Etapa 1. Prepare la actualización

Upgrade controllers

NetApp
February 22, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap-systems-upgrade/upgrade-arl-auto-affa900/stage_1_index.html on February 22, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Etapa 1. Prepare la actualización . . . 1
Descripción general . . . 1
Verifique la actualización de hardware . . . 1
Prepare los nodos para la actualización . . . 1
Gestione el cifrado del almacenamiento con el gestor de claves incorporado . . . 6

Etapa 1. Prepare la actualización

Descripción general

Durante la etapa 1, verifique que tiene el hardware correcto para la actualización, ejecute comprobaciones previas y, si es necesario, corrija la propiedad de agregado. También registra cierta información si gestiona el cifrado de almacenamiento mediante el administrador de claves incorporado y puede optar por desactivar las relaciones de SnapMirror.

Pasos

1. "Verifique la actualización de hardware"
2. "Prepare los nodos para la actualización"
3. "Gestione el cifrado del almacenamiento mediante el gestor de claves incorporado"

Verifique la actualización de hardware

Antes de iniciar la actualización, compruebe que dispone del hardware correcto para la actualización. En función de la actualización, para cada par de alta disponibilidad que vaya a actualizar, debe tener dos módulos de controladora o dos módulos de controladora y dos módulos NVRAM. Si faltan piezas, póngase en contacto con el soporte técnico o con su representante de ventas de NetApp para obtener ayuda.

Si está actualizando…	Usted debe tener…
AFF A220 configurado como ASA para ASA A150	Dos módulos de controladora
AFF A220, AFF A200 o AFF C190 a AFF A150	Dos módulos de controladora
FAS2620 o FAS2720 a FAS2820	Dos módulos de controladora
AFF A700 configurado como ASA para ASA A900	Dos controladoras y dos módulos NVRAM
AFF A700 a AFF A900	Dos controladoras y dos módulos NVRAM
FAS9000 hasta FAS9500	Dos controladoras y dos módulos NVRAM

Prepare los nodos para la actualización

El proceso de reemplazo de la controladora comienza con una serie de comprobaciones previas. También se recopila información sobre los nodos originales para usar más adelante del procedimiento y, si es necesario, determinar el tipo de unidades de cifrado automático que se están usando.

Pasos

1. Enumere la versión del firmware del Service Processor (SP) o de la controladora de gestión de la placa base (BMC) que se ejecuta en la controladora anterior:

   ```
   service-processor show
   ```

Compruebe que tiene una versión de firmware de SP o BMC compatible:

La controladora anterior	SP o BMC	Versión de firmware mínima
AFF A220	BMC	11.9P1
AFF A200	SP	5.11P1
C190 de AFF	BMC	11.9P1
FAS2620	SP	5.11P1
FAS2720	BMC	11.9P1

2. Para iniciar el proceso de sustitución de la controladora, introduzca el siguiente comando en el modo de privilegio avanzado de la línea de comandos de ONTAP:

   ```
   set -privilege advanced
   ```

   ```
   system controller replace start -nodes node_names
   ```

   Verá una salida similar a la siguiente:

   ```
   Warning:
   1. Current ONTAP version is 9.x

   2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
   and charge them if they are not. You need to physically check the new
   nodes to see if the NVMEM or NVRAM  batteries are charged. You can check
   the battery status either by connecting to a serial console or using
   SSH, logging into the Service Processor (SP) or Baseboard Management
   Controller (BMC) for your system, and use the system sensors to see if
   the battery has a sufficient charge.

   Attention: Do not try to clear the NVRAM contents. If there is a need to
   clear the contents of NVRAM, contact NetApp technical support.

   3. If a controller was previously part of a different cluster, run
   wipeconfig before using it as the replacement controller.

   Do you want to continue? {y|n}: y
   ```

3. Seleccione `y`. Verá la siguiente salida:

   ```
   Controller replacement operation: Prechecks in progress.
   Controller replacement operation has been paused for user intervention.
   ```

   Durante la fase de comprobaciones previas, el sistema ejecuta la siguiente lista de comprobaciones en segundo plano.

Comprobación previa	Descripción
Comprobación del estado del clúster	Comprueba todos los nodos del clúster para confirmar que están en buen estado.
Comprobación del estado de reubicación de agregados	Comprueba si ya hay una reubicación de agregados en curso. Si hay otra reubicación de agregado en curso, la comprobación falla.
Comprobación del nombre del modelo	Comprueba si los modelos de controlador son compatibles con este procedimiento. Si los modelos no son compatibles, la tarea falla.
Comprobación de quórum de clúster	Comprueba que los nodos que se van a sustituir tengan quórum. Si los nodos no están en quórum, la tarea falla.
Comprobación de la versión de la imagen	Comprueba que los nodos que se reemplazan ejecuten la misma versión de ONTAP. Si las versiones de la imagen ONTAP son diferentes, la tarea fallará. Los nodos nuevos deben tener la misma versión de ONTAP 9.x instalada en ellos que se haya instalado en los nodos originales. Si los nodos nuevos tienen instalada una versión diferente de ONTAP, debe reiniciar el sistema las controladoras nuevas después de instalarlas. Para obtener instrucciones sobre cómo actualizar ONTAP, consulte "Referencias" Para enlazar a *Upgrade ONTAP*.
Comprobación de estado de HA	Comprueba si los dos nodos que se van a reemplazar se encuentran en una configuración de parejas de alta disponibilidad (ha). Si no está habilitada la conmutación por error del almacenamiento para las controladoras, la tarea falla.
Comprobación del estado del agregado	Si los nodos que se van a sustituir tienen agregados propios para los que no son el propietario principal, la tarea fallará. Los nodos no deben tener ningún agregado que no sea local.
Comprobación del estado del disco	Si alguno de los nodos que se van a reemplazar tiene discos ausentes o con errores, la tarea falla. Si falta algún disco, consulte "Referencias" Para establecer un vínculo a la gestión de discos y agregados con la CLI_, *administración de almacenamiento lógico con la CLI* y *Administración de alta disponibilidad* para configurar el almacenamiento para el par de alta disponibilidad.
Comprobación del estado de LIF de datos	Comprueba si alguno de los nodos que se van a sustituir tiene LIF de datos no locales. Los nodos no deben contener ninguna LIF de datos para la cual no sean el propietario principal. Si uno de los nodos contiene LIF de datos no locales, la tarea falla.
Estado de LIF del clúster	Comprueba si los LIF del clúster están activos para ambos nodos. Si las LIF del clúster están inadas, la tarea falla.
Comprobación del estado de ASUP	Si no se configuran las notificaciones de AutoSupport, la tarea falla. Debe habilitar AutoSupport antes de iniciar el procedimiento de reemplazo de la controladora.
Comprobación del uso de CPU	Comprueba si el uso de CPU es superior al 50 % en el caso de cualquiera de los nodos que se van a sustituir. Si el uso de CPU es superior al 50 % durante un período de tiempo considerable, la tarea falla.

Comprobación previa	Descripción
Comprobación de reconstrucción de agregados	Comprueba si la reconstrucción se está produciendo en algún agregado de datos. Si la reconstrucción del agregado está en curso, la tarea falla.
Comprobación de trabajo de afinidad de nodo	Comprueba si se están ejecutando trabajos de afinidad de nodos. Si se están ejecutando trabajos de afinidad de nodo, la comprobación falla.

4. Una vez iniciada la operación de sustitución de las controladoras y que se completen las comprobaciones previas, la operación se coloca en pausa, lo que permite recopilar información de salida que se pueda necesitar más adelante en el proceso de actualización de las controladoras.
5. Ejecute el siguiente conjunto de comandos según lo indicado por el procedimiento de reemplazo de la controladora en la consola del sistema.

   Desde el puerto serie conectado a cada nodo, ejecute y guarde el resultado de los siguientes comandos de forma individual:

   - `vserver services name-service dns show`
   - `network interface show -curr-node local -role cluster,intercluster,node-mgmt,cluster-mgmt,data`
   - `network port show -node local -type physical`
   - `service-processor show -node local -instance`
   - `network fcp adapter show -node local`
   - `network port ifgrp show -node local`
   - `system node show -instance -node local`
   - `run -node local sysconfig`
   - `storage aggregate show -node local`
   - `volume show -node local`
   - `storage array config show -switch switch_name`
   - `system license show -owner local`
   - `storage encryption disk show`
   - `security key-manager onboard show-backup`
   - `security key-manager external show`
   - `security key-manager external show-status`
   - `network port reachability show -detail -node local`

   > Si el cifrado de volúmenes de NetApp (NVE) o el cifrado de agregado de NetApp (NAE) con el gestor de claves integrado están en uso, mantenga la frase de acceso del gestor de claves preparada para completar el administrador de claves de nuevo a sincronizar más adelante en el procedimiento.

6. Si su sistema utiliza unidades de autocifrado, consulte el artículo de la base de conocimientos "Cómo

saber si una unidad tiene la certificación FIPS" Para determinar el tipo de unidades de autocifrado que se están utilizando en la pareja de alta disponibilidad que se está actualizando. El software ONTAP admite dos tipos de unidades de autocifrado:

- Unidades SAS o NVMe con cifrado en almacenamiento de NetApp (NSE) certificado FIPS
- Unidades NVMe (SED) con autocifrado no FIPS

> No es posible mezclar unidades FIPS con otros tipos de unidades en el mismo nodo o la pareja de alta disponibilidad.
>
> Puede mezclar unidades de cifrado distinto de SED en el mismo nodo o par de alta disponibilidad.

"Obtenga más información sobre las unidades de autocifrado compatibles".

Corrija la propiedad del agregado si fallan las comprobaciones previas de ARL

Si falla la comprobación del estado del agregado, debe devolver los agregados propiedad del nodo asociado al nodo propietario principal e iniciar de nuevo el proceso de comprobaciones previas.

Pasos

1. Devolver los agregados que actualmente pertenecen al nodo asociado al nodo propietario principal:

   `storage aggregate relocation start -node` *`source_node`* `-destination` *`destination-node`* `-aggregate-list *`

2. Compruebe que ni el nodo 1 ni el nodo 2 siguen teniendo agregados cuyos propietarios son actualmente (pero no el propietario del hogar):

   `storage aggregate show -nodes` *`node_name`* `-is-home false -fields owner-name, home-name, state`

   En el ejemplo siguiente se muestra el resultado del comando cuando un nodo es al mismo tiempo el propietario actual y el propietario principal de los agregados:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Después de terminar

Debe reiniciar el proceso de sustitución de la controladora:

```
system controller replace start -nodes node_names
```

Licencia

Cada nodo del clúster debe tener su propio archivo de licencia de NetApp (NLF).

Si no dispone de un NLF, las funciones con licencia actualmente en el clúster están disponibles para la nueva controladora. Sin embargo, el uso de funciones sin licencia en la controladora puede provocar que no cumpla el contrato de licencia, por lo que debe instalar NLF en la nueva controladora una vez completada la actualización.

Consulte "Referencias" Para establecer un enlace al sitio de soporte de *NetApp*, donde puede obtener su NLF. Los NLF están disponibles en la sección *My Support* en *Software licenses*. Si el sitio no tiene el NLF que necesita, póngase en contacto con su representante de ventas de NetApp.

Para obtener información detallada sobre las licencias, consulte "Referencias" Para vincular a *System Administration Reference*.

Gestione el cifrado del almacenamiento con el gestor de claves incorporado

Puede utilizar Onboard Key Manager (OKM) para gestionar las claves de cifrado. Si tiene configurado OKM, debe registrar la frase de acceso y el material de copia de seguridad antes de iniciar la actualización.

Pasos

1. Registre la clave de acceso para todo el clúster.

   Esta es la frase de acceso que se introdujo cuando se configuró o actualizó OKM con la CLI o la API REST.

2. Ejecute el para realizar un backup de la información del gestor de claves `security key-manager onboard show-backup` comando.

Desactivar las relaciones de SnapMirror (opcional)

Antes de continuar con el procedimiento, debe confirmar que todas las relaciones de SnapMirror se ponen en modo inactivo. Cuando una relación de SnapMirror se pone en modo inactivo, sigue en modo inactivo tras reinicios y recuperaciones tras fallos.

Pasos

1. Compruebe el estado de la relación de SnapMirror en el clúster de destino:

   ```
   snapmirror show
   ```

   > Si el estado es "transferencia", debe anular dichas transferencias:
   > `snapmirror abort -destination-vserver vserver_name`

La anulación falla si la relación de SnapMirror no se encuentra en el estado "transfiriendo".

2. Desactive todas las relaciones entre el clúster:

```
snapmirror quiesce -destination-vserver *
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.