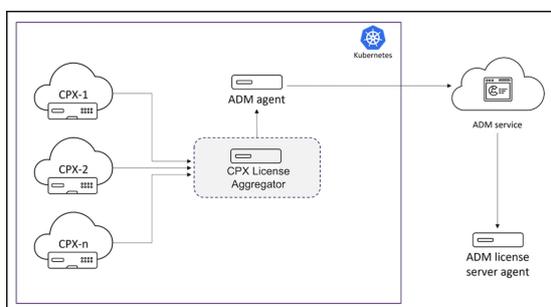
Beneficios clave de Citrix ADC CPX License Aggregator

Los siguientes son los principales beneficios de usar Citrix ADC CPX License Aggregator:

- Escalabilidad:
un servidor de licencias Citrix ADM solo puede admitir hasta 10 000 implementaciones de Citrix ADC CPX. Con la introducción del servicio Citrix ADC CPX License Aggregator, cada clúster de Kubernetes puede actuar como un único cliente para el servidor de licencias de Citrix ADM. Por lo tanto, puede escalar muchos CPX de Citrix ADC con un único servidor de licencias Citrix ADM.
- Optimización de recursos:
el servicio Citrix ADC CPX License Aggregator también admite la capacidad de licencias de todo el clúster y también puede extraer licencias del servidor Citrix ADM según sea necesario. Citrix ADC CPX License Aggregator puede devolver las licencias al servidor Citrix ADM. Citrix ADC CPX License Aggregator puede gestionar la terminación no correcta de los CPX de Citrix ADC y reclamar licencias de dichos CPX de Citrix ADC después del período de espera configurado.

Topología de implementación

El siguiente diagrama muestra una implementación de Citrix ADC CPX License Aggregator dentro de un clúster de Kubernetes.



En este diagrama:

- **CPX** significa Citrix ADC CPX
- **CPX License Aggregator** significa el agregador de licencias Citrix ADC CPX

En esta implementación de ejemplo, se implementa un servicio Citrix ADC CPX License Aggregator dentro del clúster de Kubernetes junto con los CPX de Citrix ADC y el agente Citrix ADM. El servicio Citrix ADC CPX License Aggregator actúa como intermediario entre los CPX de Citrix ADC y el agente Citrix ADM y supervisa todos los CPX de Citrix ADC dentro del clúster y administra las licencias para ellos.

Implementar Citrix ADC CPX License Aggregator mediante gráficos Helm

Requisitos previos

Se aplican los siguientes requisitos previos:

- Necesitas la versión 1.16 y posteriores de Kubernetes.
- Necesitas la versión 3.x o posterior de Helm.
- Debe obtener la dirección IP del servidor de licencias que tiene la licencia para Citrix ADC CPX.
- Debe proporcionar una contraseña para la base de datos Redis en Citrix ADC CPX License Aggregator. Puedes proporcionar la contraseña de la base de datos con el secreto de Kubernetes y puedes usar el siguiente comando para crear el secreto:

```
1 kubectl create secret generic dbsecret --from-literal=password=<
  custom-password>
```

Implementación mediante Helm Charts

Siga los siguientes pasos para implementar el agregador de licencias Citrix ADC CPX mediante los gráficos de Helm según el tipo de licencia de Citrix ADC CPX. Para obtener más información sobre los diferentes tipos de licencias de Citrix ADC CPX, consulte [Licencias de Citrix ADC CPX](#).

Instalación del gráfico Helm

Agregue el repositorio de gráficos Helm de Citrix ADC CPX License Aggregator con el siguiente comando:

```
1 helm repo add Citrix https://citrix.github.io/citrix-helm-charts/
```

Instalación del agregador de licencias CPX de Citrix ADC para administrar las licencias agrupadas en ancho de banda

Utilice uno de los siguientes comandos según el tipo de licencia agrupada de Citrix ADC CPX que tenga. En estos comandos, `my-release` se usa como nombre de la versión.

Nota:

De forma predeterminada, Helm Charts instala los roles y enlaces de roles de RBAC recomendados.

Para la licencia Platinum Bandwidth:

```
1 helm install my-release citrix/cpx-license-aggregator --set
  licenseServer.address=<License-Server-IP-or-FQDN>,redis.
  secretName=<Kubernetes-Secret-for-DB-password>,licenseAggregator
  .username=<unique-ID-for-CLA>,licenseInfo.instanceQuantum=<
  QUANTUM>,licenseInfo.instanceLowWatermark=<LOW WATERMARK>,
  licenseInfo.bandwidthPlatinumQuantum=<QUANTUM-in-Mbps>,
  licenseInfo.bandwidthPlatinumLowWatermark=<LOW WATERMARK-in-Mbps
  >
```

Para edición de ancho de banda empresarial:

```
1 helm install my-release citrix/cpx-license-aggregator --set
  licenseServer.address=<License-Server-IP-or-FQDN>,redis.
  secretName=<Kubernetes-Secret-for-DB-password>,licenseAggregator
  .username=<unique-ID-for-CLA>,licenseInfo.instanceQuantum=<
  QUANTUM>,licenseInfo.instanceLowWatermark=<LOW WATERMARK>,
  licenseInfo.bandwidthEnterpriseQuantum=<QUANTUM-in-Mbps>,
  licenseInfo.bandwidthEnterpriseLowWatermark=<LOW WATERMARK-in-
  Mbps>
```

Para edición de ancho de banda estándar:

```
1 helm install my-release citrix/cpx-license-aggregator --set
  licenseServer.address=<License-Server-IP-or-FQDN>,redis.
  secretName=<Kubernetes-Secret-for-DB-password>,licenseAggregator
  .username=<unique-ID-for-CLA>,licenseInfo.instanceQuantum=<
  QUANTUM>,licenseInfo.instanceLowWatermark=<LOW WATERMARK>,
  licenseInfo.bandwidthStandardQuantum=<QUANTUM-in-Mbps>,
  licenseInfo.bandwidthStandardLowWatermark=<LOW WATERMARK-in-Mbps
  >
```

Estos comandos implementan el agregador de licencias CPX de Citrix ADC en el clúster de Kubernetes con la configuración predeterminada. Puede configurar los parámetros en el momento de la instalación. Para obtener más información, consulte la sección de **configuración del agregador de licencias CPX de Citrix ADC** en el [repositorio de GitHub de Helm Chart](#), que enumera los parámetros obligatorios y opcionales que puede configurar durante la instalación.

Instalación del agregador de licencias CPX de Citrix ADC para administrar las licencias de vCPU

Utilice uno de los siguientes comandos según el tipo de licencia de vCPU de Citrix ADC CPX que tenga. En estos comandos, `my-release` se usa como nombre de la versión.

Nota:

De forma predeterminada, el gráfico Helm instala las funciones de RBAC recomendadas y los enlaces de funciones.

Para la edición platino de vCPU:

```
1 helm install my-release citrix/cpx-license-aggregator --set
  licenseServer.address=<License-Server-IP-or-FQDN>,redis.
  secretName=<Kubernetes-Secret-for-DB-password>,licenseAggregator
  .username=<unique-ID-for-CLA>,licenseInfo.vcpuPlatinumQuantum=<
  QUANTUM>,licenseInfo.vcpuPlatinumLowWatermark=<LOW WATERMARK>
```

Para la edición de vCPU empresarial:

```
1 helm install my-release citrix/cpx-license-aggregator --set
  licenseServer.address=<License-Server-IP-or-FQDN>,redis.
  secretName=<Kubernetes-Secret-for-DB-password>,licenseAggregator
  .username=<unique-ID-for-CLA>,licenseInfo.vcpuEnterpriseQuantum
  =<QUANTUM>,licenseInfo.vcpuEnterpriseLowWatermark=<LOW WATERMARK
  >
```

Para la edición vCPU estándar:

```
1 helm install my-release citrix/cpx-license-aggregator --set
  licenseServer.address=<License-Server-IP-or-FQDN>,redis.
  secretName=<Kubernetes-Secret-for-DB-password>,licenseAggregator
  .username=<unique-ID-for-CLA>,licenseInfo.vcpuStandardQuantum=<
  QUANTUM>,licenseInfo.vcpuStandardLowWatermark=<LOW WATERMARK>
```

Instalación del agregador de licencias CPX de Citrix ADC para administrar varias licencias

Si necesita el agregador de licencias CPX de Citrix ADC para administrar varios tipos de licencias, los argumentos relevantes de esas licencias deben especificarse en el comando Helm.

Por ejemplo:

Para implementar el agregador de licencias `pooled platinum bandwidth edition` y vCPU `platinum edition` licencias de Citrix ADC CPX:

```

1      helm install demo citrix/cpx-license-aggregator --set
      licenseServer.address=<License-Server-IP-or-FQDN>,redis.
      secretName=<Kubernetes-Secret-for-DB-password>,
      licenseAggregator.username=<unique-ID-for-CLA>,licenseInfo.
      instanceQuantum=<QUANTUM>,licenseInfo.instanceLowWatermark=<
      LOW WATERMARK>,licenseInfo.bandwidthPlatinumQuantum=<QUANTUM-
      in-Mbps>,licenseInfo.bandwidthPlatinumLowWatermark=<LOW
      WATERMARK-in-Mbps>,licenseInfo.vcpuPlatinumQuantum=<QUANTUM>,
      licenseInfo.vcpuPlatinumLowWatermark=LOW WATERMARK>

```

Configuración de Citrix ADC CPX para obtener una licencia de Citrix ADC CPX License Aggregator

Cuando se usa Citrix ADC CPX License Aggregator para obtener licencias de Citrix ADC CPX, la variable de entorno `CLA` debe proporcionarse en el YAML de implementación de Citrix ADC CPX.

El `ipaddress` o `domainname` mediante el que se puede acceder al Agregador de licencias Citrix ADC CPX se debe proporcionar en esta variable de entorno de la siguiente manera:

```

1      env:
2      - name: "CLA"
3      value: "192.0.2.2"

```

O bien:

```

1      env:
2      - name: "CLA"
3      value: "local-cla.org"

```

También debe proporcionar las siguientes variables de entorno en el Citrix ADC CPX YAML.

- `POD_NAME`: Especifica el nombre del pod. El nombre del pod se expone a Citrix ADC CPX como una variable de entorno.
- `POD_NAMESPACE`: Especifica el espacio de nombres del pod. El espacio de nombres del pod se expone a Citrix ADC CPX como una variable de entorno.
- `Bandwidth`: Especifica el ancho de banda en Mbps para asignarlo a Citrix ADC CPX.
- `Edition`: Especifica la edición de la licencia. Los valores admitidos incluyen Standard, Platinum y Enterprise.
- `CPX_CORES`: especifica el número de núcleos que desea ejecutar para Citrix ADC CPX.

Para obtener más información sobre las diferentes opciones de licencia de Citrix ADC CPX, consulte [Licencias de Citrix ADC CPX](#).

A continuación, se muestra una configuración de ejemplo con estas variables de entorno:

```
1     - name: POD_NAME
2       valueFrom:
3         fieldRef:
4           apiVersion: v1
5           fieldPath: metadata.name
6     - name: POD_NAMESPACE
7       valueFrom:
8         fieldRef:
9           apiVersion: v1
10          fieldPath: metadata.namespace
11    - name: "BANDWIDTH"
12      value: 1000
13    - name: "CPX_CORES"
14      value: 1
15    - name: "EDITION"
16      value: PLATINUM
```

También debe agregar la siguiente etiqueta al Citrix ADC CPX YAML:

```
1     labels:
2       adc: citrix
```

Para ver un ejemplo de implementación de Citrix ADC CPX License Aggregator, consulte [Citrix ADC CPX License Aggregator: Sample deployment](#).

Configuración de Citrix ADC CPX

February 23, 2022

Puede configurar una instancia CPX de Citrix ADC accediendo a la solicitud de la CLI a través del host de Linux Docker o mediante las API de Citrix ADC NITRO.

Configuración de una instancia CPX de Citrix ADC mediante la interfaz de línea de comandos

Acceda al host de Docker e inicie sesión en el indicador SSH de la instancia, como se muestra en esta ilustración. Las credenciales de administrador predeterminadas para iniciar sesión en una instancia de Citrix ADC CPX son root/linux.

```

root@ubuntu:~# ssh -p 32777 root@127.0.0.1
root@127.0.0.1's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Tue Dec 15 02:45:42 2015 from 172.17.0.1
root@10:~# █

```

Escriba el siguiente comando para usar el símbolo de línea de comandos de la instancia para ejecutar los comandos de la CLI: **cli_script.sh** “<comando>”

Ejemplo:

```

root@10:~# cli_script.sh "show ip"
exec: show ip

```

	IpAddress	Traffic	Domain	Type
	-----	-----	-----	----
1)	172.17.0.4	0		NetScaler IP VIP
2)	192.0.0.1	0		SNIP

Para cerrar sesión en el símbolo de la instancia, escriba **logout**.

Compatibilidad con el uso de una contraseña no predeterminada en Citrix ADC CPX

Citrix ADC CPX admite el uso de una contraseña no predeterminada para la cuenta raíz, es decir **nsroot**. Se genera una contraseña predeterminada y se asigna al usuario una vez que se implementa Citrix ADC CPX. Esta contraseña predeterminada también se actualiza para los usuarios de SSH: **root** y **nsroot**. Puede cambiar esta contraseña predeterminada de forma manual. También puede restablecer la contraseña SSH predeterminada para las cuentas de usuario **root** y **nsroot** de forma manual. Citrix recomienda cambiar esta contraseña manualmente para preservar la seguridad del sistema.

Una vez que restablezca su contraseña, la nueva contraseña se utilizará para las comunicaciones y ejecuciones de **cli_script.sh** de la API de NITRO.

La contraseña de la cuenta raíz predeterminada se almacena en texto sin formato en el archivo `/var/deviceinfo/random_id` en el sistema de archivos CPX de Citrix ADC.

Use la siguiente sintaxis para ejecutar **cli_script.sh** con las credenciales:

```
cli_script.sh "<command>":<user>:<password>"
```

Por ejemplo, **cli_script.sh** para ejecutar y mostrar direcciones IP con usuario **nsroot** y contraseña **password**, use lo siguiente:

```
1 cli_script.sh "show ns ip" ":nsroot:password"
```

Configuración de una instancia CPX de Citrix ADC mediante la API de NITRO

Puede usar la API NITRO de Citrix ADC para configurar instancias de Citrix ADC CPX.

Para configurar instancias de Citrix ADC CPX mediante la API de Nitro, en un explorador web, escriba:

```
http://<host_IP_address>:<port>/nitro/v1/config/<resource-type\
```

Para recuperar estadísticas mediante la API de Nitro, en un explorador web, escriba:

```
http://\<host\_IP\_address\>:\<port\>/nitro/v1/stat/\<resource-type\
```

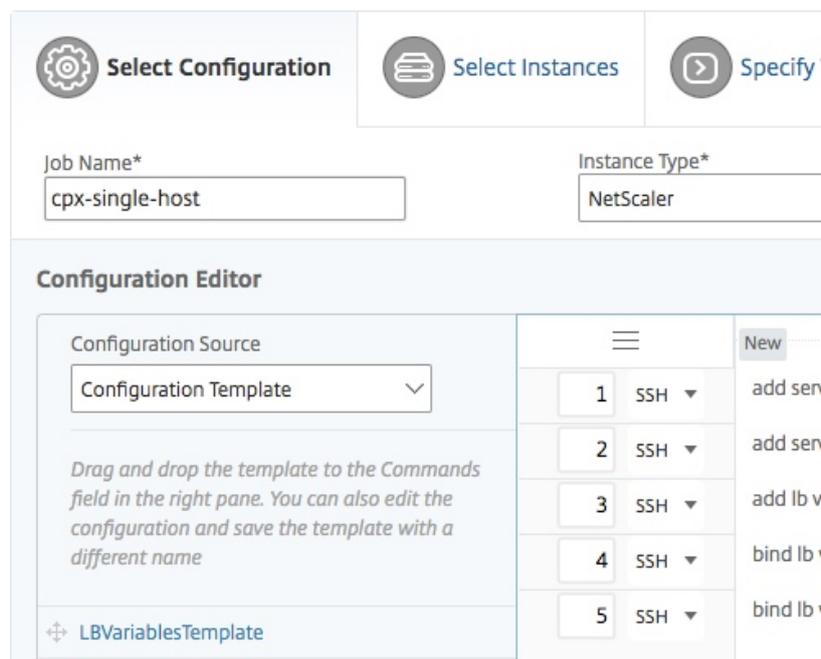
Para obtener más información sobre el uso de la API de NITRO, consulte [Servicios web REST](#). Para Citrix ADC CPX, utilice `CPX IP address:port` donde `netScaler-ip-address` se menciona.

Configuración de una instancia CPX de Citrix ADC mediante trabajos

Puede configurar instancias CPX de Citrix ADC creando y ejecutando trabajos en Citrix ADM. Puede usar las configuraciones de las plantillas de configuración, extraer configuraciones disponibles en otros dispositivos y usar configuraciones guardadas en archivos de texto. También puede registrar las configuraciones realizadas mediante la utilidad de configuración de otras instancias. A continuación, Citrix ADM muestra los comandos de la CLI correspondientes para que los utilice en la instancia de Citrix ADC CPX. Después de seleccionar la configuración, debe seleccionar las **instancias de Citrix ADC CPX en las** que quiere cargar la configuración, especificar los valores de las variables y ejecutar el trabajo.

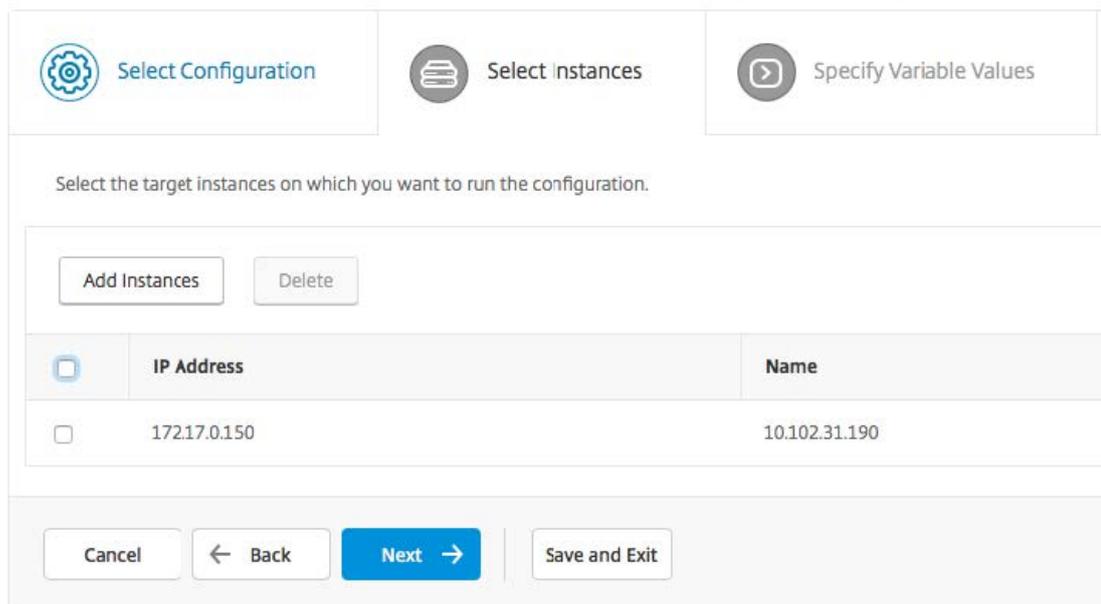
Para configurar instancias CPX de Citrix ADC mediante Trabajos:

1. Inicie sesión en Citrix ADM con las credenciales administrativas.
2. Vaya a **Redes > Trabajos de configuración**, a continuación, haga clic en **Crear trabajo**.
3. Especifique los valores requeridos y seleccione el origen de configuración. También puede es-



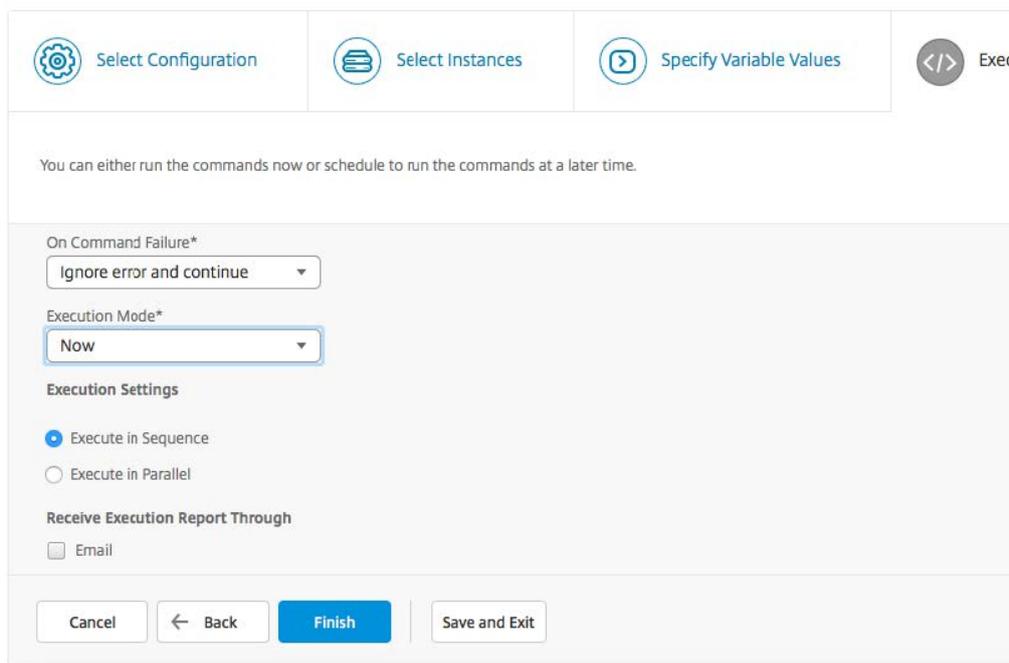
scribir los comandos que quiere ejecutar.

4. Seleccione las instancias CPX de Citrix ADC en las que quiere ejecutar la configuración y haga clic



en **Siguiente**.

5. Especifique la configuración de ejecución y haga clic en Finalizar para ejecutar los comandos en la instancia de Citrix ADC CPX. Si quiere guardar la configuración y ejecutarla más tarde, haga



The screenshot shows a configuration window with three tabs: "Select Configuration", "Select Instances", and "Specify Variable Values". Below the tabs, there is a message: "You can either run the commands now or schedule to run the commands at a later time." The "On Command Failure*" dropdown is set to "Ignore error and continue". The "Execution Mode*" dropdown is set to "Now". Under "Execution Settings", the "Execute in Sequence" radio button is selected. Under "Receive Execution Report Through", the "Email" checkbox is unchecked. At the bottom, there are buttons for "Cancel", "Back", "Finish", and "Save and Exit".

clic en **Guardar y salir**.

Configuración de AppFlow en una instancia de Citrix ADC CPX

February 19, 2022

Puede configurar la función AppFlow en una instancia de Citrix ADC CPX para recopilar datos de rendimiento de páginas web, información a nivel de flujo y sesión de usuario e información de base de datos necesaria para la supervisión y el análisis del rendimiento de las aplicaciones. Estos registros de datos se envían a Citrix ADM, donde puede ver informes históricos y en tiempo real de todas sus aplicaciones.

Para configurar AppFlow, primero, debe habilitar la función AppFlow. A continuación, especifique los recopiladores a los que se envían los registros de flujo. Después de eso, defina acciones, que son conjuntos de recopiladores configurados. A continuación, configure una o varias directivas y asocie una acción a cada directiva. La directiva indica a Citrix ADC CPX que seleccione las solicitudes cuyos registros de flujo se envían a la acción asociada. Por último, vincula cada directiva globalmente o al servidor virtual específico para ponerla en práctica.

Además, puede configurar los parámetros de AppFlow para especificar el intervalo de actualización de la plantilla y para permitir la exportación de [httpURL](#), [httpCookie](#) y la información de [httpReferer](#). En cada recopilador, debe especificar la dirección IP de Citrix ADC CPX como la dirección del exportador.

La utilidad de configuración proporciona herramientas que ayudan a los usuarios a definir las directivas y acciones. Determina exactamente cómo Citrix ADC CPX exporta los registros de un flujo deter-

minado a un conjunto de recopiladores (acción). La interfaz de línea de comandos proporciona un conjunto correspondiente de comandos basados en CLI para usuarios experimentados que prefieren una línea de comandos.

Para poder supervisar los registros, debe agregar la instancia de Citrix ADC CPX a Citrix ADM. Para obtener más información sobre cómo agregar una instancia de Citrix ADC CPX a Citrix ADM, consulte [Instalación de una instancia de Citrix ADC CPX mediante Citrix ADM](#).

Habilitar AppFlow

Para usar la función AppFlow, primero debe habilitarla.

Para habilitar la función AppFlow mediante la interfaz de línea de comandos:

Ejecute los comandos siguientes:

```
1 enable ns feature AppFlow
2 enable ns mode ulfd
```

Especificar un recopilador

Un recopilador recibe registros de AppFlow generados por Citrix ADC. Para enviar los registros de AppFlow, debe especificar al menos un recopilador. De forma predeterminada, el recopilador escucha los mensajes IPFIX en el puerto UDP 4739. Puede cambiar el puerto predeterminado al configurar el selector.

Para especificar un recopilador mediante la interfaz de línea de comandos:

Use los siguientes comandos para agregar un recopilador:

```
1 add appflow collector <name> -IPAddress <ipaddress> -port <port_number>
   -netprofile <netprofile_name> -Transport Logstream
```

Para verificar la configuración, use el siguiente comando:

```
1 show appflow collector <name>
```

Para especificar varios recopiladores mediante la interfaz de línea de comandos:

Use los siguientes comandos para agregar y enviar los mismos datos a varios recopiladores:

```
1 add appflow collector <collector1> -IPAddress <IP> -Transport Logstream
2
3 add appflow collector <collector2> -IPAddress <IP> -Transport Logstream
4
```

```
5 add appflow action <action> -collectors <collector1> <collector2> -  
    Transport Logstream  
6  
7 add appflow policy <policy> true <action> -Transport Logstream  
8  
9 bind lbvserver <lbvserver> -policy <policy> -priority <priority> -  
    Transport Logstream
```

Configuración de una acción de AppFlow

Una acción AppFlow es un recopilador de conjuntos, al que se envían los registros de flujo si coincide la directiva AppFlow asociada.

Use los siguientes comandos para configurar una acción de AppFlow:

```
1 add appflow action <name> --collectors <string> ... [-  
    clientSideMeasurements (Enabled|Disabled) ] [-comment <string>]
```

Para verificar la configuración, use el siguiente comando:

```
1 show appflow action
```

Configuración de una directiva de AppFlow

Después de configurar una acción AppFlow, debe configurar una directiva AppFlow. Una directiva de AppFlow se basa en una regla, que consta de una o más expresiones.

Para configurar una directiva de AppFlow mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba el siguiente comando para agregar una directiva de AppFlow y verificar la configuración:

```
1 add appflow policy <name> <rule> <action>  
2  
3 show appflow policy <name>
```

Vinculación de una directiva de AppFlow

Para poner en vigor una directiva, debe vincularla de forma global, de modo que se aplique a todo el tráfico que fluye a través de Citrix ADC CPX.

Para enlazar de forma global una directiva de AppFlow mediante la interfaz de línea de comandos:

Use el siguiente comando para vincular de forma global una directiva de AppFlow:

```
1 bind appflow global <policyName> <priority> [<gotoPriorityExpression [-type <type>]] [-invoke (<labelType> <labelName>)]
```

Verifique la configuración mediante el siguiente comando:

```
1 show appflow global
```

Configuración de Citrix ADC CPX mediante un archivo de configuración

February 19, 2022

En lugar de utilizar la interfaz de línea de comandos (`cli_script.sh`), la API de NITRO o los trabajos de configuración de Citrix ADM para configurar Citrix ADC CPX, puede configurar Citrix ADC CPX mediante un archivo de configuración estática al implementar la instancia de Citrix ADC CPX.

Puede proporcionar un archivo de configuración estática como archivo de entrada mientras implementa el contenedor Citrix ADC CPX. Durante el inicio del contenedor Citrix ADC CPX, el contenedor se configura en función de la configuración especificada en el archivo de configuración estática. Esta configuración incluye la configuración específica de Citrix ADC y los comandos bash shell que se pueden ejecutar dinámicamente en el contenedor Citrix ADC CPX.

Estructura del archivo de configuración estática

Como se mencionó anteriormente, cuando se implementa Citrix ADC CPX, se configura en función de las configuraciones especificadas en el archivo de configuración estática.

El archivo de configuración estática es un archivo `.conf` que incluye dos etiquetas `##NetScaler Commands` y `##Shell Commands`. Debajo de la etiqueta `##NetScaler Commands`, debe agregar todos los comandos de Citrix ADC para configurar la configuración específica de Citrix ADC en Citrix ADC CPX. Debajo de la etiqueta `##Shell Commands`, debe agregar los comandos de shell que quiere ejecutar en Citrix ADC CPX.

Durante la implementación del contenedor Citrix ADC CPX, los comandos de Citrix ADC y los comandos de shell se ejecutan en el contenedor en el orden especificado en el archivo de configuración.

Importante:

- Las etiquetas se pueden repetir varias veces en el archivo de configuración.
- Las etiquetas no distinguen entre mayúsculas y minúsculas.
- El archivo de configuración debe estar presente en el directorio `/etc` como archivo `cpx`.

`conf` en el sistema de archivos del contenedor.

- El archivo de configuración también puede incluir comentarios. Debe agregar un carácter “#” antes de sus comentarios.
- Si hay casos de error al implementar el contenedor Citrix ADC CPX con el archivo de configuración, los errores se registran en el archivo `ns.log` en el contenedor.
- Al reiniciar el contenedor Citrix ADC CPX, el archivo de configuración se vuelve a aplicar en el contenedor.

```
1 #NetScaler Commands
2
3 add lb vserver v1 http 1.1.1.1 80
4
5 add service s1 2.2.2.2 http 80
6
7 bind lb vserver v1 s1
8
9 #Shell Commands
10
11 touch /etc/a.txt
12
13 echo "this is a" > /etc/a.txt
14
15 #NetScaler Commands
16
17 add lb vserver v2 http
18
19 #Shell Commands
20
21 echo "this is a 1" >> /etc/a.txt
22
23 #NetScaler Commands
24
25 add lb vserver v3 http
26
27 #This is a test configuration file
28 <!--NeedCopy-->
```

Para instalar un contenedor Citrix ADC CPX y configurar dinámicamente el contenedor Citrix ADC CPX en función de un archivo de configuración, monte el archivo de configuración estática mediante la opción `-v` del comando `docker run`:

```
1 docker run -dt --privileged=true -e EULA=yes --ulimit core=-1 -v /tmp/
   cpx.conf:/etc/cpx.conf --name mycpx store/citrix/citrixadccpx:13.0-x
   .x
2 <!--NeedCopy-->
```

Compatibilidad con redirección dinámica en Citrix ADC CPX

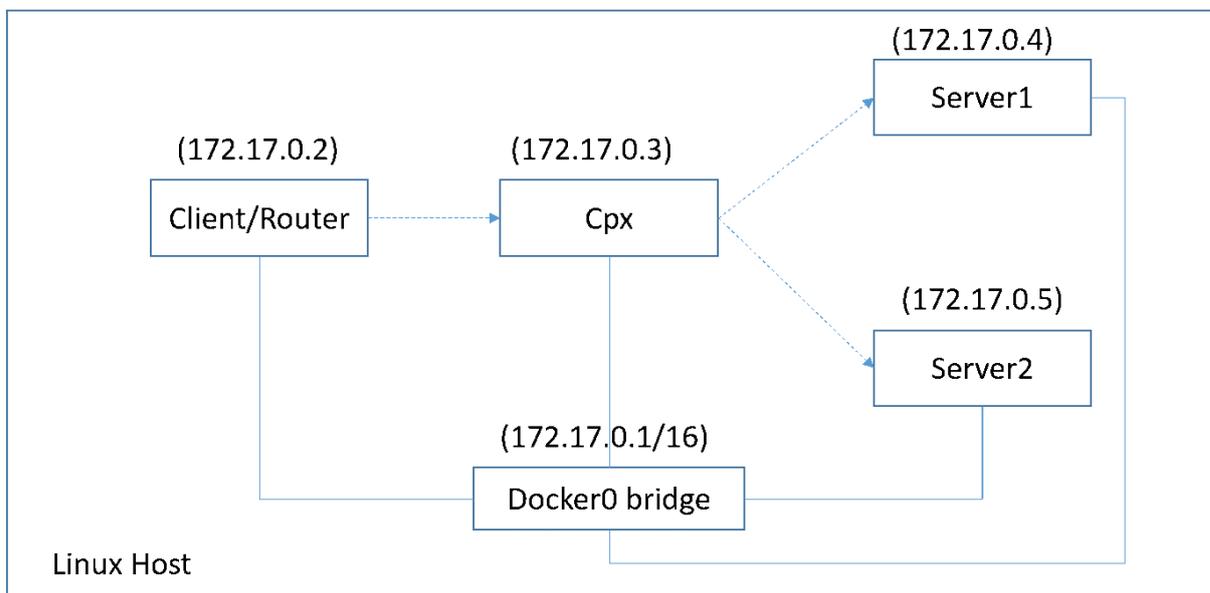
September 7, 2022

Citrix ADC CPX admite el protocolo de redirección dinámica BGP. El objetivo clave del protocolo de redirección dinámica es anunciar la dirección IP del servidor virtual en función del estado de los servicios, vinculados al servidor virtual. Ayuda a un enrutador ascendente a elegir la mejor entre varias rutas a un servidor virtual distribuido topográficamente.

Para obtener información sobre la contraseña no predeterminada en Citrix ADC CPX, consulte la sección [Support for using a non-default password in Citrix ADC CPX](#) del documento [Configuración de Citrix ADC CPX](#).

En una red de host único, el cliente, los servidores y la instancia de Citrix ADC CPX se implementan como contenedores en el mismo host de Docker. Todos los contenedores están conectados a través del puente docker0. En este entorno, la instancia CPX de Citrix ADC actúa como proxy para las aplicaciones aprovisionadas como contenedores en el mismo host de Docker. Para obtener información sobre la implementación en modo de red de host de Citrix ADC CPX, consulte [Modo de red de host](#).

Esta ilustración ilustra la topología de host único.



En esta topología, los servidores virtuales se configuran y anuncian (según el estado de los servicios) a la red o enrutador ascendente mediante BGP.

Realice los siguientes pasos para configurar BGP en Citrix ADC CPX en un solo host Docker con el modo de conexión en red puente.

Configurar la inyección de estado de ruta basada en BGP mediante la API REST en Citrix ADC CPX

1. Cree un contenedor a partir de la imagen de Citrix ADC CPX mediante el siguiente comando:

```
1 docker run -dt --privileged=true -p 22 -p 80 -p 161 -e EULA=yes --ulimit core=-1 cpx: <tag>
```

Por ejemplo:

```
1 docker run -dt --privileged=true -p 22 -p 80 -p 161 -e EULA=yes --ulimit core=-1 cpx:12.1-50.16
```

2. Inicie sesión en el contenedor con el siguiente comando:

```
1 docker exec -it <container id> bash
```

3. Habilite la función BGP con el siguiente comando:

```
1 cli_script.sh "enable ns feature bgp"
```

4. Obtenga el NSIP mediante el comando `show ns ip`:

```
1 cli_script.sh "show ns ip"
```

5. Agregue el servidor virtual mediante el siguiente comando:

```
1 cli_script.sh "add lb vserver <vserver_name> http <VIP> <PORT>"
```

6. Agregue servicios y enlace servicios al servidor virtual.

7. Habilite `hostroute` para el VIP mediante el siguiente comando:

```
1 cli_script.sh "set ns ip <VIP> -hostroute enabled"
```

Salga del contenedor y envíe comandos BGP NITRO desde el host al NSIP en el puerto 9080.

8. Configure el enrutador BGP:

Por ejemplo, si quieres configurar:

```
1 router bgp 100
2 Neighbour 172.17.0.2 remote-as 101
3 Redistribute kernel
```

Especifique el comando de la siguiente manera:

```

1  curl -u username:password http://<NSIP>:9080/nitro/v1/config/ -X
    POST --data 'object={
2  "routerDynamicRouting": {
3  "bgpRouter" : {
4  "localAS":100, "neighbor": [{
5  "address": "172.17.0.2", "remoteAS": 101 }
6  ], "afParams":{
7  "addressFamily": "ipv4", "redistribute": {
8  "protocol": "kernel" }
9  }
10 }
11 }
12 }
13 '

```

9. Instale las rutas BGP aprendidas en el PE mediante el siguiente comando NITRO:

```

1  curl -u username:password http://<NSIP>:9080/nitro/v1/config/ --
    data 'object={
2  "params":{
3  "action":"apply" }
4  ,"routerDynamicRouting": {
5  "commandstring" : "ns route-install bgp" }
6  }
7  '

```

10. Verifique el estado de adyacencia de BGP mediante el siguiente comando NITRO:

```

1  curl -u username:password http://<NSIP>:9080/nitro/v1/config/
    routerDynamicRouting/bgpRouter

```

Salida de muestra:

```

1  root@ubuntu:~# curl -u username:password http://172.17.0.3:9080/
    nitro/v1/config/routerDynamicRouting/bgpRouter
2  {
3  "errorCode": 0, "message": "Done", "severity": "NONE", "
    routerDynamicRouting":{
4  "bgpRouter":[{
5  "localAS": 100, "routerId": "172.17.0.3", "afParams": [ {
6  "addressFamily": "ipv4" }
7  , {
8  "addressFamily": "ipv6" }
9  ], "neighbor": [ {

```

```

10  "address": "172.17.0.2", "remoteAS": 101, "ASOriginationInterval
    ": 15, "advertisementInterval": 30, "holdTimer": 90, "
    keepaliveTimer": 30, "state": "Connect", "singlehopBfd":
    false, "multihopBfd": false, "afParams": [ {
11  "addressFamily": "ipv4", "activate": true }
12  , {
13  "addressFamily": "ipv6", "activate": false }
14  ]

```

11. Compruebe que las rutas aprendidas a través de BGP estén instaladas en el motor de paquetes con el siguiente comando:

```
1 cli_script.sh "show route"
```

12. Guarde la configuración mediante el siguiente comando:

```
1 cli_script.sh "save config"
```

La configuración de redirección dinámica se guarda en el archivo `/nsconfig/ZebOS.conf`.

Configuración de alta disponibilidad para Citrix ADC CPX

February 19, 2022

Un sistema con aplicaciones de misión crítica y crítica para el negocio debe estar disponible de forma continua sin tener puntos únicos de falla. Los sistemas con alta disponibilidad garantizan la disponibilidad continua de las aplicaciones sin interrumpir los servicios prestados al usuario. Citrix ADC CPX admite la implementación de alta disponibilidad de dos instancias de Citrix ADC, lo que protege los servicios del tiempo de inactividad no planificado y garantiza la continuidad empresarial en caso de que se produzca un error. Una vez que configure la alta disponibilidad, también puede actualizar el software Citrix ADC CPX sin provocar ninguna interrupción de los servicios a los usuarios.

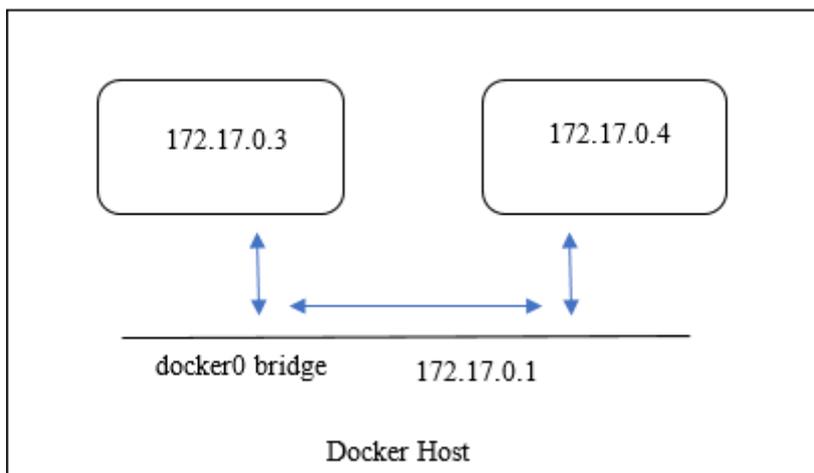
Nota:

Si la cuenta de usuario interna está inhabilitada, no se admite la alta disponibilidad de la función Citrix ADC CPX.

Topología 1: Implementar instancias de Citrix ADC CPX en un único host de Docker con modo de red puente

En esta topología, se crean dos nodos Citrix ADC CPX en el mismo host Docker con modo de red de puente. Ambos nodos están en la misma red puente y los nodos son accesibles directamente entre sí.

En el siguiente diagrama se explica esta topología.



En este ejemplo, se crean dos instancias CPX de Citrix ADC, CPX-1 (NSIP: 172.17.0.3) y CPX-2 (NSIP: 172.17.0.4), en el mismo host de Docker. Para obtener soporte de alta disponibilidad, debe configurar nodos de alta disponibilidad en ambas instancias de Citrix ADC CPX mediante el NSIP del otro nodo.

Realice los siguientes pasos para configurar el soporte de alta disponibilidad en instancias Citrix ADC CPX en un único host docker en modo puente.

1. Acceda al host de Docker e inicie sesión en el indicador SSH de la instancia de Citrix ADC CPX. Para obtener más información, consulte [Configuración de una instancia CPX de Citrix ADC mediante la interfaz de línea de comandos](#).
2. Configure un nodo de alta disponibilidad en la instancia CPX-1 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 172.17.0.4 [--inc enabled]'
```

3. Configure un nodo de alta disponibilidad en una instancia CPX-2 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 172.17.0.3 [--inc enabled]'
```

Nota:

Cuando se reinicia un nodo Citrix ADC CPX en modo de red puente, la dirección IP asignada a un Citrix ADC CPX puede cambiar en función de la versión de docker en el host. Si el NSIP de cualquiera de los nodos cambia después de reiniciar un Citrix ADC CPX, la configuración de alta disponibilidad existente no funcionará aunque se guarde la configuración. En ese caso, debe volver a configurar la alta disponibilidad en los nodos Citrix ADC CPX.

Topología 2: Implemente Citrix ADC CPX en diferentes hosts de Docker con el modo de red puente

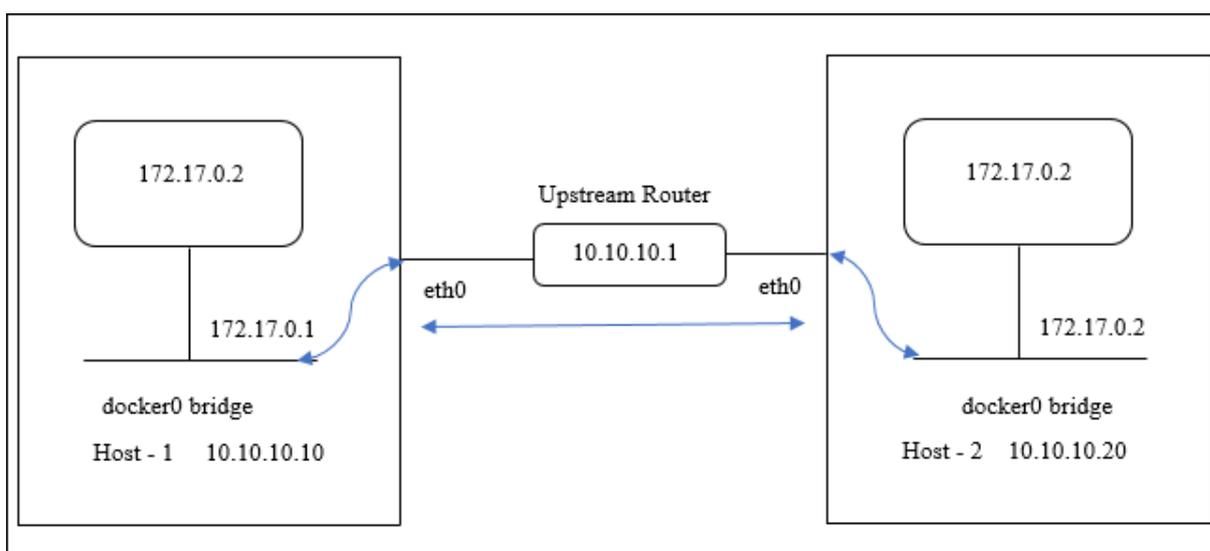
En esta topología, se implementan dos instancias de Citrix ADC CPX en modo puente en dos hosts docker diferentes a los que se puede acceder entre sí. En esta implementación, Citrix ADC CPX debe conocer la dirección IP del host. La variable de entorno **HOST** se puede utilizar en el momento de aprovisionar Citrix ADC CPX para que Citrix ADC CPX conozca la dirección IP del host.

Debe establecer la asignación de puertos para los nodos Citrix ADC CPX. Puede usar la opción **-p** del comando **docker run** al crear el nodo Citrix ADC CPX para habilitar la asignación de puertos para los puertos requeridos.

Debe asignar los siguientes puertos:

- UDP 3003
- TCP 3008
- TCP 8873

El siguiente diagrama explica la topología de la implementación de dos instancias de Citrix ADC CPX en modo puente en dos hosts de docker diferentes.



En este diagrama, la línea azul recta representa el flujo de tráfico CPX-HA entre dos hosts.

Nota: En un host Docker, solo un Citrix ADC CPX puede formar un par de alta disponibilidad. Cualquier otro Citrix ADC CPX en el mismo host no puede formar un par de alta disponibilidad con otro Citrix ADC CPX en un host diferente.

Realice los siguientes pasos para implementar instancias de Citrix ADC en modo puente en diferentes hosts de docker y configurar el soporte de alta disponibilidad mediante la topología de ejemplo.

En este ejemplo, la dirección IP de host1 se configura como 10.10.10.10/24 y la dirección IP de host2

se configura como 10.10.10.20/24.

1. Implemente Citrix ADC CPX con la asignación de puertos requerida en host1 mediante el siguiente comando.

```
1 Docker run -dt --privileged=true -e EULA=yes --ulimit core=-1 -p 8873:8873 -p 3003:3003/udp -p 3008:3008 -e Host=10.10.10.10 cpx:latest
```

2. Implemente Citrix ADC CPX en host2 mediante el mismo comando con la dirección IP del host 2.

```
1 docker run -dt --privileged=true -e EULA=yes --ulimit core=-1 -p 8873:8873 -p 3003:3003/udp -p 3008:3008 -e HOST=10.10.10.20 cpx:latest
```

3. Configure un nodo de alta disponibilidad en la instancia CPX-1 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 10.10.10.20 -inc enabled'
```

4. Configure un nodo de alta disponibilidad en una instancia CPX-2 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 10.10.10.10 -inc enabled'
```

Nota: En esta implementación, debe usar la dirección IP del host del nodo de alta disponibilidad en lugar de la dirección NSIP del nodo de alta disponibilidad.

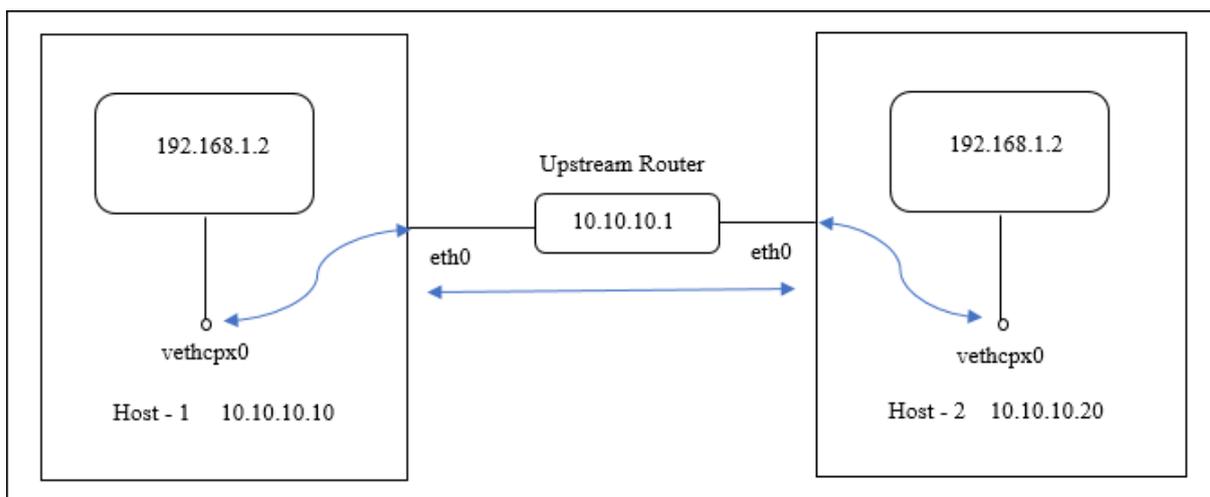
Topología 3: Implemente Citrix ADC CPX en diferentes hosts de Docker en modo de red host sin una interfaz dedicada

En esta topología, se implementan dos instancias de Citrix ADC CPX en dos hosts Docker diferentes en modo host sin una interfaz dedicada. Los anfitriones deben ser accesibles entre sí.

En esta implementación, Citrix ADC CPX debe conocer la dirección IP del host. Puede usar la variable de entorno **HOST** durante el aprovisionamiento de Citrix ADC CPX para que conozca la dirección IP del host.

Debe establecer la asignación de puertos para el nodo Citrix ADC CPX. Puede usar la opción **-p** del comando **docker run** al crear el nodo Citrix ADC CPX para habilitar la asignación de puertos para los puertos requeridos.

En el siguiente diagrama se explica la topología.



En este diagrama, la línea azul recta representa el flujo de tráfico CPX-HA entre dos hosts.

Nota: En un host Docker, solo puede implementar un Citrix ADC CPX en modo host.

Realice los siguientes pasos para implementar las instancias CPX de Citrix ADC y configurar el soporte de alta disponibilidad mediante la topología de ejemplo.

1. Implemente Citrix ADC CPX con la asignación de puertos requerida y en host1 mediante el siguiente comando.

```
1 docker run -dt --privileged=true -e EULA=yes --ulimit core=-1 --
  net=host -e NS_NETMODE=HOST -e HOST=10.10.10.10 cpx:latest
```

2. Implemente Citrix ADC CPX en host2 con la dirección IP de host2 mediante el siguiente comando.

```
1 docker run -dt --privileged=true -e EULA=yes --ulimit core=-1
2 --net=host -e NS_NETMODE=HOST -e HOST=10.10.10.20 cpx:latest
```

3. Configure un nodo de alta disponibilidad en la instancia CPX-1 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 10.10.10.20 -inc enabled'
```

4. Configure un nodo de alta disponibilidad en una instancia CPX-2 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 10.10.10.10 -inc enabled'
```

Topología 4: Implemente CPX en diferentes hosts de Docker con modo de red de host e interfaces dedicadas

En esta topología, se implementan dos instancias de Citrix ADC CPX en diferentes hosts de Docker en modo de red host. Los hosts deben tener más de una interfaz. Puede especificar la interfaz dedicada para Citrix ADC CPX mediante la variable de entorno **CPX_NW_DEV**.

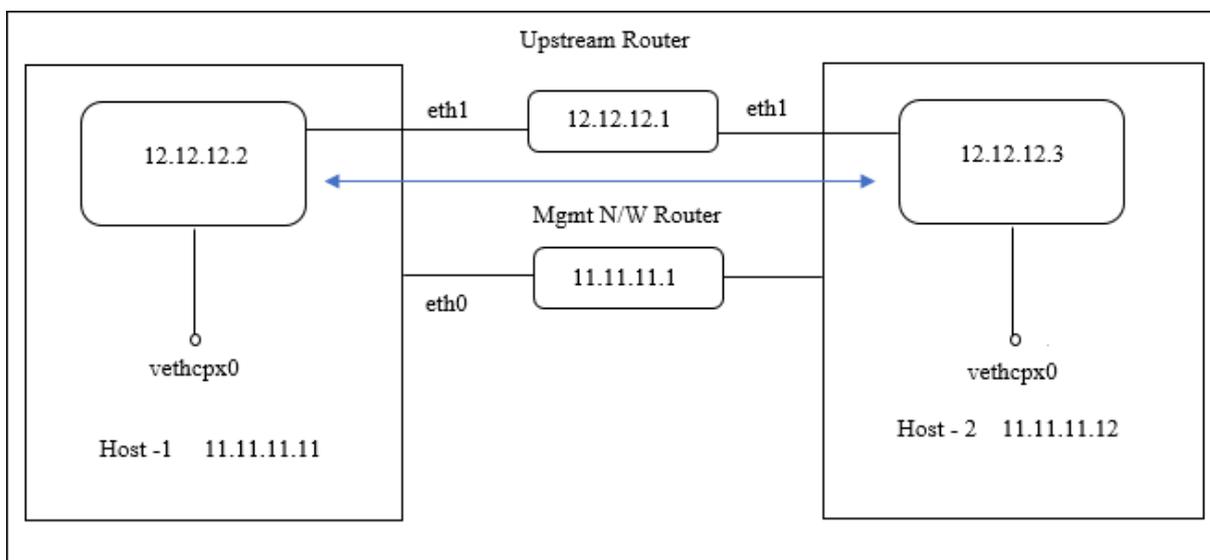
Para obtener más información sobre la asignación de interfaces de red dedicadas para Citrix ADC CPX mediante la variable de entorno CPX_NW_DEV, consulte [Implementación de la instancia CPX de Citrix ADC mediante el comando docker run](#).

Los CPX de Citrix ADC implementados en diferentes hosts de Docker deben ser accesibles entre sí en esta red de datos con la interfaz dedicada.

Esta configuración permite que los nodos de alta disponibilidad intercambien mensajes de latido y sincronicen los archivos de configuración al comunicarse directamente en los puertos 3003, 3008 y 8873. No hay necesidad de reglas NAT en el host. El NSIP predeterminado de Citrix ADC CPX creado en modo host es el mismo en ambos nodos. Por lo tanto, también debe especificar la información de **NS_IP** y **NS_GATEWAY**.

En este ejemplo, se crean dos CPX de Citrix ADC en modo host en dos hosts diferentes. Las instancias CPX de Citrix ADC poseen las interfaces **eth1** en ambos hosts y las interfaces **eth1** están conectadas a la misma red.

En el siguiente diagrama se explica la topología. En este diagrama, la flecha azul representa el flujo de tráfico CPX-HA en la red conectada a la interfaz eth1.



Nota: En un host Docker, solo puede implementar un Citrix ADC CPX en modo host.

Realice los siguientes pasos para implementar las instancias CPX de Citrix ADC y configurar el soporte de alta disponibilidad mediante la topología de ejemplo.

1. Implemente Citrix ADC CPX en modo host en host1 mediante el siguiente comando.

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -  
  e CPX_NW_DEV=eth1 -e NS_IP='12.12.12.2' -e NS_GATEWAY='  
  12.12.12.9' -e EULA=yes --ulimit core=-1 cpx:latest
```

2. Implemente Citrix ADC CPX en modo host en host2 mediante el siguiente comando.

```
1 docker run -dt --privileged=true --net=host -e NS_NETMODE="HOST" -  
  e CPX_NW_DEV=eth1 -e NS_IP='12.12.12.3' -e NS_GATEWAY='  
  12.12.12.10' -e EULA=yes --ulimit core=-1 cpx:latest
```

Nota: Debe configurar rutas estáticas para que ambos nodos de Citrix ADC CPX lleguen al otro nodo de Citrix ADC CPX para intercambiar mensajes de latido y sincronizar los archivos de configuración.

3. Configure un nodo de alta disponibilidad en la instancia CPX-1 mediante el siguiente comando.

```
1 cli_script.sh 'add ha node 1 12.12.12.3 [-inc enabled]'
```

4. Configure un nodo de alta disponibilidad en una instancia CPX-2 mediante el siguiente comando.

```
1 cli_script.sh 'add high availability node 1 12.12.12.2 [-inc  
  enabled]'
```

Configuración de controladores de registro de Docker

February 19, 2022

Docker incluye mecanismos de registro denominados “controladores de registro” para ayudarlo a obtener información de los contenedores en ejecución. Puede configurar un contenedor Citrix ADC CPX para que reenvíe los registros que genere a los controladores de registro de Docker. Para obtener más información sobre los controladores de registro de docker, consulte [Configurar controladores de registro](#).

De forma predeterminada, todos los registros generados por el contenedor Citrix ADC CPX se almacenan en un archivo `/cpx/log/ns.log` en el host de la ventana acoplable. Cuando inicia el contenedor Citrix ADC CPX con el comando `docker run`, puede configurarlo para que reenvíe todos los registros generados a un controlador de registro de docker mediante la opción `--log-driver`. Si el controlador de registro tiene parámetros configurables, puede configurarlos mediante la opción `--log-opt <NAME>=<VALUE>`.

En el siguiente ejemplo, el contenedor Citrix ADC CPX está configurado para reenviar todos los registros generados mediante syslog como controlador de registro.

```
1 docker run -dt --privileged=true --log-driver syslog --log-opt syslog-  
    address=udp://10.106.102.190:514 -e EULA=yes --ulimit core=-1 --name  
    test store/citrix/cpx:12.1-48.13  
2 <!--NeedCopy-->
```

Del mismo modo, en el siguiente ejemplo, el contenedor Citrix ADC CPX está configurado para reenviar todos los registros generados mediante Splunk como controlador de registro.

```
1 docker run -dt --privileged=true --log-driver=splunk --log-opt splunk-  
    token=176FCEBF-4CF5-4EDF-91BC-703796522D20 --log-opt splunk-url=  
    https://splunkhost:8088 -e EULA=yes --ulimit core=-1 --name test  
    store/citrix/cpx:12.1-48.13  
2 <!--NeedCopy-->
```

Actualización de una instancia CPX de Citrix ADC

February 19, 2022

Para actualizar una instancia de Citrix ADC CPX, apáguela, instale la versión más reciente en el mismo punto de montaje y, a continuación, elimine la instancia anterior. Un punto de montaje es un directorio en el que se monta el directorio **/cpx** en el host.

Por ejemplo, para montar el directorio **/cpx** de la instancia de Citrix ADC CPX existente en el directorio **/var/cpx** del host, el punto de montaje es **/var/cpx** y el directorio de montaje de Citrix ADC CPX es **/cpx**, como se muestra a continuación:

```
1 root@ubuntu:~# docker run -dt -e EULA=yes --name mycpx -v /var/cpx  
    :/cpx --ulimit core=-1 cpx:13.0-x.x  
2 <!--NeedCopy-->
```

Requisitos previos

Asegúrese de lo siguiente:

- Detalles del directorio host en el que montó el directorio **/cpx** de la instancia de Citrix ADC CPX existente. Puede usar el comando `docker inspect <containerName>`, donde `<containerName>` es el nombre del contenedor Citrix ADC CPX, para mostrar información sobre el directorio host.

El resultado del comando proporciona los detalles de las configuraciones del contenedor, incluidos los volúmenes. En la entrada “**Mounts**”, la subentrada “**Source**” muestra la ubicación del directorio del host en el host.

```
"Mounts": [
  {
    "Source": "/var/cpx",
    "Destination": "/cpx",
    "Mode": "",
    "RW": true
  }
],
```

- Descargue el archivo de imagen Docker de Citrix ADC CPX más reciente y cargue la imagen de Docker de Citrix ADC CPX. Para cargar la imagen, navega hasta el directorio en el que guardaste el archivo de imagen de Docker. Use el comando `docker load -i <image_name>` para cargar la imagen. Después de cargar la imagen de Citrix ADC CPX, puede introducir el comando `docker images` para mostrar información sobre la imagen:

```
1 root@ubuntu:~# docker load -i cpx-13.0-x.x.gz
2
3 root@ubuntu:~# docker images
4
5 REPOSITORY TAG IMAGE ID CREATED VIRTUAL SIZE
6
7 cpx 13.0-x.x 2e97aadf918b 43 hours ago 414.5 MB
8 <!--NeedCopy-->
```

Para actualizar una instancia de Citrix ADC CPX

1. Detenga la instancia CPX de Citrix ADC existente introduciendo el comando `docker stop <containerName>`, donde `<containerName>` es el nombre de la instancia de Citrix ADC CPX.

```
1 root@ubuntu:~# docker stop mycpx
2 mycpx
3 <!--NeedCopy-->
```

2. Con el comando `docker run`, implemente la última instancia de Citrix ADC CPX desde la imagen de Citrix ADC CPX que cargó en el host. Asegúrese de implementar la instancia en el mismo punto de montaje (por ejemplo, `/var/cpx:/cpx`) que usó para la instancia CPX de Citrix ADC existente.

```
1 root@ubuntu:~# docker run -dt -P -e CPX_CORES=1 --name latestcpx
  --ulimit core=-1 -e EULA=yes -v /var/cpx:/cpx --cap-add=
  NET_ADMIN cpx:13.0-x.x
```

```
2 <!--NeedCopy-->
```

Puede introducir el comando `docker ps` para comprobar que la instancia de Citrix ADC CPX implementada es la versión más reciente.

```
1 ```
2   root@ubuntu:~# docker ps
3
4   CONTAINER ID        IMAGE               COMMAND             PORTS
5   CREATED            STATUS             NAMES
6   ead12ec4e965       cpx:13.0-x.x      "/bin/sh -c 'bash -C " 5
7   seconds ago        Up 5 seconds      22/tcp, 80/tcp, 443/
8   tcp, 161/udp      latestcpx
9 <!--NeedCopy--> ```
```

- Después de comprobar que implementó la instancia CPX correcta de Citrix ADC, introduzca el comando `docker rm <containerName>` para eliminar la instancia anterior.

```
1 root@ubuntu:~# docker rm mycpx
2 mycpx
3 <!--NeedCopy-->
```

Uso de servidores virtuales comodín en la instancia de Citrix ADC CPX

February 19, 2022

Cuando aprovisiona una instancia de Citrix ADC, el motor de Docker solo asigna una dirección IP privada (una dirección IP) a una instancia de Citrix ADC CPX. Las tres funciones IP de una instancia de Citrix ADC se multiplexan en una dirección IP. Esta única dirección IP utiliza diferentes números de puerto para funcionar como NSIP, SNIP y VIP.

La dirección IP única que asigna el motor de Docker es dinámica. Agregue los servidores virtuales de equilibrio de carga (LB) o conmutación de contenido (CS) mediante la dirección IP única o la dirección IP 127.0.0.1. Los servidores virtuales creados con 127.0.0.1 se denominan Servidores virtuales comodín. De forma predeterminada, cuando crea un servidor virtual comodín, Citrix ADC CPX reemplaza la dirección IP asignada del servidor virtual comodín. La dirección IP asignada es 127.0.0.1, que se reemplaza por el NSIP asignado a la instancia CPX de Citrix ADC por el motor Docker.

En implementaciones de Citrix ADC CPX de alta disponibilidad, puede agregar servidores virtuales comodín en la instancia principal de Citrix ADC CPX. La sincronización de configuración entre nodos

configura el servidor virtual comodín en la instancia secundaria de Citrix ADC CPX. Elimina la necesidad de configurar el servidor virtual en el NSIP asignado por el motor Docker a las instancias de Citrix ADC CPX.

Puntos a tener en cuenta:

- Asegúrese de que el número de puerto que asigna al servidor virtual comodín no lo utilice ningún otro servidor virtual de la implementación.
- La incorporación de servidor virtual comodín falla si el número de puerto que asigna al servidor virtual comodín ya está siendo utilizado por los servicios internos.
- El servidor virtual comodín no admite el carácter *.

Para crear un servidor virtual de equilibrio de carga comodín, en el símbolo del sistema, introduzca el siguiente comando:

```
1 add lb vserver <name> <serviceType> 127.0.0.1 <port>
2
3 add lb vserver testlbvserver HTTP 127.0.0.1 30000
4 <!--NeedCopy-->
```

Para crear un servidor virtual de conmutación de contenido comodín, en el símbolo del sistema, escriba el siguiente comando:

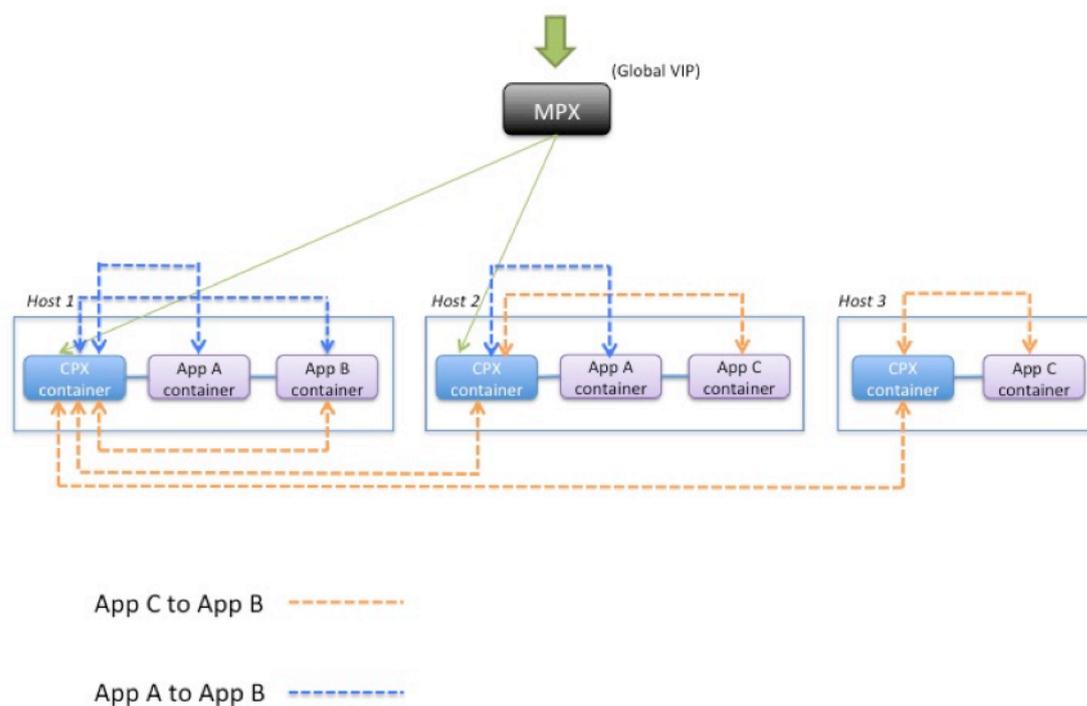
```
1 add cs vserver <name> <serviceType> 127.0.0.1 <port>
2
3 add cs vserver testcsvserver HTTP 127.0.0.1 30000
4 <!--NeedCopy-->
```

Implementar Citrix ADC CPX como proxy para habilitar el flujo de tráfico de este a oeste

February 19, 2022

En esta implementación, la instancia de Citrix ADC CPX actúa como un proxy para permitir la comunicación entre los contenedores de aplicaciones que residen en varios hosts. La instancia de Citrix ADC CPX se aprovisiona junto con las aplicaciones en varios hosts y proporciona la ruta más corta para la comunicación.

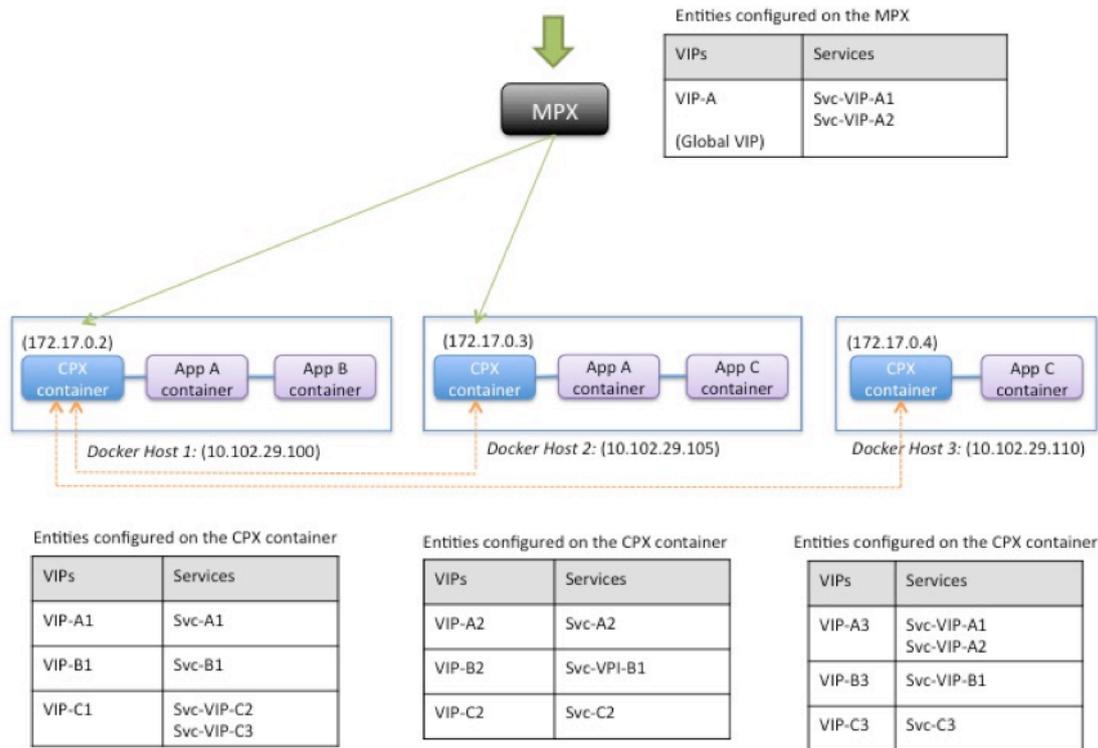
La siguiente imagen ilustra el flujo de tráfico entre dos aplicaciones a través de las instancias CPX de Citrix ADC.



Esta imagen muestra el flujo de tráfico entre la aplicación C y la aplicación B y entre la aplicación A y la aplicación B. Cuando la aplicación C (en cualquiera de los hosts) envía una solicitud a B, la solicitud se recibe primero en el contenedor Citrix ADC CPX en el mismo host que la aplicación C. A continuación, el contenedor Citrix ADC CPX pasa el tráfico al contenedor Citrix ADC CPX alojado en el mismo host que la aplicación B y, a continuación, el tráfico se reenvía a la aplicación B. Se sigue una ruta de tráfico similar cuando la aplicación A envía una solicitud a la aplicación B.

En este ejemplo, también se implementa un Citrix ADC MPX para permitir el tráfico a las aplicaciones desde Internet a través de un VIP global. El tráfico de Citrix ADC MPX se recibe en los contenedores de Citrix ADC CPX, que luego distribuyen el tráfico entre los contenedores de aplicaciones.

El siguiente diagrama ilustra esta topología con las configuraciones que deben establecerse para que se produzca la comunicación.



En la siguiente tabla se enumeran las direcciones IP y los puertos que se configuran en las instancias de Citrix ADC CPX en este ejemplo de configuración.

Docker Host 1		Docker Host 2		Docker Host 3	
VIPs	Services Bound to the VIP	VIPs	Services Bound to the VIP	VIPs	Services Bound to the VIP
VIP-A1 172.17.0.2:30000	SVC-A1 10.102.29.100:80	VIP-A2 172.17.0.3:30000	SVC-A2 10.102.29.105:80	VIP-A3 172.17.0.4:30000	SVC-VIP-A1 10.102.29.100:30000
					SVC-VIP-A2 10.102.29.105:30000
VIP-B1 172.17.0.2:30001	SVC-B1 10.102.29.100:90	VIP-B2 172.17.0.3:30001	SVC-VIP-B1 10.102.29.100:30001	VIP-B3 172.17.0.4:30001	SVC-VIP-B1 10.102.29.100:30001
VIP-C1 172.17.0.2:30002	SVC-VIP-C2 10.102.29.105:30002	VIP-C2 172.17.0.3:30002	SVC-C2 10.102.29.105:70	VIP-C3 172.17.0.4:30002	SVC-C3 10.102.29.110:70
	SVC-VIP-C3 10.102.29.110:30002				

Para configurar este caso de ejemplo, ejecute el siguiente comando en el símbolo del shell de Linux mientras crea el contenedor Citrix ADC CPX en los tres hosts de Docker:

```
1 docker run -dt -p 22 -p 80 -p 161/udp -p 30000-30002: 30000-30002 --
  ulimit core=-1 --privileged=true cpx:6.2
2 <!--NeedCopy-->
```

Ejecute los siguientes comandos mediante la función Trabajos en Citrix ADM o mediante las API de NITRO.

En la instancia de Citrix ADC CPX en Docker Host 1:

```
1 add lb vserver VIP-A1 HTTP 172.17.0.2 30000
2 add service svc-A1 10.102.29.100 HTTP 80
3 bind lb vserver VIP-A1 svc-A1
4 add lb vserver VIP-B1 HTTP 172.17.0.2 30001
5 add service svc-B1 10.102.29.100 HTTP 90
6 bind lb vserver VIP-B1 svc-B1
7 add lb vserver VIP-C1 HTTP 172.17.0.2 30002
8 add service svc-VIP-C2 10.102.29.105 HTTP 30002
9 add service svc-VIP-C3 10.102.29.110 HTTP 30002
10 bind lb vserver VIP-C1 svc-VIP-C2
11 bind lb vserver VIP-C1 svc-VIP-C3
12 <!--NeedCopy-->
```

En la instancia de Citrix ADC CPX en el host 2 de Docker:

```
1 add lb vserver VIP-A2 HTTP 172.17.0.3 30000
2 add service svc-A2 10.102.29.105 HTTP 80
3 bind lb vserver VIP-A2 svc-A2
4 add lb vserver VIP-B2 HTTP 172.17.0.3 30001
5 add service svc-VIP-B1 10.102.29.100 HTTP 30001
6 bind lb vserver VIP-B2 svc-VIP-B1
7 add lb vserver VIP-C2 HTTP 172.17.0.3 30002
8 add service svc-C2 10.102.29.105 HTTP 70
9 bind lb vserver VIP-C2 svc-C2
10 <!--NeedCopy-->
```

En la instancia de Citrix ADC CPX en el host 3 de Docker:

```
1 add lb vserver VIP-A3 HTTP 172.17.0.4 30000
2 add service svc-VIP-A1 10.102.29.100 HTTP 30000
3 add service svc-VIP-A2 10.102.29.105 HTTP 30000
4 bind lb vserver VIP-A3 svc-VIP-A1
5 bind lb vserver VIP-A3 svc-VIP-A2
6 add lb vserver VIP-B3 HTTP 172.17.0.4 30001
7 add service svc-VIP-B1 10.102.29.100 HTTP 30001
8 bind lb vserver VIP-B3 svc-VIP-B1
```

```
9   add lb vserver VIP-C3 HTTP 172.17.0.4 30002
10  add service svc-C3 10.102.29.110 HTTP 70
11  bind lb vserver VIP-C3 svc-C3
12  <!--NeedCopy-->
```

Implementar Citrix ADC CPX en una red de host único

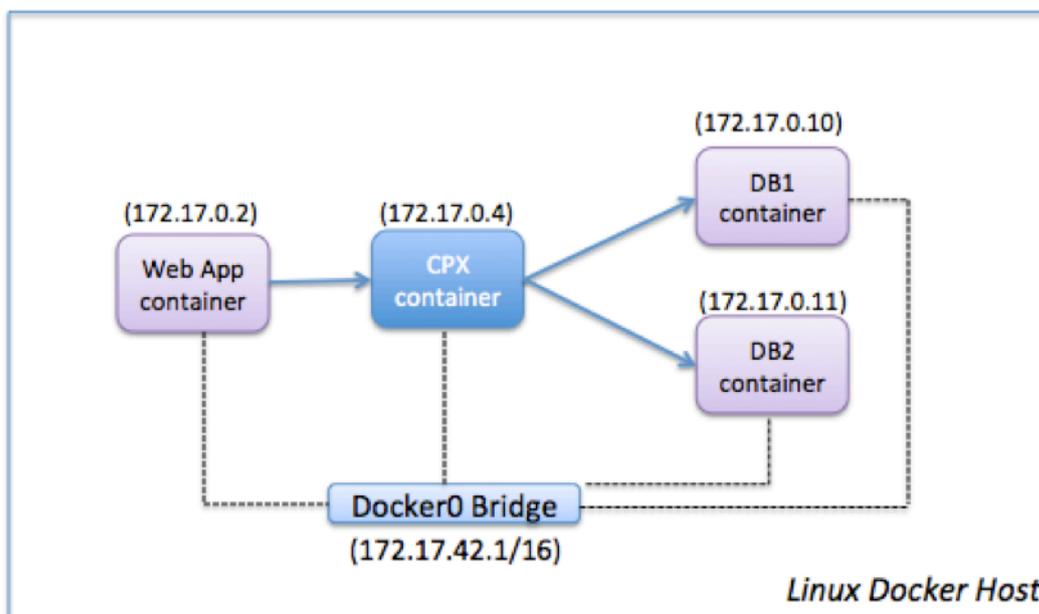
February 19, 2022

En una red de host único, la instancia de Citrix ADC CPX actúa como proxy entre los contenedores de aplicaciones en el mismo host. En esta capacidad, la instancia de Citrix ADC CPX proporciona escalabilidad y seguridad a las aplicaciones basadas en contenedores. Además, optimiza el rendimiento y también proporciona información sobre los datos de telemetría.

En una red de host único, el cliente, los servidores y la instancia de Citrix ADC CPX se implementan como contenedores en el mismo host de Docker. Todos los contenedores están conectados a través del puente docker0.

En este entorno, la instancia CPX de Citrix ADC actúa como proxy para las aplicaciones aprovisionadas como contenedores en el mismo host de Docker.

Esta ilustración ilustra la topología de host único.



En este ejemplo, un contenedor de aplicaciones web (172.17.0.2) es el cliente y los dos contenedores de base de datos, DB1 (172.17.0.10) y DB2 (172.17.0.11), son los servidores. El contenedor Citrix ADC

CPX (172.17.0.4) se encuentra entre el cliente y los servidores que actúan como proxy.

Para permitir que la aplicación web se comuniquen con los contenedores de base de datos a través de Citrix ADC CPX, primero debe configurar dos servicios en el contenedor Citrix ADC CPX para que representen a los dos servidores. A continuación, configure un servidor virtual mediante la dirección IP de Citrix ADC CPX y un puerto HTTP no estándar (como 81) porque Citrix ADC CPX reserva el puerto HTTP estándar 80 para la comunicación NITRO.

En esta topología, no tiene que configurar ninguna regla de NAT porque el cliente y el servidor están en la misma red.

Para configurar este caso, ejecute los siguientes comandos mediante la función Trabajos en Citrix ADM o mediante las API de NITRO:

```
1 add service db1 HTTP 172.17.0.10 80
2 add service db2 HTTP 172.17.0.11 80
3 add lb vserver cpx-vip HTTP 172.17.0.4 81
4 bind lb vserver cpx-vip db1
5 bind lb vserver cpx-vip db2
6 <!--NeedCopy-->
```

Implementar Citrix ADC CPX en una red multihost

February 19, 2022

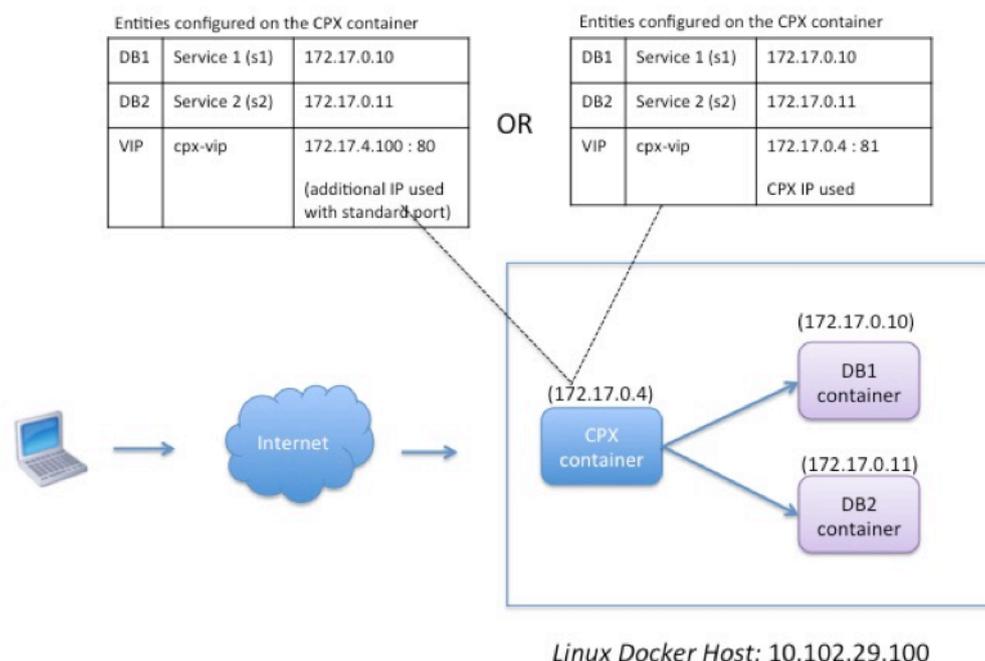
Una instancia de Citrix ADC CPX en una red multihost se puede configurar en una implementación de producción en el centro de datos, donde proporciona funciones de equilibrio de carga. Además, puede proporcionar funciones de supervisión y datos de análisis.

En una red de varios hosts, las instancias CPX de Citrix ADC, los servidores backend y los clientes se implementan en hosts diferentes. Puede utilizar topologías de varios hosts en implementaciones de producción en las que la instancia de Citrix ADC CPX equilibra la carga de un conjunto de aplicaciones y servidores basados en contenedores o incluso servidores físicos.

Topología 1: servidores Citrix ADC CPX y backend en el mismo host; cliente en una red diferente

En esta topología, la instancia de Citrix ADC CPX y los servidores de base de datos se aprovisionan en el mismo host de Docker, pero el tráfico del cliente se origina en otro lugar de la red. Esta topología se puede utilizar en una implementación de producción en la que la instancia de Citrix ADC CPX equilibra la carga de un conjunto de aplicaciones o servidores basados en contenedores.

El siguiente diagrama ilustra esta topología.



En este ejemplo, la instancia CPX de Citrix ADC (172.17.0.4) y los dos servidores, DB1 (172.17.0.10) y DB2 (172.17.0.11) se aprovisionan en el mismo host de Docker con la dirección IP 10.102.29.100. El cliente reside en otra parte de la red.

Las solicitudes de clientes que se originan en Internet se reciben en el VIP configurado en la instancia de Citrix ADC CPX, que luego distribuye las solicitudes entre los dos servidores.

Hay dos métodos que puede usar para configurar esta topología:

Método 1: uso de una dirección IP adicional y un puerto estándar para el VIP

1. Configure el VIP en el contenedor Citrix ADC CPX mediante una dirección IP adicional.
2. Configure una dirección IP adicional para el host de Docker.
3. Configure las reglas NAT para reenviar todo el tráfico recibido en la dirección IP adicional del host Docker a la dirección IP adicional del VIP.
4. Configure los dos servidores como servicios en la instancia de Citrix ADC CPX.
5. Por último, vincule los servicios al VIP.

Tenga en cuenta que en este ejemplo de configuración, la red 10.x.x.x indica una red pública.

Para configurar este caso de ejemplo, ejecute los siguientes comandos mediante la función Trabajos en Citrix ADM o mediante las API de NITRO:

```
1 add service s1 172.17.0.10 HTTP 80
```

```

2     add service s2 172.17.0.11 HTTP 80
3     add lb vserver cpx-vip HTTP 172.17.4.100 80
4     bind lb vserver cpx-vip s1
5     bind lb vserver cpx-vip s2
6 <!--NeedCopy-->

```

Configure una dirección IP pública adicional para el host de Docker y una regla NAT ejecutando los siguientes comandos en el símbolo del shell de Linux:

```

1     ip addr add 10.102.29.103/24 dev eth0
2     iptables -t nat -A PREROUTING -p ip -d 10.102.29.103 -j DNAT --to-
      destination 172.17.4.100
3 <!--NeedCopy-->

```

Método 2: utilizar la dirección IP de Citrix ADC CPX para el VIP y configurar la asignación de puertos:

1. Configure la VIP y los dos servicios en la instancia de Citrix ADC CPX. Use un puerto no estándar, 81, con el VIP.
2. Vincula los servicios al VIP.
3. Configure una regla NAT para reenviar todo el tráfico recibido en el puerto 50000 del host Docker a la VIP y al puerto 81.

Para configurar este caso de ejemplo, ejecute el siguiente comando en el símbolo del shell de Linux mientras crea el contenedor Citrix ADC CPX en los tres hosts de Docker:

```

1     docker run -dt -p 22 -p 80 -p 161/udp -p 50000:81 --ulimit core=-1
      --privileged=true cpx:6.2
2
3 <!--NeedCopy-->

```

Después de aprovisionar la instancia de Citrix ADC CPX, ejecute los siguientes comandos mediante la función Trabajos en Citrix ADM o mediante las API de NITRO:

```

1     add service s1 172.17.0.10 http 80
2     add service s2 172.17.0.11 http 80
3     add lb vserver cpx-vip HTTP 172.17.0.4 81
4     bind lb vserver cpx-vip s1
5     bind lb vserver cpx-vip s2
6 <!--NeedCopy-->

```

Nota:

Si no ha configurado la asignación de puertos durante el aprovisionamiento de la instancia CPX de Citrix ADC, configure una regla NAT ejecutando los siguientes comandos en el símbolo del shell de Linux:

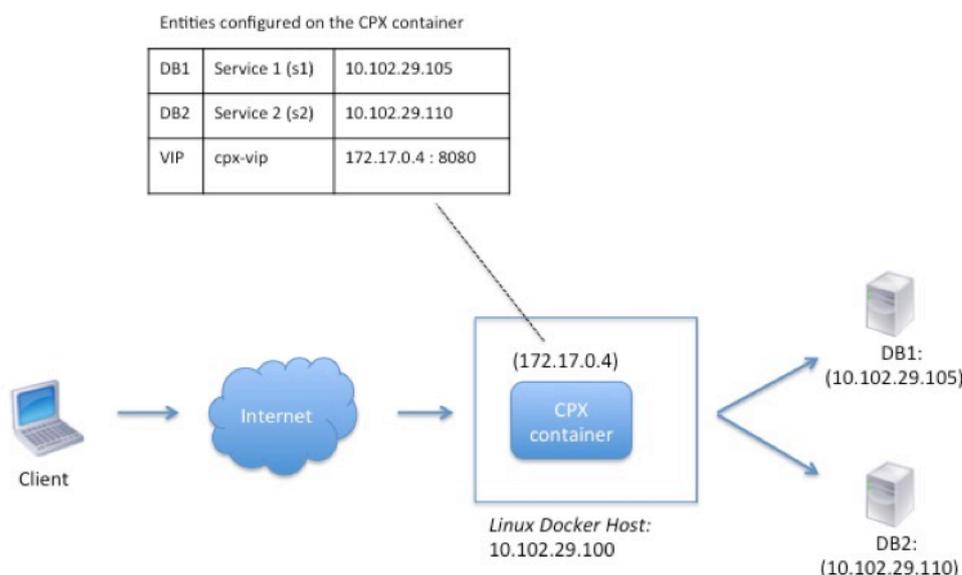
```
iptables -t nat -A PREROUTING -p tcp -m addrtype --dst-type LOCAL -m tcp --dport 50000 -j DNAT --to-destination 172.17.0.4:81
```

Topología 2: Citrix ADC CPX con servidores físicos y cliente

En esta topología, solo la instancia de Citrix ADC CPX se aprovisiona en un host Docker. El cliente y los servidores no están basados en contenedores y residen en otra parte de la red.

En este entorno, puede configurar la instancia CPX de Citrix ADC para equilibrar la carga del tráfico en los servidores físicos.

En esta ilustración se ilustra esta topología.



En este ejemplo, el contenedor Citrix ADC CPX (172.17.0.4) se encuentra entre el cliente y los servidores físicos que actúan como proxy. Los servidores, DB1 (10.102.29.105) y DB2 (10.102.29.110), residen fuera de un host Docker en la red. La solicitud del cliente se origina en Internet y se recibe en Citrix ADC CPX, que la distribuye en los dos servidores.

Para habilitar esta comunicación entre el cliente y los servidores a través de Citrix ADC CPX, primero debe configurar la asignación de puertos al crear el contenedor Citrix ADC CPX. A continuación, configure los dos servicios en el contenedor Citrix ADC CPX para que representen los dos servidores. Y, por último, configure un servidor virtual mediante la dirección IP de Citrix ADC CPX y el puerto HTTP asignado no estándar 8080.

Tenga en cuenta que en la configuración de ejemplo, la red 10.x.x.x indica una red pública.

Para configurar este caso de ejemplo, ejecute el siguiente comando en el símbolo del shell de Linux mientras crea el contenedor Citrix ADC CPX:

```
1     docker run -dt -p 22 -p 80 -p 161/udp -p 8080:8080 --ulimit core=-1
      --privileged=true cpx:6.2
2 <!--NeedCopy-->
```

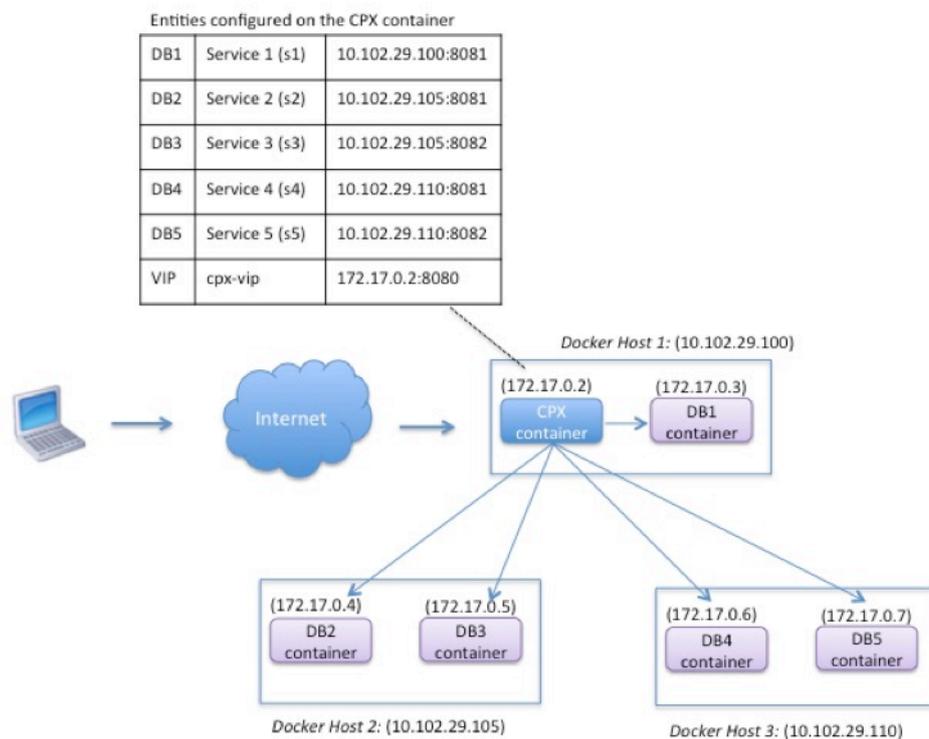
A continuación, ejecute los siguientes comandos mediante la función Trabajos en Citrix ADM o mediante las API de NITRO:

```
1     add service s1 HTTP 10.102.29.105 80
2     add service s2 HTTP 10.102.29.110 80
3     add lb vserver cpx-vip HTTP 172.17.0.4 8080
4     bind lb vserver cpx-vip s1
5     bind lb vserver cpx-vip s2
6 <!--NeedCopy-->
```

Topología 3: Citrix ADC CPX y servidores aprovisionados en diferentes hosts

En esta topología, la instancia de Citrix ADC CPX y los servidores de base de datos se aprovisionan en diferentes hosts de Docker y el tráfico del cliente se origina en Internet. Esta topología se puede utilizar en una implementación de producción en la que la instancia de Citrix ADC CPX equilibra la carga de un conjunto de aplicaciones o servidores basados en contenedores.

El siguiente diagrama ilustra esta topología.



En este ejemplo, la instancia CPX de Citrix ADC y un servidor (DB1) se aprovisionan en el mismo host de Docker con la dirección IP 10.102.29.100. Otros cuatro servidores (DB2, DB3, DB4 y DB5) se aprovisionan en dos hosts Docker diferentes, 10.102.29.105 y 10.102.29.110.

Las solicitudes de clientes que se originan en Internet se reciben en la instancia de Citrix ADC CPX, que luego distribuye las solicitudes en los cinco servidores. Para habilitar esta comunicación, debe configurar lo siguiente:

1. Configure la asignación de puertos al crear su contenedor Citrix ADC CPX. En este ejemplo, esto significa que debe reenviar el puerto 8080 del contenedor al puerto 8080 del host. Cuando la solicitud del cliente llega al puerto 8080 del host, se asigna al puerto 8080 del contenedor CPX.
2. Configure los cinco servidores como servicios en la instancia de Citrix ADC CPX. Debe usar una combinación de la dirección IP del host Docker respectivo y el puerto asignado para configurar estos servicios.
3. Configure una VIP en la instancia de Citrix ADC CPX para recibir la solicitud del cliente. Este VIP debe estar representado por la dirección IP de Citrix ADC CPX y el puerto 8080 que se asignó al puerto 8080 del host.
4. Por último, vincule los servicios al VIP.

Tenga en cuenta que en la configuración de ejemplo, la red 10.x.x.x indica una red pública.

Para configurar este caso de ejemplo, ejecute el siguiente comando en el símbolo del shell de Linux mientras crea el contenedor Citrix ADC CPX:

```
1     docker run -dt -p 22 -p 80 -p 161/udp -p 8080:8080 --ulimit core=-1
      --privileged=true cpx:6.2
2 <!--NeedCopy-->
```

Ejecute los siguientes comandos mediante la función Trabajos en Citrix ADM o mediante las API de NITRO:

```
1     add service s1 10.102.29.100 HTTP 8081
2     add service s2 10.102.29.105 HTTP 8081
3     add service s3 10.102.29.105 HTTP 8082
4     add service s4 10.102.29.110 HTTP 8081
5     add service s5 10.102.29.110 HTTP 8082
6     add lb vserver cpx-vip HTTP 172.17.0.2 8080
7     bind lb vserver cpx-vip s1
8     bind lb vserver cpx-vip s2
9     bind lb vserver cpx-vip s3
10    bind lb vserver cpx-vip s4
11    bind lb vserver cpx-vip s5
12 <!--NeedCopy-->
```

Implementar Citrix ADC CPX con acceso directo a la red

February 19, 2022

En el modo de red puente, puede configurar la instancia CPX de Citrix ADC para que tenga acceso directo a la red. En este caso, el tráfico entrante se recibe directamente en la IP (VIP) del servidor virtual Citrix ADC CPX.

Para habilitar esta comunicación, primero debe configurar una dirección IP pública en el puente docker0. A continuación, elimine la dirección IP pública del puerto de red eth0 y vincule el puerto de red al puente docker0.

Configure el equilibrio de carga agregando los dos servicios y, a continuación, configure una dirección IP pública de red como VIP en la instancia de Citrix ADC CPX. Las solicitudes de los clientes se reciben directamente en el VIP.

En la configuración de ejemplo, la red 10.x.x.x indica una red pública.

Para configurar este caso, ejecute el siguiente comando en el símbolo del shell de Linux:

```
1     ip addr add 10.102.29.100/24 dev docker0;
```

```
2 ip addr del 10.102.29.100/24 dev eth0;
3 brctl addif docker0 eth0;
4 ip route del default;
5 ip route add default via 10.102.29.1 dev docker0
6 <!--NeedCopy-->
```

Ya sea mediante la función Trabajos en Citrix ADM o mediante las API de NITRO, ejecute los siguientes comandos:

```
1 add service s1 172.17.0.8 http 80
2 add service s2 172.17.0.9 http 80
3 add lb vserver cpx-vip HTTP 10.102.29.102 80
4 bind lb vserver cpx-vip s1
5 bind lb vserver cpx-vip s2
6 <!--NeedCopy-->
```

Configurar Citrix ADC CPX en Kubernetes mediante ConfigMaps

February 19, 2022

En Kubernetes, puede configurar la instancia CPX de Citrix ADC mediante ConfigMaps. Con ConfigMaps, puede configurar dinámicamente la instancia de Citrix ADC CPX durante el inicio de la instancia.

Cree un archivo de configuración `cpx.conf` que incluya la configuración específica de Citrix ADC y los comandos bash shell que desee ejecutar dinámicamente en la instancia de Citrix ADC CPX. La estructura del archivo de configuración requiere dos tipos de etiquetas, `##Citrix ADC Commands` y `##Shell Commands`. Debajo de la etiqueta `##Citrix ADC Commands`, debe agregar todos los comandos de Citrix ADC para configurar la configuración específica de Citrix ADC en la instancia de Citrix ADC CPX. Debajo de la etiqueta `##Shell Commands`, debe agregar los comandos de shell que quiere ejecutar en la instancia de Citrix ADC CPX.

Importante:

- Las etiquetas se pueden repetir varias veces en el archivo de configuración.
- El archivo de configuración también puede incluir comentarios. Agregue un carácter “#” antes de los comentarios.
- Las etiquetas no distinguen entre mayúsculas y minúsculas.
- Si hay casos de error al implementar el contenedor Citrix ADC CPX con el archivo de configuración, los errores se registran en el archivo `ns.log`.
- Una vez iniciada la instancia de Citrix ADC CPX, si cambia el ConfigMap, la configuración

actualizada se aplica solo cuando se reinicia la instancia de Citrix ADC CPX.

A continuación se muestra un archivo de configuración de ejemplo:

```

1 #Citrix ADC Commands
2 add lb vserver v1 http 1.1.1.1 80
3 add service s1 2.2.2.2 http 80
4 bind lb vserver v1 s1
5 #Shell Commands
6 touch /etc/a.txt
7 echo "this is a" > /etc/a.txt
8 #Citrix ADC Commands
9 add lb vserver v2 http
10 #Shell Commands
11 echo "this is a 1" >> /etc/a.txt
12 #Citrix ADC Commands
13 add lb vserver v3 http
14 <!--NeedCopy-->

```

Una vez que haya creado el archivo de configuración, debe crear un ConfigMap a partir del archivo de configuración mediante el comando `kubectl create configmap`.

```

1 kubectl create configmap cpx-config --from-file=cpx.conf
2 <!--NeedCopy-->

```

En el ejemplo anterior, puede crear un ConfigMap, `cpx-config` basado en el archivo de configuración `cpx.conf`. A continuación, puede usar este ConfigMap en el archivo YAML que se utiliza para implementar la instancia CPX de Citrix ADC.

Puede ver el ConfigMap creado mediante el comando `kubectl get configmap`.

```
root@node1:~/yaml## kubectl get configmap cpx-config -o yaml
```

Ejemplo:

```

1   apiVersion: v1
2   data:
3     cpx.conf: |
4       #Citrix ADC Commands
5         add lb vserver v1 http 1.1.1.1 80
6         add service s1 2.2.2.2 http 80
7         bind lb vserver v1 s1
8       #Shell Commands
9         touch /etc/a.txt
10        echo "this is a" > /etc/a.txt
11        echo "this is the file" >> /etc/a.txt
12        ls >> /etc/a.txt

```

```
13     #Citrix ADC Commands
14         add lb vserver v2 http
15     #Shell Commands
16         echo "this is a 1" >> /etc/a.txt
17     #Citrix ADC Commands
18         add lb vserver v3 http
19     #end of file
20 kind: ConfigMap
21 metadata:
22     creationTimestamp: 2017-12-26T06:26:50Z
23     name: cpx-config
24     namespace: default
25     resourceVersion: "8865149"
26     selfLink: /api/v1/namespaces/default/configmaps/cpx-config
27     uid: c1c7cb5b-ea05-11e7-914a-926745c10b02
28 <!--NeedCopy-->
```

Puede especificar el ConfigMap creado, `cpx-config` en el archivo YAML utilizado para implementar la instancia de Citrix ADC CPX, como se muestra a continuación:

```
1  apiVersion: v1
2  kind: Pod
3  metadata:
4    name: cpx-1
5    labels:
6      app: cpx-daemon
7    annotations:
8      NETSCALER_AS_APP: "True"
9  spec:
10   hostNetwork: true
11   containers:
12     - name: cpx
13       image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-36.28"
14       securityContext:
15         privileged: true
16       volumeMounts:
17         - name: config-volume
18           mountPath: /cpx/conf
19       env:
20         - name: "EULA"
21           value: "yes"
22         - name: "NS_NETMODE"
23           value: "HOST"
24         - name: "kubernetes_url"
25           value: "https://10.90.248.101:6443"
```

```
26     - name: "NS_MGMT_SERVER"
27       value: "10.90.248.99"
28     - name: "NS_MGMT_FINGER_PRINT"
29       value: "19:71:A3:36:85:0A:2B:62:24:65:0F:7E:72:CC:DC:AD:B8:BF
30           :53:1E"
31     - name: "NS_ROUTABLE"
32       value: "FALSE"
33     - name: "KUBERNETES_TASK_ID"
34       valueFrom:
35         fieldRef:
36           fieldPath: metadata.name
37     imagePullPolicy: Never
38   volumes:
39     - name: config-volume
40       configMap:
41         name: cpx-config
42   <!--NeedCopy-->
```

Una vez que se implementa la instancia de Citrix ADC CPX is e inicia la configuración especificada en ConfigMap, `cpx-config` se aplica a la instancia de Citrix ADC CPX.

Implementar CPX de Citrix ADC como cachés DNS locales para nodos de Kubernetes

February 19, 2022

Los pods de aplicaciones de un clúster de Kubernetes dependen del DNS para comunicarse con otros pods de aplicaciones. Las solicitudes de DNS de aplicaciones dentro de un clúster de Kubernetes se gestionan mediante DNS de Kubernetes (kube-dns). Debido a la adopción más amplia de arquitecturas de microservicios, las tasas de solicitudes de DNS dentro de un clúster de Kubernetes están aumentando. Como resultado, el DNS de Kubernetes (kube-dns) está sobrecargado. Ahora puede implementar Citrix ADC CPX como una memoria caché de DNS local en cada nodo de Kubernetes y reenviar solicitudes de DNS desde los pods de aplicaciones en el nodo a Citrix ADC CPX. Por lo tanto, puede resolver las solicitudes de DNS más rápido y reducir significativamente la carga en el DNS de Kubernetes.

Para implementar Citrix ADC CPX, se utiliza una entidad de Kubernetes DaemonSet para programar pods de Citrix ADC CPX en cada nodo del clúster de Kubernetes. Un DaemonSet de Kubernetes garantiza que haya una instancia de Citrix ADC CPX en cada nodo de Kubernetes del clúster.

Para que los pods de aplicaciones dirijan el tráfico a los pods DNS de CPX, debe crear un servicio de Kubernetes con puntos finales como pods de Citrix ADC CPX. La IP de clúster de este servicio se usa como

punto de enlace DNS para los pods de la aplicación. Para asegurarse de que los pods de la aplicación usen la dirección IP del clúster de servicios Citrix ADC CPX para la resolución de DNS, debe actualizar el archivo de configuración de kubelet en cada nodo con la IP del clúster de servicios Citrix ADC CPX.

Se introducen las siguientes variables de entorno para admitir la implementación de Citrix ADC CPX como caché DNS de NodeLocal:

- **KUBE_DNS_SVC_IP**: Especifica la dirección IP del clúster del servicio `kube-dns`, que es un argumento obligatorio para desencadenar la configuración en un pod de Citrix ADC CPX. El pod de Citrix ADC CPX dirige las consultas DNS a esta dirección IP cuando la respuesta a la consulta DNS no está disponible en la memoria caché de Citrix ADC CPX.
- **CPX_DNS_SVC_IP**: Especifica la dirección IP del clúster del servicio Citrix ADC CPX. La variable de entorno `CPX_DNS_SVC_IP` se usa para configurar el DNS local en los nodos. Al configurar esta variable, se agrega una regla `iptables` para dirigir las solicitudes DNS que se originan en los pods de aplicaciones al pod CPX local de Citrix ADC dentro del nodo.
- **NS_DNS_FORCE_TCP**: Esta variable de entorno fuerza el uso de TCP para las solicitudes de DNS, incluso si las consultas se reciben a través de UDP.
- **NS_DNS_EXT_RESLV_IP**: Especifica la dirección IP del servidor de nombres externo para dirigir las solicitudes de DNS para un dominio específico.
- **NS_DNS_MATCH_DOMAIN**: Especifica la cadena de dominio externo que se va a comparar para dirigir las consultas al servidor de nombres externo.

Implementar CPX de Citrix ADC como cachés de DNS en nodos

La implementación de Citrix ADC CPX como caché de DNS local para un clúster de Kubernetes incluye las siguientes tareas:

En el nodo maestro:

- Crear un servicio de Kubernetes con puntos finales como pods de Citrix ADC CPX
- Crear un ConfigMap para definir variables de entorno para pods de Citrix ADC CPX
- Programe pods de Citrix ADC CPX en cada nodo del clúster de Kubernetes mediante un Daemon-Set de Kubernetes.

En los nodos trabajadores:

- Modifique el archivo de configuración de kubelet con la dirección IP del clúster del servicio Citrix ADC CPX para reenviar las solicitudes DNS a Citrix ADC CPX.

Configuración en el nodo maestro de Kubernetes

Realice los siguientes pasos en el nodo principal de Kubernetes para implementar Citrix ADC CPX como la memoria caché DNS local para los nodos:

1. Cree un servicio con pods de Citrix ADC CPX como puntos finales mediante el archivo `cpx_dns_svc.yaml`.

```
1 kubectl apply -f cpx_dns_svc.yaml
```

El archivo `cpx_dns_svc.yaml` se proporciona de la siguiente manera:

```
1     apiVersion: v1
2     kind: Service
3     metadata:
4       name: cpx-dns-svc
5     labels:
6       app: cpxd
7     spec:
8     ports:
9     - protocol: UDP
10      port: 53
11      name: dns
12     - protocol: TCP
13      port: 53
14      name: dns-tcp
15     selector:
16      app: cpx-daemon
```

2. Obtenga la dirección IP del servicio Citrix ADC CPX.

```
1 kubectl get svc cpx-dns-svc
```

3. Obtenga la dirección IP del servicio DNS de Kube.

```
1 kubectl get svc -n kube-system
```

4. Cree un ConfigMap para definir variables de entorno para pods de Citrix ADC CPX. Estas variables de entorno se utilizan para pasar las direcciones IP del servicio Citrix ADC CPX y el servicio DNS de Kube. En este paso, `cpx-dns-cache` se crea un ejemplo de ConfigMap utilizando las variables de entorno especificadas como datos (pares clave-valor) en un archivo.

```
1 kubectl create configmap cpx-dns-cache --from-file <path-to-file>
```

A continuación se muestra un archivo de ejemplo con las variables de entorno como pares clave-valor.

```
1 CPX_DNS_SVC_IP: 10.111.95.145
2 EULA: "yes"
3 KUBE_DNS_SVC_IP: 10.96.0.10
4 NS_CPX_LITE: "1"
5 NS_DNS_EXT_RESLV_IP: 10.102.217.142
6 NS_DNS_MATCH_DOMAIN: citrix.com
7 PLATFORM: CP1000
```

A continuación se muestra un ejemplo de ConfigMap:

```
1 apiVersion: v1
2 data:
3   CPX_DNS_SVC_IP: 10.111.95.145
4   EULA: "yes"
5   KUBE_DNS_SVC_IP: 10.96.0.10
6   NS_CPX_LITE: "1"
7   NS_DNS_EXT_RESLV_IP: 10.102.217.142
8   NS_DNS_MATCH_DOMAIN: citrix.com
9   PLATFORM: CP1000
10 kind: ConfigMap
11 metadata:
12   creationTimestamp: "2019-10-15T07:45:54Z"
13   name: cpx-dns-cache
14   namespace: default
15   resourceVersion: "8026537"
16   selfLink: /api/v1/namespaces/default/configmaps/cpx-dns-cache
17   uid: 8d06f6ee-133b-4e1a-913c-9963cbf4f48
```

5. Cree un DaemonSet de Kubernetes para Citrix ADC CPX en el nodo principal.

```
1 kubectl apply -f cpx_daemonset.yaml
```

El archivo `cpx_daemonset.yaml` se proporciona de la siguiente manera:

```
1 apiVersion: apps/v1
2 kind: DaemonSet
3 metadata:
4   name: cpx-daemon
5   labels:
6     app: cpxd
7 spec:
8   selector:
9     matchLabels:
10      app: cpx-daemon
11 template:
```

```
12  metadata:
13      labels:
14          app: cpx-daemon
15  spec:
16      containers:
17      - name: cpxd
18        imagePullPolicy: IfNotPresent
19        image: localhost:5000/dev/cpx
20        volumeMounts:
21        - mountPath: /netns/default/
22          name: test-vol
23        ports:
24        - containerPort: 53
25  envFrom:
26      - configMapRef:
27          name: cpx-dns-cache
28  securityContext:
29  privileged: true
30  allowPrivilegeEscalation: true
31  capabilities:
32      add: ["NET_ADMIN"]
33  volumes:
34      - name: test-vol
35        hostPath:
36          path: /proc/1/ns
37          type: Directory
```

Configuración en nodos de trabajo en el clúster de Kubernetes

Una vez que haya completado la configuración en el nodo maestro, lleve a cabo el siguiente paso en los nodos de trabajo:

1. Modifique el archivo de configuración de kubelet para que los pods de aplicaciones puedan usar la IP del clúster de servicios CPX de Citrix ADC para la resolución de DNS mediante uno de los siguientes pasos:

- Siga los pasos en [reconfigurar el kubelet de un nodo](#) y modifique el valor del argumento `--cluster-dns` en el siguiente formato.

```
1  --cluster-dns=<CPX_DNS_SVC_IP>,<KUBE_DNS_SVC_IP>
```

O bien:

- Modifique el archivo `/etc/systemd/system/kubelet.service.d/10-kubeadm.conf` y modifique el argumento `--cluster-dns` mediante los siguientes pasos.

- a) Modifique la configuración de kubelet y especifique la dirección IP del clúster del servicio y la dirección IP `kube-dns` del servicio Citrix ADC CPX para el argumento `--cluster-dns`.

```
1 root@node:~# cat /etc/systemd/system/kubelet.service.d/10-  
  kubeadm.conf | grep KUBELET_DNS_ARGS  
2  
3 Environment="KUBELET_DNS_ARGS=--cluster-dns  
  =10.111.95.145,10.96.0.10 --cluster-domain=cluster.  
  local"  
4 ExecStart=/usr/bin/kubelet $KUBELET_KUBECONFIG_ARGS  
  $KUBELET_CONFIG_ARGS $KUBELET_DNS_ARGS
```

- b) Vuelva a cargar el kubelet de los nodos con los siguientes comandos:

```
1 # systemctl daemon-reload  
2 # service kubelet restart
```

Implementar el proxy CPX de Citrix ADC en Google Compute Engine

February 19, 2022

En esta guía de implementación, se describe cómo puede implementar Citrix ADC CPX con Docker en Google Compute Engine (GCE) de Google Cloud con Citrix ADM ejecutándose dentro de la red empresarial. En esta implementación, Citrix ADC CPX instalado en GCE equilibra la carga de dos servidores back-end, y Citrix ADM proporciona soluciones de licencias y análisis.

Citrix ADC CPX es un proxy basado en contenedores que admite la funcionalidad completa de capa 7, la descarga SSL, varios protocolos y la API de NITRO. Citrix ADM proporciona soluciones de administración, licencias y análisis. Como servidor de licencias, Citrix ADM otorga derechos a instancias de Citrix ADC CPX que se ejecutan en las instalaciones o en la nube.

CPX y CPX Express son las mismas imágenes. Cuando licencia e instala la imagen CPX con Citrix ADM, la imagen CPX en Docker App Store (versión 11 o 12) se convierte en una instancia CPX completa. Sin licencia, la imagen CPX se convierte en una instancia CPX Express que admite conexiones SSL de 20 Mbps y 250.

Requisitos previos

- 2 GB de memoria y 1 vCPU dedicada a Citrix ADC CPX
- Código abierto de Docker disponible en GCE

- Citrix ADM se ejecuta en las instalaciones con conexión a Internet o VPN a GCE

Nota

Para obtener información sobre cómo implementar Citrix ADM, consulte [Implementación de Citrix ADM](#).

Pasos de configuración

Debe realizar los siguientes pasos para configurar esta implementación.

1. Instala Docker en una VM de GCE.
2. Configure la comunicación de API remota con la instancia de Docker.
3. Instale la imagen de Citrix ADC CPX.
4. Cree una instancia CPX.
5. Licencia de Citrix ADC CPX a través de Citrix ADM.
6. Configure los servicios de equilibrio de carga en Citrix ADC CPX y verifique la configuración.
 - a) Instale los servidores web NGINX.
 - b) Configure Citrix ADC CPX para el equilibrio de carga y verifique la distribución de la carga a ambos servicios web.

Paso 1: Instalar Docker en una VM de GCE

Desde GCE, crea una VM Linux Ubuntu. A continuación, instale Docker en la VM mediante los comandos que se muestran en el siguiente ejemplo:

```

1 $ sudo curl -ssl https://get.docker.com/ | sh
2 % Total % Received % Xferd Average Speed Time Time Time Current
3 Dload Upload Total Spent Left Speed
4 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0curl: (6) Could not resolve
   host: xn--ssl-1n0a
5 100 17409 100 17409 0 0 21510 0 --:--:-- --:--:-- --:--:-- 21492
6 apparmor is enabled in the kernel and apparmor utils were already
   installed
7 + sudo -E sh -c apt-key add -
8 + echo -----BEGIN PGP PUBLIC KEY BLOCK-----
9 Version: GnuPG v1
10
11 mQINBFWln24BEADrBl5p99uKh8+rpvqJ48u4eTtjeXAWbslJotmC/CakbNSq0b9o
12 ddfzRvGVeJVERT/Q/mlvEqgnyTQy+e6oEYN2Y2kqXceUhXagThnqCoxcEJ3+KM4R
13 mYdoe/BJ/J/6rH0jq70mk24z2qB3RU1uAv57iY5VGw5p45uZB4C4pNNsBJXoCvPn

```

```
14 TGAs/7IrekFZDDgVraPx/hdiwopQ8NltSfZCYu/jPpWFK28TR8yfvLzYFwibj5WK
15 dHM7ZTqLA1tHIG+agyPf3Rae0jPMsHR6q+arXVwMccy0i+ULU0z8mHUJ3iEMIrP
16 X+80KaN/ZjibfsB0CjcfiJSB/acn4nxQQgNZigna32velafhQivsNREFeJpzENiG
17 H0oyC6qVeOgKrRiKxzymj0FIMLru/iFF5pSwcQB7PYlt8J0G80lAcPr6VCiN+4c
18 NKv03SdvA69dC0j79Pu09IIVqsJXsSq96HB+TeEmmL+xSdpGtGdCJHm1fDeCqkZ
19 hT+RtBGQL2SEdWjxbF43oQopocT8cHvyX6Zaltn0svoGs+wX3Z/H6/8P5anog43U
20 65c0A+64Jj00rNDR8j31izhtQMRo892kGeQAaaxg4Pz6HnS7hRC+c0MHUU4HA7iM
21 zhrouAdYeTZeZEQ0A7SxtCME9ZnGwe2grxPXh/U/80WJGkzLFNcTKdv+rwARAQAB
22 tDdEb2NrZXIgmVsZWFzZSBub29sICHyZWxlyXNlZG9ja2VyKSA8ZG9ja2VyQGRv
23 Y2tldi5jb20+iQICBBABCgAGBQJWw7vdAAoJEFyzYeVS+w0QHysP/i37m4Syo0CV
24 cnybl18vzwbEcp4VCRbXvHvOXty1gccVIV8/aJqNKgBV97ly3vrp0yiIeB8ETQeg
25 srxFE7t/Gz0rsL0bqfLEHdmn5iBJRkhlFcpzje0nyB3Z0IJB6Uog0/msQVYe5CXJ
26 l6uwr0AmoiCBLrVlDAktxVh9RWch0l0KZR2FpHu8h+uM0/zySqIdlyfLa3y5oH
27 scU+nGU1i6ImwDTD3ysZC5jp9aVfvUmcESyAb4vvdcaHR+bXhA/RW8QHeeMfliWw
28 7Z2jYHyuHmDnWG2yUrnCqAJTrWV+0fKRIzzJFBs4e88ru5h2ZIXdRepw/+COYj34
29 LyzXR2cxr2u/xvxwXcKsMe7F4KZaphD+1ws61FhnUMi/PERMYFTFuvPrCkq4gyBj
30 t3fFpZ2NR/fkW87Q0eVcn1ivXl9id3MMs9KXJsg7QasT7mCsee2VIFsrxkFQ2jNp
31 D+JAERRn9Fj4ArHL5TbwkFbZzVsi6fr5h2GbCAXIGhIXKnjjorPY/YDX6X8AaH0
32 W1zblWy/CFr6VFl963jrjJgag0G6tNtBZLrclZgWh0QpeZZ5Lbvz2ZA5CqRrFAVc
33 wPNW1f0bFIRtqV6vuVluFOPCMAAnOnqR02w9t17iVQj03oVN0mbQi9vjuExXh1Yo
34 ScVeti06LSmlQfVEVRTqHLMgXyR/EMo7iQICBBABCgAGBQJXSWBAAoJEFyzYeVS
35 +w0QeH0QAI6btAfYwYPuAjrUy9qlnPhZ+xt1rnwsUzsbmo8K3XTNh+l/R08nu0d
36 sczw30Q1wju28fh1N8ay223+69f0+yICaXqR18AbGgFGKX7vo0gFEVaxdItUN3eH
37 NydGFzmeOKbAlrxIMEcnSTG/TkFVY09Ntlv9vSN2BupmTagTRErxLZKnVsWRzp+X
38
39 -----END PGP PUBLIC KEY BLOCK-----
40
41 OK
42 + sudo -E sh -c mkdir -p /etc/apt/sources.list.d
43 + dpkg --print-architecture
44 + sudo -E sh -c echo deb \[arch=amd64\] https://apt.dockerproject.org
    /repo ubuntu-yakkety main > /etc/apt/sources.list.d/docker.list
45 + sudo -E sh -c sleep 3; apt-get update; apt-get install -y -q docker-
    engine
46 Hit:1 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety InRelease
47 Get:2 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates
    InRelease [102 kB]
48 Get:3 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-backports
    InRelease [102 kB]
49 Get:4 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/restricted
    Sources [5,376 B]
50 Get:5 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/multiverse
    Sources [181 kB]
51 Get:6 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/universe
    Sources [8,044 kB]
```

```
52 Get:7 http://archive.canonical.com/ubuntu yakkety InRelease [11.5 kB]
53 Get:8 http://security.ubuntu.com/ubuntu yakkety-security InRelease [102
    kB]
54 Get:9 https://apt.dockerproject.org/repo ubuntu-yakkety InRelease [47.3
    kB]
55 Get:10 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/main
    Sources [903 kB]
56 Get:11 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    restricted Sources [2,688 B]
57 Get:12 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    universe Sources [57.9 kB]
58 Get:13 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    multiverse Sources [3,172 B]
59 Get:14 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    main Sources [107 kB]
60 Get:15 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    main amd64 Packages [268 kB]
61 Get:16 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    main Translation-en [122 kB]
62 Get:17 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    universe amd64 Packages [164 kB]
63 Get:18 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    universe Translation-en [92.4 kB]
64 Get:19 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    multiverse amd64 Packages [4,840 B]
65 Get:20 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-updates/
    multiverse Translation-en [2,708 B]
66 Get:21 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-backports/
    universe Sources [2,468 B]
67 Get:22 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-backports/
    main Sources [2,480 B]
68 Get:23 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-backports/
    main amd64 Packages [3,500 B]
69 Get:24 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-backports/
    universe amd64 Packages [3,820 B]
70 Get:25 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety-backports/
    universe Translation-en [1,592 B]
71 Get:26 http://archive.canonical.com/ubuntu yakkety/partner amd64
    Packages [2,480 B]
72 Get:27 http://security.ubuntu.com/ubuntu yakkety-security/main Sources
    [47.7 kB]
73 Get:28 https://apt.dockerproject.org/repo ubuntu-yakkety/main amd64
    Packages [2,453 B]
74 Get:29 http://security.ubuntu.com/ubuntu yakkety-security/universe
    Sources [20.7 kB]
```

```
75 Get:30 http://security.ubuntu.com/ubuntu yakkety-security/multiverse
    Sources [1,140 B]
76 Get:31 http://security.ubuntu.com/ubuntu yakkety-security/restricted
    Sources [2,292 B]
77 Get:32 http://security.ubuntu.com/ubuntu yakkety-security/main amd64
    Packages [150 kB]
78 Get:33 http://security.ubuntu.com/ubuntu yakkety-security/main
    Translation-en [68.0 kB]
79 Get:34 http://security.ubuntu.com/ubuntu yakkety-security/universe
    amd64 Packages [77.2 kB]
80 Get:35 http://security.ubuntu.com/ubuntu yakkety-security/universe
    Translation-en [47.3 kB]
81 Get:36 http://security.ubuntu.com/ubuntu yakkety-security/multiverse
    amd64 Packages [2,832 B]
82 Fetched 10.8 MB in 2s (4,206 kB/s)
83 Reading package lists... Done
84 Reading package lists...
85 Building dependency tree...
86 Reading state information...
87 The following additional packages will be installed:
88 aufs-tools cgroupfs-mount libltdl7
89 The following NEW packages will be installed:
90 aufs-tools cgroupfs-mount docker-engine libltdl7
91 0 upgraded, 4 newly installed, 0 to remove and 37 not upgraded.
92 Need to get 21.2 MB of archives.
93 After this operation, 111 MB of additional disk space will be used.
94 Get:1 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/universe
    amd64 aufs-tools amd64 1:3.2+20130722-1.1ubuntu1 [92.9 kB]
95 Get:2 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/universe
    amd64 cgroupfs-mount all 1.3 [5,778 B]
96 Get:3 http://us-west1.gce.archive.ubuntu.com/ubuntu yakkety/main amd64
    libltdl7 amd64 2.4.6-1 [38.6 kB]
97 Get:4 https://apt.dockerproject.org/repo ubuntu-yakkety/main amd64
    docker-engine amd64 17.05.0~ce-0~ubuntu-yakkety [21.1 MB]
98 Fetched 21.2 MB in 1s (19.8 MB/s)
99 Selecting previously unselected package aufs-tools.
100 (Reading database ... 63593 files and directories currently installed.)
101 Preparing to unpack .../aufs-tools_1%3a3.2+20130722-1.1ubuntu1_amd64.
    deb ...
102 Unpacking aufs-tools (1:3.2+20130722-1.1ubuntu1) ...
103 Selecting previously unselected package cgroupfs-mount.
104 Preparing to unpack .../cgroupfs-mount_1.3_all.deb ...
105 Unpacking cgroupfs-mount (1.3) ...
106 Selecting previously unselected package libltdl7:amd64.
107 Preparing to unpack .../libltdl7_2.4.6-1_amd64.deb ...
```

```
108 Unpacking libltdl7:amd64 (2.4.6-1) ...
109 Selecting previously unselected package docker-engine.
110 Preparing to unpack .../docker-engine_17.05.0~ce-0~ubuntu-yakkety_amd64
    .deb ...
111 Unpacking docker-engine (17.05.0~ce-0~ubuntu-yakkety) ...
112 Setting up aufs-tools (1:3.2+20130722-1.1ubuntu1) ...
113 Processing triggers for ureadahead (0.100.0-19) ...
114 Setting up cgroupfs-mount (1.3) ...
115 Processing triggers for libc-bin (2.24-3ubuntu2) ...
116 Processing triggers for systemd (231-9ubuntu4) ...
117 Setting up libltdl7:amd64 (2.4.6-1) ...
118 Processing triggers for man-db (2.7.5-1) ...
119 Setting up docker-engine (17.05.0~ce-0~ubuntu-yakkety) ...
120 Created symlink /etc/systemd/system/multi-user.target.wants/docker.
    service → /lib/systemd/system/docker.service.
121 Created symlink /etc/systemd/system/sockets.target.wants/docker.socket
    → /lib/systemd/system/docker.socket.
122 Processing triggers for ureadahead (0.100.0-19) ...
123 Processing triggers for libc-bin (2.24-3ubuntu2) ...
124 Processing triggers for systemd (231-9ubuntu4) ...
125 + sudo -E sh -c docker version
126 Client:
127 Version: 17.05.0-ce
128 API version: 1.29
129 Go version: go1.7.5
130 Git commit: 89658be
131 Built: Thu May 4 22:15:36 2017
132 OS/Arch: linux/amd64
133
134 Server:
135 Version: 17.05.0-ce
136 API version: 1.29 (minimum version 1.12)
137 Go version: go1.7.5
138 Git commit: 89658be
139 Built: Thu May 4 22:15:36 2017
140 OS/Arch: linux/amd64
141 Experimental: false
142
143 If you would like to use Docker as a non-root user, you should now
    consider
144 adding your user to the "docker" group with something like:
145
146 sudo usermod -aG docker albert_lee
147
148 Remember that you will have to log out and back in for this to take
```

```
    effect.
149
150 WARNING: Adding a user to the "docker" group will grant the ability to
    run
151 containers which can be used to obtain root privileges on the
152 docker host.
153 Refer to https://docs.docker.com/engine/security/security/#docker-
    daemon-attack-surface
154 for more information.
155
156 $
157
158 \*\*$ sudo docker info\*\*
159 Containers: 0
160 Running: 0
161 Paused: 0
162 Stopped: 0
163 Images: 0
164 Server Version: 17.05.0-ce
165 Storage Driver: aufs
166 Root Dir: /var/lib/docker/aufs
167 Backing Filesystem: extfs
168 Dirs: 0
169 Dirperm1 Supported: true
170 Logging Driver: json-file
171 Cgroup Driver: cgroupfs
172 Plugins:
173 Volume: local
174 Network: bridge host macvlan null overlay
175 Swarm: inactive
176 Runtimes: runc
177 Default Runtime: runc
178 Init Binary: docker-init
179 containerd version: 9048e5e50717ea4497b757314bad98ea3763c145
180 runc version: 9c2d8d184e5da67c95d601382adf14862e4f2228
181 init version: 949e6fa
182 Security Options:
183 apparmor
184 seccomp
185 Profile: default
186 Kernel Version: 4.8.0-51-generic
187 Operating System: Ubuntu 16.10
188 OSType: linux
189 Architecture: x86_64
190 CPUs: 1
```

```

191 Total Memory: 3.613GiB
192 Name: docker-7
193 ID: R5TW:VKXK:EKGR:GHWM:UNU4:LPJH:IQY5:X77G:NNRQ:HWBY:LIUD:4ELQ
194 Docker Root Dir: /var/lib/docker
195 Debug Mode (client): false
196 Debug Mode (server): false
197 Registry: https://index.docker.io/v1/
198 Experimental: false
199 Insecure Registries:
200 127.0.0.0/8
201 Live Restore Enabled: false
202
203 WARNING: No swap limit support
204 $
205
206 \*\*$ sudo docker images\*\*
207 REPOSITORY TAG IMAGE ID CREATED SIZE
208 $
209
210 \*\*$ sudo docker ps\*\*
211 CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
212 $
213 <!--NeedCopy-->

```

Paso 2: Configurar la comunicación de API remota con la instancia de Docker

Abra el puerto 4243 para la comunicación de la API con la instancia de Docker. Este puerto es necesario para que Citrix ADM se comunique con la instancia de Docker.

```

1
2 \*\*cd /etc/systemd/system\*\*
3 \*\*sudo vi docker-tcp.socket\*\*
4 \*\*cat docker-tcp.socket\*\*
5 [Unit]
6 \*\*Description=Docker Socket for the API
7 [Socket]
8 ListenStream=4243
9 BindIPv6Only=both
10 Service=docker.service
11 [Install]
12 WantedBy=sockets.target\*\*
13
14 $ \*\*sudo systemctl enable docker-tcp.socket\*\*
15 Created symlink /etc/systemd/system/sockets.target.wants/docker-tcp.

```

```
    socket → /etc/systemd/system/docker-tcp.socket.
16  \*\*sudo systemctl enable docker.socket\*\*
17  \*\*sudo systemctl stop docker\*\*
18  \*\*sudo systemctl start docker-tcp.socket\*\*
19  \*\*sudo systemctl start docker\*\*
20  $ \*\*sudo systemctl status docker\*\*
21  • docker.service - Docker Application Container Engine
22  Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor
        preset: enabled)
23  Active: \*\*active (running)\*\* since Wed 2017-05-31 12:52:17 UTC; 2s
        ago
24  Docs: https://docs.docker.com
25  Main PID: 4133 (dockerd)
26  Tasks: 16 (limit: 4915)
27  Memory: 30.1M
28  CPU: 184ms
29  CGroup: /system.slice/docker.service
30  └─4133 /usr/bin/dockerd -H fd://
31  └─4137 docker-containerd -l unix:///var/run/docker/libcontainerd/docker
        -containerd.sock --metrics-interval=0 --start-timeout 2m -
32
33  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.300890402Z" level=warning msg="Your kernel does not support
        cgroup rt peri
34  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.301079754Z" level=warning msg="Your kernel does not support
        cgroup rt runt
35  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.301681794Z" level=info msg="Loading containers: start."
36  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.417539064Z" level=info msg="Default bridge (docker0) is
        assigned with an I
37  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.465011600Z" level=info msg="Loading containers: done."
38  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.484747909Z" level=info msg="Daemon has completed
        initialization"
39  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.485119478Z" level=info msg="Docker daemon" commit=89658be
        graphdriver=aufs
40  May 31 12:52:17 docker-7 systemd[1]: Started Docker Application
        Container Engine.
41  May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
        :52:17.503832254Z" level=info msg="API listen on /var/run/docker.
        sock"
```

```

42 May 31 12:52:17 docker-7 dockerd[4133]: time="2017-05-31T12
    :52:17.504061522Z" level=info msg="API listen on [::]:4243"
43 $
44
45 (external)$ \*\*curl 104.199.209.157:4243/version\*\*
46 {
47   "Version":"17.05.0-ce","ApiVersion":"1.29","MinAPIVersion":"1.12","
    GitCommit":"89658be","GoVersion":"go1.7.5","Os":"linux","Arch":"
    amd64","KernelVersion":"4.8.0-52-generic","BuildTime":"2017-05-04
    T22:15:36.071254972+00:00" }
48
49 (external)$
50
51 <!--NeedCopy-->

```

Paso 3: instalar Citrix ADC CPX Image

Obtenga la imagen de Citrix ADC CPX en Docker App Store. El CPX Express y el CPX tienen la misma imagen. Sin embargo, cuando licencia e instala la imagen CPX con Citrix ADM, la imagen se convierte en una instancia CPX completa con un rendimiento de 1 Gbps. Sin licencia, la imagen se convierte en una instancia CPX Express que admite conexiones SSL de 20 Mbps y 250.

```

1 $ \*\*sudo docker pull store/citrix/citrixadccpx:13.0-36.29\*\*
2 13.0-36.29: Pulling from store/citrix/citrixadccpx
3 4e1f679e8ab4: Pull complete
4 a3ed95caeb02: Pull complete
5 2931a926d44b: Pull complete
6 362cd40c5745: Pull complete
7 d10118725a7a: Pull complete
8 1e570419a7e5: Pull complete
9 d19e06114233: Pull complete
10 d3230f008ffd: Pull complete
11 22bdb10a70ec: Pull complete
12 1a5183d7324d: Pull complete
13 241868d4ebff: Pull complete
14 3f963e7ae2fc: Pull complete
15 fd254cf1ea7c: Pull complete
16 33689c749176: Pull complete
17 59c27bad28f5: Pull complete
18 588f5003e10f: Pull complete
19 Digest: sha256:31
    a65cfa38833c747721c6fbc142faec6051e5f7b567d8b212d912b69b4f1ebe
20 Status: Downloaded newer image for store/citrix/citrixadccpx:13.0-36.29
21 $

```

```

22
23 $ \*\*sudo docker images\*\*
24 REPOSITORY TAG IMAGE ID CREATED SIZE
25 store/citrix/citrixadccpx:13.0-36.29 6fa57c38803f 3 weeks ago 415MB
26 $
27 <!--NeedCopy-->

```

Paso 4: crear una instancia CPX de Citrix ADC

Instale la imagen de Citrix ADC CPX en el host de Docker. Abra puertos para servicios específicos, como se muestra en el siguiente ejemplo, y especifique una dirección IP para Citrix ADM:

```

1 bash-2.05b# \*\*CHOST=${
2 1:-localhost }
3 \*\*
4 bash-2.05b# \*\*echo | openssl s_client -connect $CHOST:443 | openssl
   x509 -fingerprint -noout | cut -d'=' -f2\*\*
5 depth=0 C = US, ST = California, L = San Jose, O = Citrix NetScaler, OU
   = Internal, CN = Test Only Cert
6 verify error:num=18:self signed certificate
7 verify return:1
8 depth=0 C = US, ST = California, L = San Jose, O = Citrix NetScaler, OU
   = Internal, CN = Test Only Cert
9 verify return:1
10 DONE
11 24:AA:8B:91:7B:72:5E:6E:C1:FD:86:FA:09:B6:42:49:FC:1E:86:A4
12 bash-2.05b#
13
14 $ \*\*sudo docker run -dt -p 50000:88 -p 5080:80 -p 5022:22 -p 5443:443
   -p 5163:161/udp -e NS_HTTP_PORT=5080 -e NS_HTTPS_PORT=5443 -e
   NS_SSH_PORT=5022 -e NS_SNMP_PORT=5163 -e EULA=yes -e LS_IP=xx.xx.xx.
   xx -e PLATFORM=CP1000 --privileged=true --ulimit core=-1 -e
   NS_MGMT_SERVER=xx.xx.xx.xx:xxxx -e NS_MGMT_FINGER_PRINT=24:AA:8B
   :91:7B:72:5E:6E:C1:FD:86:FA:09:B6:42:49:FC:1E:86:A4 --env
   NS_ROUTABLE=false --env HOST=104.199.209.157 store/citrix/
   citrixadccpx:13.0-36.29\*\*
15 44ca1c6c0907e17a10ffcb9ffe33cd3e9f71898d8812f816e714821870fa3538
16 $
17
18 $ \*\*sudo docker ps\*\*
19 CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
20 44ca1c6c0907 store/citrix/citrixadccpx:13.0-36.29 "/bin/sh -c 'bash ...
   " 19 seconds ago Up 17 seconds 0.0.0.0:5022->22/tcp,
   0.0.0.0:5080->80/tcp, 0.0.0.0:50000->88/tcp, 0.0.0.0:5163->161/udp,

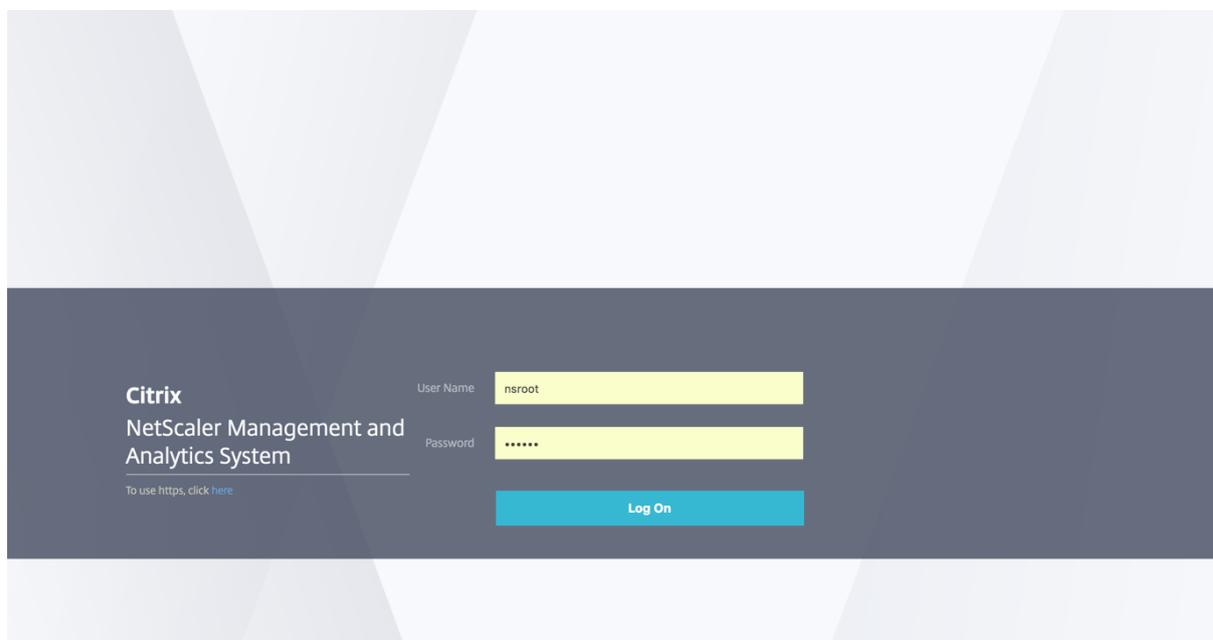
```

```
0.0.0.0:5443->443/tcp gifted_perlman
21 $
22
23 $ \*\*ssh -p 5022 root@localhost\*\*
24 root@localhost's password:
25 Welcome to nsoslx 1.0 (GNU/Linux 4.8.0-52-generic x86_64)
26
27 * Documentation: https://www.citrix.com/
28 Last login: Mon Jun 5 18:58:51 2017 from xx.xx.xx.xx
29 root@44ca1c6c0907:~#
30 root@44ca1c6c0907:~#
31 root@44ca1c6c0907:~# \*\*cli_script.sh 'show ns ip'\*\*
32 exec: show ns ip
33 Ippaddress Traffic Domain Type Mode Arp Icmp Vserver State
34 -----
35 1) 172.17.0.2 0 NetScaler IP Active Enabled Enabled NA Enabled
36 2) 192.0.0.1 0 SNIP Active Enabled Enabled NA Enabled
37 Done
38 root@44ca1c6c0907:~# \*\*cli_script.sh 'show licenseserver'\*\*
39 exec: show licenseserver
40 1) ServerName: xx.xx.xx.xxPort: 27000 Status: 1 Grace: 0 Gptimeleft: 0
41 Done
42 root@44ca1c6c0907:~# cli_script.sh 'show capacity'
43 exec: show capacity
44 Actualbandwidth: 1000 Platform: CP1000 Unit: Mbps Maxbandwidth: 3000
   Minbandwidth: 20 Instancecount: 0
45 Done
46 root@44ca1c6c0907:~#
47
48 $ \*\*sudo iptables -t nat -L -n\*\*
49 Chain PREROUTING (policy ACCEPT)
50 target prot opt source destination
51 DOCKER all -- 0.0.0.0/0 0.0.0.0/0 ADDRTYPE match dst-type LOCAL
52
53 Chain INPUT (policy ACCEPT)
54 target prot opt source destination
55
56 Chain OUTPUT (policy ACCEPT)
57 target prot opt source destination
58 DOCKER all -- 0.0.0.0/0 !127.0.0.0/8 ADDRTYPE match dst-type LOCAL
59
60 Chain POSTROUTING (policy ACCEPT)
61 target prot opt source destination
62 MASQUERADE all -- 172.17.0.0/16 0.0.0.0/0
63 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:443
```

```
64 MASQUERADE udp -- 172.17.0.2 172.17.0.2 udp dpt:161
65 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:88
66 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:80
67 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:22
68
69 Chain DOCKER (2 references)
70 target prot opt source destination
71 RETURN all -- 0.0.0.0/0 0.0.0.0/0
72 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5443 to:172.17.0.2:443
73 DNAT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5163 to:172.17.0.2:161
74 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:50000 to:172.17.0.2:88
75 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5080 to:172.17.0.2:80
76 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5022 to:172.17.0.2:22
77 $
78 <!--NeedCopy-->
```

Paso 5: Licencia de Citrix ADC CPX a través de Citrix ADM

Suponiendo que Citrix ADM se ejecuta localmente, debería poder validar que Citrix ADC CPX se está comunicando con MAS y enviando información. En las siguientes imágenes se muestra a Citrix ADC CPX recuperando una licencia de Citrix ADM.



Citrix NetScaler Management and Analytics System May 31 2017 13:14:20 GMT nsroot

Search here

Networks > License Settings

License Server Port Settings

Proxy Server Port	License Server Port	Vendor Daemon Port
0	27000	7279

License Files

The following license files are present on this server. Select **Add New License** to upload more licenses. To delete a license, select the license and click **Delete**.

[Add License File](#) [Apply Licenses](#) [Delete](#) [Download](#)

<input type="checkbox"/>	Name	Last Modified	Size
<input type="checkbox"/>	FID_3bf0b423_15ba7640cc6_2664.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_3bf0b423_15ba7640cc6_2672.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_2a2386a8_15b93284902_487e.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_2a2386a8_15b93284902_4878.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_3bf0b423_15ba7640cc6_5281.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_2a2386a8_15b93284902_4870.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_3bf0b423_15ba7640cc6_527b.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_2a2386a8_15b93284902_486a.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_3bf0b423_15ba7640cc6_5275.lic	2017-05-23 21:30:15	1.10 KB
<input type="checkbox"/>	FID_2a2386a8_15b93284902_4864.lic	2017-05-23 21:30:15	1.10 KB

License Expiry Information

Feature	Count	Days To Expiry
No items		

Citrix NetScaler Management and Analytics System Jun 05 2017 15:09:41 GMT nsroot

Search here

Networks > Instances > NetScaler CPX

NetScaler CPX

Instances: **3** Docker Host: **0**

[Add](#) [Provision](#) [Delete](#) [Dashboard](#) [Reboot](#) [Action](#) Search

<input type="checkbox"/>	IP Address	Host Name	State	Docker Host	Port Range	SSH Port	HTTP Port	HTTPS Port	SNMP Port
<input type="checkbox"/>	172.17.0.2	-NA-	Out of Service	104.196.190.229		32770	32769	32768	32768
<input type="checkbox"/>	172.17.0.5	-NA-	Out of Service	10.10.15.159	88-88	32785	32784	32783	32773
<input type="checkbox"/>	172.17.0.2	-NA-	Up	104.199.209.157		5022	5080	5443	5163

Citrix NetScaler Management and Analytics System Jun 05 2017 15:10:23 GMT nsroot

Search here

Networks > License Settings > CPX Licenses

CPX Licenses

Instances

10.0%

Total 10
Used 1

The following instances are consuming Instance license.

Name	IP Address	Instance Type	Allocation Status	Allocated Capacity
e516b1b61939	172.17.0.2	NetScaler CPX	Not available <input type="button" value="i"/>	1

Paso 6: Configurar los servicios de equilibrio de carga en Citrix ADC CPX y verificar la configuración

Primero, instale los servidores web NGINX en el host de Docker. A continuación, configure el equilibrio de carga en Citrix ADC CPX para equilibrar la carga de los dos servidores web y pruebe la configuración.

Instalar servidores web NGINX

Use los comandos que se muestran en el siguiente ejemplo para instalar servidores web NGINX.

```
1 $ sudo docker pull nginx
2 Using default tag: latest
3 latest: Pulling from library/nginx
4 Digest: sha256:41
   ad9967ea448d7c2b203c699b429abe1ed5af331cd92533900c6d77490e0268
5 Status: Image is up to date for nginx:latest
6
7
8 \*\*$ sudo docker run -d -p 81:80 nginx\*\*
9 098a77974818f451c052ecd172080a7d45e446239479d9213cd4ea6a3678616f
10
11
12 \*\*$ sudo docker run -d -p 82:80 nginx\*\*
13 bbdac2920bb4085f70b588292697813e5975389dd546c0512daf45079798db65
14
15
16 \*\*$ sudo iptables -t nat -L -n\*\*
17 Chain PREROUTING (policy ACCEPT)
18 target prot opt source destination
19 DOCKER all -- 0.0.0.0/0 0.0.0.0/0 ADDRTYPE match dst-type LOCAL
20
21 Chain INPUT (policy ACCEPT)
22 target prot opt source destination
23
24 Chain OUTPUT (policy ACCEPT)
25 target prot opt source destination
26 DOCKER all -- 0.0.0.0/0 !127.0.0.0/8 ADDRTYPE match dst-type LOCAL
27
28 Chain POSTROUTING (policy ACCEPT)
29 target prot opt source destination
30 MASQUERADE all -- 172.17.0.0/16 0.0.0.0/0
31 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:443
32 MASQUERADE udp -- 172.17.0.2 172.17.0.2 udp dpt:161
33 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:88
34 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:80
```

```

35 MASQUERADE tcp -- 172.17.0.2 172.17.0.2 tcp dpt:22
36 MASQUERADE tcp -- 172.17.0.3 172.17.0.3 tcp dpt:80
37 MASQUERADE tcp -- 172.17.0.4 172.17.0.4 tcp dpt:80
38
39 Chain DOCKER (2 references)
40 target prot opt source destination
41 RETURN all -- 0.0.0.0/0 0.0.0.0/0
42 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5443 to:172.17.0.2:443
43 DNAT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5163 to:172.17.0.2:161
44 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:50000 to:172.17.0.2:88
45 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5080 to:172.17.0.2:80
46 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5022 to:172.17.0.2:22
47 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:81 to:172.17.0.3:80
48 DNAT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:82 to:172.17.0.4:80
49 $
50 <!--NeedCopy-->

```

Configurar Citrix ADC CPX para el equilibrio de carga y verificar la distribución de la carga a ambos servicios web

```

1 $ \*\*ssh -p 5022 root@localhost\*\*
2 root@localhost's password:
3 Welcome to nsoslx 1.0 (GNU/Linux 4.8.0-52-generic x86_64)
4
5 * Documentation: https://www.citrix.com/
6 Last login: Mon Jun 5 18:58:54 2017 from 172.17.0.1
7 root@44ca1c6c0907:~#
8 root@44ca1c6c0907:~#
9 root@44ca1c6c0907:~#
10 root@44ca1c6c0907:~#
11 root@44ca1c6c0907:~# \*\*cli_script.sh "add service web1 172.17.0.3
    HTTP 80"\*\*
12 exec: add service web1 172.17.0.3 HTTP 80
13 Done
14 root@44ca1c6c0907:~# \*\*cli_script.sh "add service web2 172.17.0.4
    HTTP 80"\*\*
15 exec: add service web2 172.17.0.4 HTTP 80
16 Done
17 root@44ca1c6c0907:~# \*\*cli_script.sh "add lb vserver cpx-vip HTTP
    172.17.0.2 88"\*\*
18 exec: add lb vserver cpx-vip HTTP 172.17.0.2 88
19 Done
20 root@44ca1c6c0907:~# \*\*cli_script.sh "bind lb vserver cpx-vip web1
    "\*\*

```

```
21 exec: bind lb vserver cpx-vip web1
22 Done
23 root@44ca1c6c0907:~# \*\cli_script.sh "bind lb vserver cpx-vip web2
    "\*\*
24 exec: bind lb vserver cpx-vip web2
25 Done
26 root@44ca1c6c0907:~#
27
28 root@44ca1c6c0907:~# \*\cli_script.sh 'show lb vserver cpx-vip'\*\*
29 exec: show lb vserver cpx-vip
30
31 cpx-vip (172.17.0.2:88) - HTTP Type: ADDRESS
32 State: UP
33 Last state change was at Mon Jun 5 19:01:49 2017
34 Time since last state change: 0 days, 00:00:42.620
35 Effective State: UP
36 Client Idle Timeout: 180 sec
37 Down state flush: ENABLED
38 Disable Primary Vserver On Down : DISABLED
39 Appflow logging: ENABLED
40 Port Rewrite : DISABLED
41 No. of Bound Services : 2 (Total) 2 (Active)
42 Configured Method: LEASTCONNECTION
43 Current Method: Round Robin, Reason: A new service is bound
    BackupMethod: ROUNDROBIN
44 Mode: IP
45 Persistence: NONE
46 Vserver IP and Port insertion: OFF
47 Push: DISABLED Push VServer:
48 Push Multi Clients: NO
49 Push Label Rule: none
50 L2Conn: OFF
51 Skip Persistency: None
52 Listen Policy: NONE
53 IcmpResponse: PASSIVE
54 RHlstate: PASSIVE
55 New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
56 Mac mode Retain Vlan: DISABLED
57 DBS_LB: DISABLED
58 Process Local: DISABLED
59 Traffic Domain: 0
60 TROFS Persistence honored: ENABLED
61 Retain Connections on Cluster: NO
62
63 2) web1 (172.17.0.3: 80) - HTTP State: UP Weight: 1
```

```

64 3) web2 (172.17.0.4: 80) - HTTP State: UP Weight: 1
65 Done
66 root@44ca1c6c0907:~#
67
68 (external)$ \*\*curl 104.199.209.157:50000\*\*
69 \\





```

106														
107	100	612	100	612	0	0	1767	0	--:--:--	--:--:--				
108														
109	% Total		% Received		% Xferd		Average Speed		Time		Time		Time	
	Current													
110														
111							Dload	Upload	Total	Spent	Left			
							Speed							
112														
113	100	612	100	612	0	0	1893	0	--:--:--	--:--:--				
114														
115	% Total		% Received		% Xferd		Average Speed		Time		Time		Time	
	Current													
116														
117							Dload	Upload	Total	Spent	Left			
							Speed							
118														
119	100	612	100	612	0	0	1884	0	--:--:--	--:--:--				
120														
121	% Total		% Received		% Xferd		Average Speed		Time		Time		Time	
	Current													
122														
123							Dload	Upload	Total	Spent	Left			
							Speed							
124														
125	100	612	100	612	0	0	1917	0	--:--:--	--:--:--				
126														
127	% Total		% Received		% Xferd		Average Speed		Time		Time		Time	
	Current													
128														
129							Dload	Upload	Total	Spent	Left			
							Speed							
130														
131	100	612	100	612	0	0	1877	0	--:--:--	--:--:--				
132														
133	% Total		% Received		% Xferd		Average Speed		Time		Time		Time	
	Current													
134														
135							Dload	Upload	Total	Spent	Left			
							Speed							

136														
137	100	612	100	612	0	0	1852	0	--:--:--	--:--:--				
											1848			
138														
139	% Total	% Received	% Xferd	Average	Speed	Time	Time	Time						
	Current													
140														
141				Dload	Upload	Total	Spent	Left						
				Speed										
142														
143	100	612	100	612	0	0	1860	0	--:--:--	--:--:--				
											1865			
144														
145	% Total	% Received	% Xferd	Average	Speed	Time	Time	Time						
	Current													
146														
147				Dload	Upload	Total	Spent	Left						
				Speed										
148														
149	100	612	100	612	0	0	1887	0	--:--:--	--:--:--				
											1888			
150														
151	% Total	% Received	% Xferd	Average	Speed	Time	Time	Time						
	Current													
152														
153				Dload	Upload	Total	Spent	Left						
				Speed										
154														
155	100	612	100	612	0	0	1802	0	--:--:--	--:--:--				
											1800			
156														
157	% Total	% Received	% Xferd	Average	Speed	Time	Time	Time						
	Current													
158														
159				Dload	Upload	Total	Spent	Left						
				Speed										
160														
161	100	612	100	612	0	0	1902	0	--:--:--	--:--:--				
											1906			
162														
163	% Total	% Received	% Xferd	Average	Speed	Time	Time	Time						
	Current													
164														
165				Dload	Upload	Total	Spent	Left						
				Speed										

```

166
167 100    612  100    612    0    0    1843    0  --:--:--  --:--:--
    --:--:--  1848
168
169
170
171  % Total    % Received % Xferd  Average Speed   Time    Time       Time
    Current
172
173                Dload  Upload  Total  Spent  Left
    Speed
174
175 100    612  100    612    0    0    1862    0  --:--:--  --:--:--
    --:--:--  1860
176
177  % Total    % Received % Xferd  Average Speed   Time    Time       Time
    Current
178
179                Dload  Upload  Total  Spent  Left
    Speed
180
181 100    612  100    612    0    0    1806    0  --:--:--  --:--:--
    --:~:~:~  1810
182
183  % Total    % Received % Xferd  Average Speed   Time    Time       Time
    Current
184
185                Dload  Upload  Total  Spent  Left
    Speed
186
187 100    612  100    612    0    0    1702    0  --:~:~:~  --:~:~:~
    --:~:~:~  1704
188
189 (external)$
190
191
192
193
194
195 root@44ca1c6c0907:~# \*\*cli_script.sh 'stat lb vserver cpx-vip'\*\*
196
197 exec: stat lb vserver cpx-vip
198
199
200

```

```

201 Virtual Server Summary
202
203           vsvrIP  port  Protocol  State  Health
204   actSvcs
205 cpx-vip      172.17.0.2  88      HTTP     UP     100
206           2
207
208
209   inactSvcs
210
211 cpx-vip      0
212
213
214
215 Virtual Server Statistics
216
217           Rate (/s)
218   Total
219 Vserver hits           0
220   101
221 Requests           0
222   101
223 Responses           0
224   101
225 Request bytes           0
226   8585
227 Response bytes           0
228   85850
229 Total Packets rcvd           0
230   708
231 Total Packets sent           0
232   408
233 Current client connections  --
234   0

```

235	Current Client Est connections	--
	0	
236		
237	Current server connections	--
	0	
238		
239	Current Persistence Sessions	--
	0	
240		
241	Requests in surge queue	--
	0	
242		
243	Requests in vserver's surgeQ	--
	0	
244		
245	Requests in service's surgeQs	--
	0	
246		
247	Spill Over Threshold	--
	0	
248		
249	Spill Over Hits	--
	0	
250		
251	Labeled Connection	--
	0	
252		
253	Push Labeled Connection	--
	0	
254		
255	Deferred Request	0
	0	
256		
257	Invalid Request/Response	--
	0	
258		
259	Invalid Request/Response Dropped	--
	0	
260		
261	Vserver Down Backup Hits	--
	0	
262		
263	Current Multipath TCP sessions	--
	0	
264		

```

265 Current Multipath TCP subflows      --
      0
266
267 Apdex for client response times.    --
      1.00
268
269 Average client TTLB                 --
      0
270
271 web1          172.17.0.3    80      HTTP      UP      51
      0/s
272
273 web2          172.17.0.4    80      HTTP      UP      50
      0/s
274
275 Done
276
277 root@44ca1c6c0907:~#
278 <!--NeedCopy-->

```

Solución de problemas de Citrix ADC CPX

February 19, 2022

En este documento se explica cómo solucionar los problemas que puede encontrar al utilizar Citrix ADC CPX. Con este documento, puede recopilar registros para determinar las causas y aplicar soluciones para algunos de los problemas comunes relacionados con la instalación y la configuración de Citrix ADC CPX.

- ¿Cómo puedo ver los registros CPX de Citrix ADC?

Puede ver los registros de Citrix ADC CPX mediante el comando `kubectl logs` si Citrix ADC CPX se implementa con la opción `tty: true`. Puede ejecutar el siguiente comando para mostrar los registros:

```
1 kubectl logs <pod-name> [-c <container-name>] [-n <namespace-name>]
```

Por ejemplo,

```
1 kubectl logs cpx-ingress1-69b9b8c648-t8bgn -c cpx -n citrix-adc
```

A continuación, se muestra un ejemplo de la implementación de pods de Citrix ADC CPX con la opción `tty: true`:

```
1   containers:
2     - name: cpx-ingress
3       image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-58.30"
4       tty: true
5       securityContext:
6         privileged: true
7       env:
8
9   <!--NeedCopy-->
```

Puede encontrar más registros de arranque en el archivo `/cpx/log/boot.log` del sistema de archivos Citrix ADC CPX.

Nota: Para obtener el nombre del pod, ejecute el comando `kubectl get pods -o wide`.

- ¿Cómo puedo recopilar el paquete de soporte técnico de Citrix ADC CPX?

Puede ejecutar el siguiente comando en la interfaz shell del nodo principal de Kubernetes para recopilar el paquete de soporte técnico de Citrix ADC CPX:

```
1   kubectl exec <cpx-pod-name> [-c <cpx-container-name>] [-n <
   namespace-name>] /var/netScaler/bins/cli_script.sh "show
   techsupport"
```

Puede ver el paquete de soporte técnico en el directorio `/var/tmp/support` del sistema de archivos de Citrix ADC CPX. Use `scp` o `kubectl cp` para copiar el paquete de soporte técnico de Citrix ADC CPX al destino deseado.

Ejemplo:

```
1   root@localhost# kubectl exec cpx-ingress1-55b9b6fc75-t5kc6 -c cpx
   -n citrix-adc /var/netScaler/bins/cli_script.sh "show
   techsupport"
2   exec: show techsupport
3   Scope:  NODE
4   Done
5   root@localhost# kubectl cp cpx-ingress1-55b9b6fc75-t5kc6:var/tmp/
   support/collector_P_192.168.29.232_31Aug2020_07_30.tar.gz /tmp
   /collector_P_192.168.29.232_31Aug2020_07_30.tar.gz -c cpx
6   root@localhost# ll /tmp/collector_P_192.168.29.232
   _31Aug2020_07_30.tar.gz
7   -rw-r--r-- 1 root root 1648109 Aug 31 13:23 /tmp/collector_P_192
   .168.29.232_31Aug2020_07_30.tar.gz
```

- ¿Por qué se bloquea el pod de Citrix ADC CPX durante el arranque?

Puede comprobar el estado del pod con el comando `kubectl describe pods`. Ejecute el siguiente comando para conocer el estado del pod:

```
1 kubectl describe pods <pod-name> [-c <container-name>] [-n <namespace-name>]
```

Ejemplo:

```
1 kubectl describe pods cpx-ingress1-69b9b8c648-t8bgn
```

Si los eventos del pod muestran que el contenedor se inició, debe comprobar los registros del pod.

- ¿Cómo copio archivos entre el pod de Citrix ADC CPX y el nodo maestro de Kubernetes?

Se recomienda utilizar la función de montaje de volumen de docker para montar el directorio `/cpx` en el sistema de archivos del host. Si un contenedor Citrix ADC CPX sale de los volcados de núcleo, los registros y otros datos importantes están disponibles en el punto de montaje.

Puede usar cualquiera de los siguientes comandos para copiar archivos entre el pod de Citrix ADC CPX y el nodo maestro de Kubernetes:

kubectl cp: Puede ejecutar este comando para copiar archivos del pod al nodo:

```
1 kubectl cp <pod-name>:<absolute-src-path> <dst-path> [-c <container-name>] [-n <namespace-name>]
```

Ejemplo:

```
1 root@localhost:~# kubectl cp cpx-ingress-596d56bb6-zbx6h:cpx/log/boot.log /tmp/cpx-boot.log -c cpx-ingress
2 root@localhost:~# ll /tmp/cpx-boot.log
3 -rw-r--r-- 1 root root 7880 Sep 11 00:07 /tmp/cpx-boot.log
```

scp: puede usar el comando para copiar archivos entre el pod de Citrix ADC CPX y el nodo de Kubernetes. Ejecute el siguiente comando para copiar archivos del pod al nodo. Cuando se le pida la contraseña, proporcione la contraseña para el usuario SSH:

```
1 scp <user>@<pod-ip>:<absolute-src-path> <dst-path>
```

Ejemplo:

```
1 root@localhost:~# scp nsroot@192.168.29.198:/cpx/log/boot.log /tmp/cpx-boot.log
2 nsroot@192.168.29.198's password:
```

```
3 boot.log
4 100% 7880      5.1MB/s   00:00
5 root@localhost:~#
```

- ¿Cómo capturo paquetes en Citrix ADC CPX?

Para capturar paquetes en Citrix ADC CPX, inicie la interfaz shell de Citrix ADC CPX mediante el comando `kubectl exec`. Ejecute el siguiente comando para iniciar la interfaz shell del pod de Citrix ADC CPX:

```
1 kubectl exec -it pod-name [-c container-name] [-n namespace-name] bash
```

Ejemplo:

```
1 kubectl exec -it cpx-ingress1-69b9b8c648-t8bgn -c cpx -n citrix-adc bash
```

Y ejecute el siguiente comando para iniciar la captura de paquetes:

```
1 cli_script.sh "start nstrace -size 0"
```

Si quiere detener la captura de paquetes en curso, ejecute el siguiente comando:

```
1 cli_script.sh "stop nstrace"
```

Puede ver los paquetes capturados en un archivo `.cap` en el directorio `/cpx/nstrace/time-stamp` en el sistema de archivos Citrix ADC CPX.

- ¿Por qué el servidor de licencias no está configurado incluso cuando Citrix ADC CPX se implementa con la variable de entorno `LS_IP=<ADM-IP>`?

Asegúrese de que se pueda acceder al servidor de licencias desde el nodo en el que se implementa Citrix ADC CPX. Puede usar el comando `ping <ADM-IP>` para verificar la conectividad del nodo Citrix ADC CPX a Citrix ADM.

Si se puede acceder a Citrix ADM desde el nodo, debe verificar los registros de configuración del servidor de licencias en el archivo `/cpx/log/boot.log`. También puede comprobar la configuración del servidor de licencias mediante el siguiente comando en la interfaz shell del pod de Citrix ADC CPX:

```
1 cli_script.sh "show licenseserver"
```

Ejemplo:

```

1 root@cpx-ingress-596d56bb6-zbx6h:/cpx/log# cli_script.sh "show
  licenseserver"
2 exec: show licenseserver
3 ServerName: 10.106.102.199Port: 27000 Status: 1 Grace: 0
  Gptimeleft: 720
4 Done

```

- ¿Por qué la licencia agrupada no se configura en Citrix ADC CPX incluso después de una configuración correcta del servidor de licencias en Citrix ADC CPX?

Compruebe los registros de configuración de licencias en el archivo `/cpx/log/boot.log`. También puede verificar la licencia agrupada configurada en Citrix ADC CPX mediante el siguiente comando en la interfaz shell del pod de Citrix ADC CPX:

```
1 cli_script.sh "show capacity"
```

Por ejemplo,

```

1 root@cpx-ingress-596d56bb6-zbx6h:/cpx/log# cli_script.sh "show
  capacity"
2 exec: show capacity
3 Actualbandwidth: 1000 MaxVcpuCount: 2 Edition: Platinum
  Unit: Mbps Bandwidth: 0 ` `Maxbandwidth: 40000
  Minbandwidth: 20 Instancecount: 1
4 Done

```

Además, asegúrese de que los archivos de licencia requeridos se carguen en el servidor de licencias. También puede verificar las licencias disponibles en el servidor de licencias una vez que se haya configurado correctamente en Citrix ADC CPX mediante el siguiente comando. Ejecute el comando en la interfaz shell del pod de Citrix ADC CPX:

```
1 cli_script.sh "sh licenseserverpool"
```

Ejemplo:

```

1 root@cpx-ingress-596d56bb6-zbx6h:/cpx/log# cli_script.sh "show
  licenseserverpool"
2 exec: show licenseserverpool
3 Instance Total : 5
4 Instance Available : 4
5 Standard Bandwidth Total : 0 Mbps
6 Standard Bandwidth Availabe : 0 Mbps
7 Enterprise Bandwidth Total : 0 Mbps
8 Enterprise Bandwidth Available : 0 Mbps

```

```

 9      Platinum Bandwidth Total           : 10.00 Gbps
10      Platinum Bandwidth Available       : 9.99 Gbps
11      CP1000 Instance Total             : 100
12      CP1000 Instance Available         : 100
13      Done
14      <!--NeedCopy-->

```

- ¿Por qué las llamadas a la API NITRO obtienen *una respuesta de rechazo de conexión* de Citrix ADC CPX?

El puerto predeterminado para las API de NITRO es 9080 (no seguro) y 9443 (seguro) a partir de la versión 12.1 de Citrix ADC CPX en adelante. Asegúrese de que el puerto NITRO de Citrix ADC CPX al que intenta acceder esté expuesto en el pod. Puede ejecutar el comando `kubectl describe` para ver el puerto expuesto y asignado del contenedor Citrix ADC CPX en la sección contenedor Citrix ADC CPX:

```
1 kubectl describe pods <pod-name> | grep -i port
```

Ejemplo:

```

1      ng472 | grep -i port
2      Ports:          80/TCP, 443/TCP, 9080/TCP, 9443/TCP
3      Host Ports:     0/TCP, 0/TCP, 0/TCP, 0/TCP
4      NS_HTTP_PORT:   9080
5      NS_HTTPS_PORT:  9443
6      Port:           <none>
7      Host Port:      <none>
8      NS_PORT:        80
9      <!--NeedCopy-->

```

- ¿Por qué el proceso NSPPE en Citrix ADC CPX consume la mayor parte del uso de la CPU incluso cuando no hay tráfico o hay poco tráfico?

Si Citrix ADC CPX se implementa con la variable de entorno `CPX_CONFIG=' { "YIELD" : " NO " } '`, el proceso NSPPE consume el 100 por ciento de uso de la CPU incluso cuando no hay tráfico o hay poco tráfico. Si quiere que el proceso NSPPE no consuma el uso de la CPU, debe implementar Citrix ADC CPX sin la variable de entorno `CPX_CONFIG=' { "YIELD" : " NO " } '`. De forma predeterminada, el proceso NSPPE en CPX está configurado para no acaparar ni consumir el uso de la CPU.

- ¿Por qué Citrix ADC CPX no ilustración en Citrix ADM incluso cuando se implementó con las variables de entorno necesarias para registrarse en Citrix ADM?

Puede encontrar los registros para el registro de Citrix ADC CPX con Citrix ADM en el archivo `/cpx/log/boot.log` del sistema de archivos Citrix ADC CPX.

Puede comprobar la accesibilidad de la dirección IP de Citrix ADM desde el pod de Citrix ADC CPX mediante el comando `ping`. Además, asegúrese de que todas las variables de entorno necesarias para el registro de Citrix ADM estén configuradas para el contenedor Citrix ADC CPX.

- `NS_MGMT_SERVER`: Especifica la dirección ADM-IP o el FQDN.
 - `HOST`: Especifica la dirección IP del nodo.
 - `NS_HTTP_PORT`: Especifica el puerto HTTP- asignado en el nodo.
 - `NS_HTTPS_PORT`: Especifica el puerto HTTPS asignado en el nodo.
 - `NS_SSH_PORT`: Especifica el puerto SSH asignado en el nodo.
 - `NS_SNMP_PORT`: Especifica el puerto SNMP asignado en el nodo.
 - `NS_ROUTABLE`: La dirección IP del pod de Citrix ADC CPX no se puede redirigir desde el exterior.
 - `NS_MGMT_USER`: Especifica el nombre de usuario de ADM.
 - `NS_MGMT_PASS`: Especifica la contraseña de ADM.
- ¿Por qué `cli_script.sh` se muestra un mensaje de error de *nombre de usuario o contraseña no válidos* después de cambiar la contraseña del usuario `nsroot`?

El comando `cli_script.sh` es una utilidad de envoltura para NSCLI en Citrix ADC CPX. Ejecuta el primer argumento como cadena de comandos o ruta de archivo y el segundo argumento es opcional, que son las credenciales. Si se cambia la contraseña del usuario `nsroot`, debe proporcionar credenciales como segundo argumento para `cli_script.sh`. Puede ejecutar el siguiente comando para ejecutar NSCLI con credenciales:

```
1 cli_script.sh "<command>" " :<username>:<password> "
```

Ejemplo:

```
1 root@087a1e34642d:/# cli_script.sh "show ns ip"
2 exec: show ns ip
3
4 ERROR: Invalid username or password
5
6 root@087a1e34642d:/# cli_script.sh "show ns ip" ":nsroot:
7 nsroot123"
8
9 exec: show ns ip
10
11 Ipaddress      Traffic Domain      Type      Mode
12      Arp      Icmp      Vserver  State
13 -----      -
14      ----      -
15
16 172.17.0.3      0      NetScaler IP      Active
17      Enabled  Enabled  NA      Enabled
```

13	192.0.0.1	0		SNIP	Active
	Enabled	Enabled	NA	Enabled	
14	Done				

- ¿Por qué falla SSH a Citrix ADC CPX con un usuario `root` y `nsroot`?

A partir de la versión 13.0-64.35, Citrix ADC CPX genera una contraseña predeterminada y la actualiza para los usuarios SSH, `root` y `nsroot`. Si no ha cambiado la contraseña manualmente, la contraseña para los usuarios de SSH se puede encontrar `/var/deviceinfo/random_id` en el sistema de archivos de Citrix ADC CPX.

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).