

Guía de Seguridad de las TIC

CCN-STIC 1644

Procedimiento de Empleo Seguro

HPE SimpliVity



Mayo 2025



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid

© Centro Criptológico Nacional, 2025

NIPO: 083-25-208-6

Fecha de Edición: Mayo de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	5
4 FASE DE DESPLIEGUE E INSTALACIÓN	6
4.1 DESCRIPCIÓN DEL ENTORNO OPERACIONAL	6
4.2 ENTEGA SEGURA DEL PRODUCTO.....	6
4.2.1 DESCARGA DEL SOFTWARE.....	6
4.2.2 OBTENCIÓN DEL HARDWARE	7
4.3 INSTALACIÓN Y CONFIGURACIÓN DEL ENTORNO OPERACIONAL	9
4.4 INSTALACIÓN SEGURA	11
4.4.1 PREREQUISITOS	11
4.4.2 INSTALACIÓN	12
5 FASE DE CONFIGURACIÓN	29
5.1 ACTUALIZACIONES	35
5.2 ALTA DISPONIBILIDAD.....	41
6 FASE DE OPERACIÓN Y MANTENIMIENTO	42
6.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN.....	42
6.2 INTERPRETACIÓN DE LAS GUÍAS	43
7 REFERENCIAS	44
8 ABREVIATURAS.....	45

1 INTRODUCCIÓN

1. **HPE SimpliVity 4.2** es una plataforma software hiperconvergente que proporciona alta disponibilidad, escalabilidad, protección eficiente contra desastres y administración centralizada sobre el almacenamiento y las máquinas virtuales gestionadas por un hipervisor **VMware ESXi**.
2. Adicionalmente, los *appliances* de la familia **HPE SimpliVity** sobre los que se ejecuta el **HPE SimpliVity** proveen aceleración de cifrado por Hardware con la tecnología **HPE Smart Array**, así como aceleración por hardware de la duplicación y compresión de los datos empleando la tarjeta **HPE OmniStack Accelerator Card** (OAC).
3. La solución permite su integración con sistemas de almacenamiento de alta retención **HPE StoreOnce** y con interfaces **CSI** para contenedores, así como predicción y prevención de fallos de la infraestructura mediante el uso de la plataforma de análisis predictivo de datos **HPE InfoSight**.

2 OBJETO Y ALCANCE

4. En la presente guía se recoge el procedimiento de empleo seguro para la plataforma hiperconvergente **HPE SimpliVity 4.2** ejecutándose como una máquina virtual en un hipervisor **VMware ESXi** y soportada por el hardware de uno de los dispositivos certificados por HPE para el soporte de **HPE SimpliVity**.
5. En la siguiente tabla se muestran las plataformas que componen el producto y están cubiertas por este procedimiento de empleo seguro:

Versión del Software	Modelos Hardware
HPE SimpliVity 4.2	HPE SimpliVity 380 Gen10
	HPE SimpliVity 380 Gen10 G
	HPE SimpliVity 380 Gen10 H (DFF)
	HPE SimpliVity 325 Gen10
	HPE SimpliVity 380 Gen10
	HPE SimpliVity 2600 Gen10
	HPE SimpliVity 380 Gen10 H (LFF)

Tabla 1. Plataformas compatibles

6. El producto HPE SimpliVity 4.2 ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA/MEDIA en la familia “HIPERCONVERGENCIA”.

3 ORGANIZACIÓN DEL DOCUMENTO

7. El documento se organiza en los siguientes apartados:

- Apartado 4. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de despliegue e instalación física del producto.
- Apartado 5. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de configuración segura del producto.
- Apartado 6. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de operación y mantenimiento.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 DESCRIPCIÓN DEL ENTORNO OPERACIONAL

8. El entorno en el que se ejecutará el TOE deberá estar compuesto por los siguientes elementos:

- **VMware vCenter Server** versión **6.5** o **6.7**. Puede encontrarse instalado sobre los siguientes sistemas:
 - Windows Server 2008 R2, Windows Server 2012 R2 o 2016 (64-bit)
 - VMware vCenter Server Appliance (Linux VM, 64-bit, optimizada para ejecutar vCenter Server)
- **HPE Omnistack host:**
 - **VMware ESXi** versión 6.5 o 6.7.
 - **Datastore.**
- **HPE SimpliVity Arbiter** versión 4.2 o superior (Opcional en entornos con un número de nodos que no sea 2 ni 4).
- **HPE SimpliVity Plug-in for VSphere Client**

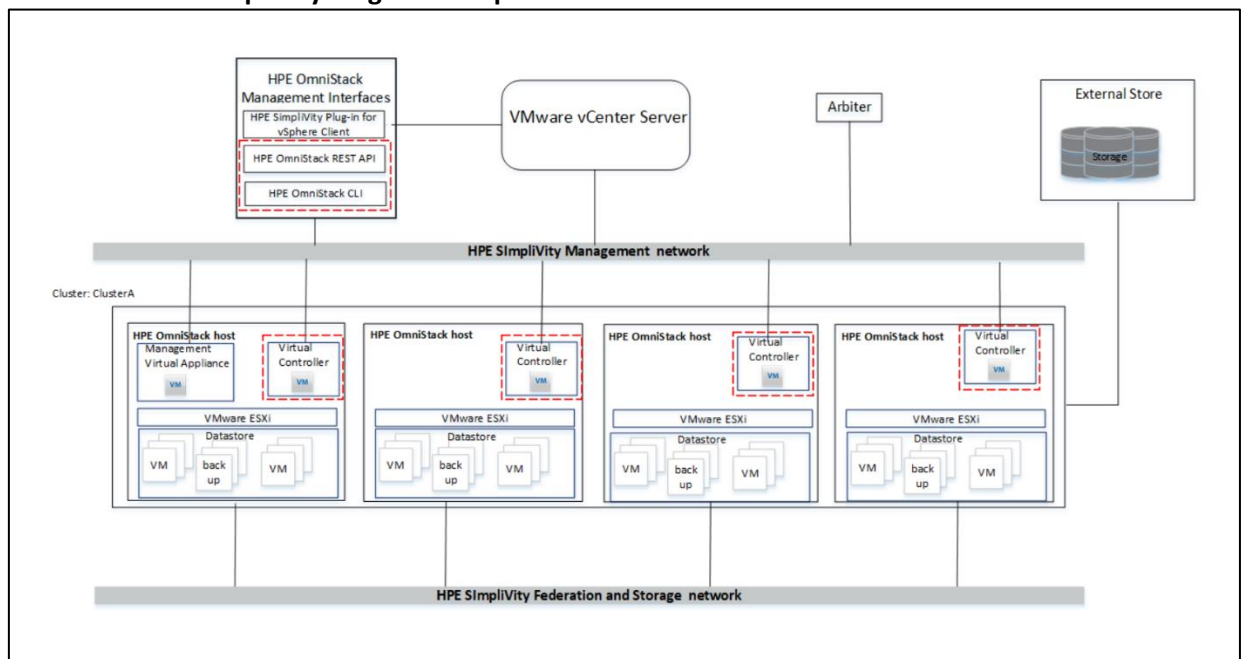


Ilustración 1 - Entorno de operación

4.2 ENTEGA SEGURA DEL PRODUCTO

4.2.1 DESCARGA DEL SOFTWARE

9. Esta sección indica cómo obtener el software del dispositivo y los componentes del entorno que serán necesarios para realizar su despliegue.

10. Exceptuando el componente **VMware vCenter Server**, que podrá ser obtenido de la página de su fabricante (<https://www.vmware.com>), todos los elementos necesarios para la preparación del entorno pueden ser descargados a través de **My HPE Software Center** (<http://www.hpe.com/software/hpesoftwarecenter>):

- Acceder a **My HPE Software Center** (<http://www.hpe.com/software/hpesoftwarecenter>).
- Autenticarse con las credenciales de la cuenta HPE Passport que habrá sido proporcionada por HPE tras la compra del producto.
- Acceder a *Software Updates*.
- En *Search Software Updates*, especificar los siguientes criterios de búsqueda:
 - *Product Name = OmniStack*.
- Localizar el paquete de deployment (Q8A57-110xx_SimpliVity_Deploy_Package_4.1.1_VMware_vSphere.zip¹), y hacer click en *More Info*.
- Hacer Click en *Update* e iniciar la descarga.
- Extraer el paquete una vez ha sido descargado.
- El paquete contendrá al menos los siguientes elementos:
 - simplivity-arbiter-4.1.1.x.msi
 - simplivity-deployment-manager-4.1.1.x.msi
 - HPE-SimpliVity-Plug-in-for-vSphere-Client-linux-x64-4.1.1.x.run
 - HPE-SimpliVity-Plug-in-for-vSphere-Client-windows-4.1.1.x.exe

4.2.2 OBTENCIÓN DEL HARDWARE

11. Los dispositivos físicos HPE Omnistack host serán enviados por parte de HPE a las instalaciones especificadas por el receptor. Los nodos incluyen las versiones de VMware ESXi 6.5 y 6.7 y la versión correcta del producto especificada por el cliente.
12. Tras su recepción, se debe comprobar que la caja no ha sido dañada ni abierta. Si tras recibir o abrir el paquete se detecta cualquier tipo de manipulación del mismo, el receptor debe ponerse en contacto con HPE a través del centro de soporte (<https://support.hpe.com>).
13. Para asegurar una correcta recepción del producto será necesario revisar que no ha sido manipulado de manera alguna durante su transporte. Para ello, se llevarán a cabo los siguientes pasos:
 - Antes de abrir el paquete, comprobar que el logo y los motivos de *HPE* están impresos en él. En caso contrario, contacte con el proveedor del producto.
 - Compruebe que la caja tiene una etiqueta blanca con un código de barras, el número de producto, número de serie y modelo y otra información relacionada con el contenido de la caja. El objetivo de esta etiqueta es evitar la alteración del interior del paquete. Si se observa que la etiqueta está rota o no está, contacte con el proveedor del producto.
 - Una vez el producto se ha desempaquetado, inspeccione la unidad. Compruebe que el número de serie que aparece en el propio producto coincide con el número de serie de la documentación de envío.

¹ Será válido cualquier paquete de software que contenga la versión 4.1.1 o superior.

14. Tras el proceso de instalación se comprobará si la versión instalada del producto es la correcta. En caso de que no lo sea, se deberá realizar una actualización del mismo siguiendo los pasos en la guía ***HPE OmniStack 4.0.1 U1 for vSphere Upgrade Guide***.

4.3 INSTALACIÓN Y CONFIGURACIÓN DEL ENTORNO OPERACIONAL

15. El administrador debe asegurarse de realizar los siguientes pasos para preparar el entorno operacional antes de comenzar la instalación:

- Instalar **VMware vCenter Server** versión 6.5 o 6.7 en una máquina que sea accesible y pueda acceder a los **HPE Omnistack hosts** que se instalarán en el entorno a través de su red de administración. Para ello se deben seguir las guías de instalación y configuración de **VMware vCenter Server** provistas por su fabricante. Una vez instalado, se deberá crear al menos un nuevo centro de datos y un clúster dentro de ese centro de datos.
- Cabe destacar que la instalación de **VMware vCenter Server** requiere la presencia de un servidor DNS que pueda resolver su nombre de dominio. El servidor DNS se deberá emplear también durante la instalación del TOE y debe ser accesible por todos los componentes que se encuentren en la red de administración.
- En **VMware vCenter Server** se debe instalar **HPE SimpliVity Plug-in for VSphere Client**. Para ello se realizarán los siguientes pasos, dependiendo si **VMware vCenter Server** ha sido instalado en Windows server o si se trata de **VMware vCenter Server Appliance**:
 - **VMware vCenter Server Appliance** sobre Windows Server:
 - Acceder al ordenador con windows en el que se encuentra instalado **VMware vCenter Server** con una cuenta de administrador.
 - Descargar el ejecutable **HPE-SimpliVity-Plug-in-for-vSphere-Client-windows-4.1.1.n.exe²** y hacer doble click sobre él para iniciar el proceso de instalación.
 - Hacer click en *next* para abrir el acuerdo de licencia.
 - Acepta el acuerdo y selecciona *next*.
 - Especificar el directorio en el que se instalará el plug-in. La ruta por defecto es `C:\Program Files\Hewlett Packard Enterprise\HPEsimpliVityPluginForVSphereClient`.
 - Hacer click en *next* para abrir la ventana de credenciales de **VMware vCenter Server**.
 - Introducir las credenciales del administrador de **VMware vCenter Server** en los campos de usuario y contraseña. En el campo de E-mail introduce la dirección de correo del administrador responsable de **HPE SimpliVity Plug-in for VSphere Client** para que pueda recibir alertas. Haz click en *Next*.
 - Hacer click en *Next* para iniciar la instalación.
 - Esperar hasta que el asistente de instalación finalice. Una vez terminado el proceso de instalación haz click en *Next* para finalizar la instalación.
 - Dejar marcada la casilla que indica que se reinicie el servicio **VMware "vsphere-ui"**. En cualquier otro caso tendrás que reiniciar el servicio manualmente para iniciar el plug-in.
 - Hacer click en *Finish*.
 - **VMware vCenter Server Appliance**:
 - Acceda mediante línea de comandos a **vCenter Server Appliance** con una cuenta con permisos de root. Por ejemplo, usando SSH.
 - Si no ve un prompt de bash (#), ejecute el comando: `shell`

² Podrá usarse cualquier build del Plug-In que contenga la versión 4.1.1 o superior.

- Suba la aplicación *HPE-SimpliVity-Plug-in-forvSphere-Client-linux-x64-4.1.1.n.run*³ a **vCenter Server Appliance**. Por ejemplo, usando `scp`, `curl`, o `wget`.
 - Garantice permisos de ejecución a la aplicación mediante el siguiente comando:
 - `chmod +x <HPE-SimpliVity-Plug-in-for-vSphere-Client-linux-4.1.1.n.run>`
 - Ejecute el instalador:
 - `./<HPE-SimpliVity-Plug-in-for-vSphere-Client.4.1.1.n.run>`
 - El instalador mostrará un aviso mostrando el acuerdo de licencia.
 - Lea el acuerdo de licencia y acéptelo para continuar la instalación.
 - Indique el directorio en el que se instalará **HPE SimpliVity Plug-in** y presione *Enter*.
 - El Sistema le pedirá sus credenciales de **VMware vCenter Server** y el E-mail del administrador, que deberán ser introducidas en los campos correspondientes.
 - Espere a que el Sistema de instalación termine de instalar la aplicación. Cuando termine verá un mensaje que indica *"Finish"*.
 - Deje marcada la casilla que indica que se reiniciará el servicio *VMware "vsphere-ui"*. En cualquier otro caso tendrás que reiniciar el servicio manualmente para iniciar el plug-in.
- Instalación de al menos dos **HPE Omnistack hosts** en el entorno. Estos nodos se deberán conectar a dos redes separadas (Red de gestión y red de almacenamiento y federación):
 - **Red de gestión:** Se trata de la red desde la que se accederá a los hipervisores ESXi. Esta red debe tener acceso a **VMware vCenter Server** y **HPE Arbiter** (Si aplica). Para conectar los nodos a esta red se llevarán a cabo los siguientes pasos:
 - Conectar un cable entre uno de los puertos físicos del nodo y un *switch* o *router* que le proporcione acceso a la red de administración. Tras ser arrancados, los equipos adquirirán una dirección IP mediante DHCP, por lo que será necesario que la red de administración disponga de un servidor DHCP que les proporcione dichas direcciones. También existe la posibilidad de establecer las direcciones IP de forma manual mediante la conexión de una pantalla y teclado a los equipos o usando la interfaz iLO, de esta forma no será necesaria la presencia de un servidor DHCP en el entorno.
 - **Red de almacenamiento y federación:** Se trata de la red aislada y protegida físicamente, de manera que solo usuarios autorizados puedan tener acceso a dicha red. Los nodos **HPE Omnistack host de un** clúster serán los únicos elementos interconectados por esta red. Para conectar los nodos a esta red se llevarán a cabo los siguientes pasos.
 - En los casos en los que se vayan a desplegar dos nodos, éstos se pueden interconectar directamente entre ellos usando uno de los puertos que soporte velocidades de al menos 10 Gb/s. Es decir, se conectará un extremo del cable directamente a un puerto de cada nodo.

³ Podrá usarse cualquier build del Plug-In que contenga la versión 4.1.1 o superior.

- Para dos o más nodos, las interconexiones se podrán realizar a través de un switch que soporte velocidades de transmisión de 10Gb/s o superiores. Todos los nodos se conectarán a uno o más de los puertos del switch a través de al menos uno de sus puertos 10Gb.
 - Una vez conectados a las dos redes y a la corriente, se encenderán todos los nodos que se pretenden desplegar pulsando su botón físico de arranque. Se esperará a que hayan arrancado por completo y se comprobará que han obtenido una dirección IP de forma correcta. Esta comprobación se puede realizar a través del puerto iLO o mediante la conexión de una pantalla a través del puerto VGA del servidor.
 - (Opcional) En caso de que se desplieguen 2 o 4 nodos será necesario realizar este paso. En cualquier otro caso será opcional.

En la misma máquina en la que se ha instalado **VMware vCenter Server** o en cualquier host con *Windows Server 2016, 2012 R2, 2008 R2 o Windows 10* y con acceso a la red de administración se deberá instalar el software **HPE SimpliVity Arbiter**. Para ello se seguirán los siguientes pasos:

 - Hacer doble click sobre el archivo `simplivity-arbiter-n.n.n.n.msi`.
 - Aceptar la ventana que muestra la licencia y hacer click en *Install*.
 - Una vez completada la instalación seleccionar *Finish*.
 - Los elementos de la red de administración (**vCenter**, **HPE Arbiter** y nodos **HPE Omnistack host**) deben ser capaces de comunicarse con un servidor NTP que les proporcione el tiempo. Si la red de administración tiene acceso a internet no será necesario realizar ningún paso para cumplir este requisito. En caso de que no se tenga acceso a internet o que se quiera utilizar un servidor NTP que no sea público, se deberá configurar dicho servidor en un punto accesible por la red de administración.
 - Se realizará una comprobación de la correcta conectividad entre los diferentes elementos que se han instalado en el entorno mediante el uso de la herramienta *ping*. Para ello se comprobará que la máquina en la que se encuentra instalado **VMware vCenter Server** es capaz de alcanzar a todos los nodos **HPE Omnistack host** que se han incluido en el entorno. La misma comprobación se llevará a cabo desde la máquina que contiene el software **Arbiter** si se ha decidido incluirla en el entorno. En caso de existir problemas de conectividad se deberán volver a configurar las interfaces de todos los elementos del entorno con el rango de direcciones IP adecuado y con la topología adecuada de tal manera que todos los elementos sean capaces de alcanzarse entre ellos.
16. Una vez se hayan llevado a cabo estos pasos, el entorno en el que se ejecutará el TOE habrá quedado debidamente instalado y configurado.

4.4 INSTALACIÓN SEGURA

4.4.1 PREREQUISITOS

17. Durante el proceso de instalación de cada uno de los nodos será necesario el empleo de la herramienta **HPE Deployment Manager**. Esta herramienta puede ser obtenida usando el mismo proceso mediante el que se descargó el software necesario para la configuración del entorno; a través de **My HPE Software Center** (<http://www.hpe.com/software/hpesoftwarecenter>). Siguiendo esos pasos se obtendrá el siguiente ejecutable:

- `simplivity-deployment-manager-4.1.1.x.msi`⁴
18. Sólo durante el proceso de instalación, será necesario que esta herramienta se encuentre instalada en una máquina con acceso a la red de administración de los nodos **HPE Omnistack host**. Una vez finalizado el proceso la máquina que contiene esta herramienta puede ser retirada del entorno.
 19. Este software es compatible con los siguientes sistemas operativos:
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2008 R2
 - Windows 10
 20. Para la instalación de **HPE Deployment Manager** se seguirán los siguientes pasos:
 - Instalar en la máquina los siguientes paquetes:
 - Microsoft® .NET Framework 4.7.1 o una versión superior.
 - Una versión de Java equivalente a OpenJDK 8, como puede ser Azul o AdoptOpenJDKOracle.
 - Ejecutar el instalador `simplivity-deployment-manager-4.1.1.x.msi`.
 - Hacer click en *Run* y aceptar el acuerdo de la licencia.
 - Seleccionar la carpeta en la que se instalará el software e indicar si queremos que se instale para todos los usuarios del sistema (*Everyone*) o solo para el usuario que ejecuta la instalación (*Just me*). Hacer click en *Next*.
 - En la siguiente ventana hacer click en *Next* para iniciar el proceso de instalación.
 - Una vez concluida la instalación hacer click en *Close*.

4.4.2 INSTALACIÓN

21. La instalación se llevará a cabo desde la máquina en la que se ha instalado **HPE Deployment Manager**. Cabe destacar que, tras el proceso de instalación, el TOE debe quedar instalado en al menos dos de los nodos **HPE Omnistack host** que se han incluido como parte del entorno.
22. Para la instalación se llevarán a cabo los siguientes pasos:
23. Ejecutar **HPE Deployment Manager**. Tras ello, se introducirá la dirección IP y credenciales de administración de **VMware vCenter Server** y se hará click en *Login*.

⁴ Se podrá emplear cualquier versión de **HPE Deployment Manager** 4.1.1 o superior.

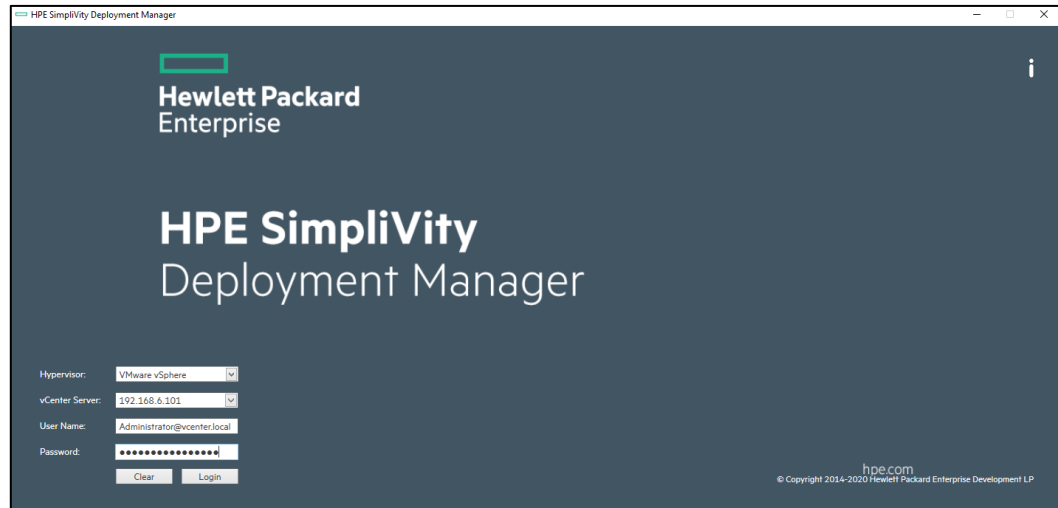


Ilustración 2 - Deployment Manager

24. Se le presentará al usuario el certificado de vCenter, que deberá ser aceptado tras verificar que es correcto.
25. En la siguiente pantalla se debe seleccionar el clúster en el que se instalará el TOE. Si es la primera vez que se despliega un host, se mostrará una alerta indicando si se quiere habilitar HPE InfoSight. Se seleccionará *OFF* para deshabilitar esta función por defecto.

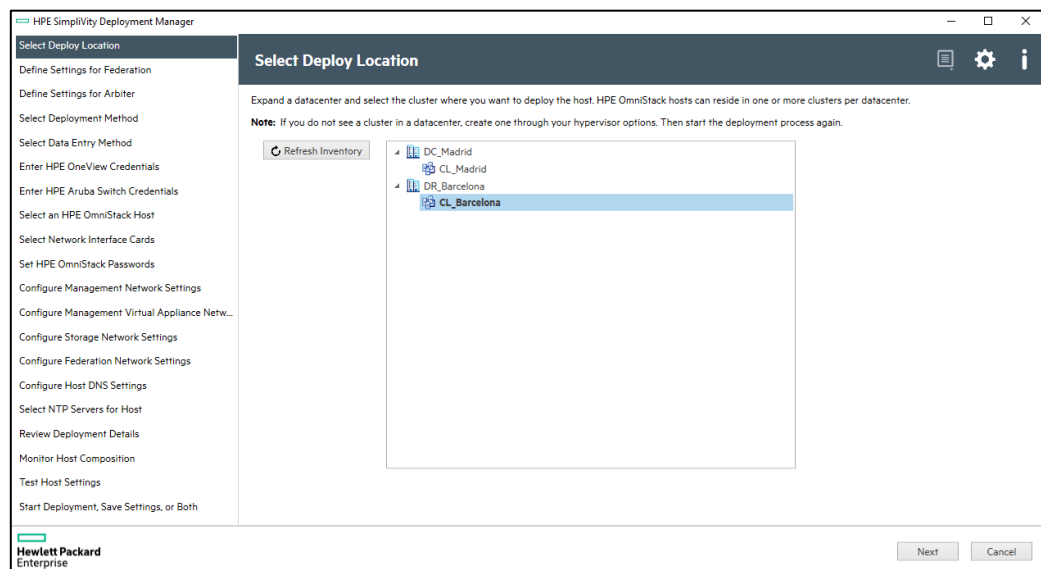


Ilustración 3 - Deploy Location

26. Si es la primera vez que se despliega un host, en la siguiente ventana se debe crear una federación. Cualquier tipo de federación seleccionado cumplirá los requisitos de la evaluación, sin embargo, la selección de “centrally-managed HPE SimpliVity Federation” es recomendada cuando se despliegan 10 o más hosts. Se recomienda la selección de “centrally-managed HPE SimpliVity Federation” cuando se planea que en el futuro haya una gran cantidad de hosts en la federación y la selección de “peer managed HPE SimpliVity Federation” si la cantidad de hosts no será elevada. Adicionalmente, si se quiere incluir el host en una federación existente, se debe seleccionar la opción “Join an existing HPE SimpliVity Federation” y proporcionar la dirección IP del controlador virtual que la gestiona:

Ilustración 4 - Federation

27. Seleccionaremos que no vamos a usar “*Stretch Clusters*” e indicaremos el número de nodos **HPE Omnistack host** que se van a desplegar. Si el número de nodos es 2 o 4, será necesaria la presencia de **HPE SimpliVity Arbiter**. En ese caso, seleccionaremos la segunda opción e indicaremos la dirección IP en la que se encuentra **HPE SimpliVity Arbiter**.

Ilustración 5 - Arbiter

28. Seleccionaremos el modo de despliegue *Basic*:

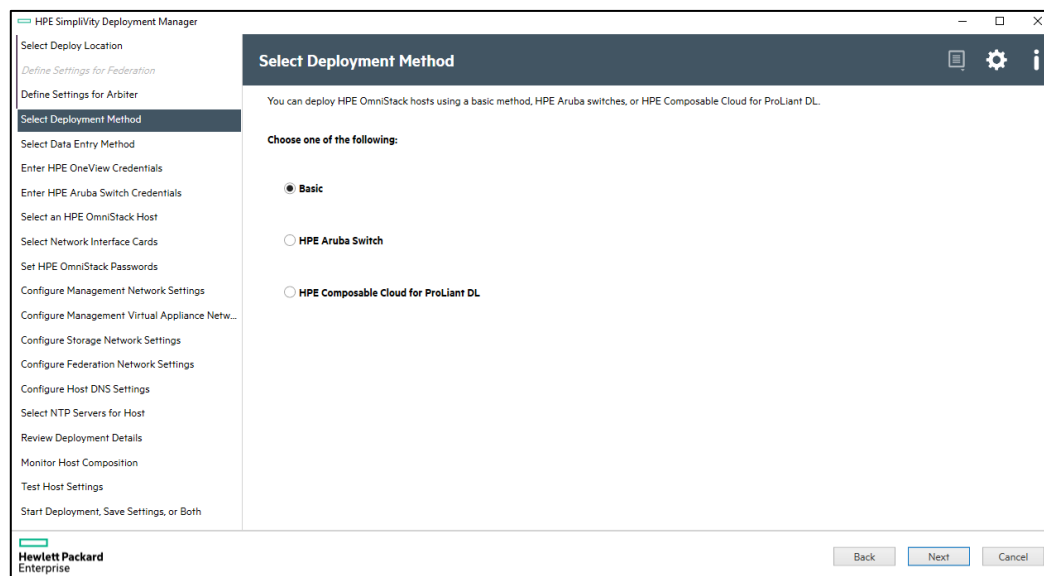


Ilustración 6 - Deployment Method

29. Seleccionaremos una de las siguientes opciones:

- **Manually enter settings:** Si se trata de la primera instalación o si no se quiere emplear un fichero de configuración se debe seleccionar esta opción.
- **Import configuration (XML) file:** Si se dispone de un fichero de configuración de una instalación previa se puede seleccionar esta opción e incluir dicho fichero de configuración. La selección de esta opción supondrá que algunos de los pasos del despliegue aparecerán automáticamente completados con la información incluida en el fichero de configuración.

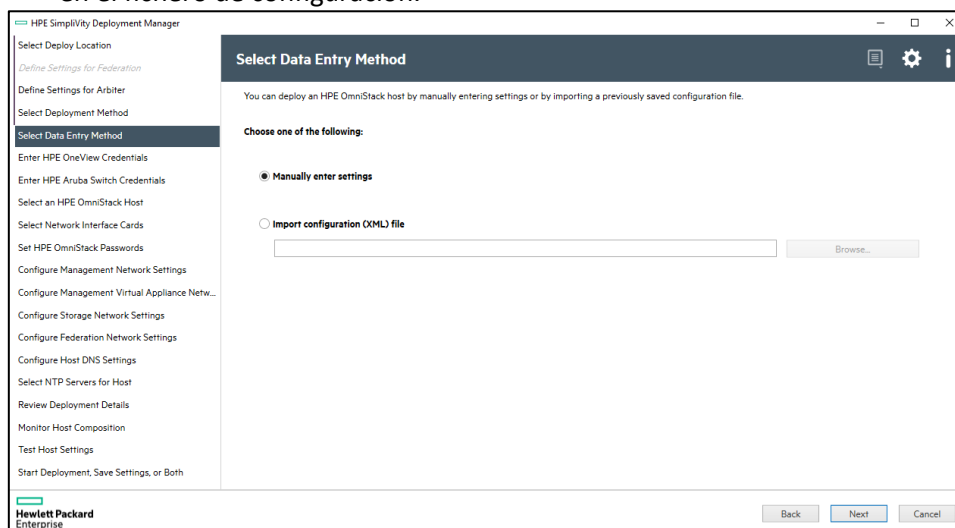


Ilustración 7 - Entry Method

30. En la siguiente pantalla se debe seleccionar el **HPE OmniStack Host** sobre el que se realizará el despliegue. Para ello es necesario buscar el host en la red haciendo click en *scan* o introduciendo manualmente la dirección IP en el campo “Add host IP address” y seleccionando *Add*. Una vez se haya añadido, el host aparecerá en la lista de hosts. Se deberá marcar solo la casilla del host sobre el que se quiere realizar el despliegue:

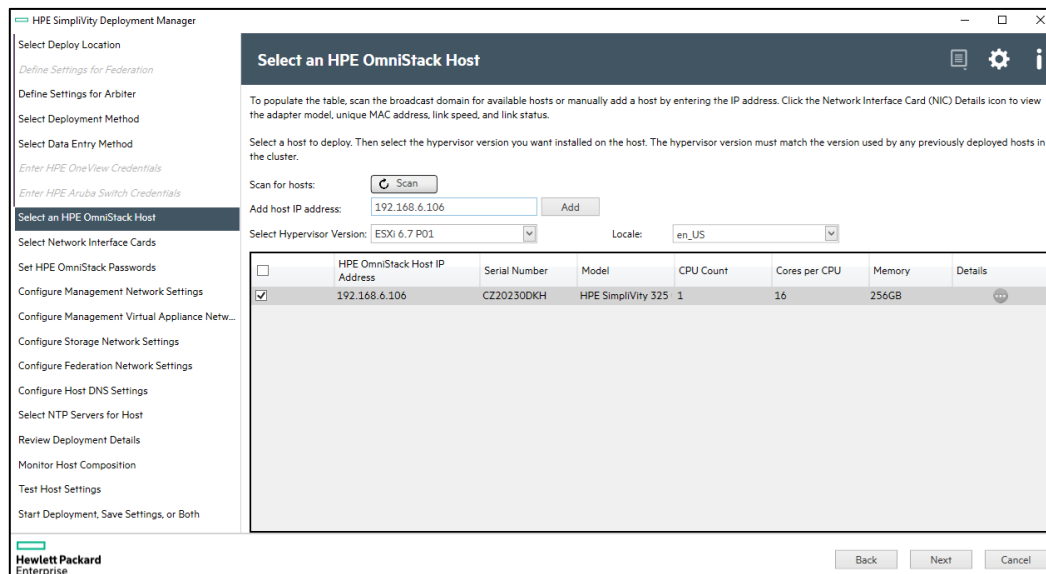


Ilustración 8 - OmnStack Host Selection

31. En esa misma ventana, se debe seleccionar la versión de ESXi que se desea desplegar en el host. Para ello se utilizará la lista “Select Hypervisor Version”⁵. Adicionalmente, a través de la columna de “Details” se puede comprobar con qué hipervisores es compatible el host e identificar sus interfaces. Una vez seleccionado el hipervisor se hará click en *Next*:

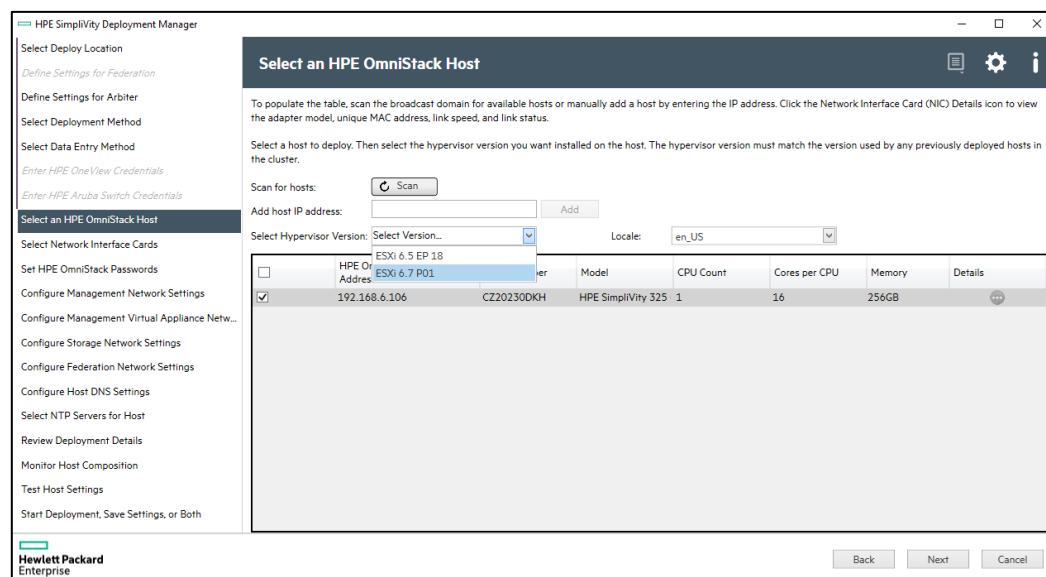


Ilustración 9 - OmnStack Host Selection 2

32. A través de la columna de “Details” de la pantalla anterior se deben identificar los NICs que se encuentran conectados en este momento. Si se ha realizado correctamente la preparación del entorno operacional, deberían aparecer dos NICs conectados (red de administración y red de almacenamiento y federación). En la siguiente pantalla, se debe seleccionar el NIC que se asignará a la red de gestión y a la red de almacenamiento y

⁵ Todos los hosts desplegados dentro del mismo clúster deben usar la misma versión de Hipervisor.

federación. Solo se nos presentará una opción a la hora de elegir el NIC de administración, sin embargo, debemos identificar el NIC de la red de almacenamiento que se encuentra conectado para seleccionarlo en esta pantalla⁶. Una vez seleccionados los dos NICs correctos se debe hacer click en *Next*.

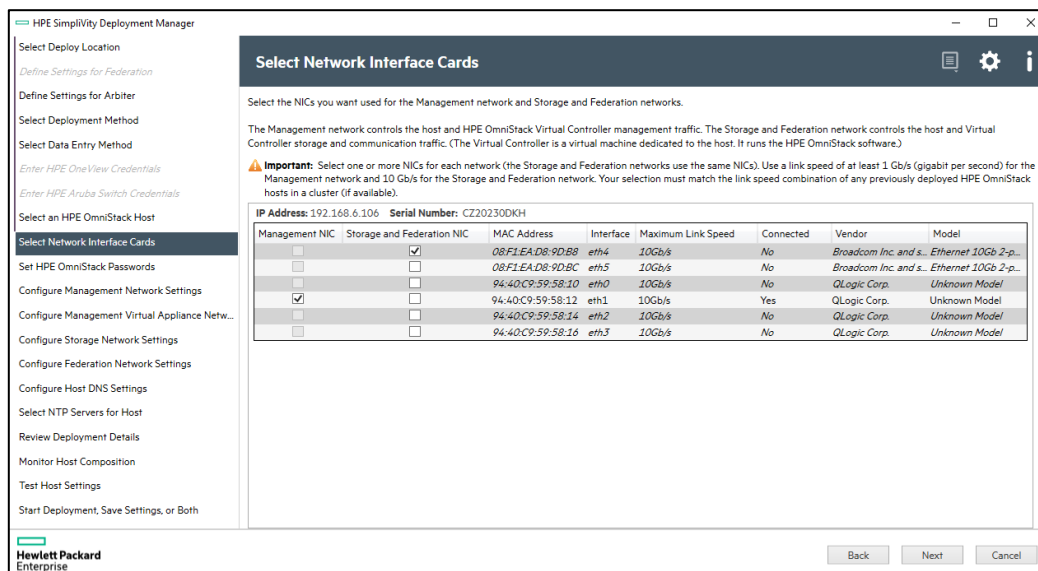


Ilustración 10 - Network Interfaces

33. Tras ello, estableceremos las contraseñas del host **ESXi** y de **HPE SimpliVity** (TOE). La contraseña de **HPE OmniStack Host** será la contraseña que se debe usar para acceder al hipervisor ESXi a través de su página de administración. Por otro lado, la contraseña **HPE OmniStack Command Line Interface** se corresponde con la contraseña del usuario *svtci* del TOE, que podrá ser usada para acceder a la CLI del controlador **HPE SimpliVity**.
34. **Nota:** Se seguirán las recomendaciones para la creación de contraseñas establecidas en la sección 6.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN.

⁶ Si se han conectado varios puertos 10Gb al switch de la interfaz de almacenamiento y federación, se pueden seleccionar todos ellos. De esta forma se activará automáticamente el NIC teaming

Set HPE OmniStack Passwords

Create the password for the root user account to log in to the HPE OmniStack host. Follow the password guidelines required by your hypervisor. Then create a Command Line Interface (CLI) password to access the HPE OmniStack Virtual Controller. Use this password to run commands if you cannot use your hypervisor single sign-on account.

HPE OmniStack Host Password

Host Password: [masked] Confirm Host Password: [masked]

HPE OmniStack Command Line Interface Password

CLI Password: [masked] Confirm CLI Password: [masked]

Back Next Cancel

Ilustración 11 - OmniStack Passwords

35. El siguiente paso consistirá en configurar la interfaz de administración del host. Si se ha desplegado algún host en la federación, estos campos podrán aparecer completados con opciones por defecto que no podrán ser cambiadas:

- **Management vSwitch Name:** Se deberá elegir el vSwitch de **vCenter** que proporcione acceso a la interfaz de administración. Si se trata del primer despliegue este campo no se puede modificar.
- **Host Port Group Name:** Si se trata del primer despliegue este campo no se puede modificar. En otro caso, seleccionar el grupo de puertos de **vCenter** que da acceso a la interfaz de administración.
- **Host Gateway y Virtual Controller Gateway:** El Gateway de la red de administración a través del cual se puede acceder al resto de componentes de la red o a otras redes.
- **Host Netmask y Virtual Controller Netmask:** La máscara de red de la red de gestión (típicamente 255.255.255.0).
- **Host VLAN ID y Virtual Controller VLAN ID:** Si la red de administración se encuentra configurada como una VLAN, se debe introducir en este campo el VLAN ID. En cualquier otro caso el campo se debe dejar en blanco.
- **MTU:** Introducir un valor entre 1000 y 9000. Para la red de administración se recomienda un tamaño de MTU de 1500.

Configure Management Network Settings

Specify the network settings for management traffic between HPE OmniStack hosts and Virtual Controllers. In the **IP Addresses** tab, enter the IP addresses for one or more hosts and Virtual Controllers. Management traffic includes host actions such as move, shut down, and upgrade.

Network Settings		IP Addresses	
Management vSwitch Name:	vSwitch0	MTU:	1500
Host Port Group Name:	Management Network	Virtual Controller Port Group Name:	VM Network
Host Gateway:	192.168.6.1	Virtual Controller Gateway:	192.168.6.1
Host Netmask:	255.255.255.0	Virtual Controller Netmask:	255.255.255.0
Host VLAN ID:	6	Virtual Controller VLAN ID:	6

Back Next Cancel

Ilustración 12 - Management Network Settings 1

36. Haga click en la pestaña *IP Addresses* y configure las direcciones IP de ESXi (Host IP Address) y de la máquina virtual del controlador (Virtual Controller IP Address). Ambas direcciones deben estar dentro del rango de direcciones permitidas en la red de administración. Una vez establecidos los valores se hará click en *Next*.

Configure Management Network Settings

Specify the network settings for management traffic between HPE OmniStack hosts and Virtual Controllers. In the **IP Addresses** tab, enter the IP addresses for one or more hosts and Virtual Controllers. Management traffic includes host actions such as move, shut down, and upgrade.

Temporary Host IP Address	Serial Number	Host IP Address	Virtual Controller IP Address
192.168.6.106	CZ20230DKH	192.168.6.106	192.168.6.107

Back Next Cancel

Ilustración 13 - Management Network Settings 2

37. Si se ha seleccionado una *peer-based managed federation*, avanza al paso 38. Si el despliegue se está realizando en una *centrally-managed federation* deberá configurar las opciones de red de la máquina virtual de administración. Para ello se deberán rellenar los siguientes campos:

- **Management Virtual Appliance IP Address:** La dirección IPv4 de la máquina virtual de administración. Deberá encontrarse dentro del rango de la red de administración.
- **Management Virtual Appliance Gateway:** El Gateway de la red de administración a través del cual se puede acceder al resto de componentes de la red o a otras redes.

- **Management Virtual Appliance Netmask:** La máscara de red de la red de gestión (típicamente 255.255.255.0).
- **Management Virtual Appliance CLI Password:** La contraseña de la cuenta de administración que se establecerá en la máquina virtual de gestión.
- **MTU:** Introducir un valor entre 1000 y 9000. Para la red de administración se recomienda un tamaño de MTU de 1500.
- **Port Group Name:** El grupo de puertos seleccionado para el Virtual Controller en la red de gestión.
- **VLAN ID:** Si la red de administración se encuentra configurada como una VLAN, se debe introducir en este campo el VLAN ID. En cualquier otro caso el campo se debe dejar en blanco.
- **Confirm Management Virtual Appliance CLI Password:** La contraseña de la cuenta de administración que se establecerá en la máquina virtual de gestión.

The screenshot displays the 'Configure Management Virtual Appliance Network Settings' window within the HPE SimpliVity Deployment Manager. The window is titled 'Configure Management Virtual Appliance Network Settings' and includes a subtitle: 'Specify the Management Virtual Appliance Network settings. The Management Virtual Appliance is a VM that manages operations across the HPE OmniStack hosts and requires connectivity to all federation hosts as well as vCenter.' The 'Network Settings' tab is active, showing a form with the following fields:

- Management Virtual Appliance IP Address: [Empty text box]
- Management Virtual Appliance Gateway: [Empty text box]
- Management Virtual Appliance Netmask: [Empty text box]
- Management Virtual Appliance CLI Password: [Empty text box]
- MTU: [1500]
- Port Group Name: [VM Network]
- VLAN ID: [0]
- Confirm Management Virtual Appliance CLI Password: [Empty text box]

The left sidebar contains a list of configuration steps, with 'Configure Management Virtual Appliance Network Settings' highlighted. The bottom of the window features the HP logo and three buttons: 'Back', 'Next', and 'Cancel'.

Ilustración 14 - Management Virtual Appliance Network Settings 1

38. Tras ello se procederá a configurar la interfaz de almacenamiento. Si se ha desplegado algún host en la federación, estos campos podrán aparecer completados con opciones por defecto que no podrán ser cambiadas:

- **Storage vSwitch Name:** Se deberá elegir el vSwitch de **vCenter** que proporcione acceso a la interfaz de almacenamiento deseada. Si se trata del primer despliegue este campo no se puede modificar.
- **Host Port Group Name y Virtual Controller Port Group Name:** Si se trata del primer despliegue este campo no se puede modificar. En otro caso, seleccionar el grupo de puertos de **vCenter** que da acceso a la interfaz de almacenamiento.
- **Host Gateway y Virtual Controller Gateway:** El Gateway de la red de almacenamiento (Opcional).
- **Host Netmask y Virtual Controller:** **Netmask** La máscara de red de la red de almacenamiento.

- **Host VLAN ID y Virtual Controller VLAN ID:** Si la red de almacenamiento se encuentra configurada como una VLAN, se debe introducir en este campo el VLAN ID. En cualquier otro caso el campo se debe dejar en blanco.
- **MTU:** Introducir un valor entre 1000 y 9000. Para la red de almacenamiento se recomienda un tamaño de MTU de 9000.

Ilustración 15 - Storage Network Settings 1

39. Haga click en la pestaña *IP Addresses* y configure las direcciones IP de ESXi (Host IP Address) y de la máquina virtual del controlador (Virtual Controller IP Address). Ambas direcciones deben estar dentro del rango de direcciones permitidas en la red de almacenamiento. Si es el primer nodo que se configura, se podrá indicar cualquier dirección IP siempre y cuando todos los nodos que se instalen en el mismo clúster acaben teniendo el mismo rango de direcciones. Una vez establecidos los valores se hará click en *Next*.

Temporary Host IP Address	Serial Number	Host IP Address	Virtual Controller IP Address
192.168.6.106	CZ20230DKH	192.168.7.106	192.168.7.107

Ilustración 16 - Storage Network Settings 2

40. El siguiente paso consistirá en configurar la interfaz de federación⁷. Si se ha desplegado algún host en la federación, estos campos podrán aparecer completados con opciones por defecto que no podrán ser cambiadas:

- **Federation vSwitch Name:** Se deberá elegir el vSwitch de **vCenter** que proporcione acceso a la interfaz de federación deseada. Si se trata del primer despliegue este campo vendrá completado por defecto y no se podrá modificar.
- **Virtual Controller Port Group Name:** Si se trata del primer despliegue este campo no se puede modificar. En otro caso, seleccionar el grupo de puertos de **vCenter** que da acceso a la interfaz de federación.
- **Virtual Controller Gateway:** El Gateway de la red de federación (Opcional).
- **Virtual Controller Netmask:** La máscara de red de la red de federación.
- **Virtual Controller VLAN ID:** Si la red de federación se encuentra configurada como una VLAN, se debe introducir en este campo el VLAN ID. En cualquier otro caso el campo se debe dejar en blanco.
- **MTU:** Introducir un valor entre 1000 y 9000. Para la red de federación se recomienda un tamaño de MTU de 9000.

The screenshot shows the 'Configure Federation Network Settings' window in the HPE SimpliVity Deployment Manager. The left sidebar lists various configuration steps, with 'Configure Federation Network Settings' currently selected. The main panel has a title bar and a subtitle: 'Specify the network settings for federation traffic between HPE OmniStack Virtual Controllers. In the IP Addresses tab, enter the IP addresses for one or more Virtual Controllers.' Below this, there are two tabs: 'Network Settings' and 'IP Addresses'. The 'IP Addresses' tab is active, displaying a form with the following fields: 'Federation vSwitch Name' (vSwitch1), 'MTU' (9000), 'Virtual Controller Port Group Name' (SVT_FedPortGroup), 'Virtual Controller Gateway' (Optional), 'Virtual Controller Netmask' (255.255.255.0), and 'Virtual Controller VLAN ID' (0-4094). At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Ilustración 17 - Federation Network Settings 1

41. Haga click en la pestaña *IP Addresses* y configure las direcciones IP de la máquina virtual del controlador (Virtual Controller IP Address). La dirección debe estar dentro del rango de direcciones permitidas en la red de federación. Si es el primer nodo que se configura, se podrá indicar cualquier dirección IP siempre y cuando todos los nodos que se instalen en el mismo clúster acaben compartiendo el mismo rango de direcciones. Una vez establecidos los valores se hará click en *Next*.

⁷ Las interfaces de federación y almacenamiento comparten los mismos NICs, sin embargo, son dos interfaces lógicas diferentes y por ello debemos configurarlas por separado.

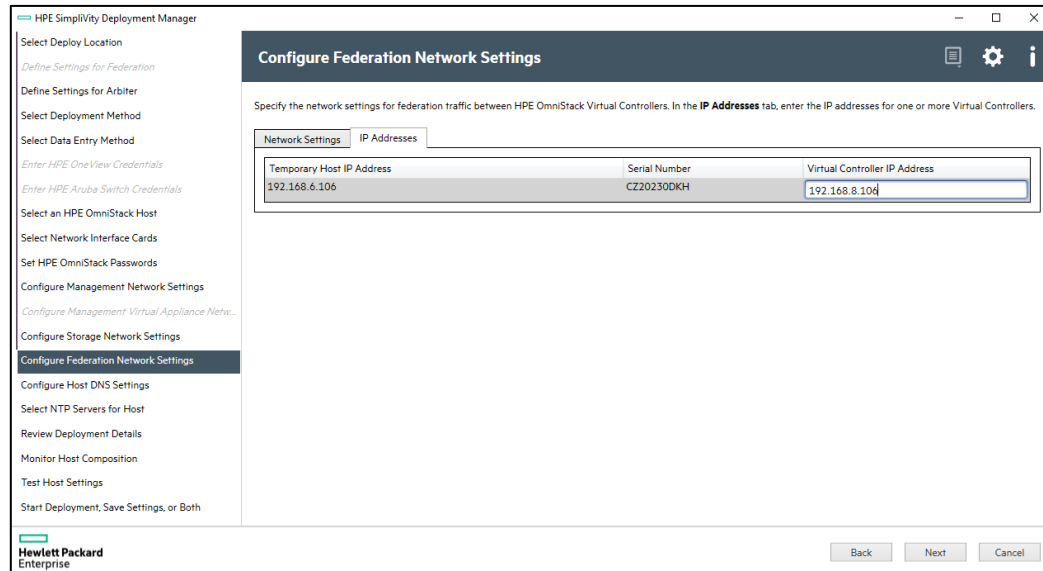


Ilustración 18 - Federation Network Settings 2

42. Configure la dirección y el dominio de los servidores DNS que empleará el nodo **HPE OmniStack Host**. Para ello se debe introducir la siguiente información:

- **Domain:** Introduzca el nombre de dominio con el sufijo de su DNS. Se trata del dominio de DNS configurado para la instalación de vCenter.
- **Search Domain:** Introduzca el dominio de búsqueda de su DNS para resolver dominios que no sean FQDN.
- **Primary Server:** Dirección IP del servidor DNS principal. La dirección del DNS que es capaz de resolver el nombre de dominio de vCenter. Este servidor DNS se debería haber configurado durante la instalación de **VMware vCenter Server**.
- **Secondary Server:** Dirección IP del servidor DNS secundario (Opcional)
- **Find and register the host by domain name:** Deje esta opción seleccionada si desea que el DNS realice una búsqueda inversa y los controladores virtuales se almacenen con su nombre de dominio en **vCenter**. Si la búsqueda inversa no se puede realizar, **HPE Deployment Manager** desplegará el controlador usando como nombre su dirección IP. Si su red no soporta búsquedas de DNS inversas deje esta opción sin marcar.

43. Una vez realizados estos pasos se hará click en *Next*.

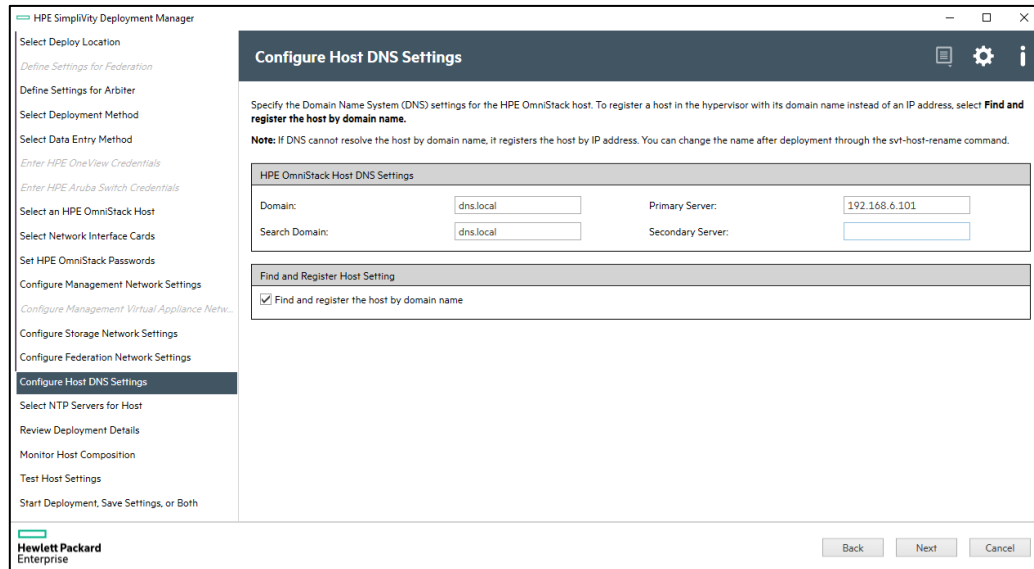


Ilustración 19 - DNS Settings

44. Selección de los servidores NTP. Por defecto aparecerá la siguiente lista de servidores:

- 0.us.pool.ntp.org
- 1.us.pool.ntp.org
- 2.us.pool.ntp.org
- 3.us.pool.ntp.org

45. Si la red de configuración tiene acceso a internet y no se quiere usar un servidor NTP alternativo, se recomienda seleccionar los servidores NTP por defecto y hacer click en *Add* para añadirlos a la lista de servidores seleccionados. En caso de usar un servidor alternativo, se debe introducir su dirección en el campo *Alternate Server* y hacer click en *Add*. Existe la posibilidad de añadir varios servidores NTP a la vez y seleccionar su prioridad mediante los botones *Up* y *Down*. Una vez añadidos los servidores deseados se hará click en *Next*.

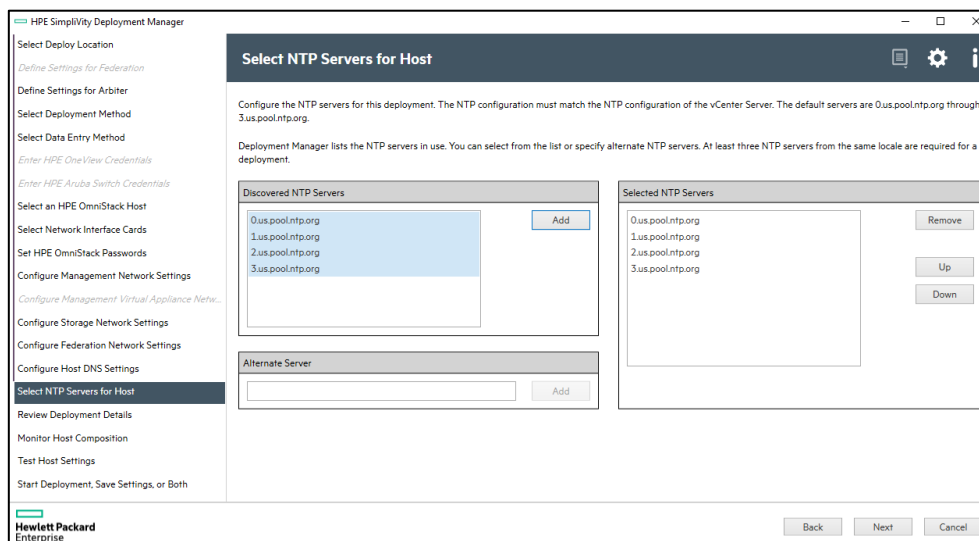


Ilustración 20 - NTP Servers

46. La siguiente pantalla mostrará un resumen de las opciones que se han seleccionado durante los pasos anteriores. Se deben revisar todos los datos introducidos y comprobar que son correctos. En caso de encontrar algún fallo se puede volver al paso en el que se introdujo el dato y corregirlo haciendo click en *Back* hasta llegar a la pantalla de configuración deseada. Una vez se haya comprobado que todos los datos sean correctos se hará click en *Next*.

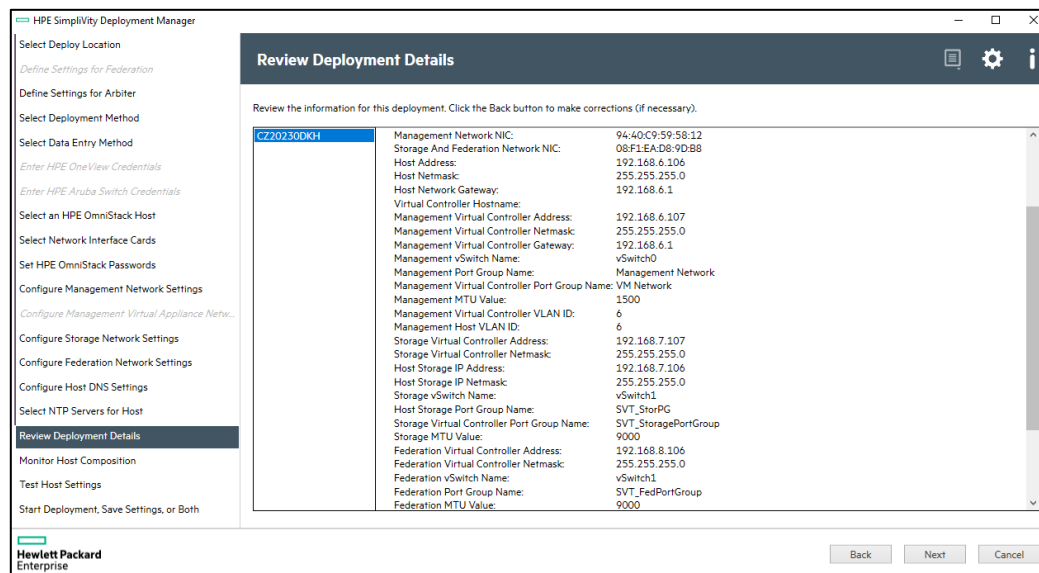


Ilustración 21 - Deployment Details

47. Haga click en *Start Test* y espere a que **HPE Deployment Manager** compruebe que todos los datos introducidos son correctos y que el despliegue se puede llevar a cabo. Si **HPE Deployment Manager** detecta un fallo, se mostrará un mensaje con los pasos a realizar para corregir dicho fallo e indicando la naturaleza del mismo.
48. Si algún test falla, el botón *Start Test* cambiará a *Rerun Test*. De esta forma se podrán realizar las correcciones necesarias en el entorno basándose en los errores mostrados y se podrá relanzar el test hasta que todos los pasos hayan obtenido un resultado satisfactorio. Una vez el test haya pasado satisfactoriamente se hará click en *Next*⁸.
49. Los tests que muestran el resultado **Caution** no impedirán el despliegue del nodo, sin embargo, **deberán ser corregidos antes de desplegar el nodo para prevenir posibles errores**.

⁸ Algunos de los tests pueden aparecer como *Skipped*. Esto es debido a que no aplican o no es preciso realizarlos para el despliegue que se ha configurado.

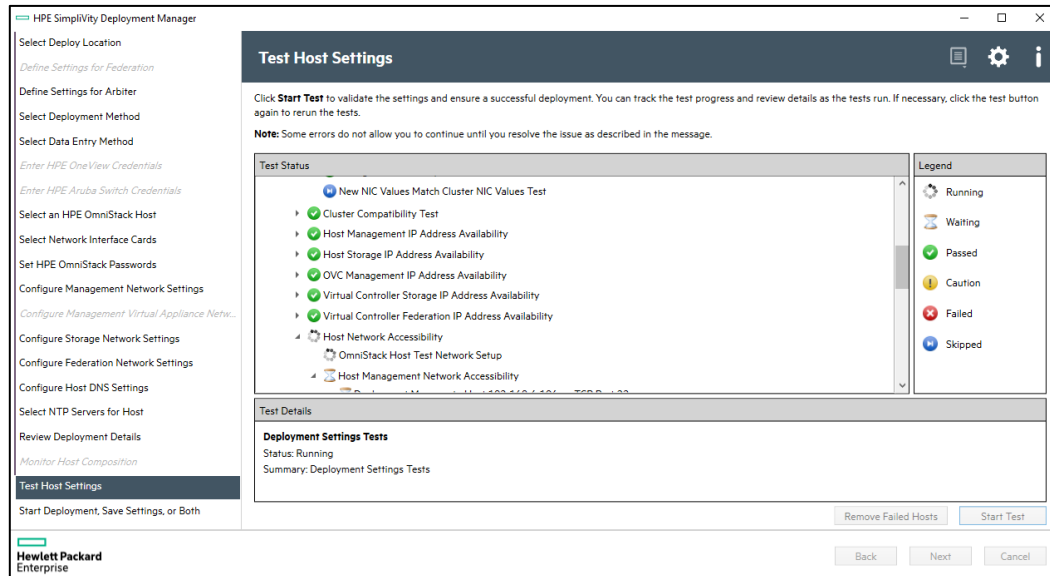


Ilustración 22 - Test Host

50. En la siguiente pantalla se realizará una de las siguientes acciones:

- Seleccionar ambas opciones para desplegar el nodo **HPE OmniStack Host** y guardar la configuración establecida en un archivo de configuración.
- Seleccionar solo *Start Deployment* si no se quiere guardar el fichero de configuración.
- Seleccionar solo *Save settings in a configuration file* si no se quiere realizar el despliegue. **Si solo se selecciona esta opción, el TOE no quedará instalado y por tanto habrá que volver a realizar toda la configuración nuevamente.** El archivo de configuración podrá usarse en futuras instalaciones como se indicó en el paso 7.

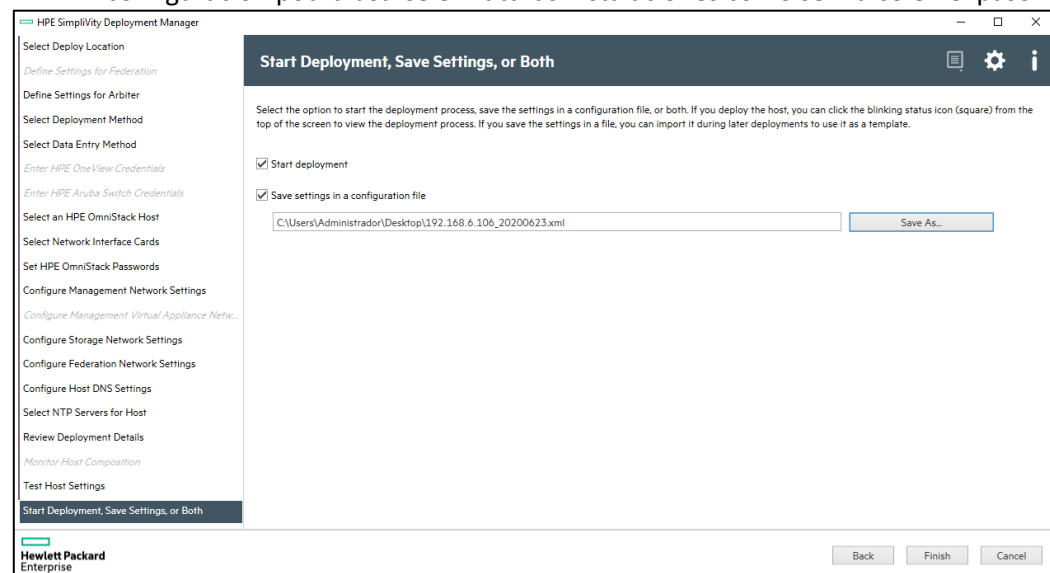


Ilustración 23 - Start Deployment

51. Una vez se haga click en *Finish*, comenzará el despliegue y se mostrará la ventana de despliegue de **HPE Deployment Manager**. Si se trata de la primera instalación, se debe esperar a que el despliegue del primer nodo finalice. En caso de que ya exista un nodo

desplegado en el clúster, se puede hacer click en *New Deployment* para comenzar el despliegue de otro nodo.

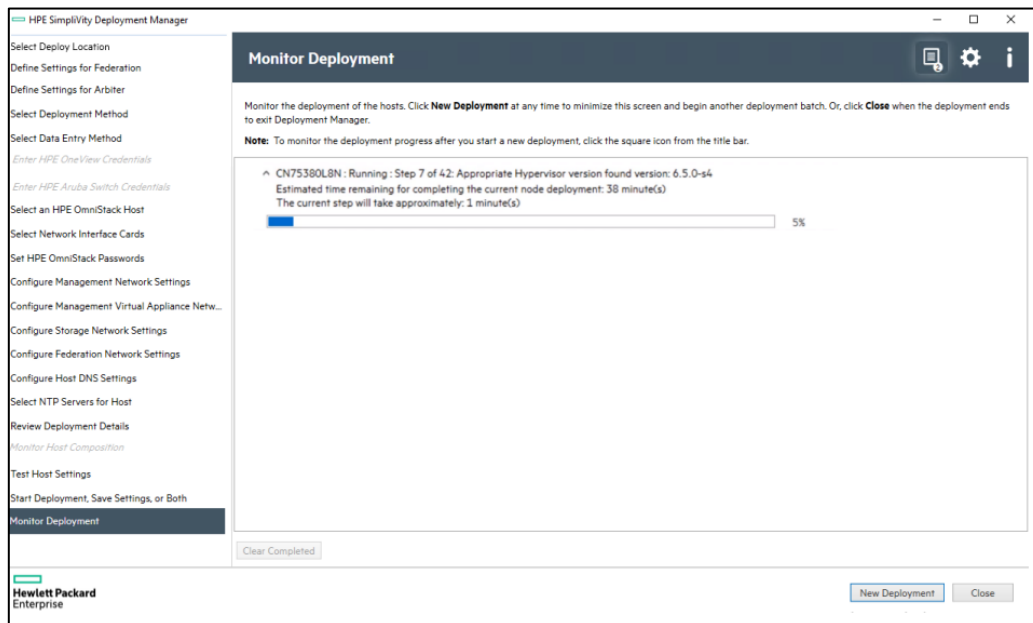


Ilustración 24 - Monitor Deployment

52. Una vez realizados estos pasos, **HPE SimpliVity** habrá quedado debidamente instalado en uno de los nodos **HPE Omnistack host** y aparecerá como un nuevo host en **VMware vCenter Server**. Se deberá comprobar que el primer nodo ha sido debidamente instalado entrando en la página web de administración de **VMware vCenter Server**. El TOE (*Virtual Controller*) debería aparecer como una nueva máquina virtual dentro de la página de administración de **VMware vCenter Server** tal y como se muestra en la siguiente imagen:

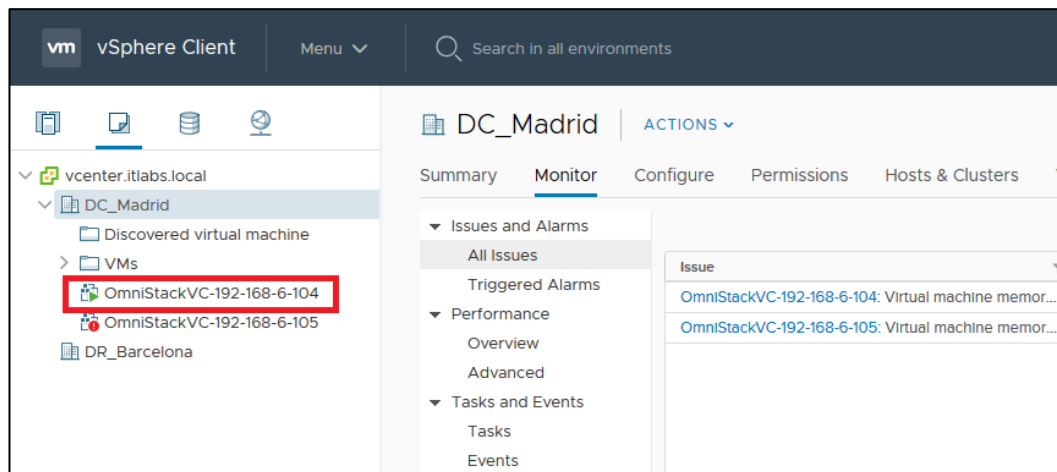


Ilustración 25 - Comprobación de la Instalación del Nodo

53. Por cada nodo que se despliegue en el sistema se debe comprobar que aparecer un nuevo controlador virtual en **VMware vCenter Server**.
54. Tras el despliegue del primer nodo, se debe proceder a desplegar el resto de nodos del clúster. El entorno de ejecución requiere que al menos dos nodos **HPE OmniStack Host** sean desplegados para cumplir los requisitos del entorno evaluado.

55. Para desplegar el segundo nodo dentro del mismo clúster se deberán repetir los pasos indicados previamente en esta sección. Una gran parte de los pasos de instalación aparecerán con valores autocompletados y otros serán omitidos por la interfaz de **HPE Deployment Manager**, por lo que durante la instalación simplemente se debe pasar al siguiente paso.
56. **Nota:** Tras la instalación existe la posibilidad de que **VMware vCenter Server** muestre una incidencia en cada uno de los Controladores virtuales desplegados indicando “*Virtual machine memory usage*” o en cada uno de los hosts indicando “*SimpliVity Virtual Controller using swap memory, error*”. Sin embargo, se trata de un bug de la interfaz de **VMware vCenter Server**, por lo que el error puede ser ignorado:

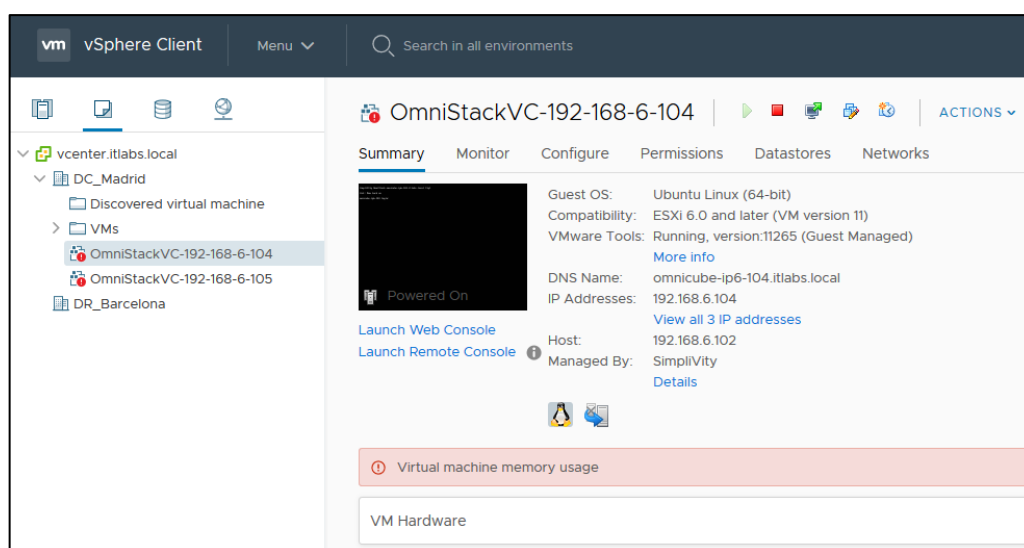


Ilustración 26 - Virtual Machine Memory Usage Error

57. Finalmente, una vez concluida la instalación se debe comprobar que la versión de **HPE SimpliVity** que ha sido instalada es la correcta. Para ello se llevarán a cabo los siguientes pasos:
- A través de **VMware vCenter Server** se accederá a la consola del nodo HPE Omnistack que ha sido instalado (Seleccionando el nodo y haciendo click en “*Launch Remote Console*”).
 - Una vez en la consola, se debe iniciar sesión en la máquina como el usuario administrador de **VMware vCenter Server** (E.g Administrator@vcenter.local), ya que este administrador tendrá el rol **administrator** dentro de la máquina.
 - Una vez iniciada la sesión se invocará el comando `svt-federation-show`, que mostrará el conjunto de todos los nodos de la federación. En esa lista, debemos fijarnos en la columna *Version* del nodo que acaba de ser instalado y verificaremos que la versión instalada coincide con la versión evaluada del producto.
 - En caso de que la versión no coincida con la versión evaluada del producto, se deberán seguir los pasos en la guía **HPE OmniStack 4.0.1 U1 for vSphere Upgrade Guide** para realizar una actualización del software del TOE a la versión evaluada. Los pasos de dicha guía son aplicables a la versión evaluada del TOE a pesar de que se mencione explícitamente la versión 4.0.1 en la misma. La guía será interpretada sustituyendo la versión 4.0.1 por la versión evaluada en los lugares donde aparezcan menciones a la versión del Software del Controlador HPE Omnistack.

5 FASE DE CONFIGURACIÓN

58. Una vez se hayan desplegado dos o más nodos **HPE OmniStack host** en el entorno en su versión correcta, se deberá realizar la siguiente configuración a través de **VMware vCenter Server** o los controladores virtuales para alcanzar la configuración evaluada:

- **Activación de HA en vCenter:** Para ello se accederá a la página de administración de **VMware vCenter Server** (vSphere Client) mediante un navegador usando la dirección IP del servidor de vCenter. Una vez autenticado en vCenter con un usuario administrador, se seleccionará el clúster en el que se encuentran los nodos que hemos activado y se accederá a *Configure -> Services -> vSphere Availability* tal y como se muestra en la siguiente imagen:

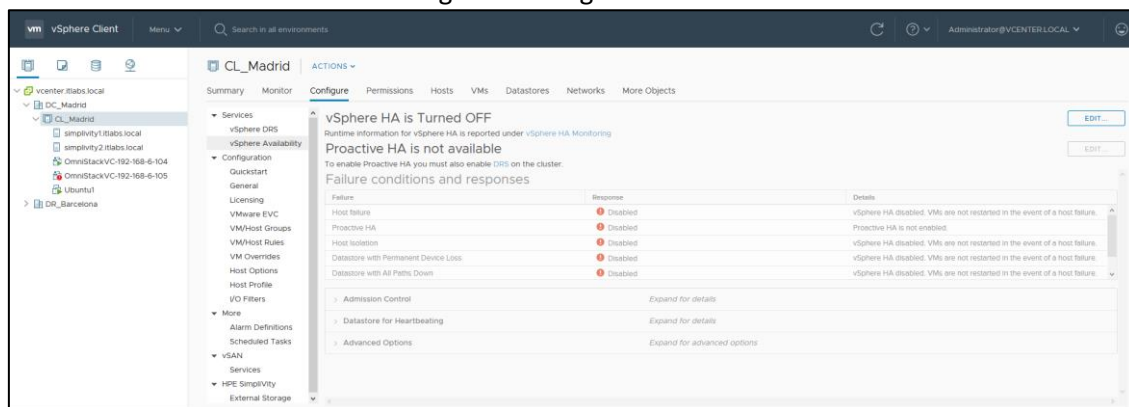


Ilustración 27 - Configuración de vSphere availability

59. Tras ello, se debe hacer click en *Edit*, lo que abrirá una nueva pantalla de configuración. En la nueva pantalla se hará click sobre el botón que indica *vSphere HA*, de forma que éste se volverá de color verde. Finalmente se seleccionará *OK*.

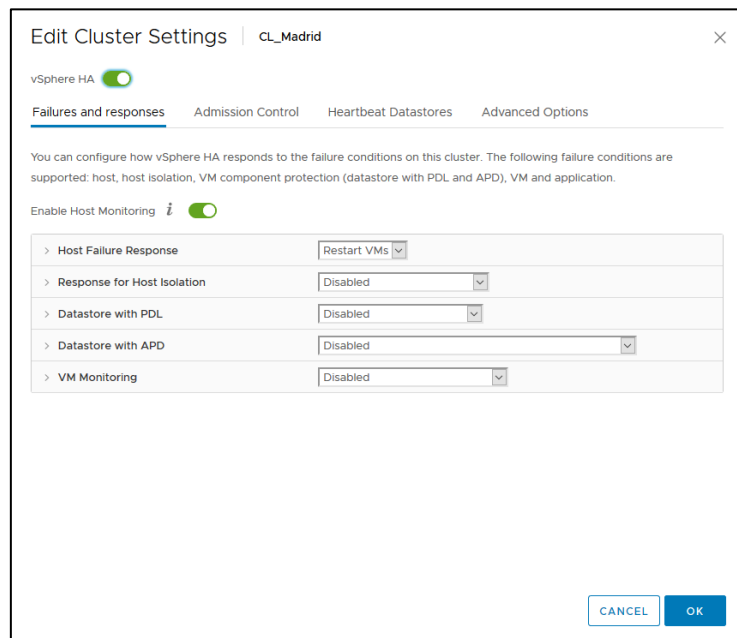


Ilustración 28 - Configuración del Cluster

60. **VMware vCenter Server** se encargará de asegurar la ejecución de las máquinas virtuales de cada uno de los nodos si el nodo falla.
- **Creación de políticas de copia de seguridad:** Se deberá crear una política de copias de seguridad que se aplicará más tarde a los almacenes de datos. De esta forma, todos los almacenes de datos que tengan esta política asignada realizarán copias de seguridad de sus máquinas virtuales siguiendo estas políticas.
61. Para configurar una política de datos se seleccionará el menú desplegable de **VMware vCenter Server** y se hará click en *HPE SimpliVity Federation*:

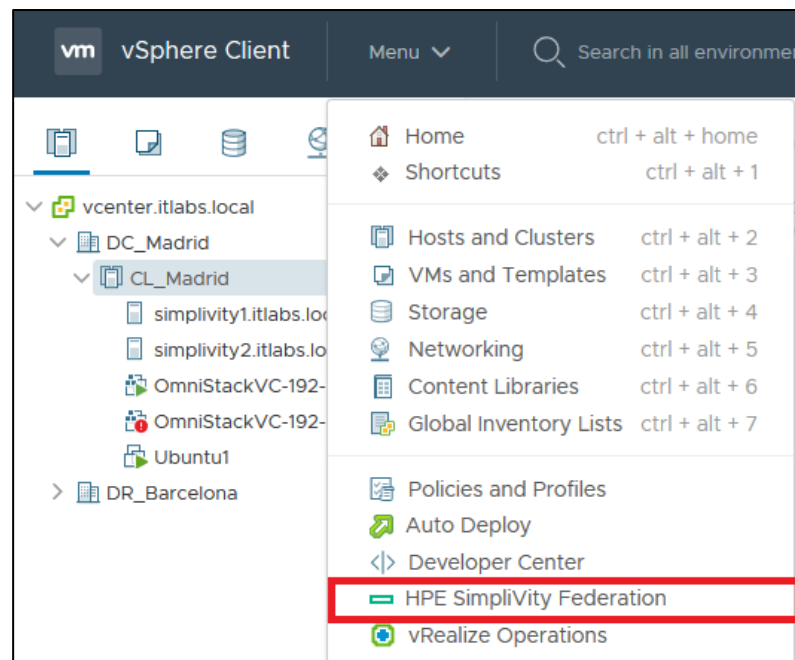


Ilustración 29 - Localización de "HPE SimpliVity Federation"

62. Desde la página de administración del Plug-in seleccionaremos *CREATE BACKUP POLICY*:

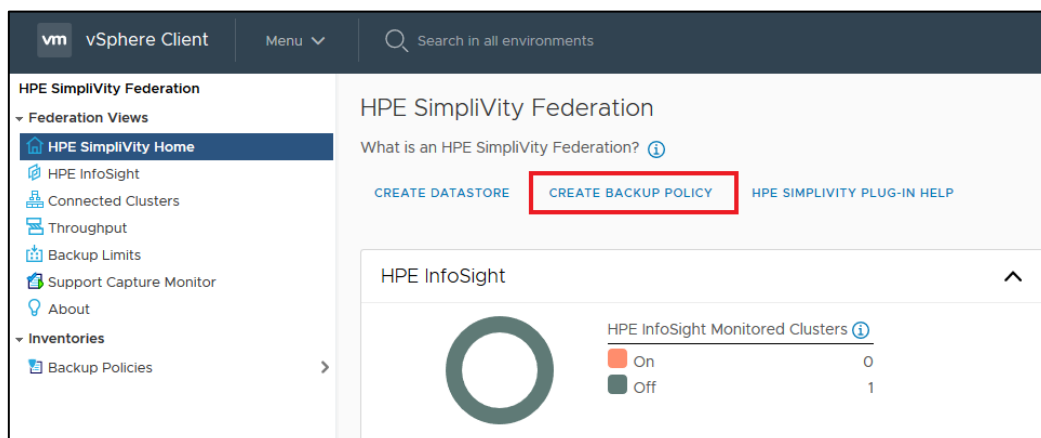


Ilustración 30 - Localización de "Create backup Policy"

63. Tras ello, se abrirá una nueva ventana de configuración que nos permitirá crear una nueva política de copia de seguridad:

Create Backup Policy

Backup policy name: Backup_Policy_1

+ ADD RULE - DELETE RULE EDIT RULE

☒	Frequency	Expiration Time	Destination	Backup Days	Application Consistent	Server Start Time	Server Stop Time
☒	1 hour	1 day	<local>	Every Day	No	00 : 00	00 : 00

☒ 1 1 rule

Hewlett Packard Enterprise

OK CANCEL HELP

Ilustración 31 - Creación de política de copia de seguridad

64. Estableceremos un nuevo nombre para la política que se va a crear y configuraremos las reglas que debe cumplir esta política.
65. Para añadir nuevas reglas se debe hacer uso del botón *ADD RULE*.
66. Una vez añadida una regla podremos modificarla seleccionándola y haciendo click en *EDIT RULE*. Mediante la edición de las reglas podremos configurar los siguientes campos:
 - **Frequency:** Indicará la frecuencia con la que se realizará una nueva copia de seguridad.
 - **Expiration Time:** Indica el tiempo de validez de las copias de seguridad. Una vez pasado este tiempo las copias se borrarán.
 - **Destination:** El clúster en el que se almacenarán las copias de seguridad.
 - **Backup Days:** Los días del mes o de la semana en los que se aplicará la política.
 - **Application Consistent:** El tipo de copia de seguridad. Podremos elegir entre copias de seguridad que mantengan o no el estado completo de ejecución de la máquina en el momento en el que se realizó la copia.
 - **Server Start Time:** Hora a partir de la cual el servidor comenzará a realizar copias de seguridad.
 - **Server Stop Time:** Hora a partir de la cual el servidor parará de realizar copias de seguridad.

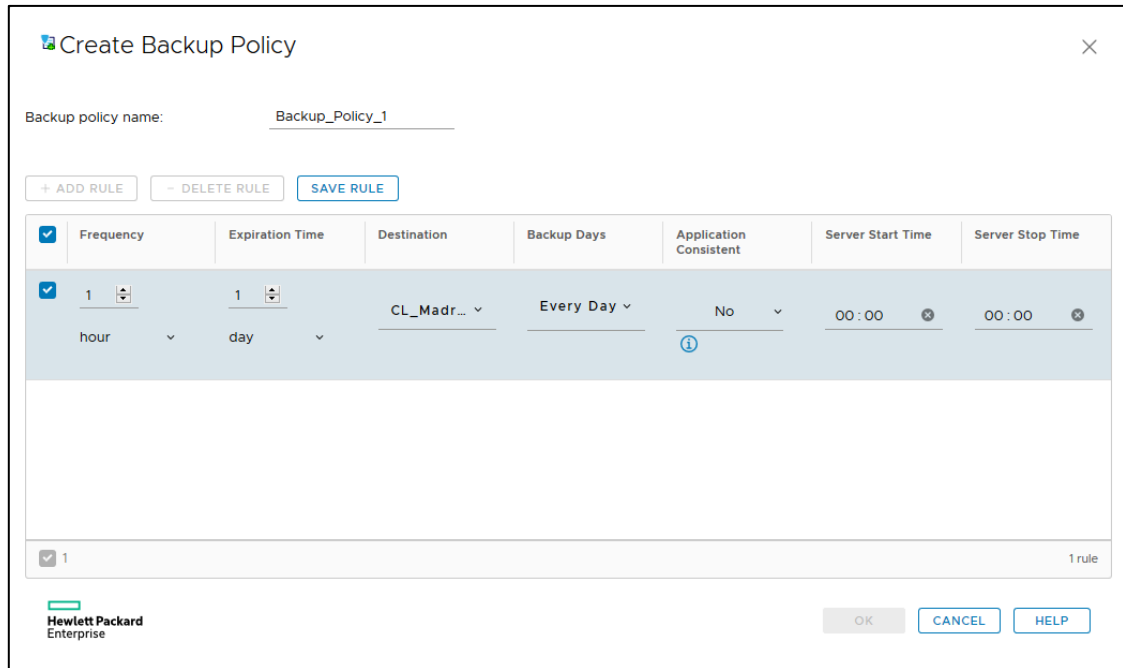


Ilustración 32 - Modificación de regla de backup

67. Una vez establecidas las reglas deseadas las guardaremos mediante el botón *SAVE RULE* y crearemos la política haciendo click en *OK*.

- **Creación de un almacén de datos SimpliVity:** Finalmente, se debe crear al menos un almacén de datos gestionado por **HPE SimpliVity** sobre el que se desplegarán las máquinas virtuales.

68. Para ello, desde vSphere Client se hará click derecho sobre el clúster que hemos creado durante la instalación, lo que desplegará una lista de opciones. En la lista de opciones seleccionaremos *All HPE SimpliVity Actions -> Create Datastore*:

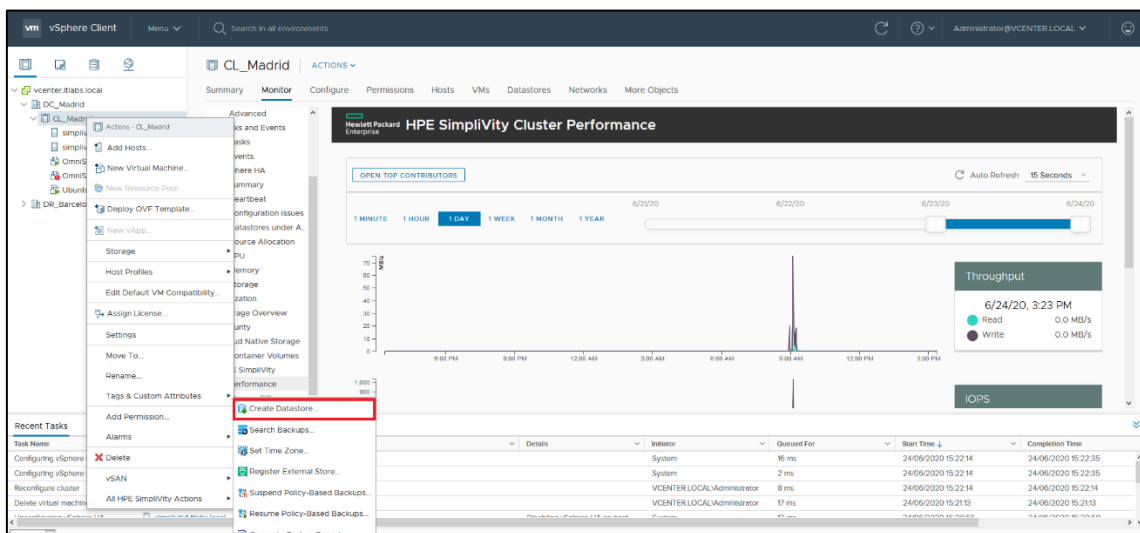


Ilustración 33 - Localización de "Create Datastore"

69. Se abrirá una nueva ventana de configuración en la que se deben rellenar los siguientes campos:

- **Cluster:** Elegiremos de la lista el nombre del clúster en el que se desplegaron los nodos **HPE OmniStack host**.
- **New Datastore name:** Introduciremos el nombre con el que se mostrará el almacén de datos.
- **Backup policy:** En caso de haber creado una política de copia de seguridad podremos escogerla aquí desde la lista presentada. Si no se quiere aplicar una política de copia de seguridad sobre el almacén de datos, seleccionaremos *Fixed Default Backup Policy*.
- **Size:** El tamaño que tendrá el almacén de datos. Dicho tamaño deberá ser seleccionado en función del almacenamiento total del que disponga el Hardware de HPE SimpliVity. El tamaño seleccionado podrá ser superior al que posea el hardware, sin embargo, se deberá tener en cuenta que el sistema presentará errores indicando un espacio insuficiente cuando ocupe el espacio de almacenamiento disponible.

The screenshot shows a 'Create Datastore' window with the following fields:

- Cluster:** CL_Madrid
- New datastore name:** DS_Madrid
- Backup policy:** Backup_Lince
- Size:** 3 TB

At the bottom left is the Hewlett Packard Enterprise logo. At the bottom right are three buttons: OK, CANCEL, and HELP.

Ilustración 34 - Creación del Datastore

70. Una vez realizados todos estos pasos tanto el entorno como el **HPE SimpliVity** habrán quedado debidamente configurados de manera segura y podrán comenzar a usarse.

- **Cambio de Contraseña del usuario svtcli:** Tras la instalación, el usuario debe realizar un cambio de contraseña para el usuario svtcli de cada nodo. Para ello se deben seguir los siguientes pasos:
 - Primero, se debe realizar una conexión por SSH o consola local al nodo de forma que se pueda acceder a la consola de administración desde una cuenta con permisos de administración o la propia cuenta svtcli.
 - Tras ello, se debe montar el sistema de archivos read-only como read-write:


```
sudo mount -o remount,rw /rortoot
```

```
sudo touch /rortoot/disable-root-ro
```
 - Se debe reiniciar el Controlador Virtual:


```
sudo reboot
```
 - Una vez reiniciado el Controlador Virtual, el usuario debe iniciar sesión nuevamente como el usuario svtcli y cambiar la contraseña mediante el siguiente comando:


```
sudo passwd svtcli
```

- Finalmente, se montará nuevamente el sistema de archivos como read-only y se reiniciará el Controlador Virtual:


```
sudo rm /disable-root-ro
sudo reboot
```
- **Configuración del tiempo de finalización de sesión (Opcional):** Por defecto, el TOE finalizará las sesiones de forma automática cuando transcurran 1680 segundos. Con el objetivo de modificar dicho tiempo de inactividad, se debe realizar la siguiente configuración:
 - Primero, se debe realizar una conexión por SSH o consola local al controlador virtual de forma que se pueda acceder a la consola de administración desde una cuenta con permisos de administración o la propia cuenta svtcli.
 - Tras ello, se debe montar el sistema de archivos read-only como read-write:


```
sudo mount -o remount,rw /roroot
sudo touch /roroot/disable-root-ro
```
 - Se debe reiniciar el Controlador Virtual:


```
sudo reboot
```
 - Una vez reiniciado el Controlador Virtual, el usuario debe iniciar sesión nuevamente como el usuario svtcli y modificar el archivo /etc/ssh/sshd_config.
 - El parámetro *ClientAliveInterval* dentro de dicho fichero indicará el número de segundos que deben transcurrir antes de que se finalice la sesión. Dicho parámetro puede ser modificado por el usuario para cambiar dicho intervalo.
 - Finalmente, se montará nuevamente el sistema de archivos como read-only y se reiniciará el Controlador Virtual:


```
sudo rm /disable-root-ro
sudo reboot
```
- **Configuración SSH:** Se deben realizar los siguientes pasos para configurar las ciphersuites y versiones de SSH que debe aceptar el TOE en la configuración evaluada:
 - Primero, se debe realizar una conexión por SSH o consola local al controlador virtual de forma que se pueda acceder a la consola de administración desde una cuenta con permisos de administración o la propia cuenta svtcli.
 - Tras ello, se debe montar el sistema de archivos read-only como read-write:


```
sudo mount -o remount,rw /roroot
sudo touch /roroot/disable-root-ro
```
 - Se debe reiniciar el Controlador Virtual:


```
sudo reboot
```
 - Una vez reiniciado el Controlador Virtual, el usuario debe iniciar sesión nuevamente como el usuario svtcli y aplicar la siguiente configuración:
 - En el archivo /mnt/etc/ssh/sshd_config se debe establecer la siguiente configuración sustituyendo la configuración presente:


```
Ciphers      aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com

MACs         hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com

HostKeyAlgorithms rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-
nistp256
```

```
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-
nistp384,ecdh-sha2-nistp521,curve25519-sha256@libssh.org
```

- Finalmente, se montará nuevamente el sistema de archivos como read-only y se reiniciará el Controlador Virtual:

```
sudo rm /disable-root-ro
```

```
sudo reboot
```

5.1 ACTUALIZACIONES

71. Los pasos a seguir para llevar a cabo una actualización del software vienen descritos en la guía **HPE OmniStack 4.0.1 U1 for vSphere Upgrade Guide**. Los pasos de dicha guía son aplicables a la versión evaluada del TOE (4.2) a pesar de que se mencione explícitamente la versión 4.0.1 en la misma. La guía será interpretada sustituyendo la versión 4.0.1 por 4.2 en los lugares donde aparezcan menciones a la versión del Software del Controlador HPE Omnistack. Estos pasos son los siguientes:
72. El primer paso será descargar la actualización de software del **HPE Omnistack**. Para ello, se accede a la url <http://www.hpe.com/software/hpesoftwarecenter>, se introducen las credenciales de acceso, se accede a la sección *Software Updates > Updates*, se especifica el producto que se desea actualizar y se descarga el fichero comprimido que se corresponde a la actualización que se quiere llevar a cabo, que se extrae en una ubicación accesible.
73. El siguiente paso es descargar el nuevo software para el ESXi. Para ello, en la sección *Search Software Updates* se filtra por el nombre de producto "*HPE SimpliVity custom ESXi*". Tras esto se localiza la versión que se desea descargar y se hace click en "*Update*". Esto descarga un archivo que se extrae en la misma carpeta donde se extrajo el paquete de **HPE Omnistack**.



Ilustración 35 - Captura de la guía para descargar la actualización

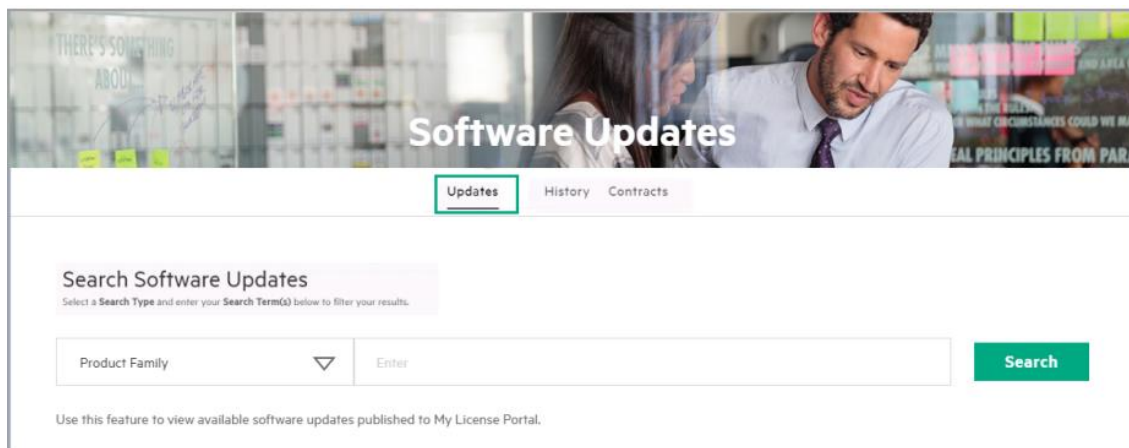


Ilustración 36 - Captura de la guía para descargar la actualización

74. El siguiente paso es actualizar el **Arbiter**, que tiene que tener la misma versión que el **HPE Omnistack**. Para ello hay que mandar el instalador de la versión del **Arbiter** al host que lo ejecuta, hacer doble click en el instalador y, al llegar a la ventana de “*Setup Type*”, se selecciona “*Complete*” y se da a instalar. En caso de que haya ficheros en uso, se selecciona la opción “*Do not close applications*”. Una vez hecho esto, se reinicia el host para completar su instalación.
75. Para actualizar el software del **HPE Omnistack**, es necesario que los ficheros con el siguiente nombre estén en el mismo directorio: *simplivity-upgrade-manager-x.x.x.exe* y *SimpliVity-OmniCube-Software-revA-x.x.x.tar*. el siguiente paso es hacer doble click en el ejecutable del *Update Manager* para abrir la pantalla de login. Una vez hecho esto, se introduce la dirección IP del **vCenter Server**, las credenciales de administrador y se hace click en *Login*. Tras esto, se aceptan tanto el **certificado** como los **prerrequisitos de actualización** y las **buenas prácticas**.

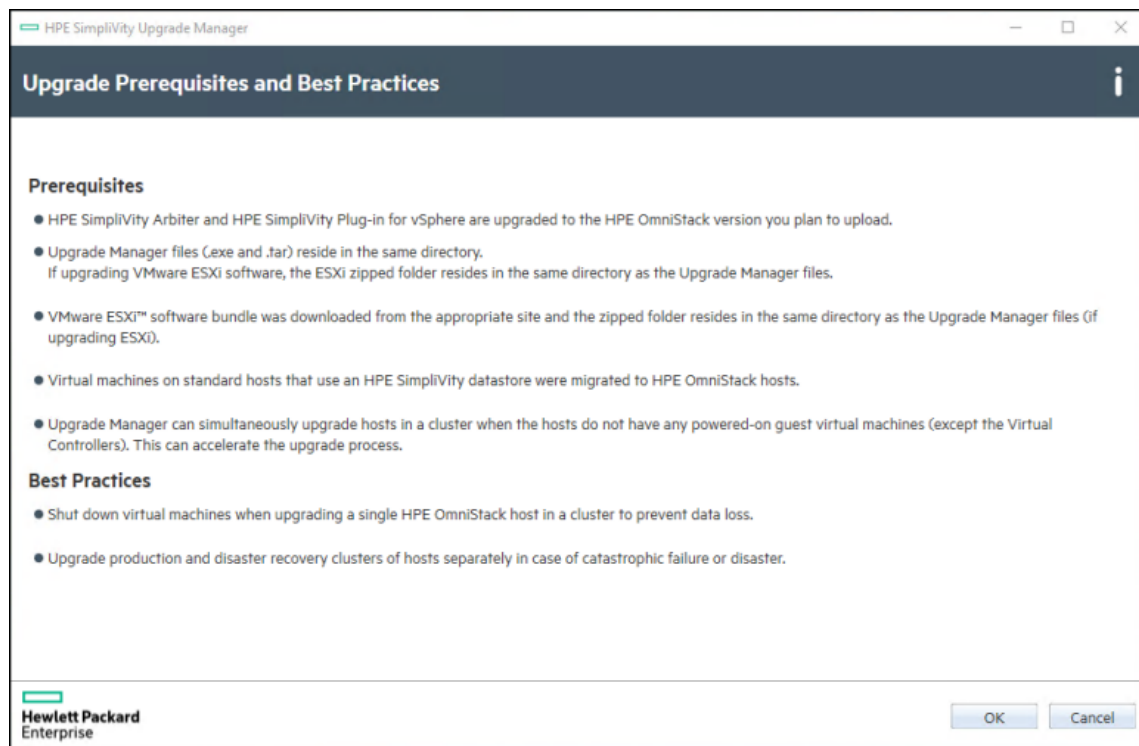


Ilustración 37 - Captura de la guía para aceptar prerequisites y buenas prácticas

76. Una vez aceptado lo anterior, aparece la pantalla de *HPE SimpliVity Software Upgrade*. En esa pantalla se seleccionan los hosts que se desean actualizar. Para ello, deben estar en el estado “Ready for upgrade”:

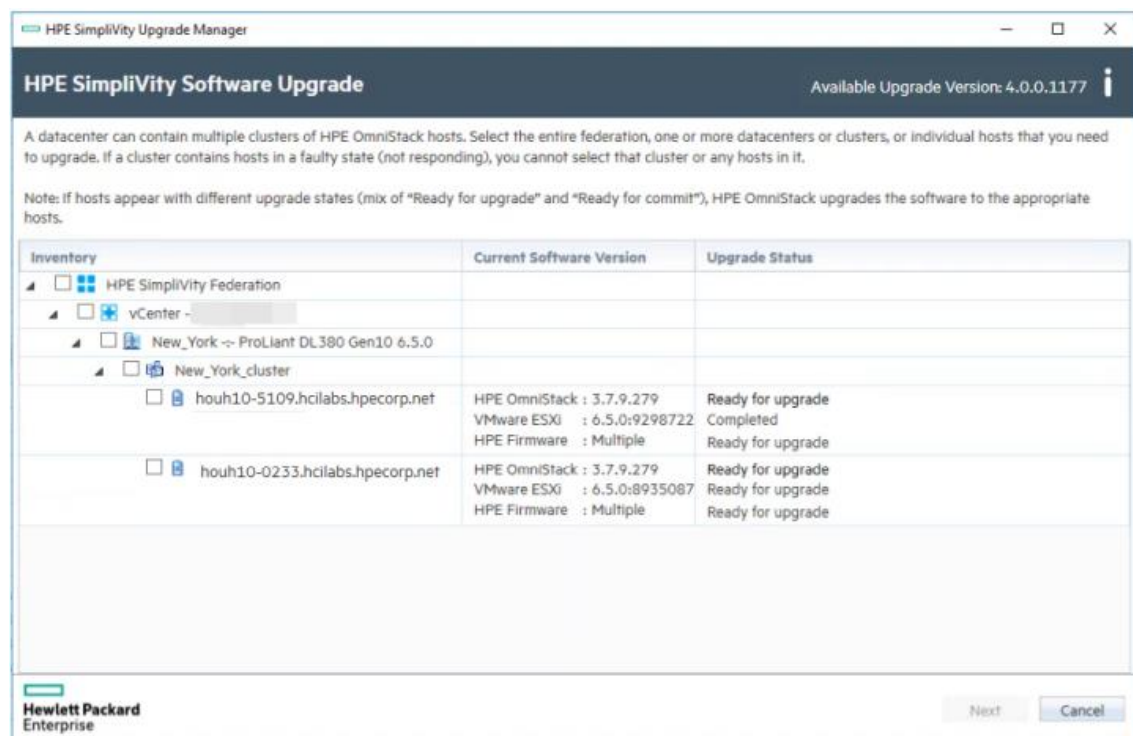


Ilustración 38 - Captura de la guía para ver estado previo a la actualización

77. Una vez seleccionados los elementos a actualizar, se accede a una pantalla en la que permite seleccionar el software a actualizar:

Select Software to Upgrade Available Upgrade Version: 4.0.0.1177

Select the version for each product you want to upgrade. You can upgrade the HPE OmniStack software, VMware ESXi software, HPE SimpliVity firmware, or all three products on the selected hosts.

vCenter Server	Cluster	Selected Hosts	HPE OmniStack	VMware ESXi	HPE Firmware
	New_York_cluster	houh10-0233.hcilabs.hp	4.0.0.1177	6.5.0:9298722:2...	2019090301:201...

Hewlett Packard Enterprise

Back Next Cancel

Ilustración 39 - Captura de la guía para seleccionar el software a actualizar

78. En caso de actualizar alguno de los componentes, se accede al apartado de “Enter iLO Credentials to Upgrade Firmware”, en el que se solicita la dirección IP del iLO para cada uno de los hosts a actualizar.

Enter iLO Credentials to Upgrade Firmware Available Upgrade Version: 4.0.0.1177

Upgrade Manager needs access to the Integrated Lights Out (iLO) remote management system to upgrade the firmware on the hosts. Enter the iLO IP address and credentials for each host.

vCenter Server	Cluster	Host	iLO IP Address	User Name	Password
	New_York_cluster	houh10-5109.hcilabs.hpeco	192.0.2.0		
	New_York_cluster	houh10-0233.hcilabs.hpeco	198.51.100.0		

Hewlett Packard Enterprise

Back Next Cancel

Ilustración 40 - Captura de la guía para introducir la iLO IP

79. Una vez hecho eso, se accede a una pantalla en la que se determina si la configuración está lista para ser actualizada.

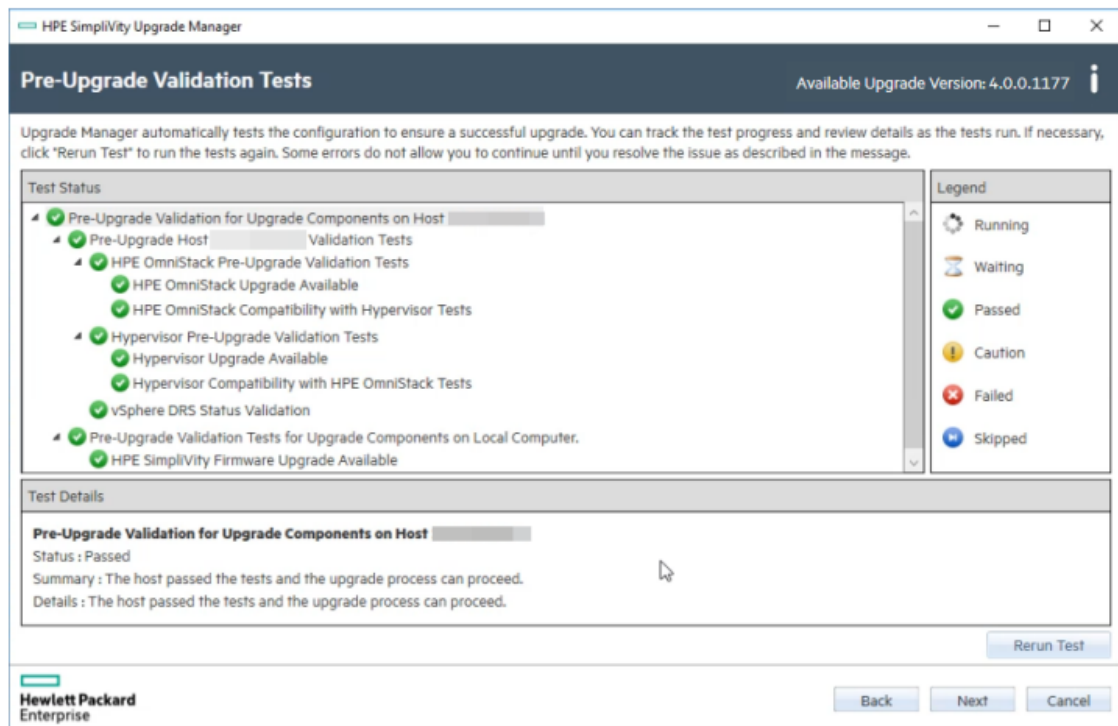


Ilustración 41 - Captura de la guía para los tests previos a la actualización

80. En caso de que todos los tests hayan pasado con éxito, se accederá a la pantalla de “*Ready to Upgrade*”, en la que se hace click en el botón “*Finish*” para subir los paquetes de software y comenzar el proceso de actualización.

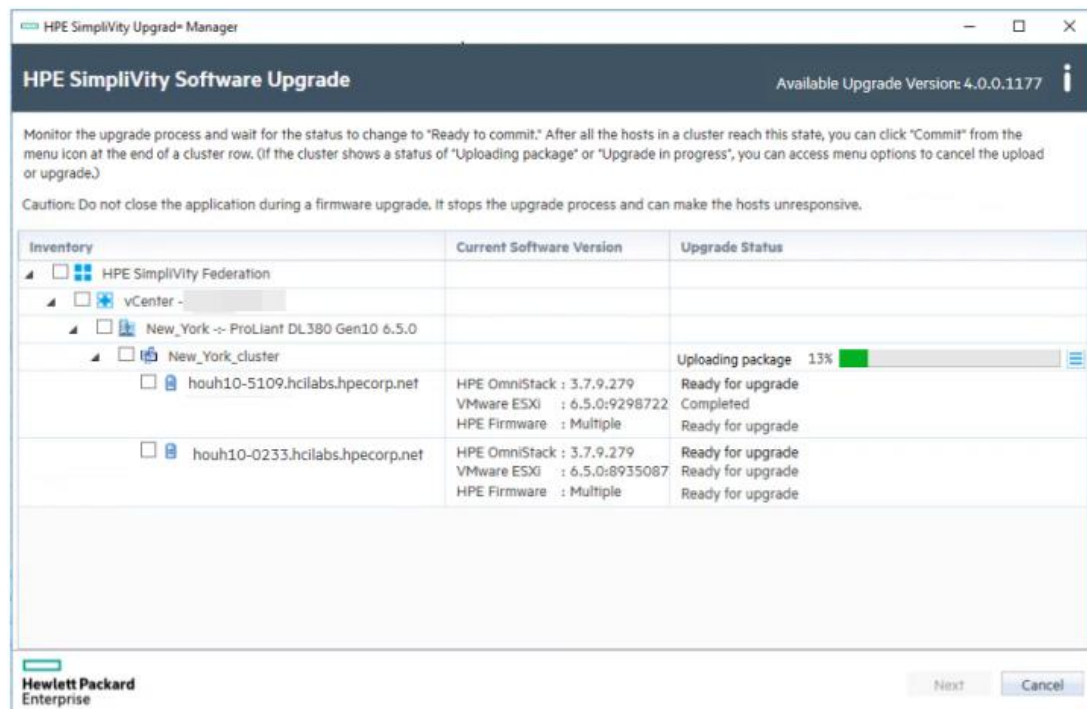


Ilustración 42 - Captura de la guía para seguir el proceso de actualización

81. Una vez completado el proceso, el estado se actualiza a *“Ready for commit”*. Al alcanzar este estado en todos los elementos actualizados, se hace click en *“Commit”* (anterior botón *“Next”*) para completar el proceso de actualización.

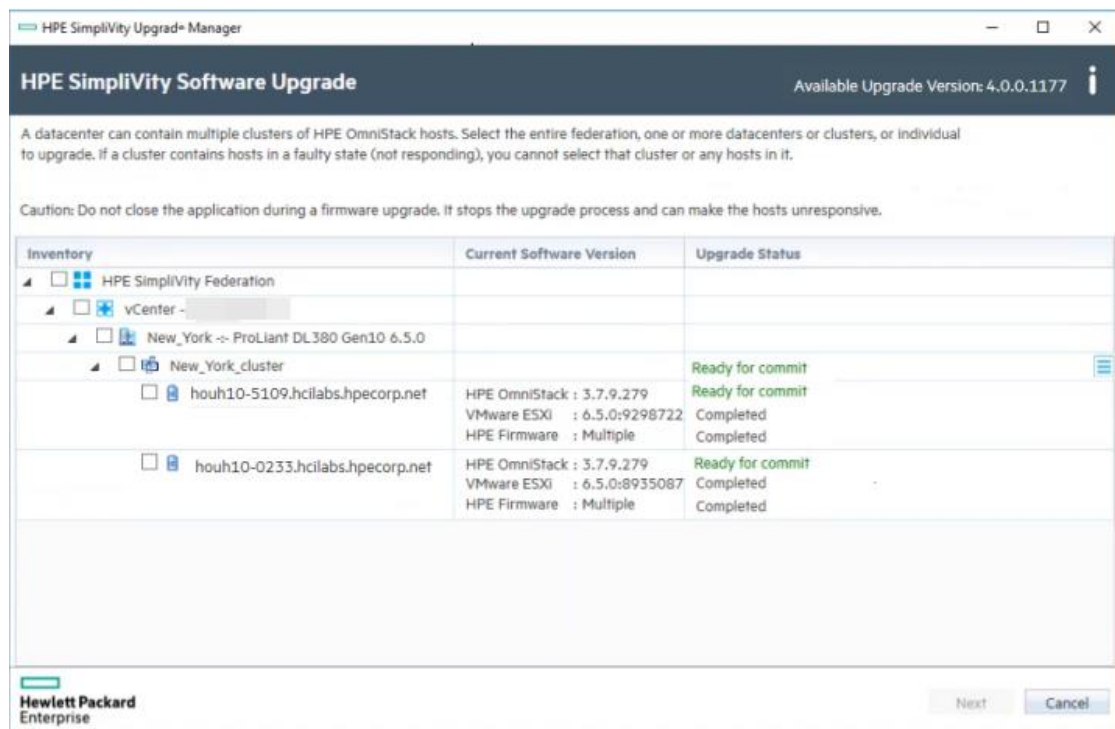


Ilustración 43 - Captura de la guía con actualización del estado

82. Una vez hecho esto, el estado pasa a *“Completed”* y se cierra el instalador.

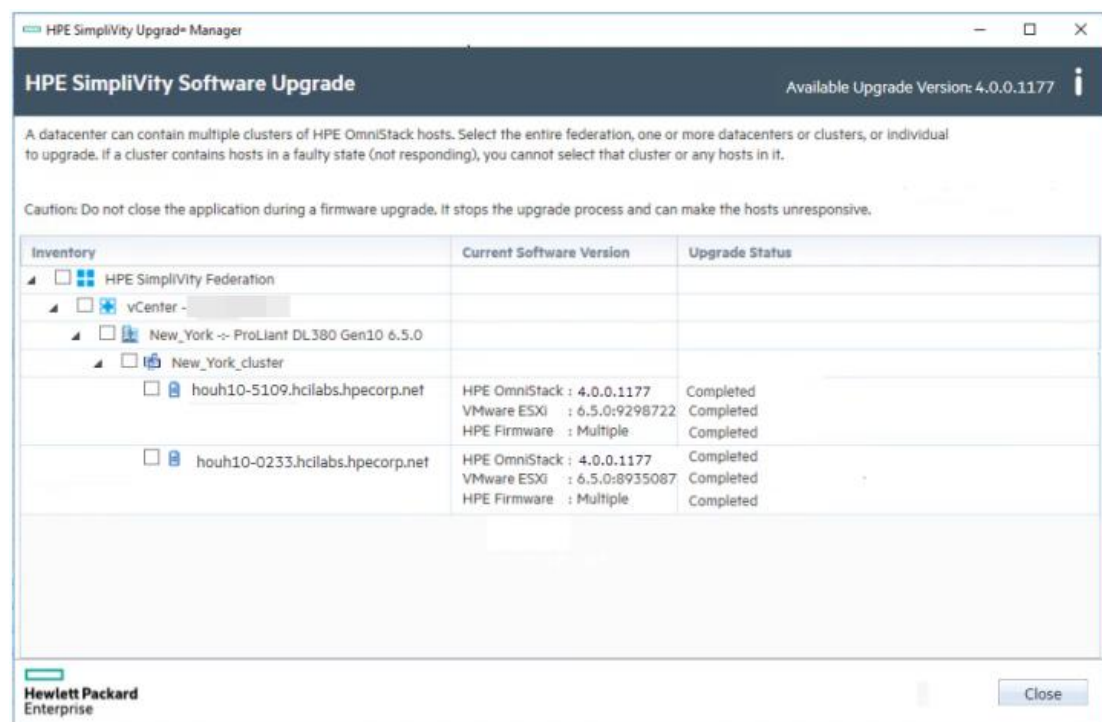


Ilustración 44 - Captura de la guía con las actualizaciones completadas

5.2 ALTA DISPONIBILIDAD

83. El proceso de habilitar el servicio de alta disponibilidad del TOE se describe entre los pasos 58 y 67 de la guía. El funcionamiento de este servicio consiste en crear copias de seguridad periódicas que permitirán la replicación de una máquina que haya fallado en otro de los nodos que haya desplegados.

6 FASE DE OPERACIÓN Y MANTENIMIENTO

6.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN

84. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es la responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

- **Protección Física:** El TOE no ofrece medidas de protección físicas ni de su red de almacenamiento. Por tanto, se asume que la red de almacenamiento es una red aislada que solo interconectará las interfaces de almacenamiento de los nodos HPE OmniStack Host y que se encontrará protegida por otras medidas de seguridad físicas. De igual forma, los nodos HPE OmniStack Host deben encontrarse en un entorno donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
- **Administración confiable:** El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
- **Integridad de la plataforma:** La plataforma hardware no debe haber sido comprometida con anterioridad a la instalación del producto de hiperconvergencia. Esta comprobación se llevará a cabo como parte del proceso de recepción del TOE, observando que el paquete entregado no presenta señales de haber sido abierto.
- **Actualizaciones periódicas:** El administrador será responsable de que el software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- Se realizarán comprobaciones periódicas del hardware del dispositivo para asegurar que ha sido manipulado.
- Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
- Los administradores deben eliminar toda la información residual sensible que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.
- Los auditores se encargarán de examinar de forma periódica los registros de auditoría buscando eventos específicos relacionados con los cambios de la configuración del sistema y que puedan indicar que éste ha sido comprometido.
- Las funciones de administración del producto serán llevadas a cabo exclusivamente utilizando el **Plug-In HPE SimpliVity Plug-in for VSphere Client**, la interfaz de administración de SSH o la consola CLI. Los usuarios no deben utilizar la interfaz **HPE OmniStack REST API** para realizar acciones de administración del dispositivo de forma manual.
- Realización de copias de seguridad automáticas de la información gestionada por la plataforma software hiperconvergente, de forma que los datos puedan ser recuperados en caso de fallo.
- Las tareas que requieren una gran carga de operaciones de lectura/escritura, como la eliminación de una gran cantidad de máquinas virtuales o la realización de copias de seguridad, deben realizarse de forma separada y controlada, de manera que no se produzca una sobrecarga en las operaciones de lectura/escritura. Si se produce dicha sobrecarga, existe la posibilidad de que se alcance el tiempo máximo de espera

de **VMware vCenter Server** (20 minutos) y que la operación sea cancelada. Para evitar estos posibles errores se deben seguir las siguientes recomendaciones:

- Antes de iniciar tareas que generen una alta actividad de lectura/escritura se comprobará que no se está llevando a cabo otra tarea similar.
- Si se inicia una de estas tareas se debe esperar a que dicha tarea termine antes de comenzar la siguiente.
- En caso de que se produzca un error debido a que se ha alcanzado el tiempo máximo de espera se planificará la tarea para un periodo de tiempo en el que se espere una carga reducida de las operaciones de lectura/escritura.

85. Con el fin de prevenir que los administradores escojan contraseñas inseguras, estas deben de cumplir con los siguientes requisitos:

- Deberán observarse y tenerse en cuenta las recomendaciones expuestas en la guía *CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40*.
- Las contraseñas deben de tener una longitud recomendada de 15 caracteres.
- Deben de estar compuestas por una combinación de caracteres pertenecientes, al menos, a 3 o 4 de los siguientes grupos de caracteres: letras en minúscula, letras en mayúscula, números y los caracteres especiales: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")".

6.2 INTERPRETACIÓN DE LAS GUÍAS

86. Durante la fase de operación e instalación del TOE se hará uso de este propio documento y de las guías identificadas en la sección **2.2 Identificación de las Guías de Uso, Instalación y Configuración Seguras del TOE** de la declaración de seguridad **Hiperconvergencia HPE SimpliVity Declaración de Seguridad** en su versión **1.6**.

87. Sin embargo, se deben seguir las siguientes pautas a la hora de interpretar la información encontrada en dichas guías:

- Los pasos indicados en este propio documento serán los pasos a seguir para realizar la instalación y configuración segura del TOE, sirviendo la guía **HPE OmniStack 4.0.1 U1 for vSphere Deployment Guide** como un documento de apoyo.
- La información presentada en este documento tendrá preferencia respecto a la presentada en el resto de guías.
- La versión del producto a la que hacen referencia las guías incluidas en la declaración de seguridad es la versión **4.0.1U1**. Sin embargo, la versión evaluada será la versión **4.2**. Las guías deberán ser interpretadas como si hiciesen referencia a la versión **4.2**, sustituyendo la versión **4.0.1U1** por **4.2** cuando se haga referencia a la misma.

7 REFERENCIAS

- [HPE.1] “HPE OmniStack 4.0.1 U1 for vSphere Administration Guide”, P00118-407/November 2020
- [HPE.2] “HPE OmniStack 4.0.1 U1 Command Reference Guide”, P00119-407/November 2020
- [HPE.3] “HPE OmniStack 4.0.1 U1 for vSphere Deployment Guide”, P00121-407/November 2020
- [HPE.4] “HPE OmniStack 4.0.1 U1 for vSphere Upgrade Guide”, P00126-407/November 2020
- [CCN.1] “CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40”, 2018
- [CCN.2] “CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad”, 2017
- [CCN.3] “CCN-STIC 836 Seguridad en VPN”, 2017

8 ABREVIATURAS

AES	Advanced Encryption Standard
CCN	Centro Criptológico Nacional
CLI	Command Line Interface
CPSTIC	Catálogo de productos de Seguridad TIC
CSI	Container Storage Interface
DH	Diffie – Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
FQDN	Fully Qualified Domain name
GCM	Galois/Counter Mode
HPE	Hewlett Packard Enterprise
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
RSA	Rivest, Shamir y Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell Protocol
STIC	Seguridad de Tecnologías de Información y Comunicación
TOE	Target of Evaluation
TLS	Transport Layer Security Protocol
VLAN	Virtual Local Area Network

