



acens

Part of Telefónica Tech

Manual de Usuario

Disaster Recovery as a Service (DRaaS) On-Premise



**Telefónica
Empresas**

Índice

Contenido

Índice	2
Compatibilidad de VCDA 4.0 en CDC.....	3
Descripción del servicio y casos de uso	5
<i>Documentación oficial</i>	5
<i>Descripción de la solución</i>	5
<i>Migraciones</i>	5
<i>Protecciones</i>	7
Posibilidades y conceptos de VCDA (DRaaS)	9
<i>¿Qué permite el servicio de draas (VCDA 4.0)?</i>	9
<i>RPO: Cuando consumen mis VMs en mi CDC</i>	10
Instalación de Appliances	12
Actualización del appliance On-Premise a 4.0.2	16
Configuración de appliance	18
Ejemplo de migración a CDC	25
Requisitos necesarios y consejos en On-Premise.....	26
Troubleshooting	27
<i>Autenticación de sitios</i>	27
<i>Réplica que cae en estado unknow</i>	28
<i>Appliance deshabilitado dentro de vCenter</i>	28
<i>Mensaje de “Permisos denegado” en la configuración del appliance</i>	30
<i>Contraseña del appliance bloqueada</i>	30
<i>Hardware virtual no compatible con onpremise; invalid status al levantar vms</i>	31
<i>Réplicas bloqueadas si posibilidad de detenerlas</i>	31
Instalación de appliance en legacy sites.....	32

Compatibilidad de VCDA 4.0 en CDC

Para poder hacer migraciones desde su servidor ESXi, este tiene que contar con una de las siguientes licencias:

- vSphere Essentials Plus
- vSphere Standard
- vSphere Enterprise
- vSphere Enterprise Plus

[vSphere Replication Licensing \(vmware.com\)](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php)

Para saber si su plataforma cliente (On-Premise), cumple con los requisitos de compatibilidad, lo mejor es comprobar las versiones en la siguiente URL:

https://www.vmware.com/resources/compatibility/sim/interop_matrix.php

Seleccione como producto a comparar el producto “VMWare Cloud Director Availability” y la versión que esté desplegada en el proveedor, hoy en día es la versión 4.0.

Sobre “Add Platform/Solution” agregue su versión de vCenter Server y ESXi:

Interoperability Solution/Database Interoperability Upgrade Path

1. Select a Solution

If you do not know the *solution's* version leave it blank.

VMware Cloud Director Availability

AKA VMware vCloud Availability & VMware vCloud Availability for Cloud-to-Cloud DR

2. Add Platform/Solution

Add *platforms/solutions* to see if they are compatible with the selected *solution*.

VMware vCenter Server

VMware vSphere Hypervisor (ESXi)

Hide empty rows/columns Hide unsupported releases

VMware Cloud Director Availability	4.0
▼ VMware vCenter Server	
7.0	✓
6.7 U3	✓
6.7 U2	✓
6.7 U1	✓
6.5 U3	✓
▼ VMware vSphere Hypervisor (ESXi)	
7.0	✓
6.7 U3	✓
6.7 U2	✓
6.7 U1	✓
6.5 U3	✓

Aunque puede ver que las versiones anteriores no están contempladas, hay que hacer una notación al respecto. Esta compatibilidad está referida al uso de la parte On-Premise y no a su uso desde el portal de CDC. Esto quiere decir que VEDA puede administrarse en el portal de vCloud Director (CDC) pero no como plugin del vCenter cuando las versiones no son compatibles.

Las incompatibilidades no implican que no pueda usarlo con versiones anteriores de vCenter y ESXi, el problema es que en versiones anteriores solo podrá usar la solución desde el portal de CDC y no podrá usarlo desde su sitio On-Premise. La razón es porque el desarrollo de la solución está hecho en HTML5 y esta característica solo comenzó a estar disponible a partir de la versión 6.5U3 de vCenter, por lo tanto, no es posible ver la interface de administración de VEDA en su vCenter Local (On-Premise) y sin embargo sí verlo en su portal de vCloud Director (CDC).

Descripción del servicio y casos de uso

DOCUMENTACIÓN OFICIAL

Aunque vamos a describir el funcionamiento de la solución, la mejor manera de conocer en profundidad el funcionamiento y las posibilidades del servicio, es a través la página oficial del propio fabricante. Aquí dispone del enlace con toda la documentación completa de la solución:

Guía de usuario:

<https://docs.vmware.com/en/VMware-Cloud-Director-Availability/4.0/VMware-Cloud-Director-Availability-40-User-Guide/GUID-1827B289-289F-45C3-B42A-E2C788C888F2.html>

Instalación, configuración y actualización:

<https://docs.vmware.com/en/VMware-Cloud-Director-Availability/4.0/VMware-Cloud-Director-Availability-40-Install-Config-Upgrade-On-Prem/GUID-A8907B9E-F24D-4A43-B6A7-F38F0BA27727.html>

No obstante, vamos a explicar cómo se instala la parte cliente, los casos básicos de uso y algunos conceptos que podrán ayudarle a usar mejor esta solución.

DESCRIPCIÓN DE LA SOLUCIÓN

VCDA (VMWare Cloud Director Availability) es una solución que está diseñada para hacer **migraciones y protecciones** de máquinas virtuales que se encuentran en una infraestructura de VMWare remota On-Premise a la nube de su CDC. Las acciones de migración pueden ocurrir en ambos sentidos, es decir, entre On-Premise → CDC y CDC → On-Premise.

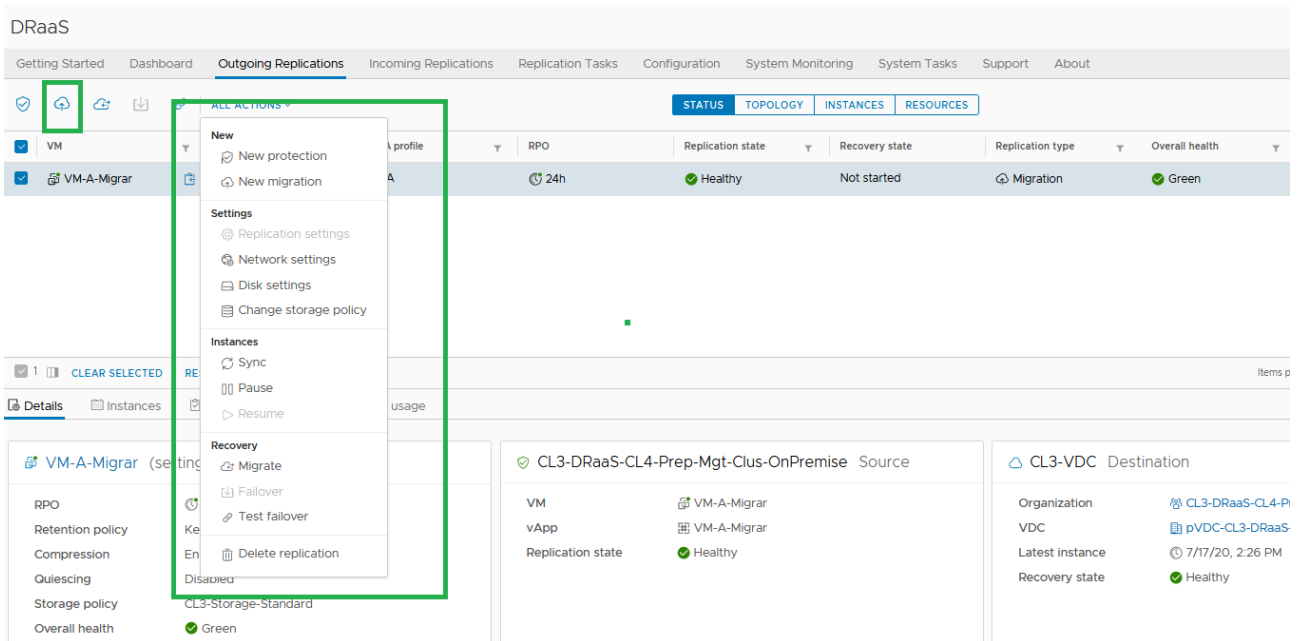
El site desde el que está usted subiendo sus VMs se denomina "ON-PREMISE" y es el lugar donde están sus servicios, para poder comenzar con sus migraciones o réplicas necesita tener instalada una máquina cliente de VMWare (appliance) a la que tiene que poner una IP en la misma red de sus vCenter y de sus ESXi. Esta máquina debe tener conexión a Internet y poder acceder a nuestro receptor de túneles. Este appliance hará de Proxy para las réplicas de sus instancias puedan replicar la información a su cloud público de forma encriptada, pudiendo hacer esta comunicación de forma bidireccional. No necesita abrir ningún puerto en su sitio On-Premise, con que este appliance tenga conexión con Internet, será suficiente.

MIGRACIONES

La configuración de una migración tiene como objetivo subir sus VMs a su plataforma en la nube. Para ello tiene que configurar su VM para que comience el proceso de migración. Una vez realizado puede hacer el proceso o acción de MIGRACIÓN final. Este proceso consistente en levantar la máquina virtual en remoto y apagar la original en su On-Premise Site.

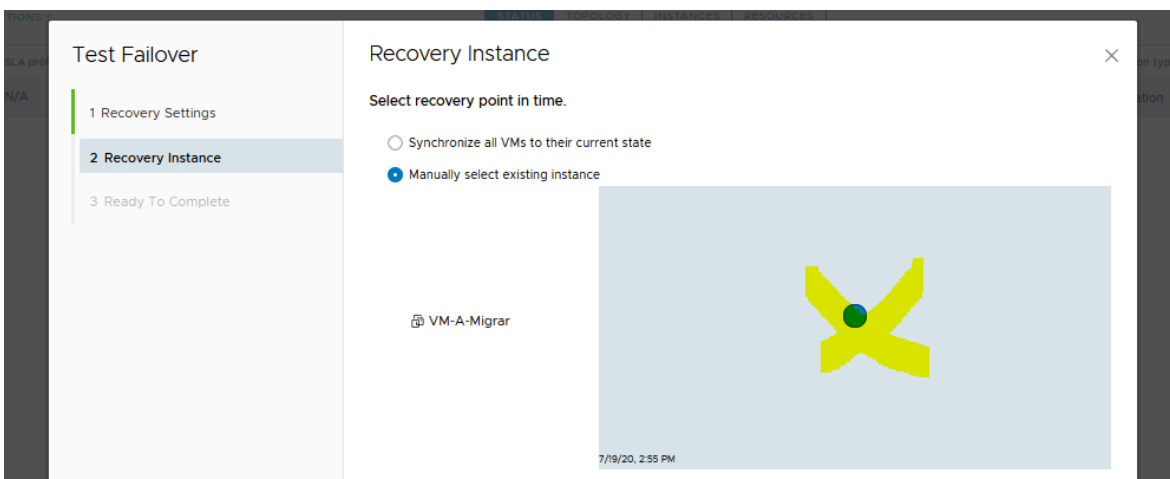
A la hora de arrancar la VM en su CDC alojado en acens, esta podrá cambiar de red, tener una nueva IP o incluso un nuevo nombre. También podrá evitar que alguno de los discos se suba o bien, elegir el Storage

Profile donde quiere ubicar la VM. Recuerde que para las operaciones de personalizado se realicen de forma correcta deberá tener instaladas las VMware Tools y sus máquinas tienen que ser compatibles con la personalización, esto ocurre en la mayoría de los casos:



El proceso de migración no tiene la posibilidad de trabajar con SLAs y por lo tanto, tiene las funcionalidades básicas que son: el copiado inicial de la VM (fullsync) y la sincronización final en el momento de ejecutar la acción de migración.

En caso de que quiera realizar una sincronización intermedia entre el momento que la subió por primera vez y la sincronización final deberá utilizar el botón “Sync” antes de realizar el proceso de migración definitivo o bien un “Test Failover”, esto le evitará que se prolongue el tiempo de copiado de datos en la última parte del proceso. No obstante, el sistema de migración guarda un punto intermedio que podrá usar también como opción alternativa.



PROTECCIONES

El proceso de protección consiste en mantener una copia sincronizada de una o varias de sus máquinas virtuales. El proceso de protección puede tener lugar en un sentido u en otro, no en ambos sentidos a la vez. Para poder proteger una máquina virtual debe configurar la protección y adecuarse a uno de los SLAs contratados. Puede contratar diferentes SLAs en función la disponibilidad que requiera su servicio.

¿Qué es un SLA?

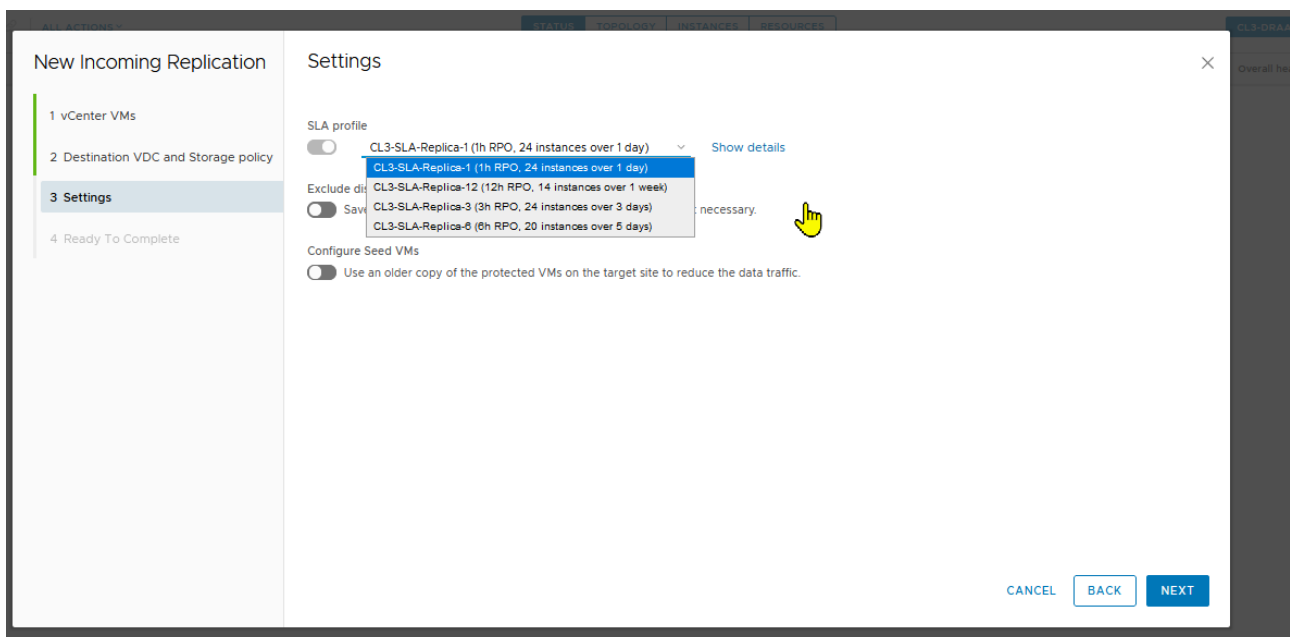
Un SLA es la calidad a nivel de servicio que está definida cuantitativamente y que se le ofrece como protección de su máquina virtual, cada SLA es un producto diferente del catálogo, contacte con su comercial si quiere optar por más opciones de SLAS.

Cuando hace la protección de un VM, puede elegir entre estos SLAs y cada uno de ellos le ofrece una protección diferente.

El SLA está basado en varios conceptos, que son los valores de protección que se le asignan a sus instancias y son los siguientes:

- **MPTIs** : Son una cantidad de puntos de restauración que permanecen un tiempo determinado y que podrán ser utilizados como puntos de restauración a los que usted podrá llevar su máquina virtual en el momento que necesita hacer un proceso de Failover. Estos puntos no son snapshot y no permiten ir en el tiempo, cuando se elige un punto, este será el que recupere y después no tendrá marcha atrás.
- **RPOs**: Es la cantidad de cambios, expresado en tiempo, que puede perder de su VM si no puede recuperar un estado anterior con MPTIS o bien, quiera recuperar el último momento de su VM y no es posible una última sincronización final. Esto ocurre cuando la máquina origen no responde en el site que inicia la réplica y no es posible hacer la
- última sincronización al no estar disponible la máquina original. Podríamos expresarlo como el último punto disponible de su VM.

Como puede ver a continuación, configuramos una réplica y seleccionamos un SLA para ella:



Como puede ver hay 4 tipos de SLA y estos tienen preestablecidos la cantidad de MPTIs en función de un tiempo y la RPO. Así, si por ejemplo queremos usar el SLA: "CL3-SLA-Replica-1" podrá ver que su configuración dice: "1h RPO, 24 instances over 1 day". En este caso si el sitio desde el que se realizan las replicas sufre un downtime total, podrá recuperar o levantar su VM con los cambios que hubiera replicados con una hora de anterioridad (RPO).

La RPO siempre está sujeta a la cantidad de datos que se pueden copiarse a través de la red. Si su VM tiene más cambios que cantidad de datos que puede transferir en su línea de tiempo de 1 hora (valor de la RPO), no se podrá garantizar la RPO y sufrirá lo que se llama RPO Violation. En este caso se recuperará la última sincronización completa disponible.

Como recomendación ante un downtime total, se recomienda optar por el último punto de restauración, puesto que es posible que si la VM tenía un problema nos llevemos el problema con la última sincronización.

Es muy aconsejable que marque en el calendario un momento en el que probar su protección haciendo un TEST FAILOVER. Esto levantará su máquina en el sitio remoto y podrá asegurar la consistencia. Luego, podrá hacer un CLEAN TEST y dejar la sincronización ejecutándose nuevamente como estaba antes del proceso de test. Durante este proceso no se replican cambios y las máquinas que se han levantado en remoto, aunque pueden reiniciarse y pueden tener cambios en disco, se levantan en modo lectura por lo que cuando hace un CLEAN TEST la réplica vuelve a continuar desde el momento en el que lanzó el TEST FAILOVER.

Durante el proceso de replicación la máquina virtual no se ve en el sitio remoto y es solo cuando se realiza un TEST FAILOVER o UN FAILOVER, cuando puede comenzar a verla dentro de su organización.

Posibilidades y conceptos de VCDA (DRaaS)

Debemos conocer los conceptos y posibilidades de la solución para saber cómo podemos usar nuestro sistema de DRaaS. Como hemos mencionado en puntos anteriores DRaaS nos brinda la posibilidad de poder realizar migraciones y protecciones entre nuestro servidor vCenter y nuestro entorno de CDC. Además, puede también hacer protecciones hacia el exterior, pudiendo proteger las máquinas virtuales de su CDC hacia un sitio On-Premise con ESXi y vCenter Server.

Los sistemas de DRaaS no son sistema de clústerización donde hay nodos en modo activo y en modo standby, los cuales se vigilan y cuando alguno no funciona bien levantan el servicio en el sitio remoto. Los sistemas DRaaS están diseñados para que la acción de recuperación se produzca de forma manual, el concepto está pensado así porque debe ser el factor humano quién tome la decisión de levantar el servicio en el sitio remoto. Cuando se produce un FAILOVER el servicio cambia y comienza a darse en el lugar remoto, las máquinas origen que están en OnPremise site quedan descartadas como principales y la réplica deja de producirse. Los cambios que se hagan en el CDC después de hacer el FAILOVER ya no estará en su OnPremise Site.

Cuando hacemos un FAILOVER no hay ya réplicas y hay que configurar el proceso siguiente de REPROTECT que implicará una nueva configuración que explicaremos más adelante donde se hace una protección inversa.

Existen diferentes posibilidades para el uso de la solución:

¿QUÉ PERMITE EL SERRVICIO DE DRAAS (VCDA 4.0)?

- Migraciones de VMs de entornos vCenter OnPremise a entornos en la nube.
- Migraciones de VMs de entornos de la nube a nuestro OnPremise Site con vCenter.
- Permite **administración y monitorización de nuestras réplicas entre** nuestro servidor de vCenter y nuestra nube (CDC) en ambos sentidos.
- Puedes trabajar con VMs o bien puede hacerlo con vAPPs.
- Puede usarse para replicación de VMs de forma asíncrona entre vCenter y CDC y viceversa, pudiendo hacer **Test Failover, Failover Task y Reverse Task**.
- Permite la **sincronización con semilla “seed**. Permite hacer una réplica partiendo de una máquina subida previamente para no comenzar la réplica desde el principio
- Gestión **self-service** de las réplicas del cliente **desde el portal HTML5** de CDC.
- **No es necesario tener puertos** abiertos en los Firewalls perimetrales de la infraestructura On-Premise.
- **Plug-In integrado en vCenter** en On-Premise Site, solo para versiones de Web Client con HTML5, si son antiguas, tendrá que administrarse desde CDC.
- Permite **RPOs definida** en el proveedor por medio de SLAs.
- Permite puntos de restauración intermedios (MPITs) en función de los SLAs contratados.
- Permite “Quiesce Snapshot” de las máquinas virtuales cuando se guardan instantáneas descritas en el punto anterior.
- Permite solo migrar los discos que seleccione de su VM
- Permite levantar su VM en una red o con una configuración específica mediante la “Customización”, incluso cambiar el nombre su VM.

- Permite seleccionar un perfil de almacenamiento pudiendo colocar sus VMs, en almacenamiento standard, plus o extreme.
- Permite mover grupos de máquinas virtuales basado en vAPPs.
- En algunos casos la solución se usa como desbordamiento de recursos.

RPO: CUANDO CONSUMEN MIS VMS EN MI CDC

Una de los conceptos que tenemos que conocer es como se consumen los recursos en nuestra organización de CDC cuando estamos haciendo nuestras réplicas. Esto es muy importante porque nos permite conocer si tendremos espacio suficiente para que nuestras máquinas levanten ante una caída en un OnPremise Site. No solo servirá para saber si todas nuestras máquinas levantarán ante un desastre, nos servirá también para saber qué espacio y qué recursos necesitamos en nuestro CDC para hacer una migración.

Antes de hacer algún ejemplo tenemos que conocer los puntos siguientes:

- La réplica **NO CONSUME CPU** hasta que se realiza un TEST o un FAILOVER
- La réplica **NO CONSUME RAM** hasta que se realiza un TEST o un FAILOVER
- Si a la hora de hacer TEST o FAILVER no hay recursos libres suficientes en nuestro CDC, la VM NO ARRANCARÁ. Solo arrancarán las VMs que dispongan de CPU y RAM disponible libre en la organización.
- Las réplicas SÍ CONSUMEN EL ALMACENAMIENTO
- El almacenamiento PROVISIONADO se añade al Storage-Profile para ver si hay espacio para levantar la VM en caso de failover al activar la réplica. Si no hay espacio suficiente falla la configuración de la réplica falla.
- Si una VM tiene espacio suficiente para ser configurada en el Storage-Profile, la replicación será creada si no fallará.
- Una vez creada la réplica, se crea un disco independiente que ocupa el espacio real consumido por la VM.

Name	Status	Storage Policy	Bus Type	Owner	Size
C4-0fab1091-2d15-4f64-b77a-3ba2eae7e8a4	Ready	CL3-Storage-Standard	LSI Logic Parallel (SCSI)	admin	15.00 GB

Ejemplo: Tenemos un Storage-Profile de 500 GB con 100 GB ocupados. Vamos a configurar la réplica de una VM que tiene configurado un disco de 50 GB (PROVISIONADOS) de los cuales, solo 10 GB están escritos en disco (GB ALLOCATED, USADOS). Cuando damos a configurar la réplica, el sistema suma a nuestro Storage-Profile 50 GB y ve si puede ubicar la VM.

100 GB+50GB=150 Es menos de 500, por lo que la VM no tendrá problemas para arrancar

Recursos requeridos en nuestro **CDC Allocated** para que levanten las réplicas

Storage (GB) = GB Ocupado en Storage-Profile + Suma en GB provisionados de VMs replicando

Memoria = suma memoria de VMs replicando + suma memoria de VMs en CDC

vCPU = suma de GHz de VMs replicando + suma en GHz de VMs en CDC

Recursos requeridos en nuestro **CDC Pay-As-You-Go** para que levanten las réplicas:

Storage (GB) = Suma de GB provisionados de VMs replicando y suma del ocupado en CDC. Tenga en cuenta que nosotros marcamos un límite en CDC en el Storage-Profile, por motivos de seguridad, si necesitas más espacio, pídale a través de un ticket de soporte.

Memoria = No hay problema es ilimitado

vCPU = No hay problema es ilimitado

Instalación de Appliances

Para proceder a la instalación de la parte cliente y poder interactuar con nuestro portal de vCloud Director, es necesario instalarse una VM cliente llamada "VCDa Onpremise". Esta máquina conecta el túnel y controla las réplicas contra la infraestructura de su nube pública. Es muy importante tener clara cual es la URL de acceso a su cloud, puesto que es muy importante acceder a la infraestructura que tiene contratada y no a otra que no disponga del servicio o no le corresponda. Pregunte qué URL le corresponde.

Para comenzar, debe descargar de la página de VMWare el siguiente appliance, esta descarga contiene un archivo ".ova" que deberá importar en su vcenter.

El nombre en la versión de este documento es:

"VMware Cloud Availability 4.0.0.2 On-Premises Appliance"

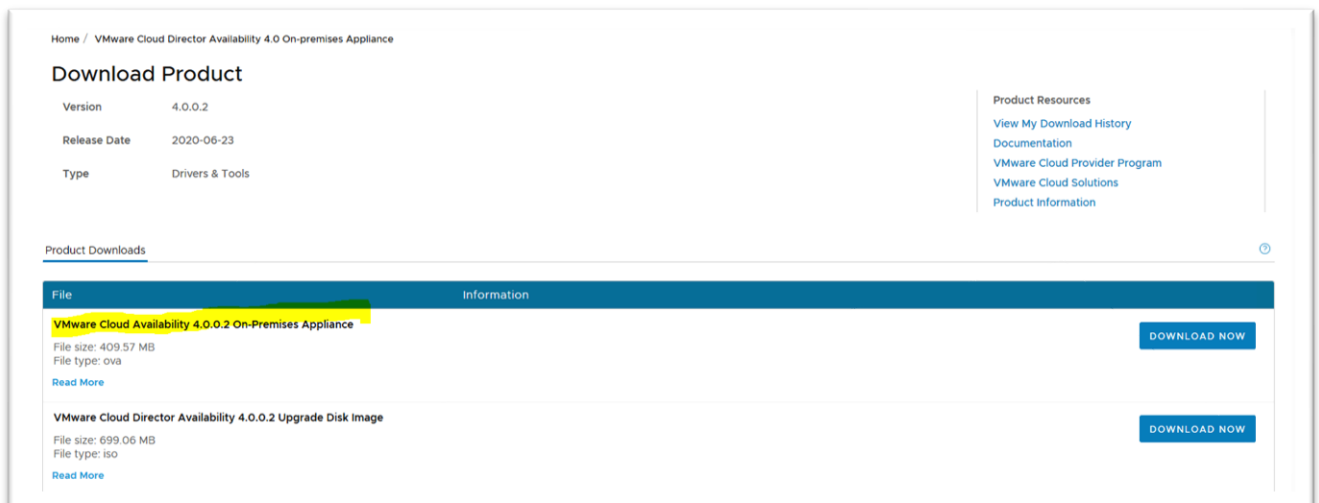
Proceda con la descarga y tenga muy presente que tiene que descargar el que está nombrado con la palabra: "ON-PREMISE", la versión que pone "Upgrade" es para actualizar versiones de appliances On-Premise más antiguos, puede ver la sección de actualización.

Si descarga otro appliance no podrá hacer las réplicas.

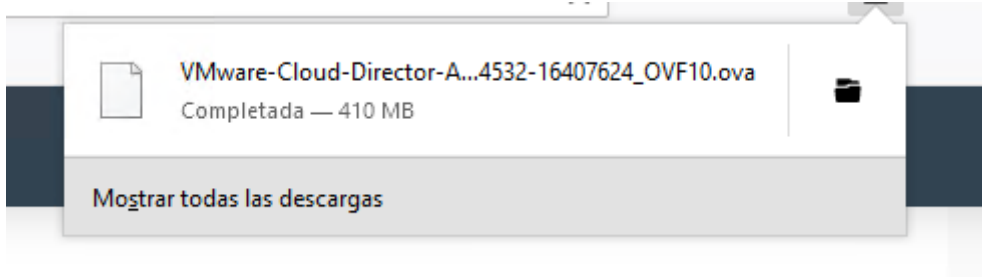
Versiones antiguas del appliance no funcionan correctamente con el producto con todas las funcionalidades.

Para versiones superiores a ESXi y vCenter 6.5U3 instale el appliance ONPREMISE 4.x, para versiones inferiores de ESXi y vCenter inferiores a 6.5U3 instale la versión del appliance cliente ONPREMISE 3.5.2

Imagen de la descarga:



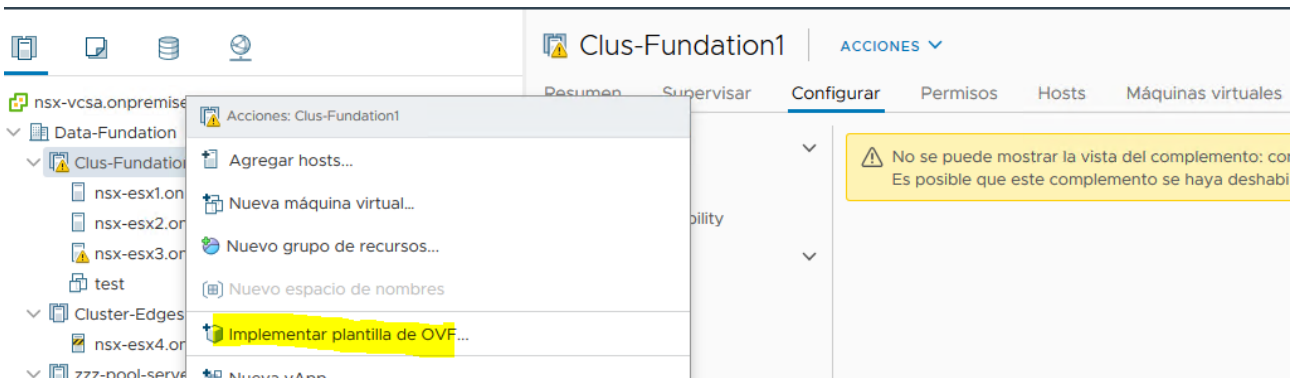
Actualmente está descargable la versión 4.0.2, efectúa la instalación con este appliance.



Configure un registro DNS para su appliance en su infraestructura, este será utilizado para configurar el hostname cuando arranque el dispositivo virtual:

vcda-onpremise	Host (A)	10.8.23.240
_msdcs		
_sites		

Suba la plantilla a su. Puede utilizar también herramientas como ovftools o el portal HTML5 si está usando vCenter 7 o posterior:



Implementar plantilla de OVF

1 Seleccione una plantilla d... Seleccione una plantilla de archivo OVF
 Seleccione una plantilla de archivo OVF en una URL remota o un sistema de archivos local

2 Seleccione un nombre y ...
 Seleccione un nombre y una ubicación de destino.

3 Seleccione un recurso in...
 Introduzca una URL para descargar e instalar el paquete de OVF desde Internet o desplácese hasta una ubicación accesible desde el equipo, como un disco duro local, un recurso de red compartido o una unidad de CD/DVD.

4 Revisar detalles

5 Seleccione almacenamie...
 URL
 Archivo local

6 Listo para completar

VMware-Cloud-Director-Availability-On-Premises-4.0.0.4532-16407624_OVF10.ova

Implementar plantilla de OVF

✓ **1 Seleccione una plantilla d...** Seleccione un nombre y una carpeta
 Seleccione un nombre y una ubicación de destino.

2 Seleccione un nombre y ...
 Seleccione un nombre y una ubicación de destino.

3 Seleccione un recurso in...
 Nombre de máquina virtual:

4 Revisar detalles

5 Seleccione almacenamie...
 Seleccione una ubicación para la máquina virtual.

6 Listo para completar

nsx-vcsa.onpremise.local
 Data-Fundation

Implementar plantilla de OVF

- ✓ 1 Seleccione una plantilla d...
- ✓ 2 Seleccionar un nombre y ...
- 3 Seleccionar un recurso in...**
- 4 Revisar detalles
- 5 Seleccionar almacenamie...
- 6 Listo para completar

Seleccionar un recurso informático

Seleccione el recurso informático de destino para esta operación.

- ▼ Data-Fundation
 - ▼ Clus-Fundation1
 - nsx-esx1.onpremise.local
 - nsx-esx2.onpremise.local
 - nsx-esx3.onpremise.local

Implementar plantilla de OVF

- ✓ 1 Seleccione una plantilla d...
- ✓ 2 Seleccionar un nombre y ...
- ✓ 3 Seleccionar un recurso in...
- ✓ 4 Revisar detalles
- ✓ 5 Contratos de licencia
- 6 Seleccionar almacenamie...**
- 7 Seleccionar redes
- 8 Personalizar plantilla
- 9 Listo para completar

Seleccionar almacenamiento

Seleccione el almacenamiento para los archivos de configuración y de disco

Cifrar esta máquina virtual (Requiere un servidor de administración de claves)

Seleccione el formato de disco virtual:

Aprovisionamiento fino ▾

Directiva de almacenamiento de máquina virtual:

Valor predeterminado de almacén de datos ▾

Nombre	Capacidad	Aprovisionado	Libre	Tipo	Clúster
Datastore1	196,16 GB	44,27 GB	196,1 GB	NFS v3	
Local-Disk-esx1	99,75 GB	1,41 GB	98,34 GB	VMFS 6	

Implementar plantilla de OVF

- ✓ 1 Seleccione una plantilla d...
- ✓ 2 Seleccionar un nombre y ...
- ✓ 3 Seleccionar un recurso in...
- ✓ 4 Revisar detalles
- ✓ 5 Contratos de licencia
- ✓ 6 Seleccionar almacenamie...
- 7 Seleccionar redes**
- 8 Personalizar plantilla
- 9 Listo para completar

Seleccionar redes

Seleccione una red de destino para cada red de origen.

Red de origen	Red de destino
VM Network	VM Network

1 items

Configuración de asignación de IP

Asignación de IP:

Estática - Manual

Protocolo IP:

IPv4

Implementar plantilla de OVF

- ✓ 1 Seleccione una plantilla d...
- ✓ 2 Seleccionar un nombre y ...
- ✓ 3 Seleccionar un recurso in...
- ✓ 4 Revisar detalles
- ✓ 5 Contratos de licencia
- ✓ 6 Seleccionar almacenamie...
- ✓ 7 Seleccionar redes
- 8 Personalizar plantilla
- 9 Listo para completar

Personalizar plantilla

Personalice las propiedades de implementación de esta solución de software.

✓ Todas las propiedades tienen valores válidos

Application	3 configuración
Root password	Password for root. Single and double quotes are not allowed. Contraseña <input type="password" value="....."/> Confirmar contraseña <input type="password" value="....."/>
Enable SSH	Enable SSH <input checked="" type="checkbox"/>
NTP Server	NTP Servers to use (e.g 10.23.108.1,10.23.108.2). 10.8.23.1
Networking Properties	6 configuración
Hostname	The hostname of the VM. Leave blank if DHCP is desired. vcda-onpremise
Address	IP address in CIDR notation (e.g. 10.71.219.227/21). Leave blank if DHCP is desired. 10.8.23.240
Gateway	Gateway address (e.g. 10.71.223.253). This field is ignored if the address is

CANCEL

- nsx-vcsa.onpremise.local
- Data-Foundation
 - Clus-Foundation
 - nsx-esx1.onpremise.local
 - nsx-esx2.onpremise.local
 - nsx-esx3.onpremise.local
 - test
 - vcda-OnPremise

nsx-esx1.onpremise.local ACCIONES

Resumen **Supervisar** Configurar Permisos Máquinas virtuales Almacenes de datos Redes Actualizaciones

Tareas

Nombre de T...	Destino	Condición	Detalles	Iniciador	En cola por	Hora de inici...	Hora de final...	Tiempo de ej...	Servidor
Implementar pl...	vcda-OnP...	55%		VSPHERE LOC...	2 ms	07/07/2020 12...			nsx-vcsa.onpre...
Import OVF pe...	nsx-esx1.o...	42%		vsphere.local...	45 ms	07/07/2020 12...			nsx-vcsa.onpre...
Desconectar m...	test	✓ Completado		VSPHERE LOC...	4 ms	07/07/2020 12...	07/07/2020 12...	125 ms	nsx-vcsa.onpre...

15

Actualización del appliance On-Premise a 4.0.2

Es posible que necesite hacer una actualización del appliance OnPremise si la versión en Acens actualiza la parte de proveedor. No es necesario que instale el appliance nuevamente, puede hacer una actualización y sus réplicas seguirán funcionando, para ello descargue la versión del producto que corresponda, siempre revisando la documentación para verificar que el path de actualización es posible. En este caso, vamos a actualizar de la versión 3.5.1 a la versión 4.0.2. En este caso el producto cambia de nombre y en lugar de recibir el nombre de vCloud Availability pasa a llamarse VMware Cloud Director Availability.

Puedes descargar aquí la ISO de actualización:

<https://my.vmware.com/group/vmware/downloads/details?downloadGroup=VCDAT4&productId=1003>

Home / VMware Cloud Director Availability 4.0 On-premises Appliance

Download Product

Version	4.0.0.2
Release Date	2020-06-23
Type	Drivers & Tools

Product Downloads

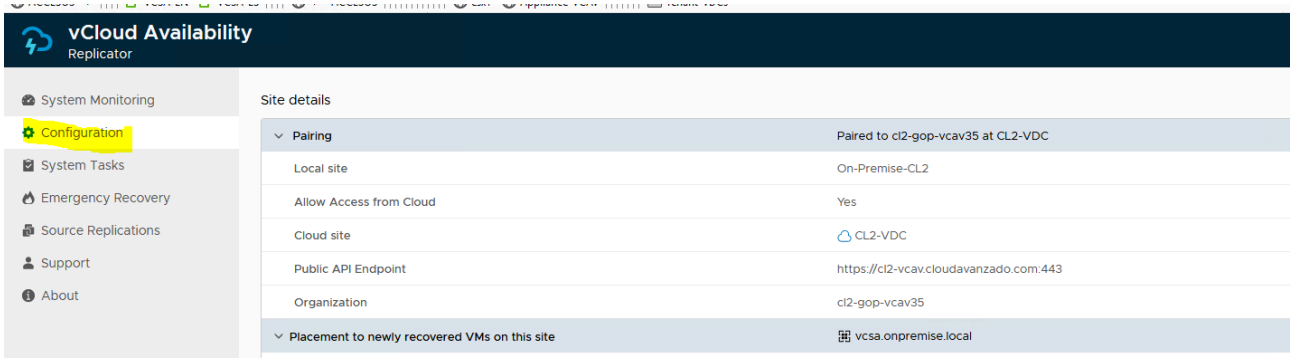
File	Information
VMware Cloud Availability 4.0.0.2 On-Premises Appliance	File size: 409.57 MB File type: ova Read More
VMware Cloud Director Availability 4.0.0.2 Upgrade Disk Image	File size: 699.06 MB File type: iso Read More

[MD5 checksums](#), [SHA1 checksums](#) and [SHA256 checksums](#).

Para hacer una instalación del appliance descarga la primera ISO y **para actualizar** con CD la segunda. Recuerda que nosotros vamos a hacer la actualización directamente in-place a través de Internet, no vamos a utilizar el CD. Para hacer la actualización con la ISO, monte el CD en el appliance y a la hora de actualizar diga que vaya a buscar el CD.

Proceso de actualización directamente desde el appliance y a través de Internet

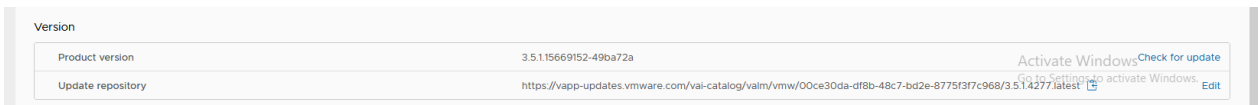
Entra en el appliance con el usuario root:



The screenshot shows the 'vCloud Availability Replicator' interface. On the left is a navigation menu with 'Configuration' highlighted. The main area displays 'Site details' for a site named 'CL2-VDC'. The details include:

- Paired to: cl2-gop-vcav35 at CL2-VDC
- Local site: On-Premise-CL2
- Allow Access from Cloud: Yes
- Cloud site: CL2-VDC
- Public API Endpoint: https://cl2-vcav.cloudavanzado.com:443
- Organization: cl2-gop-vcav35
- Placement to newly recovered VMs on this site: vcasa.onpremise.local

Ve a la parte de versión:

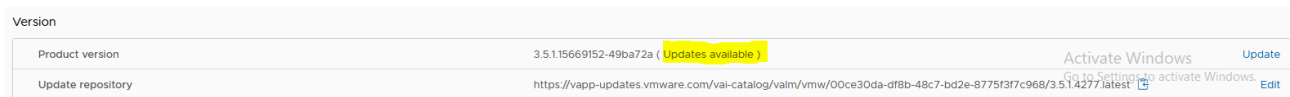


The screenshot shows the 'Version' section of the interface. It contains the following information:

Product version	3.5.1.15669152-49ba72a	Activate Windows Check for update
Update repository	https://vapp-updates.vmware.com/vai-catalog/vaim/vmw/00ce30da-df8b-48c7-bd2e-8775f37c968/3.5.1.4277/latest	Go to Settings to activate Windows. Edit

Pulsa en “check for updates”

Ves como el appliance comprueba que hay una versión:



The screenshot shows the 'Version' section after an update check. The 'Product version' is now 3.5.1.15669152-49ba72a, and a yellow highlight indicates '(Updates available)'. The 'Update' button is now visible.

Product version	3.5.1.15669152-49ba72a (Updates available)	Activate Windows Update
Update repository	https://vapp-updates.vmware.com/vai-catalog/vaim/vmw/00ce30da-df8b-48c7-bd2e-8775f37c968/3.5.1.4277/latest	Go to Settings to activate Windows. Edit

Pulsa sobre “Update” y sigue las instrucciones. Tendrás que aceptar la licencia y aplicar la actualización, espera que se reinicie el appliance. Ahora vuelve a entrar y reconecta tu site a la organización de CDC y el registro de lookservice .

Revisa la configuración IP. Si es necesario tendrás que volver a rellenarla.

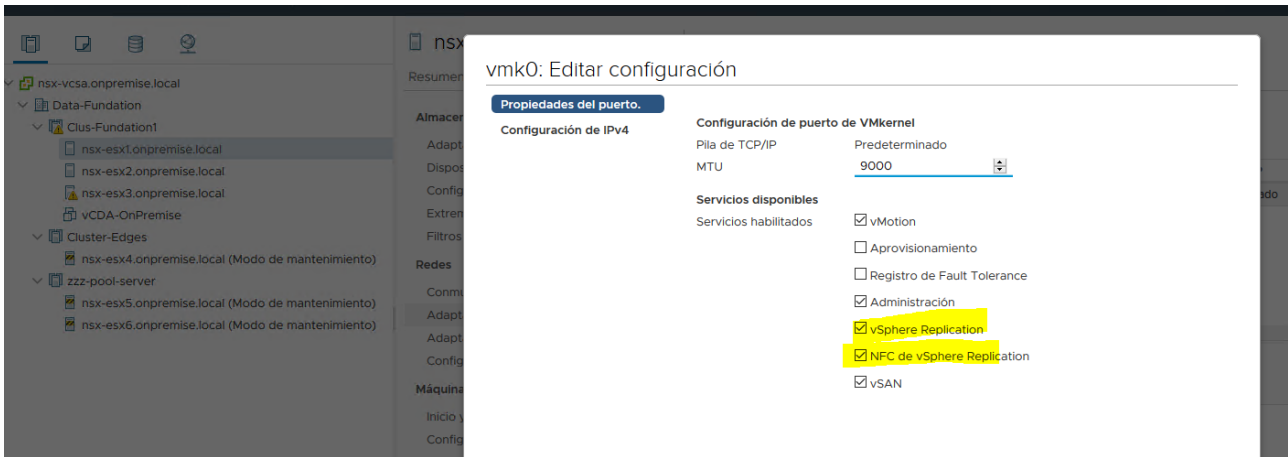
Configuración de appliance

Una vez ha sido instalado el appliance, podemos comenzar a configurarlo.

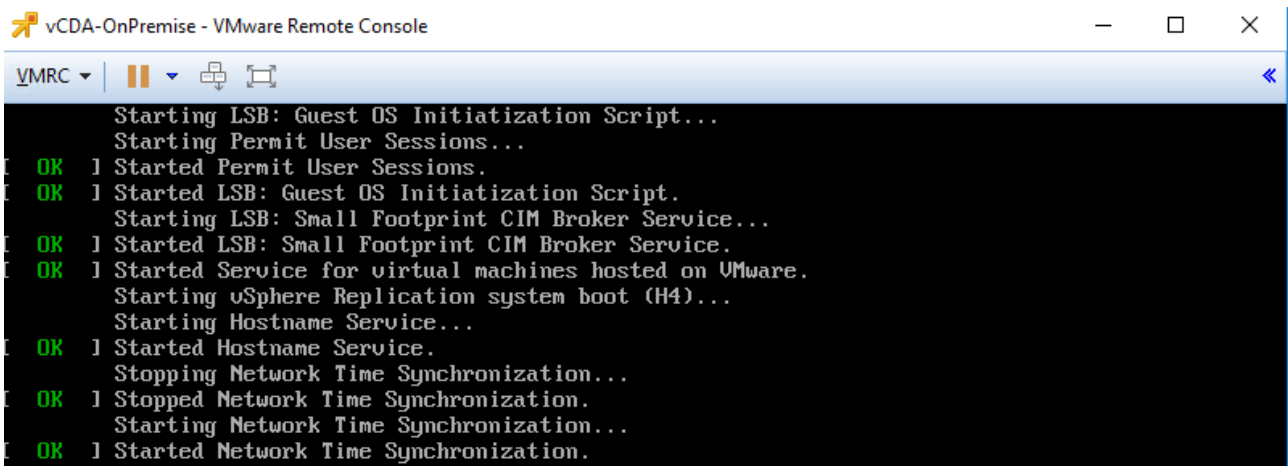
Asegúrate que todos nuestros ESXi tienen configurada la siguiente opción en VMKernel de administración:

- vSphere Replication
- vSphere Replication NFS

Estas opciones marcan el VMKernel por el que se mueve el tráfico de replicación. Si no lo tiene configurado le fallará la réplica de datos entre el appliance On-Premise y el túnel de su nube.



Ahora enciende el appliance cliente On-Premise de DRaaS (VCDA):

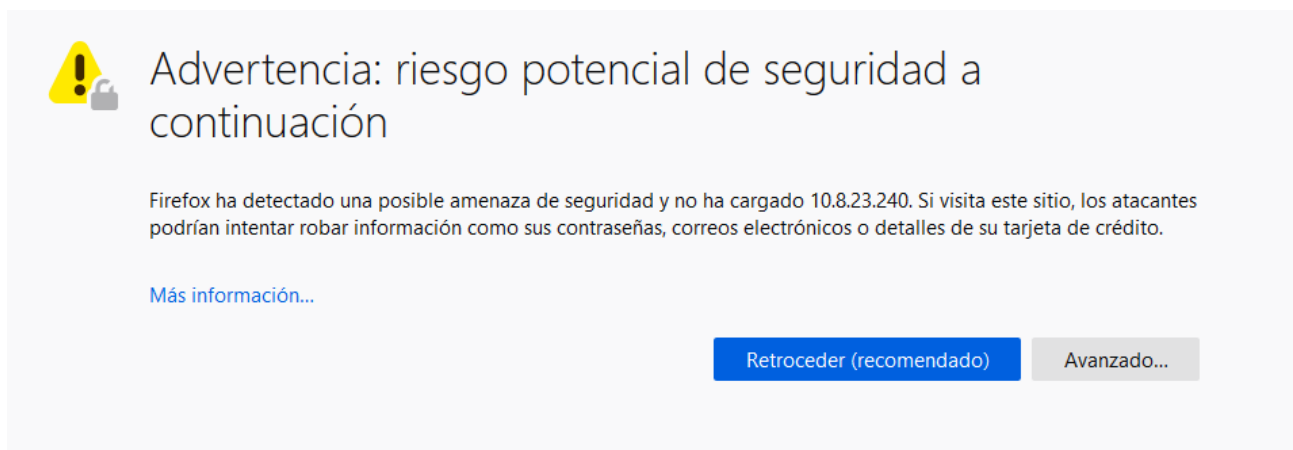


Es importante tener el DNS bien configurado ya que la VM se autoconfigurará en base a ello. La primera vez que entres a la VM te pedirá el cambio de contraseña, así que es una buena práctica poner en la instalación una contraseña temporal y en el primer inicio de sesión poner la contraseña definitiva:

```
Appliance-OnPremise-VCAV x
vreplicator5.vcloud.lab login: root
Password:
You are required to change your password immediately (administrator enforced)
Changing password for root.
Current password:
New password:
Retype new password:
root@vreplicator5 [ ~ ]# _
```

Una vez has configurado la nueva contraseña, podremos entrar en el appliance vía web a través de la siguiente URL (Si el appliance no te asigna la IP, revisa que la IP la hayas puesto en formato CIRD (x.x.x.x/x))

<https://IPAppliance/ui/admin>

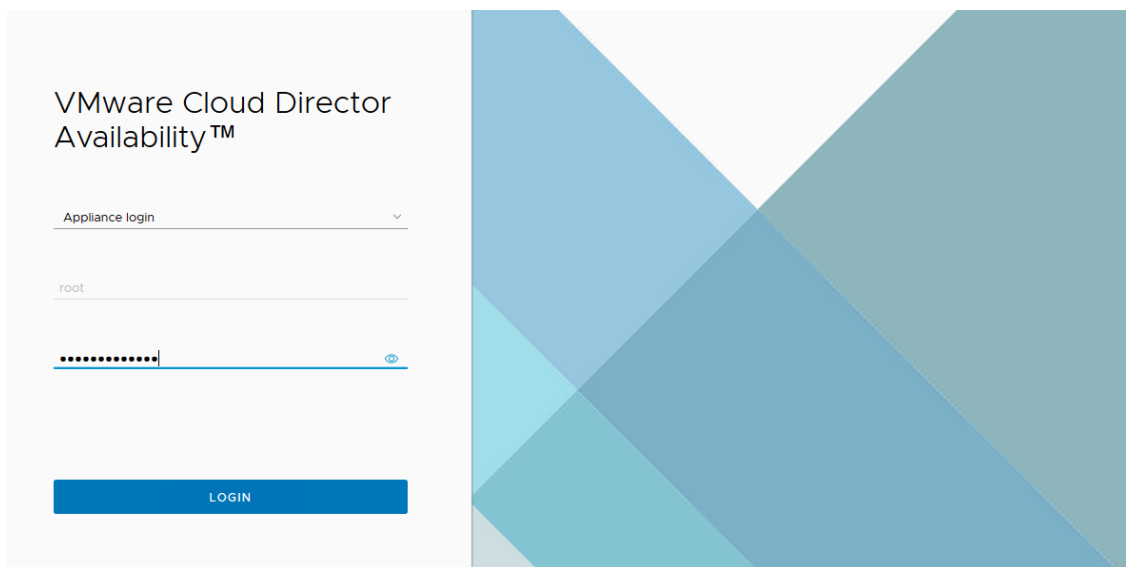


Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado 10.8.23.240. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

[Más información...](#)

[Retroceder \(recomendado\)](#) [Avanzado...](#)



VMware Cloud Director Availability™

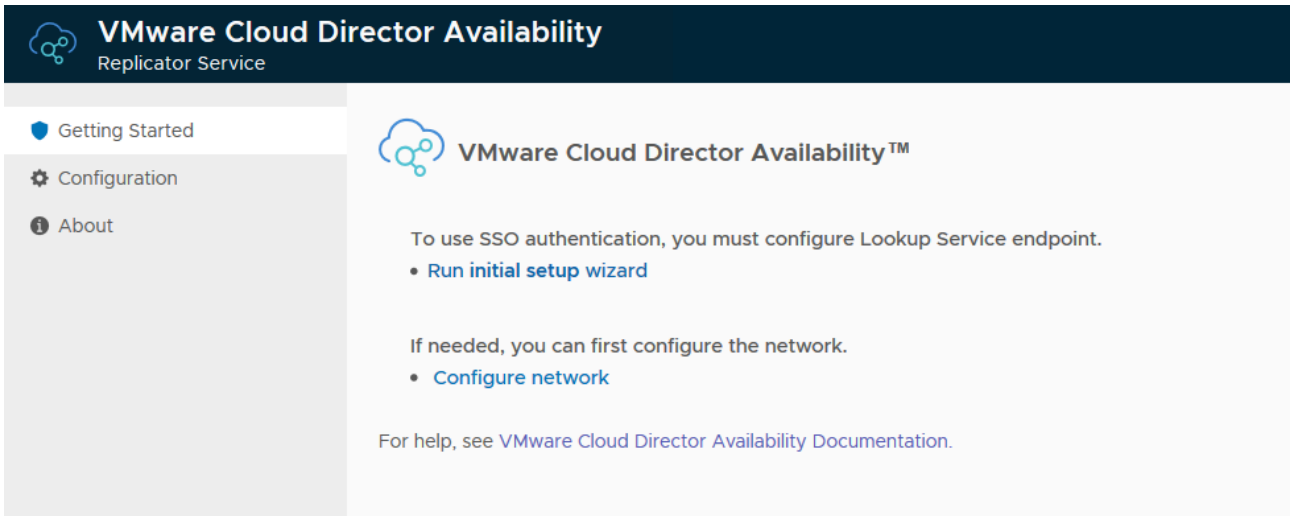
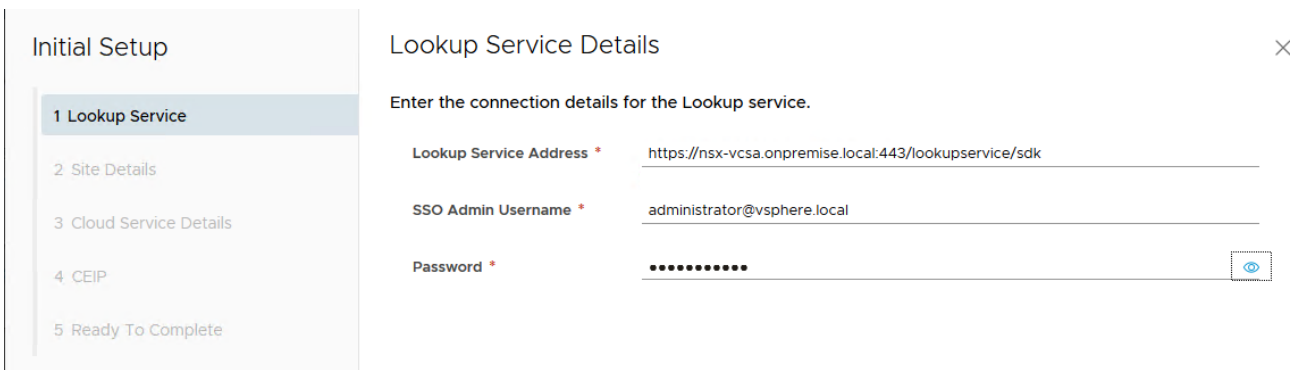
Appliance login

root

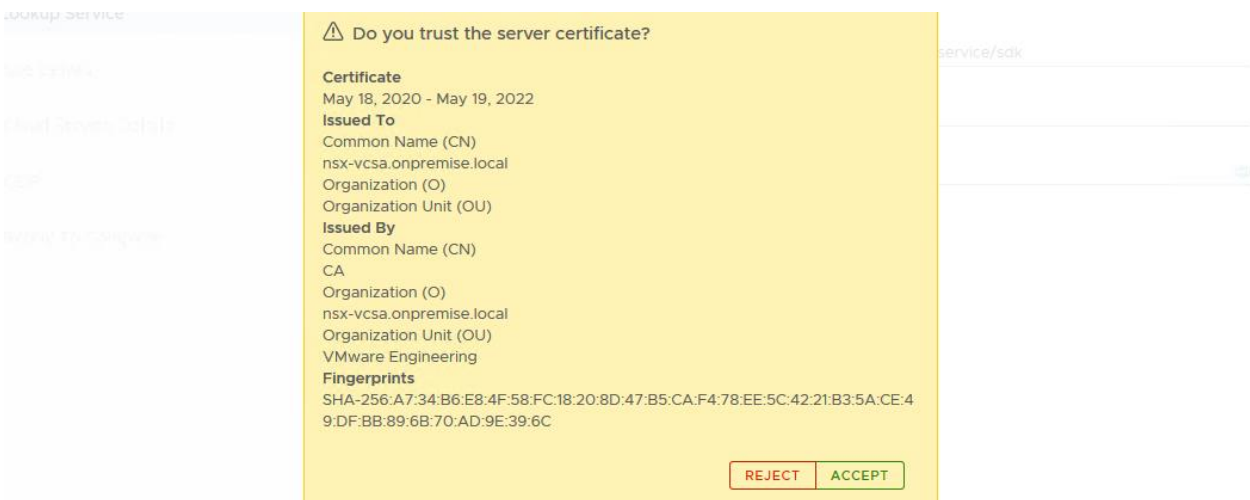
.....

LOGIN

Una vez entramos, el primer paso es configurar el SSO (normalmente en el propio vCenter)

Aceptamos el certificado:



Ahora procedemos a la configuración del appliance para que haga la conexión con el extremo del túnel de VCDA en nuestra nube. Para ello tendremos que elegir un nombre. Este será el que se mostrará dentro de nuestro portal de vCloud Director y hará referencia a nuestra infraestructura On-Premise. Pon un nombre descriptivo que te resulte sencillo a la hora de identificarlo.

Nombre del site On-Premise:

Initial Setup

- 1 Lookup Service
- 2 Site Details
- 3 Cloud Service Details
- 4 CEIP
- 5 Ready To Complete

Site Details ✕

Enter a name that will identify your vSphere site to the cloud provider.

Site name *

Description

Enter some meaningful information about the site.

Provide cloud pairing details later

Usuario y password de nuestro administrador de SSO de nuestro vCenter Server:

New Pairing

- 1 Site Details
- 2 Lookup Service
- 3 Cloud Details
- 4 Ready To Complete

Lookup Service Details ✕

Enter the connection details for the Lookup service.

Lookup Service Address *

SSO Admin Username *

Password *

En la siguiente pantalla tendrá Dirección URL del túnel remoto de su nube pública. Dependiendo del producto contratado podrá ser diferente, tenga presente la plataforma a la que se conecta, si tiene alguna duda consulte con el soporte técnico.

Las URLs de acceso podrán ser:

- <https://cl1-VCDA.cloudavanzado.com:443>
- <https://cl2-VCDA.cloudavanzado.com:443>
- <https://cl3-VCDA.vcloud-datacenter.org:443>

Tiene que introducir el usuario administrator y nombre de su organización separados por una “@”. Normalmente su usuario administrador será un número que corresponde con el nombre de su organización y, por lo tanto, será similar a la siguiente: **6321548@6321548**

New Pairing

- 1 Site Details
- 2 Lookup Service
- 3 Cloud Details
- 4 Ready To Complete

Cloud Details ✕

Enter vCloud Availability Cloud Site details.

Public API Endpoint *

Organization Admin *

Organization Password *

Allow Access from Cloud

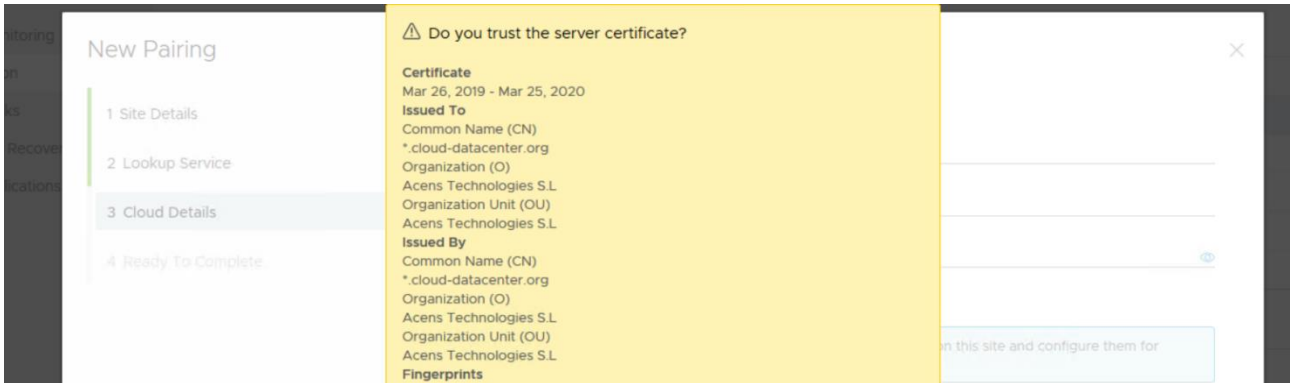
Privileged vCloud Director users are allowed to remotely browse the VMs on this site and configure them for replication.

Debe activarse la siguiente opción:

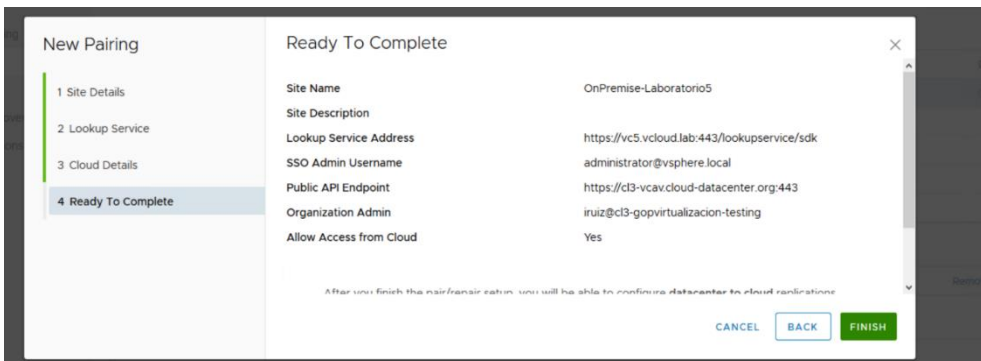
Allow Access from Cloud

i Privileged VMware Cloud Director users are allowed to remotely browse the VMs on this site and configure them for replication.

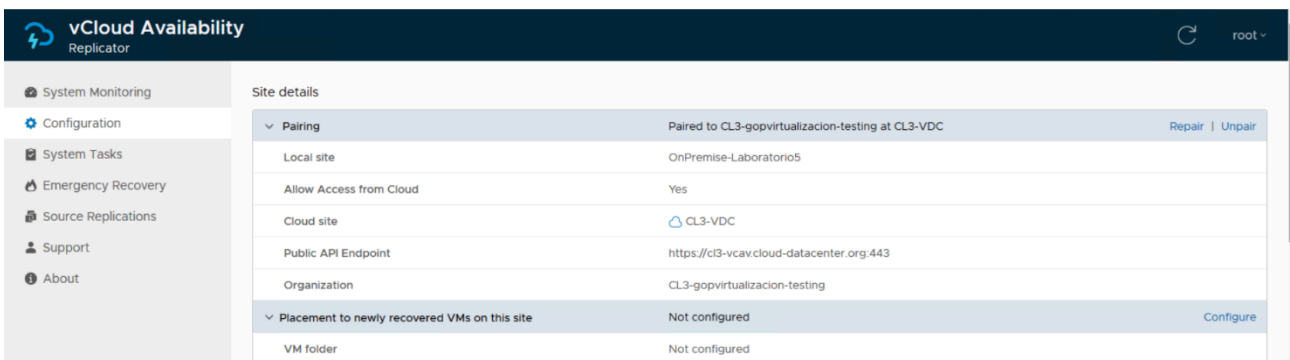
Acepta el certificado:



Revisa los datos y finaliza el asistente:



Revisión de los datos una vez el appliance ha sido configurado:



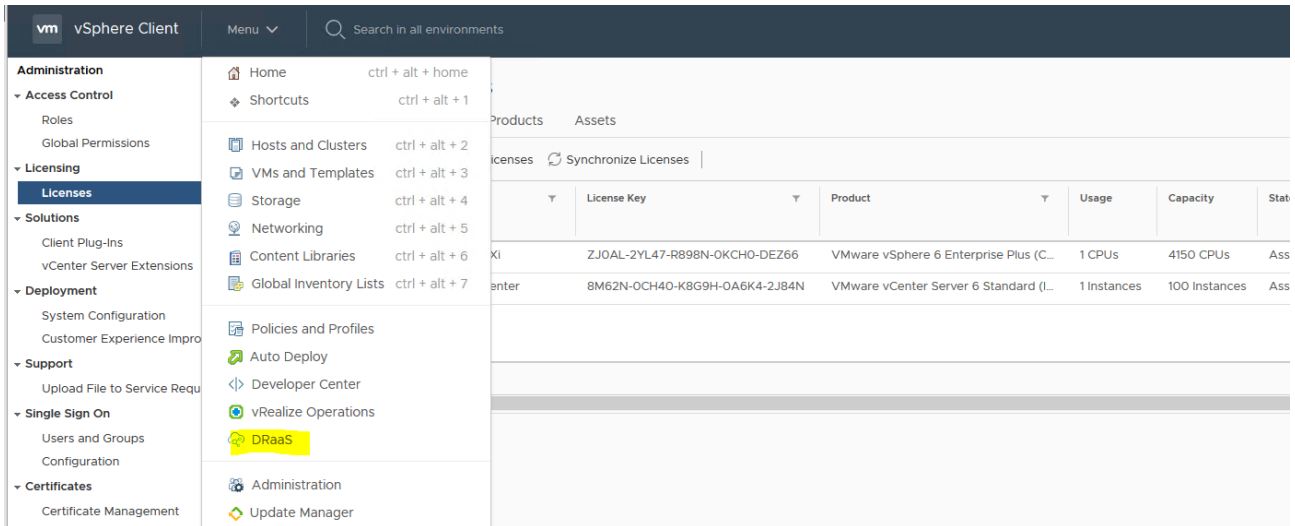
Se puede configurar la opción: "placement to newly recovered VMs on this site".

Esta opción servirá para indicar a la solución donde se recuperarán las VMs que vengan de su cloud si hace migraciones en sentido CDC → On-Premise

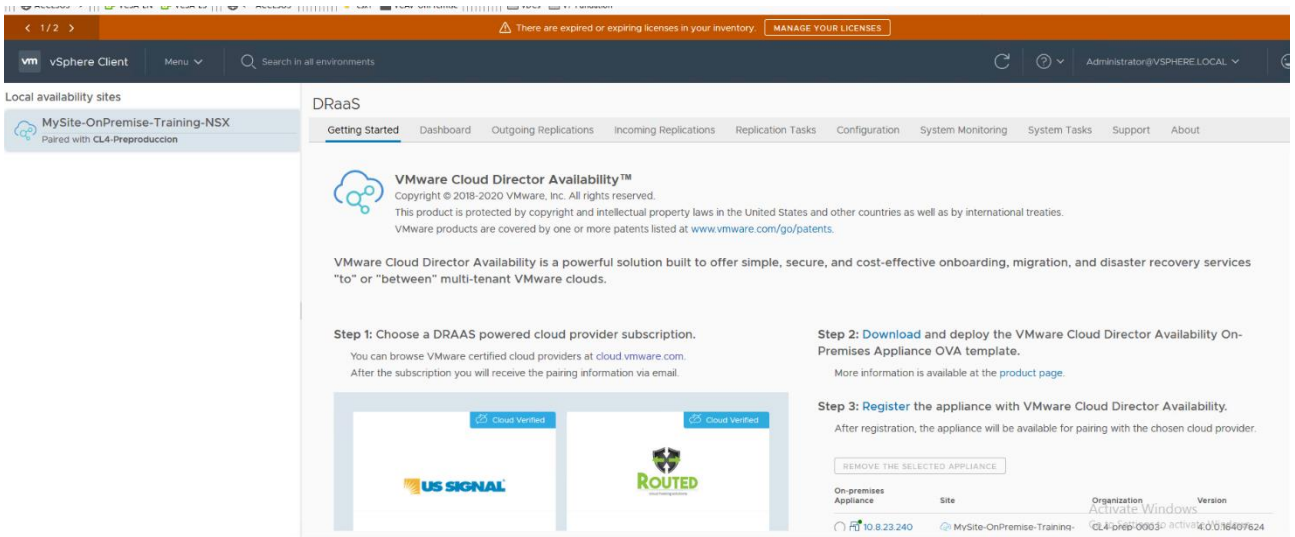
Tienes que seleccionar también la opción: Allow Access from Cloud y poner a “YES”

Ahora sal de la sesión de tu vCenter y vuelve a entrar podrás ver un plugin donde podrás interactuar con la solución desde la parte “On-Premise”.

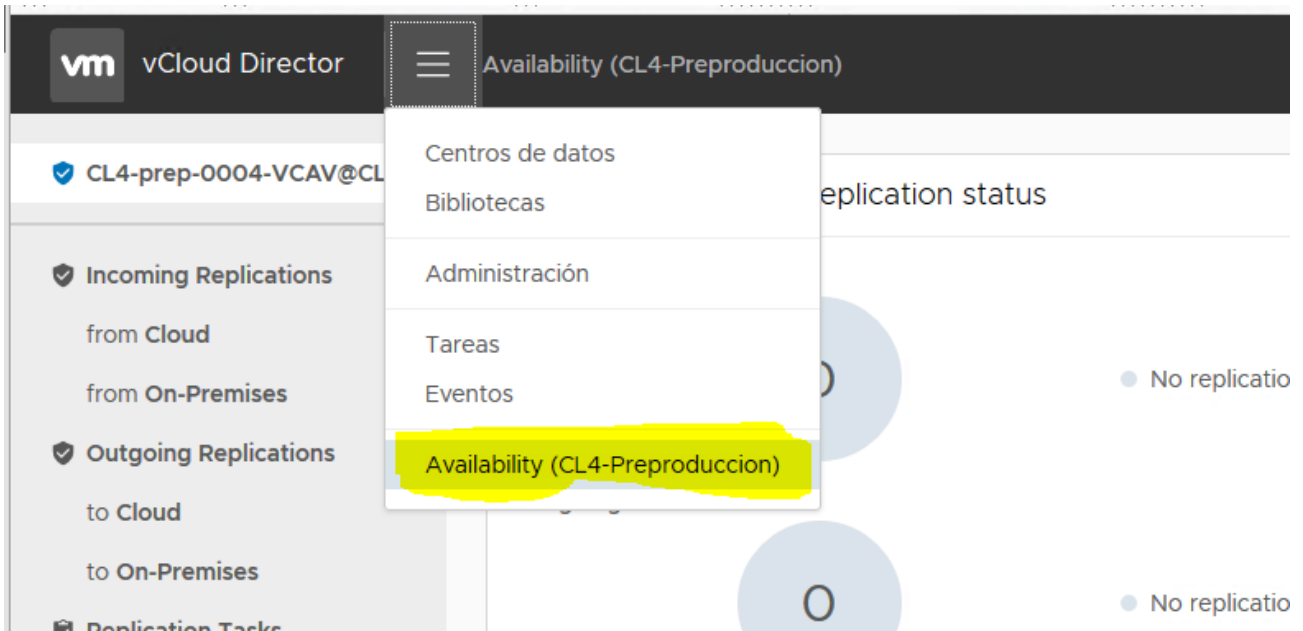
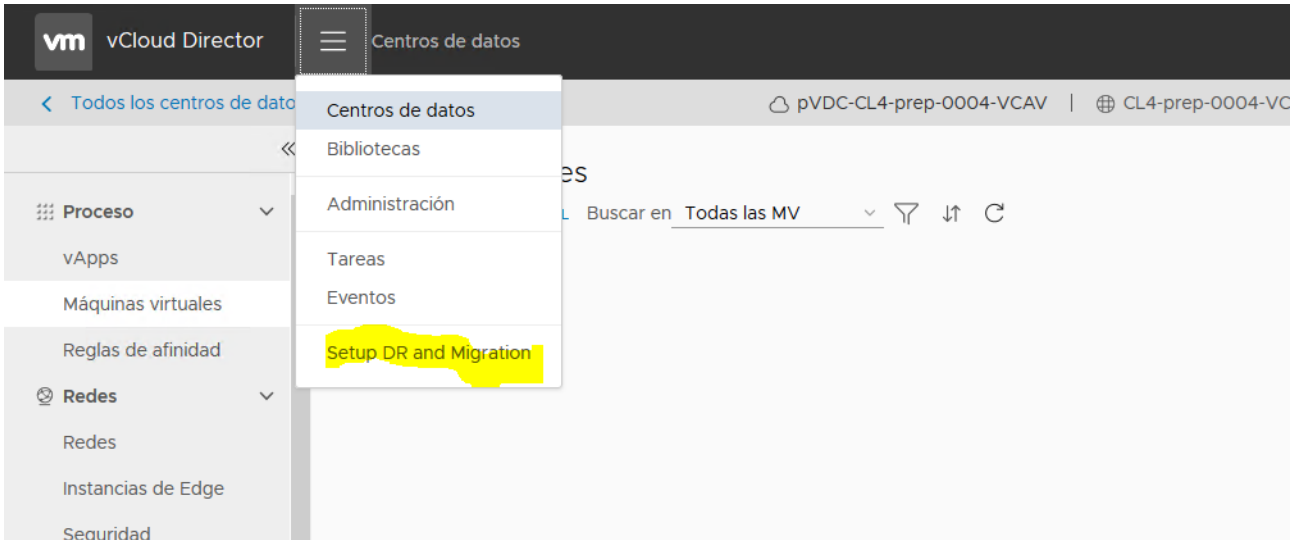
Podrás ver un nuevo icono:



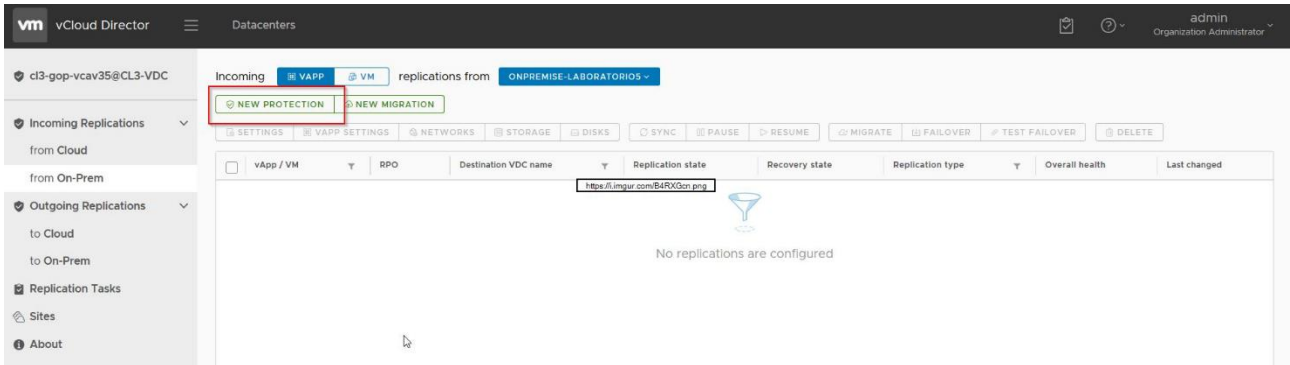
Pulsa sobre este icono y accede a la parte de VCDA desde On-Premise. Aquí también puedes trabajar en la solución. No es necesario hacerlo siempre desde el portal de vCloud Director.



Ahora si entras en tu portal de vCloud Director podrás ver que también puedes manejar tus réplicas:



Ejemplo de migración a CDC



Requisitos necesarios y consejos en On-Premise

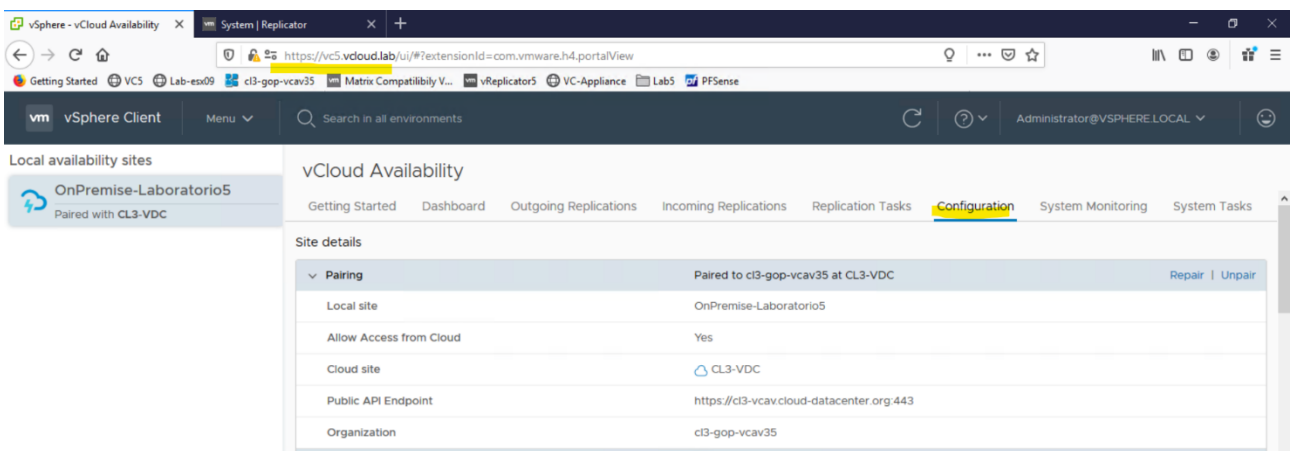
- En migraciones si hay en On-Premise servidores DNS dejar para el final mantener resolución DNS.
- Siempre será necesarios hacer pruebas de TEST por tipologías de VMs.
- En migraciones no tocar sistemas de comunicaciones hasta el final.
- Tener en cuenta si hay discos RAW solo compatible **Virtual Disk Raw** y copia bloque a bloque es muy lento.
- Los volúmenes de discos conectados por iSCSI o NFS no se migran.
- Tener en cuenta máquinas con muchos cambios, puesto que no podrán las RPO con ellas.
- Revisar cantidad de I/O de disco para determinar cambios y con ellos calcular tasa de transferencia / RPO.
- Revisar latencias de máquinas virtuales a migrar.
- Revisar conectividad con el túnel por medio del explorador o comandos como telnet, curl, wget.
- Comprobar la resolución DNS en Appliance On-Premise, vCenter y ESXi.
- Solo se migran las VMs que están encendidas, muy importante no apagarlas.
- Tener en cuenta que primero antes de migrar hay un Fullsync que hace una copia completa.
- Las VMs que no se puedan migrar por alguna razón y tengan que ser de forma manual, tardarán y deberán importarse desde acens Technologies, lo cual tendrá un coste adicional.
- Hacer primeramente unas pruebas con máquinas de TEST.
- Se recomienda manejar siempre la misma interface del UI para la migración On-Premise o bien desde CDC.
- OnPremise tiene que hacer una resolución de todas las URLs de vCloud implicadas en el proceso y tiene que poder conectarse a ellas por HTTPS a través del puerto 443. Tanto el servidor vCenter como el servidor vSphere Replication tiene que poder conectarse a todas las IPs y poder hacer la resolución tanto de los componentes internos (vCenter, ESXi, vShere Replication ... etc) como de los peer externos: <https://www.cloud-datacenter.org> y <https://cl3-VCDA.cloud-datacenter.org>
- La resolución DNS es primordial.
- Si utilizas el plugin del sitio On-Premise debes hacerlo desde la misma red. Esto es porque el plugin es el que hace las conexiones. Si lo estás haciendo desde tu explorador conectado al vCenter On-Premise, puedes tener problemas.
- Si una VM cae en error durante la réplica lo mejor es reconfigurar la réplica y no borrarla.
- Si las réplicas dejan de funcionar revisa los logs del appliance On-Premise.
- Cuando haces el plan de migración final, hay que tener muy presente quitar la personalización de las VMs, actualizar el HW virtual y configurar la tarjeta como DHCP para que no la personalice.
- En migraciones antes de hacer el arranque definitivo hacer un snapshot por seguridad de configuración.
- Revisa que las VMS tengan el "Guest Customization" deshabilitado.
- Siempre es preferible que los discos de las VMs sean VMFS
- Solo se puede hacer una migración entre un On-Premise y una organización de CDC no a varias.

Troubleshooting

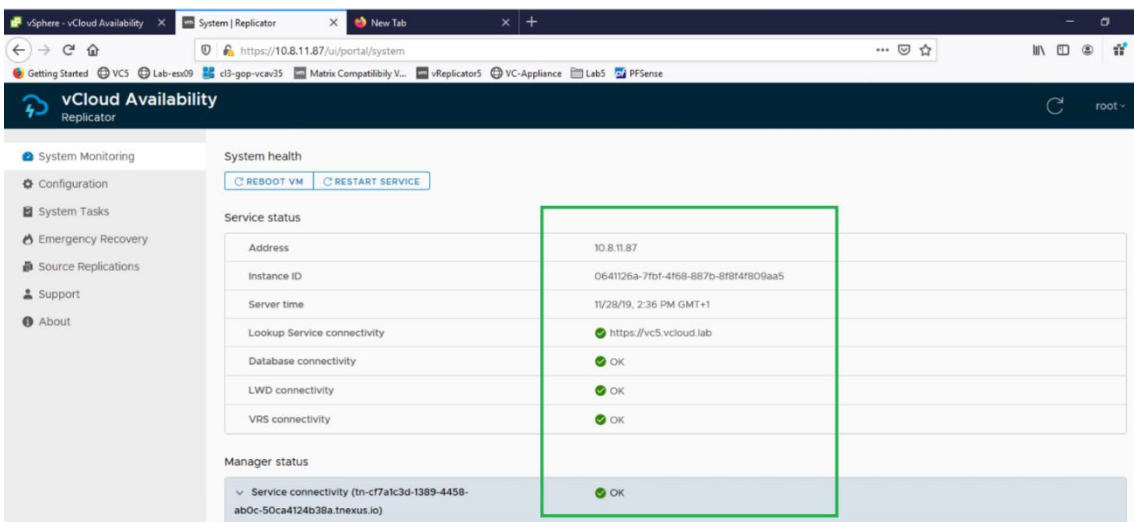
AUTENTICACIÓN DE SITIOS

Una de las cosas a tener en cuenta que podrían dar algún problema es el mantenimiento de la autenticación. Debes saber que el appliance On-Premise no solo tiene que estar autenticado con tu entorno CDC de tu nube pública sino que también tiene que estarlo con tu vCenter Server. Por lo tanto, si te ocurre algo que tenga que ver con la autenticación, vigila si existe algún problema de autenticación dentro de la URL de configuración del appliance como o bien en el plug-in que está dentro del vCenter y se conectar con tu nube pública haya autenticación.

Plug-In dentro de vCenter



URL de configuración del appliance:

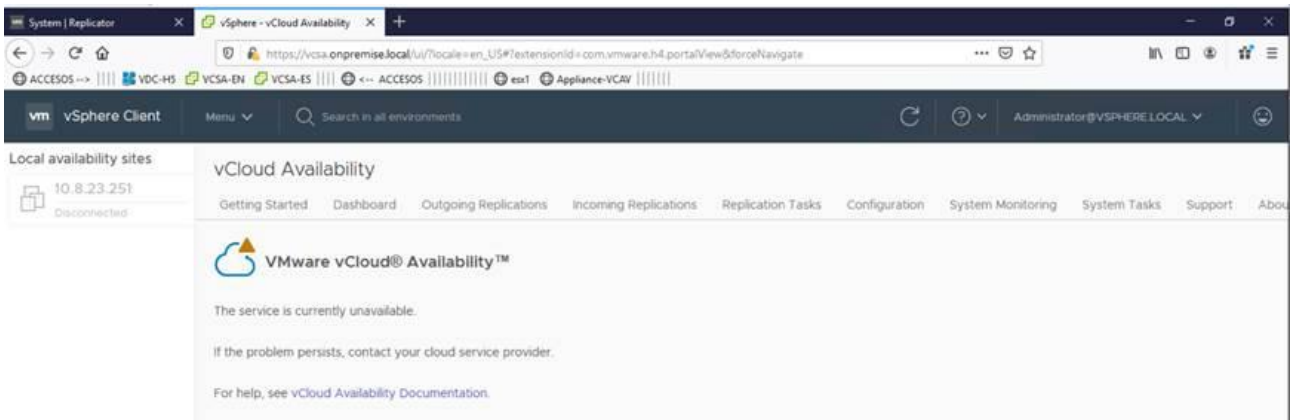
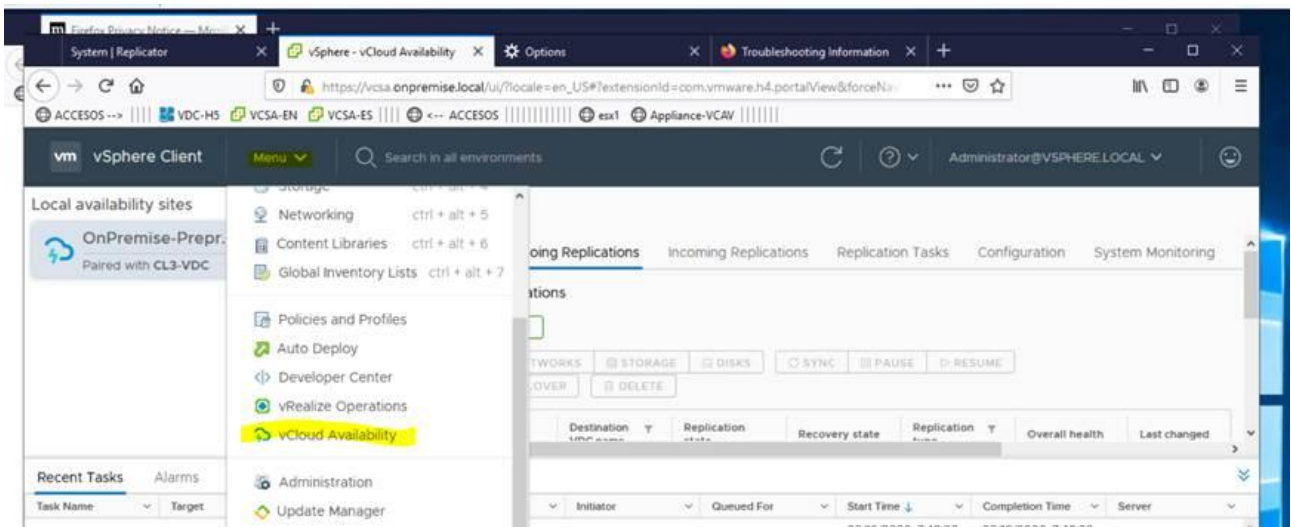


REPLICA QUE CAE EN ESTADO UNKNOW

Si una de las réplicas cae en fallo con estado desconocido, puedes reiniciar la VM en On-Premise. Esto provocará que el fallo sea reparado.

APPLIANCE DESHABILITADO DENTRO DE VCENTER

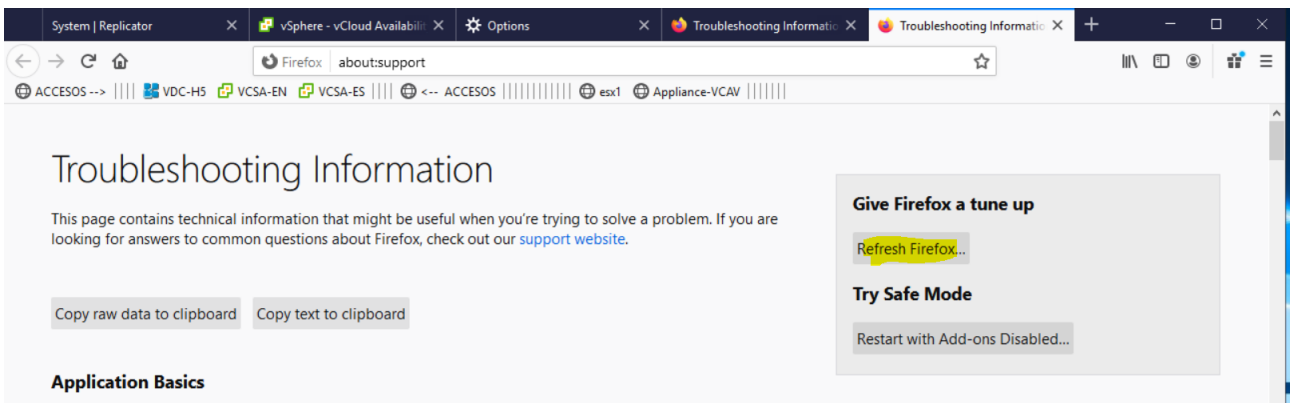
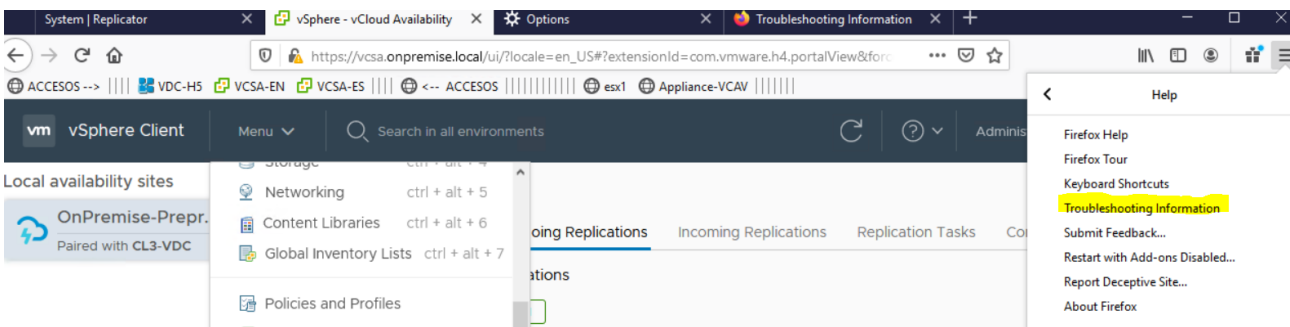
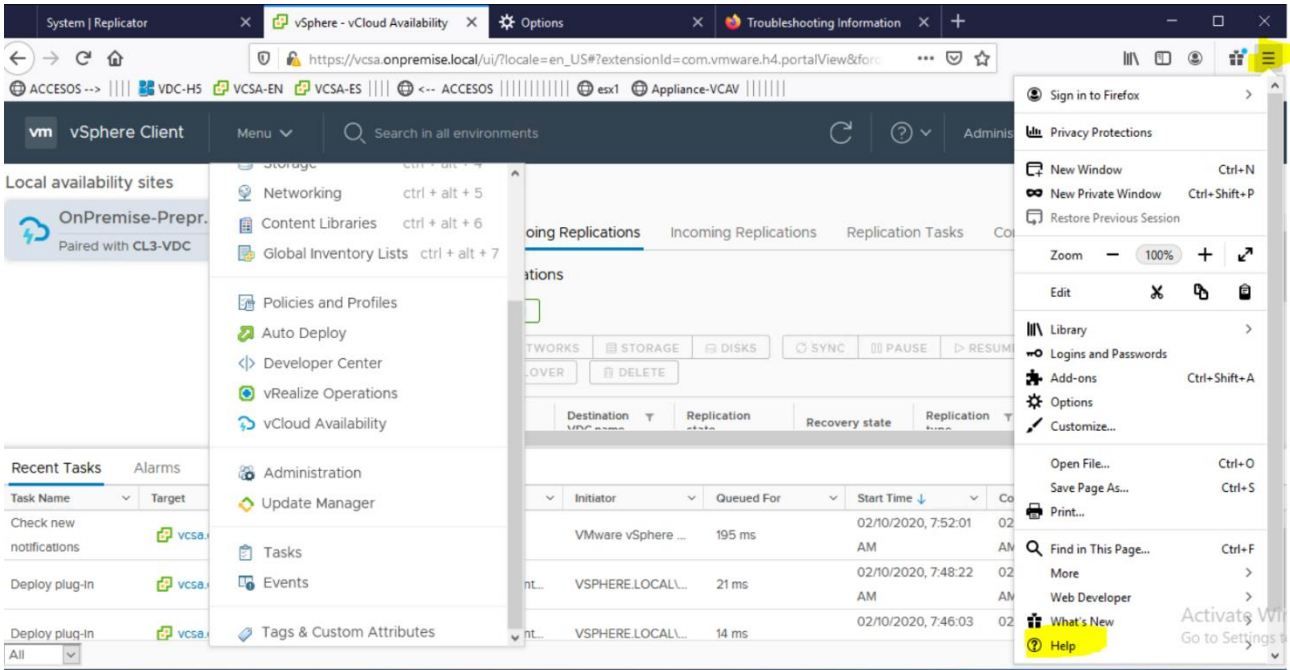
En algunas ocasiones al entrar en la parte de VCDA dentro del vCenter a través del menú, podemos ver como deshabilitado nuestro appliance:



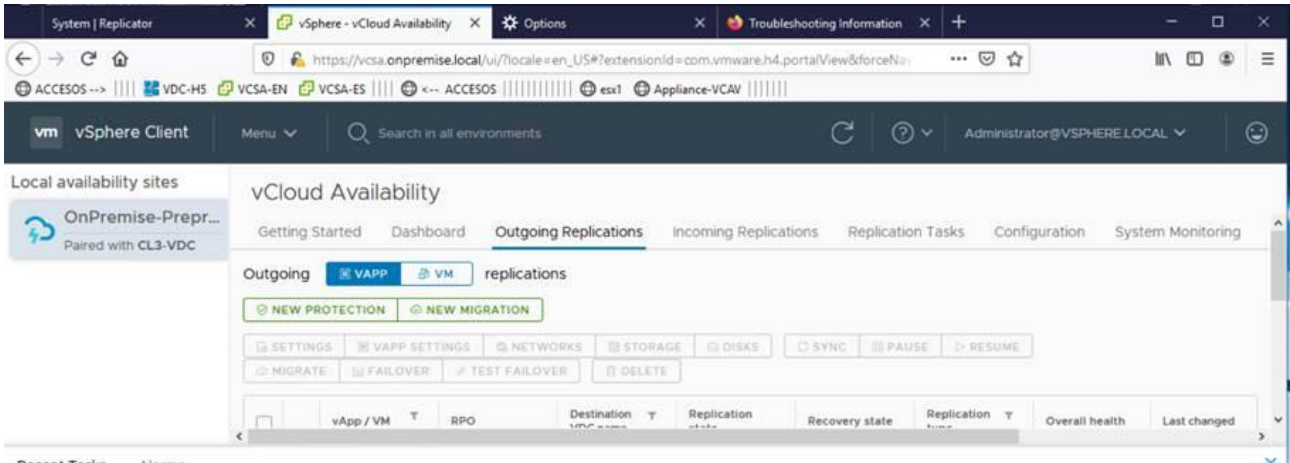
Esto es debido a la caché de nuestro explorador, en este caso Firefox. Para solucionarlo debes limpiar la caché. El procedimiento es el siguiente:

Menú  Help  Troubleshooting information  Botón: "Refresh Firefox"

Procedimiento a seguir:

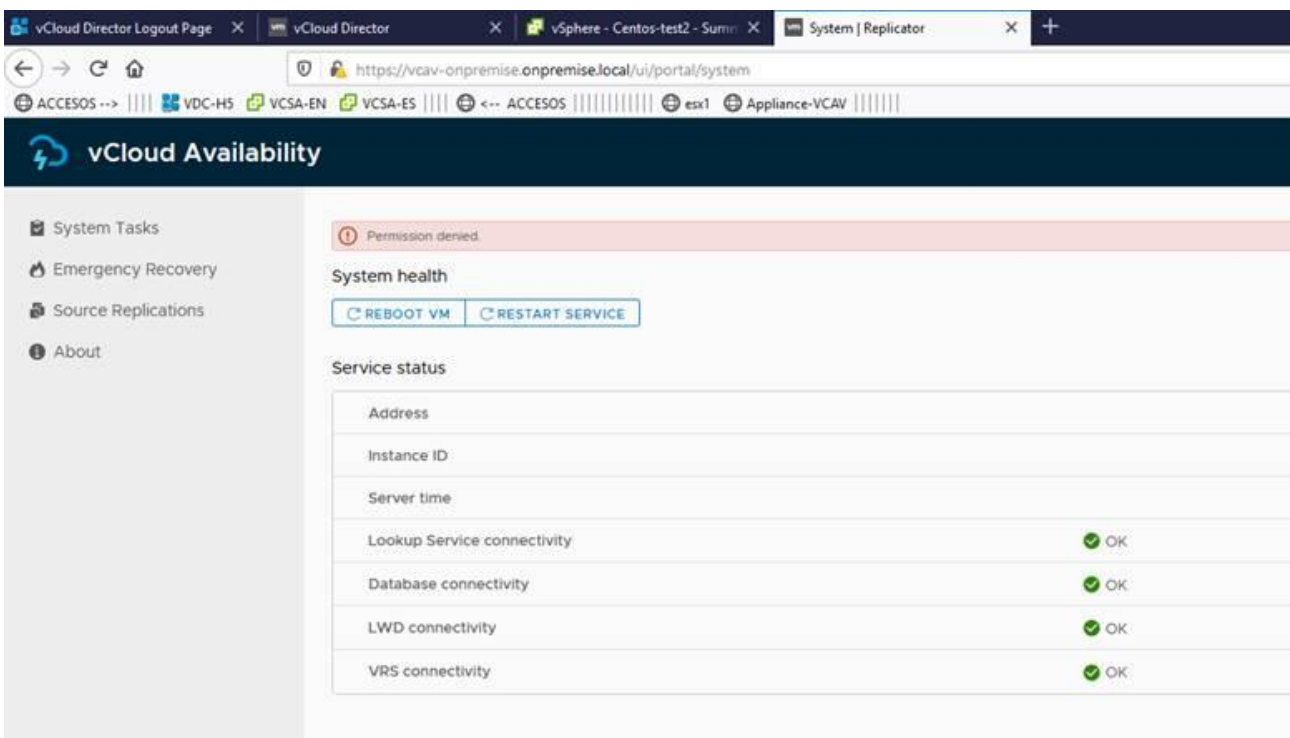


Una vez realizado el navegador se reiniciará y podrás restaurar las pestañas que estaba utilizando. Vuelve a entrar en la sección de VCDA y verás disponible el appliance:



MENSAJE DE “PERMISOS DENEGADO” EN LA CONFIGURACIÓN DEL APPLIANCE

Es posible que una vez entres en la IP del appliance de On-Premise, tengas un mensaje de permiso denegado:



Para resolver el problema, debes limpiar la caché con el método de la sección: [“APPLIANCE DESHABILITADO DENTRO DE VCENTER”](#)

CONTRASEÑA DEL APPLIANCE BLOQUEADA

Debes abrir una consola del appliance en vCenter y seguir el siguiente procedimiento:

1. Entrar en el gestor de arranque “GRUB”

2. Sigue el siguiente procedimiento: <https://kb.vmware.com/s/article/67961>
3. Si quieres aumentar el número de intentos o de tiempo de bloqueo del password, edita a tu antojo:
/etc/pam.d/system-aut
4. Reinicia el appliance “reboot -f”

HARDWARE VIRTUAL NO COMPATIBLE CON ONPREMISE; INVALID STATUS AL LEVANTAR VMS

Cuando hacemos una migración en sentido CDC a On-Premise, podemos encontrarnos que el HW virtual del sitio On-Premise no es compatible, esto ocurre porque la versión de HW de la máquina en CDC es superior al sitio On-Premise, suele ocurrir cuando los ESXi son antiguos.

El escenario que nos encontraremos será:

Las VMs se quedan en estado inválido y nos las podemos arrancar, el sistema de replicación VCDA tampoco ha podido arrancarlas.

Si las quitamos del inventario y desde el almacenamiento las registramos nos dice que el HW virtual es incompatible.

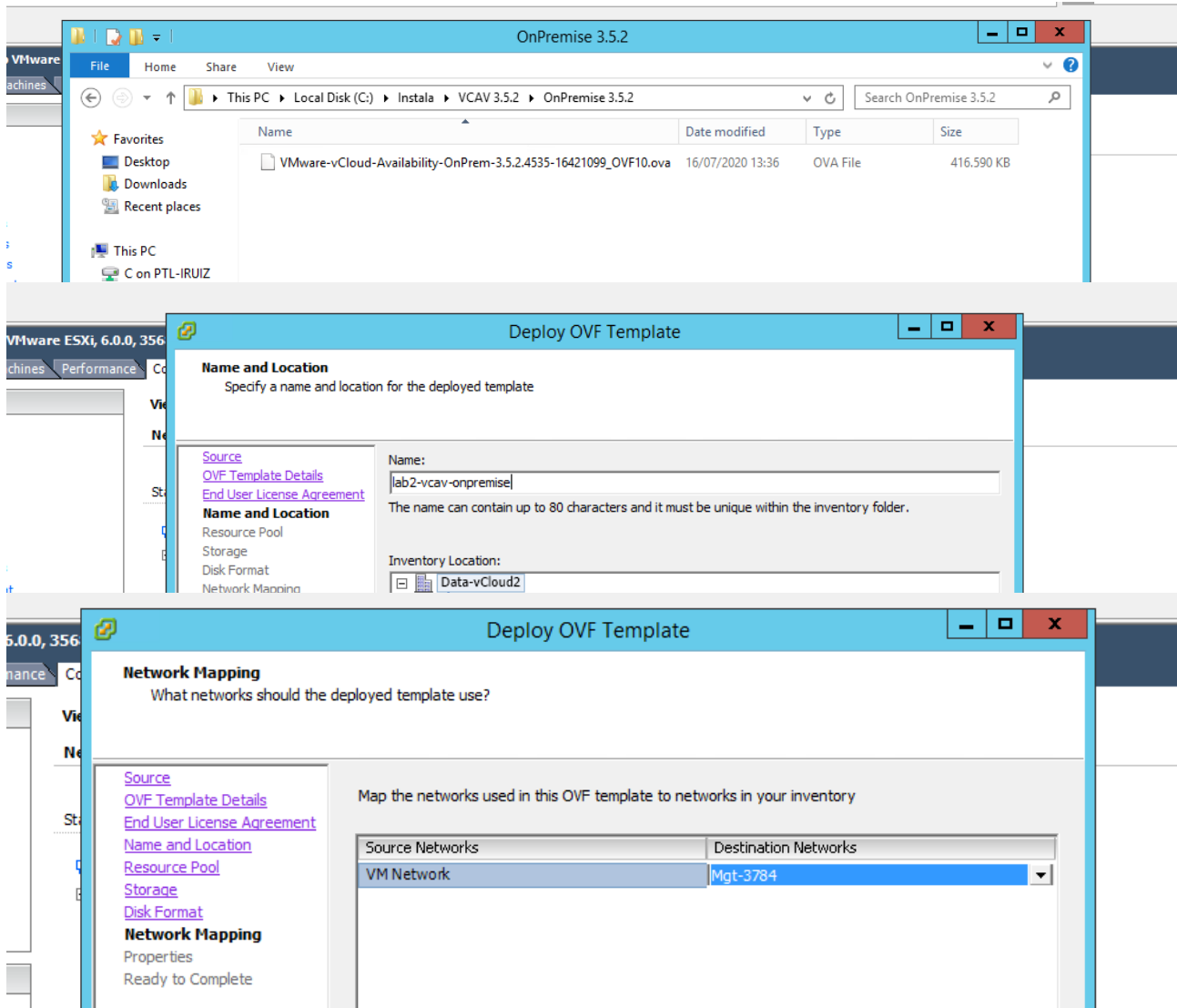
Para solucionar el problema debes abrir el archivo .vmx de configuración de la máquina y en la línea de Hardware Virtual y tienes que escribir la versión compatible con tu plataforma. Antes de arrancar la máquina deberás asignar el tipo de sistema operativo y la tarjeta de red, ahora arrancarla manualmente. Al ser incompatible le HW no se pudieron realizar estas acciones de forma automatizada.

RÉPLICAS BLOQUEADAS SI PONSIBILIDAD DE DETENERLAS

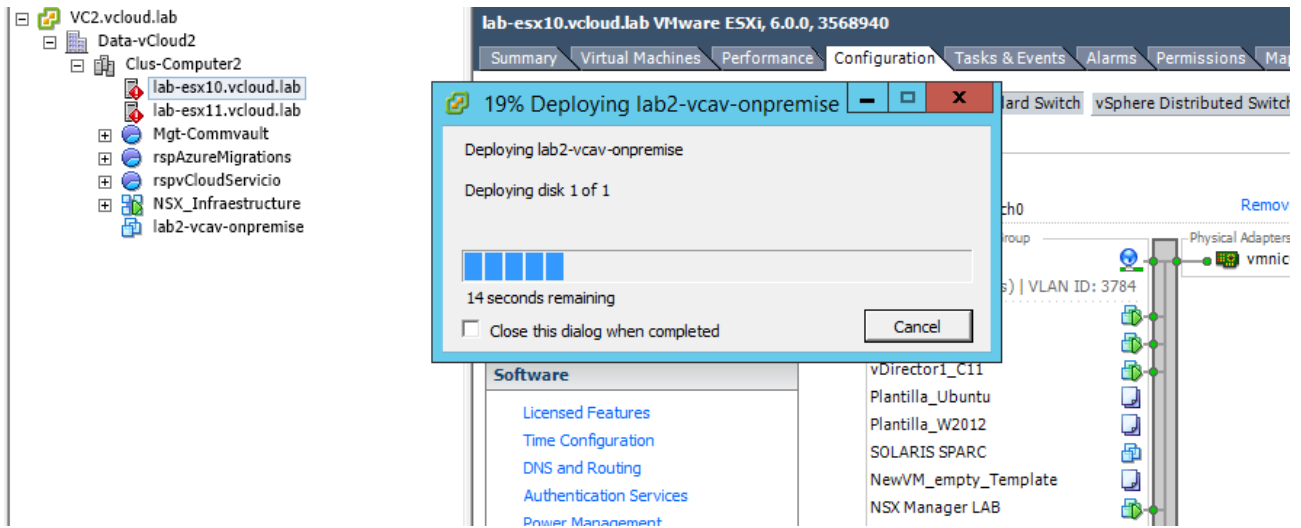
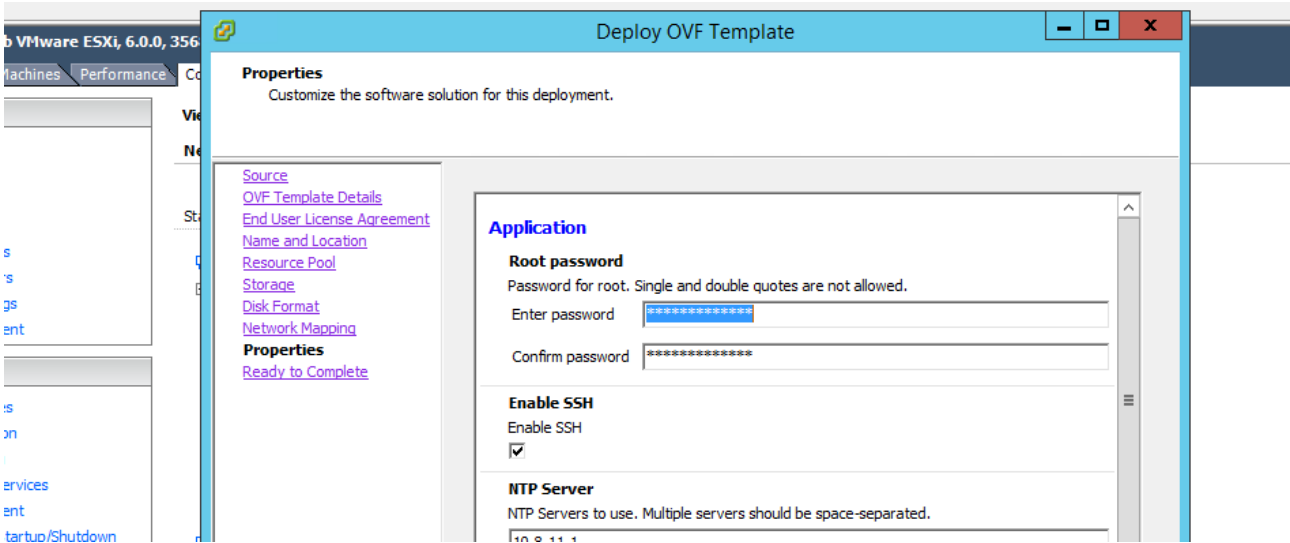
Conéctate al ESXi donde está la VM usando la consola de ESXi y deshabilita la réplica de la VM:

```
vim-cmd vmsvc/getallvms  
vim-cmd hbrsvc/vmreplica.disable 30
```

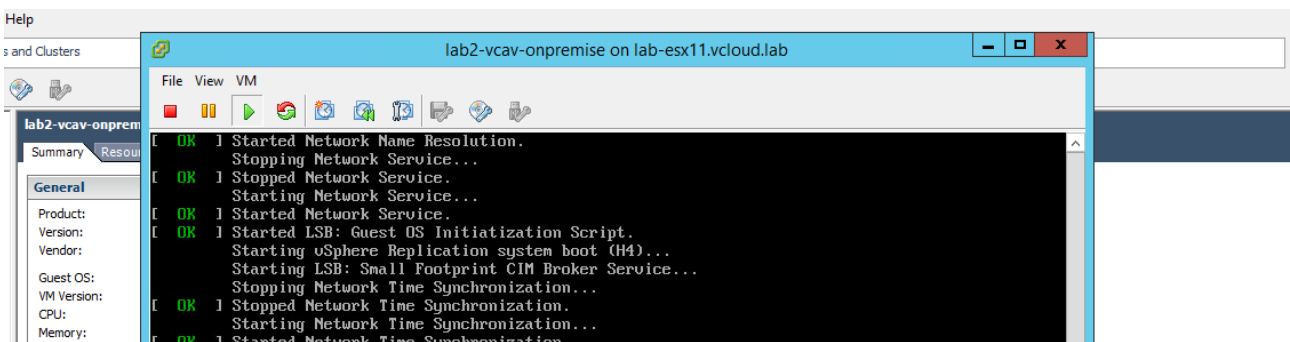
Instalación de appliance en legacy sites

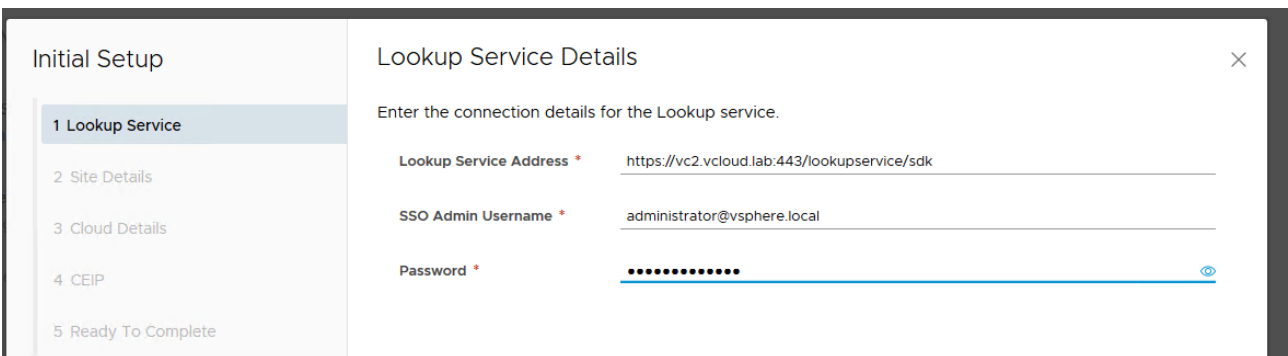
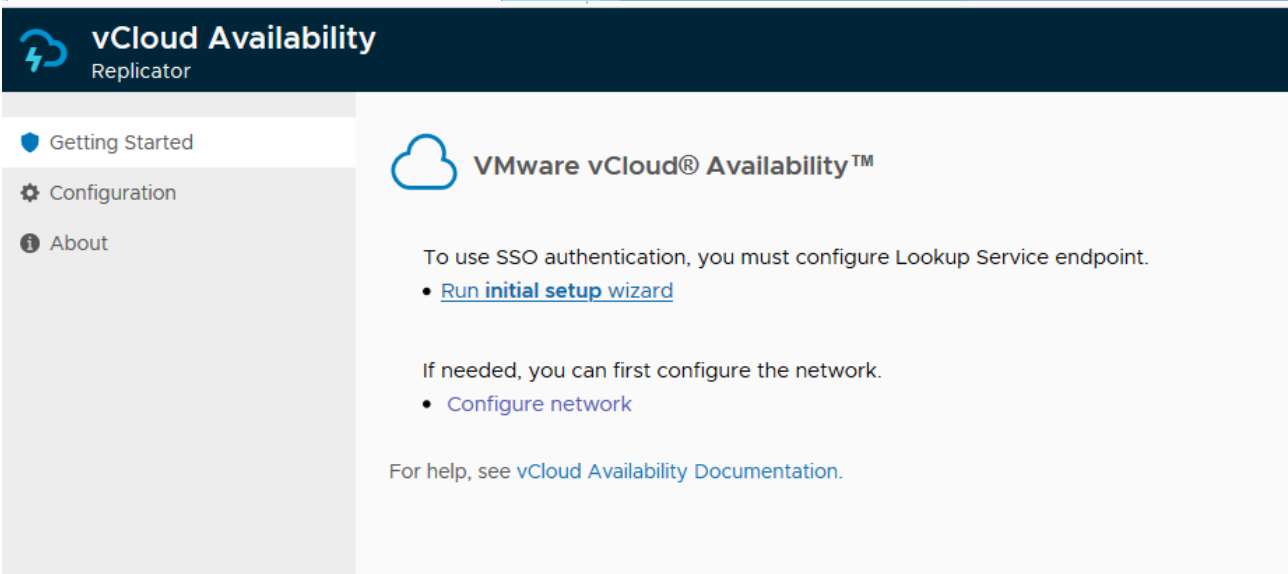
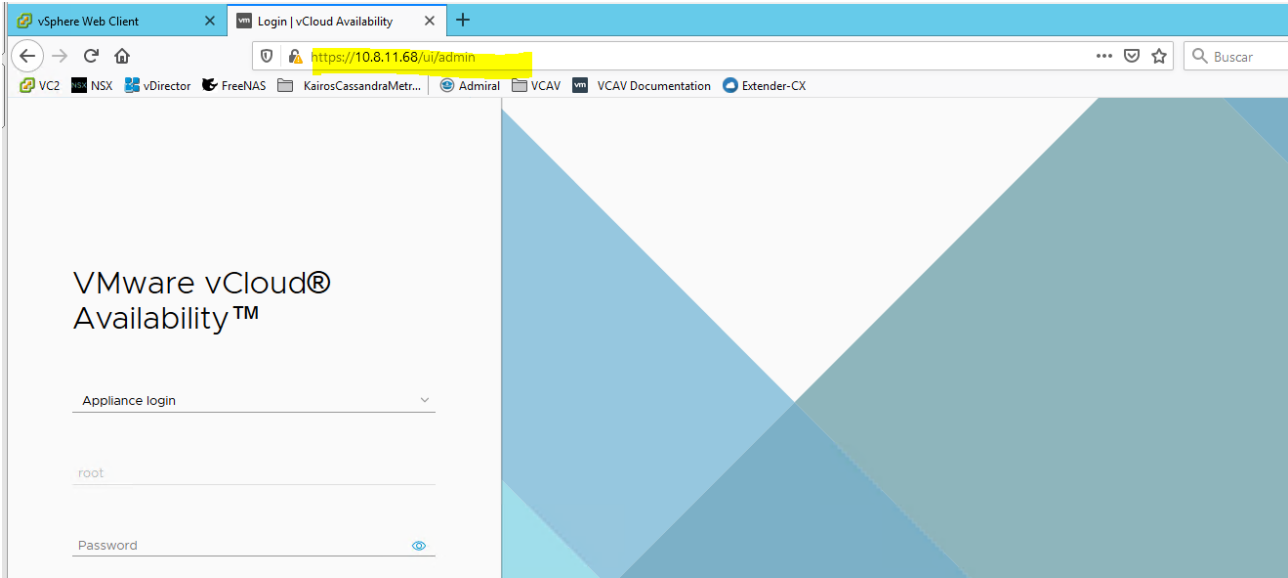


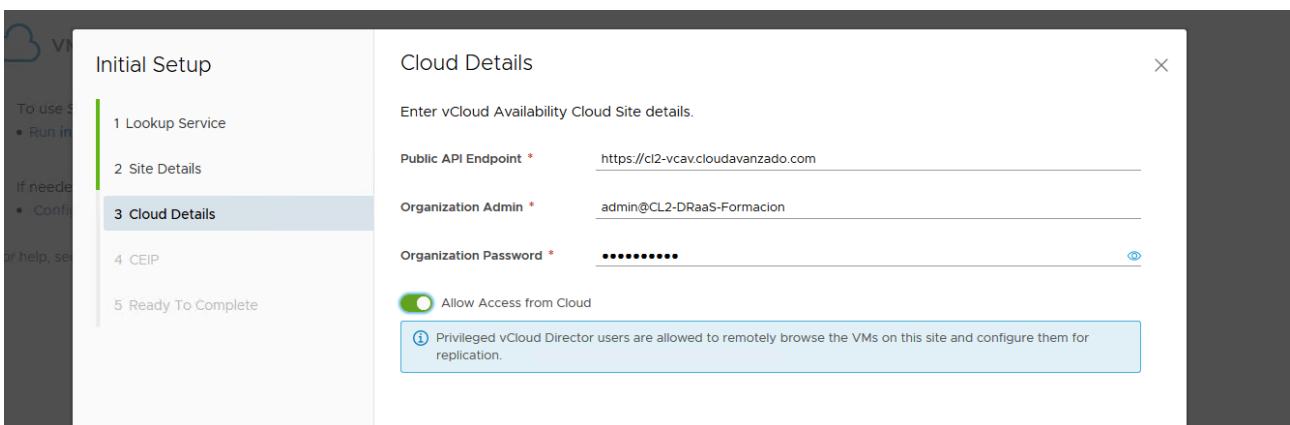
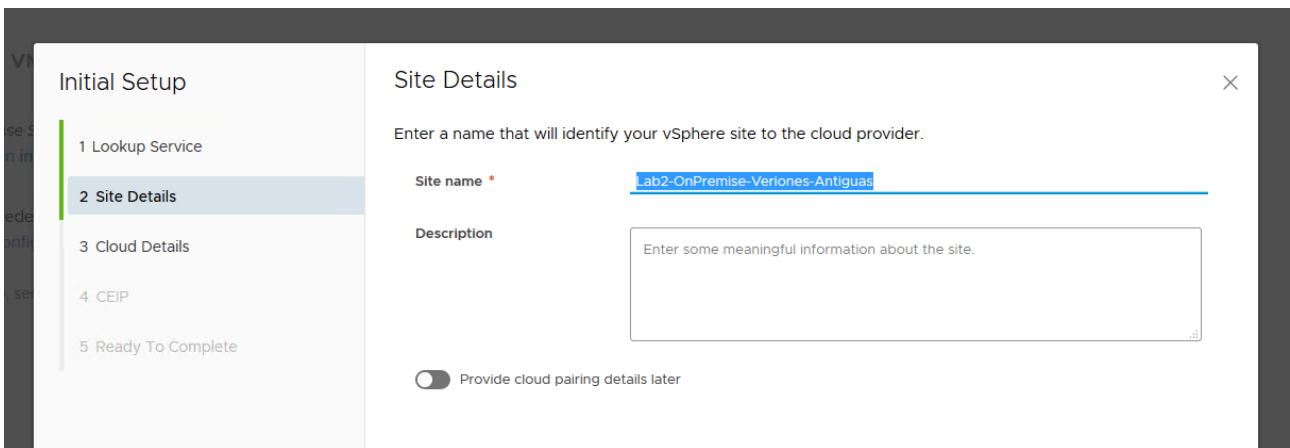
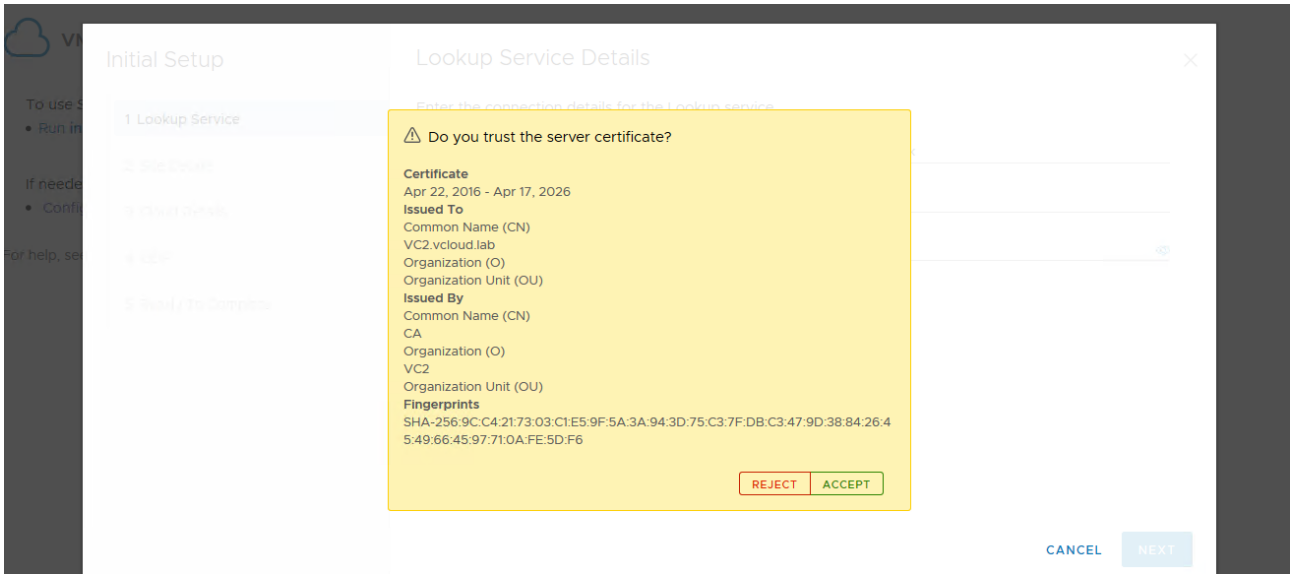
Introduce un password, que no sea el definitivo porque tendrás que cambiarlo en el primer arranque.



Una vez esté desplegado arráncalo y entra en el appliance:







The screenshot shows the 'Initial Setup' wizard with the 'Cloud Details' step selected. A yellow dialog box is displayed in the foreground asking 'Do you trust the server certificate?'. The dialog contains the following information:

- Certificate:** Mar 27, 2020 - May 16, 2021
- Issued To:** Common Name (CN) *.cloudavanzado.com, Organization (O) Acens Technologies S.L, Organization Unit (OU) Acens Technologies S.L
- Issued By:** Common Name (CN) Thawte TLS RSA CA G1, Organization (O) DigiCert Inc, Organization Unit (OU) www.digicert.com
- Fingerprints:** SHA-256:94:D3:60:F6:FB:19:12:EE:CF:E5:39:08:E9:5D:0F:E7:6A:A7:73:90:A7:F1:85:C7:CC:B3:B7:EB:26:79:C2:C9

Buttons for 'REJECT' and 'ACCEPT' are visible at the bottom of the dialog. In the background, the 'Initial Setup' progress bar shows steps 1 through 5, with '3 Cloud Details' currently active.

The screenshot shows the 'Initial Setup' wizard at the 'Configure participation in CEIP' step. The progress bar on the left indicates that step 4 is active. The main content area contains the following text:

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual.

Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>. If you prefer not to participate in VMware's CEIP for this product, you should uncheck the box below. You may join or leave VMware's CEIP for this product at any time.

Join the VMware Customer Experience Improvement Program

Buttons for 'CANCEL', 'BACK', and 'NEXT' are visible at the bottom right.

The screenshot shows the 'Initial Setup' wizard at the 'Ready To Complete' step. The progress bar on the left indicates that step 5 is active. The main content area displays a summary of the configuration:

Site Name	Lab2-OnPremise-Veriones-Antiguas
Site Description	
Lookup Service Address	https://vc2.vcloud.lab:443/lookupservice/sdk
SSO Admin Username	administrator@vsphere.local
Public API Endpoint	https://cl2-vcav.cloudavanzado.com
vCloud Director Username	admin@CL2-DRaaS-Formacion
Allow Access from Cloud	Yes
Participate in CEIP	Yes

Below the summary, there is an information icon and text: 'After you finish the initial setup, you will be able to configure **datacenter to cloud** replications. To enable **cloud to datacenter** replications, you must specify local placement settings.'

A toggle switch for 'Configure local placement now' is currently turned off.

Buttons for 'CANCEL', 'BACK', and 'FINISH' are visible at the bottom right.

Cloud site	CL2-VDC	
Public API Endpoint	https://cl2-vcav.cloudavanzado.com	
Organization	CL2-DRaaS-Formacion	
> Placement to newly recovered VMs on this site	Not configured	Configure

Service endpoints

Configure Placement

- 1 VM Folder
- 2 Compute Resource**
- 3 Default Network
- 4 Datastore
- 5 Ready To Complete

Compute Resource

Select the destination compute resource for the recovered virtual machines.

- ▼ Data-vCloud2
 - > **Clus-Computer2**

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network**
- 4 Datastore
- 5 Ready To Complete

Default Network

Select the network to connect VM network interfaces after failover.

- ▼ Resources
 - 3786-Azure-Migrations-Lab-JuanJo
 - dvPortGroup
 - Mgt-3784**
 - PortG_vlan2686_Ext
 - PortG_vlan3784_Ext
 - PortG_vlan3785_Ext
 - PortG_vlan3786_Ext
 - PortG_vlan3789_Ext

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network
- 4 Datastore**
- 5 Ready To Complete

Datastore

Select the datastore in which to store the replicated VMs and disk files

- ▼ Resources
 - Local-lab-esx10
 - Local-lab-esx11
 - NFS-vCloud01-Win
 - NFS-vCloud02-Linux**
 - VDP

Configure Placement

- 1 VM Folder
- 2 Compute Resource
- 3 Default Network
- 4 Datastore
- 5 Ready To Complete

Ready To Complete

Verify the selected configuration is correct.

VC	VC2.vcloud.lab
VM Folder	Data-vCloud2
Compute Resource	Clus-Computer2
Default Network	Mgt-3784
Datastore	NFS-vCloud02-Linux

vm vCloud Director
Datacenters

< All datacenters
pVDC-CL2-DRaaS-Formacion | CL2-DRaaS-Formacion, www.cloudavanzado.com

- Datacenters
- Datacenter Groups
- Libraries
- Administration
- Tasks
- Events
- Availability (CL2-VDC)

No VMs found

CL2-DRaaS-Formacion@CL2...
ALL ACTIONS
STATUS TOPOLOGY INSTANCES RESOURCES

- Incoming Replications
 - from Cloud
 - from On-Premises
- Outgoing Replications
 - to Cloud
 - to On-Premises
- Replication Tasks

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Repl...

CL2-DRaaS-Formacion@CL2...
ALL ACTIONS
STATUS TOPOLOGY INSTANCES RESOURCES
LAB2-ONPREMISE-VERIONES-ANTIGUAS
VAPP

- Incoming Replications
 - from Cloud
 - from On-Premises
- Outgoing Replications

VM	vApp	SLA profile	RPO	Replication state	Recovery state	Replication type	Overall health	Last changed
<input type="checkbox"/>	test-Replication	N/A		Mixed	Mixed	Protection	Configure	