



# Administración y supervisión

ASA r2

NetApp  
September 26, 2024

# Tabla de contenidos

- Administración y supervisión ..... 1
  - Gestione el acceso de clientes a las máquinas virtuales de almacenamiento en los sistemas de almacenamiento R2 de ASA ..... 1
  - Gestione las redes de clúster en sistemas de almacenamiento R2 de ASA ..... 3
  - Supervise el uso y aumente la capacidad ..... 5
  - Actualice el firmware en los sistemas de almacenamiento R2 de ASA ..... 8
  - Optimice la seguridad y el rendimiento del clúster con las estadísticas del sistema de almacenamiento R2 de ASA ..... 10
  - Vea los eventos y las tareas del clúster en los sistemas de almacenamiento R2 de ASA ..... 11
  - Gestione los nodos ..... 12
  - Gestione cuentas de usuario y roles en sistemas de almacenamiento R2 de ASA ..... 13
  - Gestione certificados de seguridad en sistemas de almacenamiento R2 de ASA ..... 15
  - Verifique la conectividad de host en el sistema de almacenamiento R2 de ASA ..... 17

# Administración y supervisión

## Gestione el acceso de clientes a las máquinas virtuales de almacenamiento en los sistemas de almacenamiento R2 de ASA

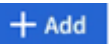
Las unidades de almacenamiento de un sistema ASA R2 se encuentran dentro de las máquinas virtuales de almacenamiento (VM). Los equipos virtuales de almacenamiento se utilizan para suministrar datos a sus clientes SAN. Use System Manager de ONTAP para crear una LIF (interfaz de red) para los clientes de SAN con el fin de conectarse a una máquina virtual de almacenamiento y acceder a los datos de las unidades de almacenamiento. Opcionalmente, puede utilizar subredes para simplificar la creación de LIF y los espacios IP para proporcionar a las máquinas virtuales de almacenamiento su propio almacenamiento, administración y enrutamiento seguros.

### Cree espacios IP

Un espacio IP es un espacio de direcciones IP distinto en el que residen las máquinas virtuales de almacenamiento. Cuando se crean espacios IP, se permite que las máquinas virtuales de almacenamiento tengan su propio almacenamiento, administración y enrutamiento seguros. También puede habilitar a los clientes en dominios de red independientes de forma administrativa para que utilicen direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

Debe crear un espacio IP para poder crear una subred.

#### Pasos

1. Seleccione **Red > Descripción general**.
2. En **IPspaces**, seleccione  **+ Add**.
3. Introduzca un nombre para el espacio IP o acepte el nombre predeterminado.

Un nombre de espacio IP no puede ser "all" porque "all" es un nombre reservado por el sistema.

4. Seleccione **Guardar**.

#### El futuro

Ahora que ha creado un espacio IP, puede utilizarlo para crear una subred.

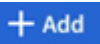
### Crear subredes

Una subred le permite asignar bloques específicos de direcciones IPv4 o IPv6 que deben usarse al crear una LIF (interfaz de red). Una subred simplifica la creación de LIF al permitirle especificar el nombre de subred en lugar de una dirección IP y una máscara de red específicas para cada LIF.

#### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El "[dominio de retransmisión](#)" espacio IP y en el que desea agregar la subred debe existir.

#### Pasos

1. Seleccione **Red > Descripción general**.
2. Seleccione **subredes**; luego seleccione  .
3. Introduzca el nombre de la subred.

Todos los nombres de subred deben ser únicos en un espacio IP.

4. Introduzca la dirección IP de subred y la máscara de subred.
5. Especifique el rango de direcciones IP para la subred.

Cuando especifique el rango de direcciones IP para la subred, no superponga las direcciones IP con otras subredes. Se pueden producir problemas de red cuando las direcciones IP de subred se superponen y diferentes subredes o hosts intentan utilizar la misma dirección IP.

6. Seleccione el dominio de retransmisión de la subred.
7. Seleccione **Agregar**.

### El futuro

Ha creado una subred que ahora puede usar para simplificar la creación de sus LIF.

## Crear una LIF (interfaz de red)


Una LIF (interfaz de red) es una dirección IP asociada a un puerto físico o lógico. Cree LIF en los puertos que desee utilizar para acceder a los datos. Los equipos virtuales de almacenamiento sirven datos a los clientes a través de una o más LIF. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, de modo que la comunicación de la red no se interrumpa.

Cuando se crea una LIF de datos de IP, puede atender tanto el tráfico iSCSI como NVMe/TCP de forma predeterminada. Es necesario crear LIF de datos independientes para el tráfico FC y NVMe/FC.

### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El puerto de red físico o lógico subyacente debe haberse configurado en el `up` estado administrativo.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.
- Una LIF que gestiona tráfico dentro del clúster entre nodos no debe estar en la misma subred que una LIF que gestiona el tráfico de gestión o una LIF que gestiona el tráfico de datos.

### Pasos

1. Seleccione **Red > Descripción general**.
2. Seleccione **Interfaces de red**; luego seleccione  .
3. Seleccione el tipo de interfaz y el protocolo y, a continuación, seleccione la máquina virtual de almacenamiento.
4. Escriba un nombre para la LIF o acepte el nombre predeterminado.
5. Seleccione el nodo de inicio de la interfaz de red y, a continuación, introduzca la dirección IP y la máscara de subred.
6. Seleccione **Guardar**.


### Resultado

Ha creado una LIF para el acceso a los datos.

## Modificar una LIF (interfaces de red)

Las LIF se pueden deshabilitar o cambiar su nombre según sea necesario. También puede cambiar la dirección IP de LIF y la máscara de subred.

### Pasos

1. Seleccione **Red > Descripción general** y, a continuación, seleccione **Interfaces de red**.
2. Coloque el cursor sobre la interfaz de red que desea editar y, a continuación,  seleccione .
3. Seleccione **Editar**.
4. Puede deshabilitar la interfaz de red, cambiar el nombre de la interfaz de red, cambiar la dirección IP o cambiar la máscara de subred.
5. Seleccione **Guardar**.

### Resultado

Se ha modificado su LIF.

## Gestione las redes de clúster en sistemas de almacenamiento R2 de ASA

Es posible usar System Manager de ONTAP para realizar administración básica de red de almacenamiento en el sistema ASA R2. Por ejemplo, puede agregar un dominio de retransmisión o reasignar puertos a un dominio de retransmisión diferente.

### Añada un dominio de retransmisión

Utilice dominios de retransmisión para simplificar la gestión de la red de clúster agrupando los puertos de red que pertenecen a la misma red de capa 2. Las máquinas virtuales de almacenamiento (VM) pueden usar los puertos del grupo para el tráfico de datos o de gestión.

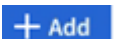
El dominio de retransmisión “default” y el dominio de retransmisión “Cluster” se crean durante la configuración del clúster. El dominio de difusión “predeterminado” contiene puertos que están en el espacio IP “predeterminado”. Estos puertos se utilizan principalmente para servir datos. Los puertos de gestión de clústeres y gestión de nodos también están en este dominio de retransmisión. El dominio de difusión “Cluster” contiene puertos que están en el espacio IP “Cluster”. Estos puertos se utilizan para la comunicación del clúster e incluyen todos los puertos de clúster de todos los nodos del clúster.

Puede crear dominios de retransmisión adicionales después de inicializar el clúster. Cuando se crea un dominio de retransmisión, se crea automáticamente un grupo de conmutación por error que contiene los mismos puertos.

### Acerca de esta tarea

La unidad de transmisión máxima (MTU) de los puertos agregados a un dominio de retransmisión se actualiza al valor MTU establecido en el dominio de retransmisión.

### Pasos

1. En System Manager, seleccione **Red > Descripción general**.
2. En Dominios **Broadcast**, seleccione  .

3. Escriba un nombre para el dominio de retransmisión o acepte el nombre predeterminado.

Todos los nombres de dominio de retransmisión deben ser únicos en un espacio IP.

4. Seleccione el espacio IP del dominio de retransmisión.

Si no especifica un nombre de espacio IP, el dominio de difusión se crea en el espacio IP “predeterminado”.

5. Introduzca la unidad de transmisión máxima (MTU).

MTU es el paquete de datos más grande que se puede aceptar en su dominio de retransmisión.

6. Seleccione los puertos deseados y luego seleccione **Guardar**.


### Resultado

Ha añadido un nuevo dominio de retransmisión.

## Reasigne los puertos a un dominio de retransmisión diferente

Los puertos solo pueden pertenecer a un dominio de retransmisión. Si desea cambiar el dominio de retransmisión al que pertenece un puerto, deberá reasignar el puerto del dominio de retransmisión existente a un nuevo dominio de retransmisión.

### Pasos

1. En System Manager, seleccione **Red > Descripción general**.
2. En **Dominios de difusión**, seleccione  junto al nombre de dominio; luego seleccione **Editar**.
3. Anule la selección de los puertos Ethernet que desea reasignar a otro dominio.
4. Seleccione el dominio de difusión al que desea reasignar el puerto y, a continuación, seleccione **Reasignar**.
5. Seleccione **Guardar**.

### Resultado

Ha reasignado los puertos a un dominio de retransmisión diferente.

## Cree una VLAN

Una VLAN consta de puertos de switch agrupados en un dominio de retransmisión. Las VLAN le permiten aumentar la seguridad, aislar problemas y limitar las rutas disponibles dentro de su infraestructura de red IP.

### Antes de empezar


Los switches implementados en la red deben cumplir los estándares IEEE 802.1Q o tener una implementación de VLAN específica por proveedor.

### Acerca de esta tarea

- No se puede crear una VLAN en un puerto de grupo de interfaces que no contenga puertos miembro.
- Cuando se configura una VLAN por primera vez en un puerto, el puerto podría estar inactivo, lo que podría dar lugar a una desconexión temporal de la red. Las adiciones posteriores de VLAN al mismo puerto no afectan al estado del puerto.
- No debe crear una VLAN en una interfaz de red con el mismo identificador que la VLAN nativa del switch. Por ejemplo, si la interfaz de red e0b se encuentra en una VLAN 10 nativa, no se debe crear una VLAN

e0b-10 en esa interfaz.

### Pasos

1. En el Administrador del sistema, seleccione **Red > Puertos Ethernet** y, a continuación, seleccione  **VLAN**.
2. Seleccione el nodo y el dominio de retransmisión para la VLAN.
3. Seleccione el puerto para la VLAN.

La VLAN no se puede conectar a un puerto que aloje una LIF de clúster ni a los puertos asignados al espacio IP del clúster.

4. Introduzca un ID de VLAN.
5. Seleccione **Guardar**.

### Resultado

Creó una VLAN para aumentar la seguridad, aislar problemas y limitar las rutas disponibles dentro de la infraestructura de red IP.

## Supervise el uso y aumente la capacidad

### Supervise el rendimiento de los clústeres y de la unidad de almacenamiento en los sistemas de almacenamiento R2 de ASA


Utilice System Manager de ONTAP para supervisar el rendimiento general de su clúster y el rendimiento de unidades de almacenamiento específicas para determinar cómo la latencia, las IOPS y el rendimiento afectan a sus aplicaciones vitales para el negocio. El rendimiento se puede supervisar en varios períodos de tiempo que van de una hora a un año.

Por ejemplo, supongamos que una aplicación crítica está experimentando alta latencia y bajo rendimiento. Cuando se observa el rendimiento del clúster de los últimos cinco días laborables, se observa una disminución del rendimiento a la misma hora cada día. Se utiliza esta información para determinar que la aplicación crucial está compitiendo por los recursos del clúster cuando un proceso no crítico comienza a ejecutarse en segundo plano. A continuación, puede modificar la política de calidad de servicio para limitar el impacto de la carga de trabajo no crítica en los recursos del sistema y garantizar que la carga de trabajo crítica cumpla con los objetivos de rendimiento mínimos.

### Supervise el rendimiento del clúster

Use las métricas de rendimiento del clúster para determinar si necesita cambiar cargas de trabajo para minimizar la latencia y maximizar las IOPS y el rendimiento para sus aplicaciones críticas.

### Pasos

1. En System Manager, seleccione **Panel**.
2. En **Rendimiento**, vea la latencia, IOPS y rendimiento del clúster por hora, día, semana, mes o año.
3.  Seleccione para descargar los datos de rendimiento.

### El futuro


Use las métricas de rendimiento del clúster para analizar si necesita modificar las políticas de calidad de

servicio o realizar otros ajustes en las cargas de trabajo de la aplicación para maximizar el rendimiento general del clúster.

### Supervise el rendimiento de la unidad de almacenamiento

Utilice métricas de rendimiento de unidad de almacenamiento para determinar el impacto de aplicaciones específicas en la latencia, las operaciones de IOPS y el rendimiento.

#### Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione la unidad de almacenamiento que desea supervisar; luego seleccione **Descripción general**.
3. En **Rendimiento**, vea la latencia, IOPS y rendimiento de la unidad de almacenamiento por hora, día, semana, mes o año.
4.  Seleccione para descargar los datos de rendimiento.

#### El futuro

Utilice las métricas de rendimiento de su unidad de almacenamiento para analizar si necesita modificar las políticas de calidad de servicio asignadas a sus unidades de almacenamiento para reducir la latencia y maximizar las IOPS y el rendimiento.

### Supervise el uso del clúster y de la unidad de almacenamiento en los sistemas de almacenamiento R2 de ASA

Utilice System Manager de ONTAP para supervisar la utilización del almacenamiento y garantizar que dispone de la capacidad de almacenamiento necesaria para satisfacer las cargas de trabajo actuales y futuras.

#### Supervise el uso del clúster

Supervise regularmente la cantidad de almacenamiento que consume el clúster para garantizar que, si es necesario, esté preparado para expandir la capacidad del clúster antes de quedarse sin espacio.

#### Pasos

1. En System Manager, seleccione **Panel**.
2. En **Capacidad**, vea la cantidad de espacio físico utilizado y la cantidad de espacio disponible en su clúster.

La proporción de reducción de datos representa la cantidad de espacio ahorrado gracias a la eficiencia del almacenamiento.

#### El futuro

Si su clúster se está quedando sin espacio o si no tiene capacidad para satisfacer una demanda futura, debe planificar la "[añadir unidades nuevas](#)" puesta en marcha de su sistema ASA R2 para aumentar la capacidad de almacenamiento.

#### Supervisar el uso de la unidad de almacenamiento

Supervisar la cantidad de almacenamiento consumido por una unidad de almacenamiento para aumentar de forma proactiva el tamaño de la unidad de almacenamiento en función de las necesidades de su negocio.



## Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione la unidad de almacenamiento que desea supervisar; luego seleccione **Descripción general**.
3. En **Almacenamiento**, vea lo siguiente:
  - Tamaño de la unidad de almacenamiento
  - Cantidad de espacio utilizado
  - De reducción de datos

La relación de reducción de datos representa la cantidad de espacio ahorrado gracias a la eficiencia del almacenamiento

- Instantánea utilizada

Snapshot utilizada representa la cantidad de almacenamiento que usan las instantáneas.

## El futuro

Si la unidad de almacenamiento se está acercando a su capacidad, debe ["modifique la unidad de almacenamiento"](#) aumentar su tamaño.

## Aumente la capacidad de almacenamiento en los sistemas de almacenamiento R2 de ASA

Añada unidades a un nodo o bandeja para aumentar la capacidad de almacenamiento del sistema ASA R2.

### Utilice NetApp Hardware Universe para preparar la instalación de una unidad nueva

Antes de instalar una unidad nueva en un nodo o bandeja, utilice NetApp Hardware Universe para confirmar que la unidad que desea añadir es compatible con la plataforma ASA R2 y para identificar la ranura correcta para la unidad nueva. Las ranuras correctas para añadir unidades varían según el modelo de plataforma y la versión de ONTAP. En algunos casos, es necesario añadir unidades a ranuras específicas en secuencia.

## Pasos

1. Vaya a la ["NetApp Hardware Universe"](#).
2. En **Productos**, seleccione tus configuraciones de hardware.
3. Seleccione su plataforma ASA R2.
4. Seleccione su versión de ONTAP; luego seleccione **Mostrar resultados**.
5. Debajo del gráfico, seleccione **Haga clic aquí para ver vistas alternativas**; luego elige la vista que coincida con tu configuración.
6. Utilice la vista de su configuración para confirmar que la unidad nueva es compatible y la ranura correcta para la instalación.

## Resultado

Ha confirmado que la unidad nueva es compatible y conoce la ranura adecuada para la instalación.

### Instale una nueva unidad en el ASA R2

La cantidad mínima de unidades que debe añadir en un solo procedimiento es de seis. Al añadir una sola

unidad, se puede reducir el rendimiento.

### **Acerca de esta tarea**

Debe repetir los pasos de este procedimiento con cada unidad.

### **Pasos**

1. Puesta a tierra apropiadamente usted mismo.
2. Retire con cuidado el bisel de la parte delantera de la plataforma.
3. Inserte la nueva unidad en la ranura correcta.
  - a. Con la palanca de leva en posición abierta, utilice ambas manos para insertar la nueva transmisión.
  - b. Presione hasta que la unidad se detenga.
  - c. Cierre el asa de leva de forma que la unidad esté completamente asentada en el plano medio y el asa encaje en su lugar.

Asegúrese de cerrar el mango de leva lentamente para que quede alineado correctamente con la cara de la transmisión.

4. Verifique que el LED de actividad de la unidad (verde) esté iluminado.
  - Si el LED está fijo, la unidad tiene alimentación.
  - Si el LED parpadea, la unidad se enciende y las operaciones de I/O están en curso. El LED también parpadeará si se está actualizando el firmware de la unidad.

El firmware de la unidad se actualiza automáticamente (sin interrupciones) en las unidades nuevas que no tienen versiones de firmware actuales.

5. Si el nodo está configurado para la asignación automática de unidades, puede esperar a que ONTAP asigne automáticamente las nuevas unidades a un nodo. Si el nodo no está configurado para la asignación automática de unidades o si se prefiere, es posible asignar las unidades manualmente.

Las unidades nuevas no se reconocen hasta que se asignan a un nodo.

### **¿Cuál es el siguiente?**

Una vez que se reconozcan las unidades nuevas, verifique que se hayan añadido y se haya especificado correctamente su propiedad.


## **Actualice el firmware en los sistemas de almacenamiento R2 de ASA**

ONTAP descarga y actualiza automáticamente los archivos de firmware y sistema en el sistema ASA R2 de forma predeterminada. Si desea obtener flexibilidad para visualizar las actualizaciones recomendadas antes de descargar e instalar, puede usar ONTAP System Manager para deshabilitar las actualizaciones automatizadas o para editar los parámetros de actualización para mostrar las notificaciones de las actualizaciones disponibles antes de realizar cualquier acción.

## Active las actualizaciones automáticas

Las actualizaciones recomendadas para el firmware de almacenamiento, el firmware de SP/BMC y los archivos del sistema se descargan e instalan automáticamente en el sistema ASA R2 de forma predeterminada. Si se han desactivado las actualizaciones automáticas, puede habilitarlas para restablecer el comportamiento predeterminado.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** seleccione  y luego seleccione **Activar**.
3. Lea y acepte el contrato de licencia para usuario final.
4. Acepte las opciones predeterminadas para actualizar automáticamente los archivos del firmware y del sistema. Opcionalmente, seleccione para mostrar notificaciones o para descartar automáticamente las actualizaciones recomendadas.
5. Seleccione esta opción para confirmar que las modificaciones de la actualización se aplicarán a todas las actualizaciones actuales y futuras.
6. Seleccione **Guardar**.


### Resultado

Las actualizaciones recomendadas se descargan e instalan automáticamente en su sistema ASA R2 según sus selecciones de actualización.

## Desactive las actualizaciones automáticas

Desactive las actualizaciones automáticas si desea tener la flexibilidad de ver las actualizaciones recomendadas antes de instalarlas. Si deshabilita las actualizaciones automáticas, tendrá que realizar las actualizaciones de firmware y los archivos del sistema manualmente.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** seleccione  y luego seleccione **Desactivar**.


### Resultado

Las actualizaciones automáticas están desactivadas. Debe comprobar regularmente si hay actualizaciones recomendadas y decidir si desea realizar una instalación manual.

## Ver actualizaciones automáticas

Vea una lista de las actualizaciones de archivos del sistema y firmware que se han descargado en el clúster y están programadas para la instalación automática. Vea también las actualizaciones que se han instalado previamente automáticamente.


### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** selecciona  y luego selecciona **Ver todas las actualizaciones automáticas**.

## Editar actualizaciones automáticas

Puede seleccionar que las actualizaciones recomendadas del firmware de almacenamiento, el firmware de SP/BMC y los archivos del sistema se descarguen e instalen automáticamente en el clúster, o bien puede seleccionar que se descarten automáticamente las actualizaciones recomendadas. Si desea controlar manualmente la instalación o el despedido de las actualizaciones, seleccione para recibir una notificación cuando haya disponible una actualización recomendada; a continuación, puede seleccionar manualmente para instalarla o descartarla.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** selecciona  y luego selecciona **Editar actualizaciones automáticas**.
3. Actualice las selecciones para actualizaciones automáticas.
4. Seleccione **Guardar**.


### Resultado

Las actualizaciones automáticas se modifican en función de las selecciones.

## Actualice el firmware manualmente

Si desea la flexibilidad de ver las actualizaciones recomendadas antes de que se descarguen e instalen, puede deshabilitar las actualizaciones automatizadas y actualizar el firmware manualmente.

### Pasos

1. Descargue el archivo de actualización de firmware en un servidor o cliente local.
2. En System Manager, seleccione **Clúster > Descripción general** y, a continuación, seleccione **Actualizar**.
3. Seleccione **Actualización de firmware**; seleccione .

### Resultado

El firmware se ha actualizado.

## Optimice la seguridad y el rendimiento del clúster con las estadísticas del sistema de almacenamiento R2 de ASA

Vea *Insights* en ONTAP System Manager para identificar las prácticas recomendadas y las modificaciones de configuración que puede implementar en su sistema ASA R2 para optimizar la seguridad y el rendimiento de los clústeres.

Por ejemplo, suponga que tiene servidores de protocolo de tiempo de redes (NTP) configurados para el clúster. Sin embargo, no sabe que tiene menos de la cantidad recomendada de servidores NTP necesarios para gestionar el tiempo del clúster de forma óptima. Para ayudarlo a evitar los problemas que pueden producirse cuando la hora del clúster no es precisa, Insights le notificará que tiene demasiados pocos servidores NTP configurados y le dará opciones para obtener más información acerca de este problema, solucionarlo o ignorarlo.

**Insights**

Take action to address concerns and apply best practices to optimize the security and performance of your system.

### Apply best practices

**Login banner isn't configured**

You haven't configured one or more login banner messages. You can create a custom login banner for the cluster or storage VM to inform visitors about terms and conditions, acceptable use, and site permissions.

[Learn more about best practices for security.](#)

**Too few NTP servers are configured**

Problems can occur when the cluster time is inaccurate. Configure Network Time Protocol (NTP) servers to synchronize the cluster time with external NTP servers. For redundancy and accuracy, you should associate at least three NTP servers with the cluster.

[Learn more about best practices for security.](#)

**Cluster isn't configured for automatic updates**

You aren't receiving automatic updates for this cluster. Enable automatic updates to always get the latest disk qualification package, disk firmware, shelf firmware, and SP/BMC firmware files when available.

**Global FIPS 140-2 compliance is disabled**

Global FIPS 140-2 compliance is disabled on this cluster. For security reasons, you should ensure ONTAP communicates with external clients or server components outside of ONTAP by using SSL communication that uses FIPS 140-2 compliant cryptography.

[Learn more about best practices for security.](#)

**Cluster isn't configured for notifications**

You aren't receiving notifications from ONTAP about potential problems on the cluster. You can configure ONTAP to send notifications using email, a webhook, or an SNMP traphost.

## Pasos

1. En System Manager, selecciona **Insights**.
2. Revise las recomendaciones.

## El futuro

Realice las acciones necesarias para implementar las prácticas recomendadas y optimizar la seguridad y el rendimiento del clúster.

# Vea los eventos y las tareas del clúster en los sistemas de almacenamiento R2 de ASA

Utilice System Manager de ONTAP para ver una lista de errores o alertas que se han producido en el sistema junto con las acciones correctivas recomendadas. También es posible ver los registros de auditoría del sistema y una lista de los trabajos activos, completados o con errores.

## Pasos

1. En System Manager, seleccione **Eventos y trabajos**.
2. Ver los eventos y los trabajos del clúster.


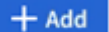
Para ver esto...	Realice lo siguiente...
Eventos del clúster	Selecciona <b>Eventos</b> ; luego selecciona <b>Registro de eventos</b> .
Sugerencias de Active IQ	Selecciona <b>Eventos</b> ; luego selecciona <b>Sugerencias de Active IQ</b> .
Alertas del sistema	<ol style="list-style-type: none"> <li>a. Selecciona <b>Alertas del sistema</b>.</li> <li>b. Seleccione la alerta del sistema cuya acción desea realizar.</li> <li>c. Confirme o suprima la alerta.</li> </ol>

Para ver esto...	Realice lo siguiente...
Trabajos del clúster	Seleccione <b>Jobs</b> .
Registros de auditoría	Seleccione <b>Registros de auditoría</b> .

## Envíe notificaciones por correo electrónico de eventos del clúster y registros de auditoría

Configure su sistema para enviar una notificación a direcciones de correo electrónico específicas cuando haya un evento del clúster o una entrada del registro de auditoría.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Gestión de notificaciones** seleccione .
3. Para configurar un destino de evento, seleccione **Ver destinos de evento**; luego seleccione **Destinos de evento**. Para configurar un destino de registro de auditoría, seleccione **Ver destinos de auditoría** y, a continuación, seleccione **Destinos de registro de auditoría**.
4. Seleccione .
5. Ingrese la información de destino y luego seleccione **Agregar**.

### Resultado


La dirección de correo electrónico que añadió ahora recibirá las notificaciones por correo electrónico especificadas para los eventos del clúster y los registros de auditoría.

## Gestione los nodos

### Reinicie un nodo en un sistema de almacenamiento ASA R2

Es posible que necesite reiniciar un nodo para mantenimiento, solucionar problemas, actualizaciones de software u otros motivos administrativos. Cuando un nodo se reinicia, su compañero de alta disponibilidad ejecuta automáticamente una toma de control. A continuación, el nodo del partner realiza una devolución al control automática cuando el nodo reiniciado vuelve a conectarse.

### Pasos

1. En System Manager, seleccione **Clúster > Descripción general**.
2. Seleccione  junto al nodo que desea reiniciar y, a continuación, seleccione **Reiniciar**.
3. Introduzca el motivo por el que está reiniciando el nodo; a continuación, seleccione **Reiniciar**.

El motivo por el que se introduce el reinicio se registra en el registro de auditoría del sistema.


### El futuro

Mientras el nodo se está reiniciando, su compañero de alta disponibilidad realiza una toma de control para que no haya interrupción en el servicio de datos. Cuando el reinicio se completa, el partner de alta disponibilidad realiza un retorno al nodo primario.

## Cambie el nombre de un nodo en un sistema de almacenamiento ASA R2

Puede usar ONTAP System Manager para cambiar el nombre de un nodo en el sistema ASA R2. Es posible que deba cambiar el nombre de un nodo para alinearlos con las convenciones de nomenclatura de la organización o por otros motivos administrativos.

### Pasos

1. En System Manager, seleccione **Clúster > Descripción general**.
2. Seleccione  junto al nodo al que desea cambiar el nombre y, a continuación, seleccione **Cambiar nombre**.
3. Introduzca el nuevo nombre para el nodo y, a continuación, seleccione **Renombrar**.

### Resultado

Se aplica el nuevo nombre al nodo.

## Gestione cuentas de usuario y roles en sistemas de almacenamiento R2 de ASA

Use System Manager para configurar el acceso a la controladora de dominio de Active Directory, la autenticación LDAP y SAML para sus cuentas de usuario. Cree roles de cuenta de usuario para definir funciones específicas que los usuarios asignados a los roles pueden realizar en el clúster.

### Configure el acceso del controlador de dominio de Active Directory

Configurar el acceso de la controladora de dominio de Active Directory (AD) al clúster o a la máquina virtual de almacenamiento para poder habilitar el acceso de la cuenta de AD.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, en **Active Directory**, selecciona **Configurar**.

### El futuro

Ahora puede habilitar el acceso a la cuenta de AD en su sistema ASA R2.


### Configurar LDAP

Configure un servidor de protocolo ligero de acceso a directorios (LDAP) para mantener de forma centralizada la información de usuario para la autenticación.

### Antes de empezar

Debe haber generado una solicitud de firma de certificación y añadido un certificado digital de servidor firmado por CA.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, junto a **LDAP**, selecciona .

3. Introduzca el servidor LDAP necesario y la información de enlace; a continuación, seleccione **Guardar**.

### El futuro

Ahora puede usar LDAP para información y autenticación de usuario.

## Configurar la autenticación SAML

La autenticación del lenguaje de marcado de aserción de seguridad (SAML) permite a los usuarios autenticarse mediante un proveedor de identidad (IdP) seguro en lugar de los proveedores de servicios directos, como Active Directory y LDAP.


### Antes de empezar

- Se debe configurar el IDP que se planea usar para la autenticación remota.

Consulte la documentación de IdP para la configuración.

- Debe tener el URI del IDP.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Autenticación SAML**, seleccione .
3. Seleccione **Habilitar autenticación SAML**.
4. Introduzca la URL del IdP y la dirección IP del sistema host; a continuación, seleccione **Guardar**.

Una ventana de confirmación muestra la información de metadatos, que se ha copiado automáticamente en el portapapeles.

5. Vaya al sistema IdP que especificó y, a continuación, copie los metadatos desde el portapapeles para actualizar los metadatos del sistema.
6. Vuelva a la ventana de confirmación en System Manager; luego seleccione **He configurado el IdP con el URI del host o metadatos**.
7. Seleccione **Logout** para habilitar la autenticación basada en SAML.

El sistema IDP mostrará una pantalla de autenticación.


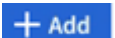
### El futuro

Ahora puede usar la autenticación SAML para las cuentas de usuario.

## Crear roles de cuenta de usuario

Los roles para los administradores del clúster y los administradores de máquinas virtuales de almacenamiento se crean automáticamente cuando se inicializa el clúster. Cree roles de cuenta de usuario adicionales para definir funciones específicas que los usuarios asignados a los roles pueden realizar en el clúster.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, junto a **Usuarios y roles**, seleccione .
3. En **Roles**, seleccione .
4. Seleccione los atributos de rol.



Para agregar varios atributos, seleccione **+ Add**.

5. Seleccione **Guardar**.

### Resultado

Se creará una nueva cuenta de usuario que estará disponible para usar en su sistema ASA R2.

## Cree una cuenta de administrador

Cree una cuenta de usuario de administrador para permitir al usuario de la cuenta realizar acciones específicas en el clúster en función del rol asignado a la cuenta. Para mejorar la seguridad de las cuentas, configure la autenticación multifactor (MFA) al crear la cuenta.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, junto a **Usuarios y roles**, seleccione **→**.
3. En **Usuarios**, seleccione **+ Add**.
4. Introduzca un nombre de usuario y, a continuación, seleccione un rol para asignarlo al usuario.
5. Seleccione el método de inicio de sesión de usuario y el método de autenticación.
6. Para habilitar MFA, seleccione **+ Add**; y, a continuación, seleccione un método de inicio de sesión secundario y un método de autenticación.
7. Introduzca una contraseña para el usuario.
8. Seleccione **Guardar**.

### Resultado

Se creará una nueva cuenta de administrador y estará disponible para usar en el clúster de ASA R2.

## Gestione certificados de seguridad en sistemas de almacenamiento R2 de ASA

Utilice certificados de seguridad digital para verificar la identidad de los servidores remotos.

El protocolo de estado de certificados en línea (OCSP) valida el estado de las solicitudes de certificados digitales de los servicios de ONTAP mediante conexiones SSL y de seguridad de la capa de transporte (TLS).

### Genere una solicitud de firma de certificación

Genere una solicitud de firma de certificación (CSR) para crear una clave privada que se pueda utilizar para generar un certificado público.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, seleccione **→**; y luego seleccione **+ Generate CSR**.
3. Introduzca el nombre común del asunto y, a continuación, seleccione el país.
4. Si desea cambiar los valores predeterminados de GSR, seleccionar el uso de clave ampliada o agregar nombres alternativos de asunto, seleccione **↶ More options**; y, a continuación, realice las

actualizaciones deseadas.

5. Seleccione **generar**.



### Resultado

Ha generado una CSR en la que se puede utilizar para generar un certificado público.

## Agregue una autoridad de certificación de confianza

ONTAP proporciona un conjunto predeterminado de certificados raíz de confianza para aplicaciones que utilizan Seguridad de la capa de transporte (TLS). Puede agregar autoridades de certificación de confianza adicionales según sea necesario.

### Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, seleccione .
3. Seleccione **Autoridades de certificación de confianza**.
4. Introduzca o importe los detalles del certificado y, a continuación, seleccione .


### Resultado



Añadió una nueva entidad de certificación de confianza al sistema ASA R2.

## Renueve o elimine una entidad de certificación de confianza

Las autoridades certificadoras de confianza deben renovarse anualmente. Si no desea renovar un certificado caducado, debe eliminarlo.

### Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, seleccione .
3. Seleccione **Autoridades de certificación de confianza**.
4. Seleccione la autoridad de certificación de confianza que desea renovar o eliminar.
5. Renueve o elimine la entidad de certificación.

Para renovar la autoridad de certificación, haga lo siguiente...	Para eliminar la autoridad del certificado, haga lo siguiente...
<ol style="list-style-type: none"><li>a.  Seleccione ; y, a continuación, seleccione <b>Renovar</b>.</li><li>b. Ingrese o importe la información del certificado; luego seleccione <b>Renovar</b>.</li></ol>	<ol style="list-style-type: none"><li>a.  Seleccione ; y, a continuación, seleccione <b>Eliminar</b>.</li><li>b. Confirme que desea eliminar y, a continuación, seleccione * Eliminar *.</li></ol>

### Resultado



Renovó o eliminó una entidad de certificación de confianza existente en el sistema ASA R2.

## Agregue un certificado de cliente/servidor o autoridades de certificación locales

Agregue un certificado de cliente/servidor o autoridades de certificación locales para habilitar servicios web

seguros.

### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, seleccione .
3. Seleccione **Certificados de cliente/servidor** o **Autoridades de certificación locales**.
4. Agregue la información del certificado y, a continuación, seleccione .


### Resultado



Ha agregado un nuevo certificado de cliente/servidor o autoridades locales al sistema ASA R2.

## Renovar o eliminar un certificado de cliente/servidor o autoridades de certificación locales

Los certificados de cliente/servidor y las autoridades de certificación locales deben renovarse anualmente. Si no desea renovar un certificado caducado o autoridades de certificación locales, debe eliminarlos.

### Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, seleccione .
3. Seleccione **Certificados de cliente/servidor** o **Autoridades de certificación locales**.
4. Seleccione el certificado que desea renovar o eliminar.
5. Renueve o elimine la entidad de certificación.

Para renovar la autoridad de certificación, haga lo siguiente...	Para eliminar la autoridad del certificado, haga lo siguiente...
<ol style="list-style-type: none"><li>a.  Seleccione ; y, a continuación, seleccione <b>Renovar</b>.</li><li>b. Ingrese o importe la información del certificado; luego seleccione <b>Renovar</b>.</li></ol>	<ol style="list-style-type: none"><li>a.  Seleccione ; y, a continuación, seleccione <b>Eliminar</b>.</li></ol>

### Resultado

Ha renovado o eliminado un certificado de cliente/servidor o una autoridad de certificación local existente en el sistema ASA R2.

## Verifique la conectividad de host en el sistema de almacenamiento R2 de ASA

Si existe un problema con las operaciones de datos del host, puede usar ONTAP System Manager para verificar que la conexión del host al sistema de almacenamiento ASA R2 esté activa.

### Pasos

1. En System Manager, seleccione **Host**.

El estado de conectividad de host se indica junto al nombre del grupo de hosts de la siguiente manera:

- **OK:** Indica que todos los iniciadores están conectados a ambos nodos.
- **Parcialmente conectado:** Indica que algunos de los iniciadores no están conectados a ambos nodos.
- **Ninguno conectado:** Indica que no hay iniciadores conectados.

#### **El futuro**

Realice actualizaciones en el host para corregir los problemas de conectividad. ONTAP volverá a comprobar el estado de la conexión cada quince minutos.

## 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.