DOCUMENTO TÉCNICO

NEVERFAIL
CONTINUOUS AVAILABILITY

CONTINUITY ENGINE: DOCUMENTO TÉCNICO

Protección Proactiva Contra el Tiempo de Inactividad para su Negocio

Objetivo

Este documento técnico fue diseñado para ayudar al personal de Infraestructura y Operaciones de TI y a los administradores de las aplicaciones a comprender mejor la manera en que Neverfail Continuity Engine (CE) mantiene operando a las aplicaciones críticas y los servicios en el centro de datos las 24 horas del día y los 7 días de la semana, protegiéndolos contra el tiempo de inactividad debido a cualquier tipo de amenaza o condición de fallo.

Este documento cubre las tecnologías esenciales para mantener una disponibilidad continua de las aplicaciones críticas, destaca las limitaciones de otras soluciones alternativas de respaldo y replicación y proporciona información técnica sobre las características y la infraestructura del producto CE.

Protección de las Aplicaciones Más Importantes

Las operaciones empresariales modernas dependen de un alto de automatización de la TI y muchos de estos sistemas están expuestos directamente a los clientes a través de la web, por lo que cada vez es más importante contar con una disponibilidad permanente de los sistemas más críticos. En un entorno altamente competitivo, las consecuencias derivadas de una interrupción en los sistemas pueden ser graves, incluyendo los daños a la reputación, la pérdida de ingresos e incluso el riesgo de que no sobreviva la organización. Mientras que los gerentes de TI en la mayoría de las empresas tienen algún tipo de plan de recuperación o continuidad de las operaciones, la gran mayoría de esos planes no se ejecutan con regularidad y pudiera ser que la infraestructura de resiliencia no tenga la capacidad de proteger a los activos de TI más importantes.

A medida que la infraestructura de virtualización se ha convertido en algo común en los centros de datos, los profesionales de TI han aprovechado los servicios de recuperación ante desastres (DR) y clusterización virtual para proteger la mayoría de las cargas de trabajo de TI por primera vez, reduciendo los costos y la complejidad en comparación con los métodos anteriores. Sin embargo, aunque el desempeño provisto por la infraestructura virtual nativa es lo “suficientemente bueno” para la mayoría de las aplicaciones, inevitablemente no podrá ofrecer una disponibilidad continua de las aplicaciones más críticas. Por ejemplo, el restablecimiento total del servicio en aplicaciones multi-nivel más complejas desplegadas en plataformas virtuales y físicas pudiera tardar varias horas después de una interrupción. Lo mismo ocurre con los sistemas protegidos únicamente por soluciones de respaldo y replicación de tipo comercial, ya que se enfocan principalmente en la recuperación del sistema y no en la detección y resolución de los problemas antes de que un fallo en la infraestructura o la aplicación provoque un tiempo de inactividad. Los sistemas críticos requieren de una disponibilidad continua, la cual es necesaria para garantizar la operación las 24 horas del día y los 7 días de la semana. Estas son las tecnologías clave que debe tener cualquier infraestructura diseñada para mantener la disponibilidad continua de las aplicaciones críticas:

- **Tecnología consciente de la aplicación.** La mayoría de las soluciones de respaldo y replicación no pueden detectar la degradación en el servicio ni los fallos en las aplicaciones. Como resultado, siempre serán reactivas a las interrupciones que afectan a las operaciones normales de la empresa. Por el contrario, una verdadera solución de disponibilidad continua detecta y resuelve de manera proactiva cualquier fallo inminente, en vez de reiniciar un servidor de forma reactiva para restablecer el servicio de la aplicación. Esta tecnología consciente de la aplicación también es crítica para asegurar

> La infraestructura de respaldo, replicación y recuperación de tipo comercial no protege a las aplicaciones críticas.

que la conmutación por error se realice de manera exitosa en aplicaciones multi-nivel complejas.

- **Apoyo del Punto Objetivo de Recuperación (RPO) en cuestión de segundos.** Las copias de respaldo o de réplica de una aplicación protegida o de una imagen de servidor sólo son tan buenas como la sincronización de datos más reciente. La mayoría de las soluciones de respaldo y replicación no pueden manejar un RPO menor a 15 minutos, lo que significa que seguramente se perderán datos críticos durante una interrupción. Por el contrario, la disponibilidad continua requiere de una pérdida de datos mínima o nula, lo que suele requerir de la implementación de una costosa infraestructura de replicación de matrices de almacenamiento y/o de optimización de la WAN. Por otra parte, la infraestructura dedicada de disponibilidad continua provee los objetivos de RPO requeridos a una fracción del costo.
- **Apoyo del Tiempo Objetivo de Recuperación (RTO) en cuestión de segundos a minutos.** Cuando ocurre un desastre, especialmente a nivel de todo el sitio, a menudo puede tomar horas reconfigurar la red y conectar los múltiples componentes para luego verificar si todo funciona correctamente. La mayoría de las soluciones de respaldo y replicación necesitan recuperar la imagen de un equipo físico o una máquina virtual de la copia replicada antes de poder activar los servidores individuales, lo que podría llevar horas.
  Si a esto se añade la necesidad de recuperar grupos de aplicaciones y servidores de servicios críticos en un orden de prioridad designado, casi todas estas soluciones se quedan cortas en términos de una recuperación oportuna. Las aplicaciones críticas no pueden permitir un tiempo de inactividad de este nivel, por lo que la instrumentación y la automatización deben hacer frente a estos temas importantes en su infraestructura de conmutación por error.
- **Bajo costo total de propiedad.** El nivel de protección que ofrece una infraestructura avanzada de disponibilidad continua debe ser fácil de justificar considerando la necesidad de mantener siempre activas las aplicaciones críticas. Esto es válido por lo menos en teoría, hasta el momento de informar a la gerencia el costo total de propiedad de los sistemas de respaldo y replicación basados en el almacenamiento. Muchos profesionales de TI asumen que solamente las empresas con grandes presupuestos pueden costear este nivel de protección. Curiosamente este no es el caso, ya que existen proveedores especializados como Neverfail que ofrecen una infraestructura de protección eficaz y de alto rendimiento a un costo total de propiedad favorable para las PYMES.

En la siguiente sección, explicaremos cómo CE resuelve estos problemas y cumple con su promesa de “tiempo de inactividad cero” en cualquier tipo de infraestructura sin importar las amenazas o los fallos.

Sinopsis de Continuity Engine

CE provee una protección total a las aplicaciones críticas, asegurando su disponibilidad las 24 horas del día y los 7 días de la semana sin importar el tipo de amenaza. CE evita el fallo de las aplicaciones detectando de manera proactiva las firmas de fallo y cambiando las aplicaciones degradadas a un servidor de respaldo antes de que el fallo cause un tiempo de inactividad. Con las funcionalidades de replicación integrada, optimización de la WAN, disponibilidad continua, recuperación ante desastres y protección de datos, CE provee una protección total para los servicios críticos de su empresa.

Las características clave de CE y los beneficios que aporta incluyen:

- **Disponibilidad continua y recuperación ante desastres unificadas.** CE ofrece una protección total a los sistemas y servicios críticos contra el fallo de las aplicaciones, los servidores, la red, los equipos de almacenamiento o los sitios.
- **Replicación integrada.** La replicación integrada de CE reduce considerablemente el umbral de la pérdida de datos al proveer un RPO cercano a cero. Los costos totales se reducen significativamente, ya que CE puede operar con servidores o equipos de almacenamiento heterogéneos, no requiere de un almacenamiento compartido ni depende de otro software de replicación del almacenamiento y tiene la capacidad de replicar los datos de aplicaciones, registros y sistemas de archivos.
- **Monitoreo proactivo de la salud de las aplicaciones.** CE previene el fallo de las aplicaciones mediante un monitoreo proactivo de la salud en tiempo real y la detección de los patrones de degradación antes de que ocurra un fallo. En caso de que se detecten dichos patrones, automáticamente se activan los mecanismos de resolución para preservar la continuidad de las aplicaciones.
- **Protección de grupos de aplicaciones multi-nivel.** CE puede coordinar la conmutación por error acelerada de cualquier conjunto arbitrario de componentes de aplicación en diversos servidores, especialmente en el contexto de una conmutación por error del sitio, y recuperarlos en un orden de prioridad designado.
- **Aceleración WAN integrada.** Las funciones incorporadas de compresión y deduplicación de datos de CE reducen significativamente los costos operativos para la recuperación ante desastres al disminuir el tráfico de replicación de la WAN y los requisitos de ancho de banda de la red asociada hasta en un 80%.
- **Integración con vMotion y vSphere (HA) de Vmware.** CE amplía la inteligencia y el monitoreo proactivo de la salud de las aplicaciones en las cargas de trabajo que se ejecuten en la infraestructura de VMware vSphere al permitir que los administradores configuren los activadores de corrección automatizados asociados con las acciones de VMware vSphere HA, vMotion, Storage vMotion o vMotion mejorado, cuando se detecten fallos en las aplicaciones o condiciones de salud degradadas.
- **Integración con SRM de VMware.** CE incorpora capacidades de recuperación ante desastres para los equipos físicos de la solución Site Recovery Manager (SRM) de VMware al permitir que las réplicas sincronizadas de las máquinas virtuales de los equipos físicos protegidos se recuperen durante la ejecución de los planes de recuperación de SRM.
- **Protección de datos integrada.** CE cuenta con un Módulo de Reversión de Datos (DRM) que se integra con el Servicio de Instantáneas de Volumen de Windows (VSS) para evitar la corrupción y la pérdida de datos mediante la creación de instantáneas de datos de las aplicaciones que pueden utilizarse

durante la recuperación para revertir el estado de la aplicación a un punto anterior en el tiempo.

- **Soporte de nodos terciarios.** CE provee opciones de topología flexibles para ofrecer una redundancia extendida que combina conmutación por error local (HA) y remota (DR), así como para la recuperación ante desastres (DR) en múltiples sitios. CE también puede realizar la transición de un par de HA o DR existente a un servidor terciario de forma rápida y fácil.
- **Opciones de configuración flexibles de la red.** CE permite que los administradores implementen múltiples configuraciones de red, ya sea una configuración de NIC individual o configuraciones de NIC dobles. Estas pueden configurarse en la misma subred o en subredes distintas.
- **Cliente web del Servicio de Gestión de CE.** El cliente web de gestión de CE está diseñado para facilitar el despliegue de clústeres de CE con sólo apuntar y hacer click, ofreciendo una administración centralizada de todos los despliegues de CE. Consulte la Figura 1 en la página siguiente.

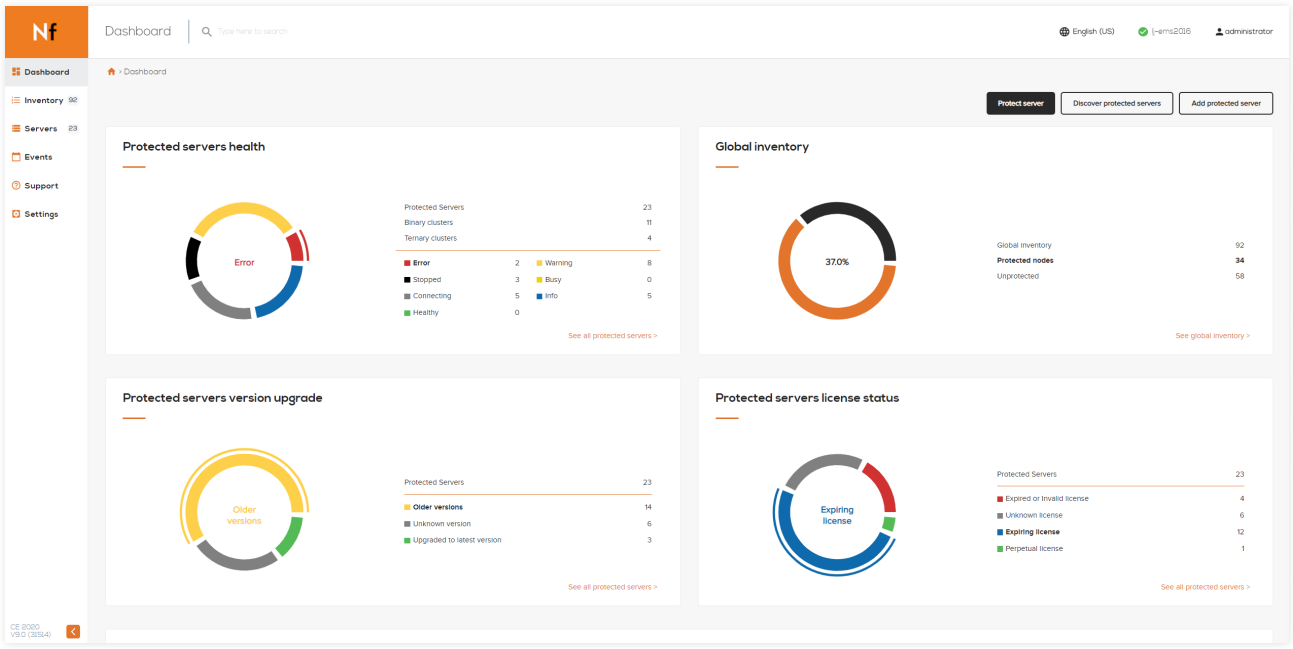


Figura 1: Consola Web del Servicio de Gestión de Engine

Continuity Engine a Detalle

Las siguientes secciones se enfocan en la arquitectura de CE y en las operaciones básicas de continuidad disponibles en CE.

Arquitectura de la Solución

CE mantiene la disponibilidad continua de las aplicaciones críticas realizando la conmutación por error a las instancias de respaldo configuradas en una topología de par o trío de protección, según el número de nodos de servidores que participen en el "clúster" de CE. Un par de protección se refiere a un clúster de aplicación en dos servidores, mientras que un trío de protección (o terciario) se refiere a un clúster de aplicación distribuido en tres servidores. La implementación de CE en servidores asociados con un clúster de CE resulta en la asignación de una identidad (primaria, secundaria o terciaria) a cada uno de los servidores, lo que significa una configuración de par de CE o una configuración terciaria de CE. Consulte la Figura 2.

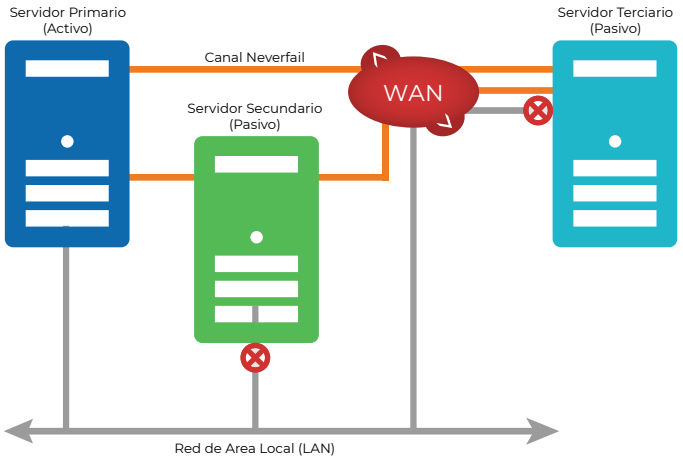


Figure 2: Engine Protection Pair

Además de una identidad, a cada servidor del clúster de CE se le asigna un rol (activo o pasivo). Mientras que la identidad del servidor describe el orden de membresía en el clúster de CE, el rol del servidor describe el estado de la aplicación protegida en ese nodo del servidor. Aunque la identidad del servidor generalmente no cambiará entre los nodos del clúster, el rol del servidor puede cambiar dependiendo del estado de la instancia de la aplicación en cada nodo del clúster según lo determine CE.

En su forma más simple, CE opera como un par de protección con un servidor que desempeña un rol activo (normalmente el servidor primario) y el otro servidor un rol pasivo (normalmente el servidor secundario). El servidor con el rol activo provee los servicios de

la aplicación a los usuarios finales y sirve como el origen de la replicación, mientras que el servidor con el rol pasivo sirve como el servidor de respaldo y es el destino de los datos replicados. Esta configuración permite la replicación de datos entre el servidor activo y pasivo por el canal Neverfail.

Cuando se despliega con una configuración de par, CE puede implementarse para HA utilizando una conexión de red de área local (LAN) de alta velocidad o para la recuperación ante desastres (DR) utilizando una conexión de red de área amplia (WAN) con un menor ancho de banda, la cual pudiera requerir de una optimización del ancho de banda (utilizando la función de Aceleración de la WAN integrada en CE).

Cuando se despliega con una configuración terciaria, CE ofrece una alta disponibilidad (HA) de las aplicaciones protegidas a través de la LAN y simultáneamente permite la recuperación ante desastres (DR) a través de una conexión de WAN con un tercer servidor localizado en un sitio remoto. CE también puede realizar la transición de un par de HA o DR existente a un servidor terciario de forma rápida y fácil. Solamente se requiere una clave de licencia actualizada.

> ***Tome Nota:***
> Un clúster de Engine puede incluir equipos físicos y máquinas virtuales, además de servidores que ya participen en un clúster de vSphere de VMware.

Replicación de Datos

CE mantiene sincronizados a los servidores en su clúster mediante una funcionalidad de replicación integrada. Consulte la Figura 3. Una vez configurada esta función, CE registra los cambios de I/O en el disco que contiene los datos de la aplicación protegida y coloca en una cola del servidor activo las actualizaciones a los archivos protegidos (la cola de envío), listas para enviarse al servidor pasivo con cada solicitud numerada para mantener su orden en la cola.

Cuando la “cola de envío” alcanza un tamaño previamente configurado o al cumplirse el tiempo establecido, las actualizaciones se envían al servidor pasivo, el cual coloca todas las solicitudes en una matriz de archivos de registro denominada “cola de recepción”. A continuación, el servidor pasivo confirma que los cambios han sido registrados mediante el envío de un mensaje al servidor activo. La “cola de recepción” del servidor pasivo se lee en orden numérico y posteriormente se aplica un conjunto duplicado de operaciones de archivo al disco del servidor pasivo.

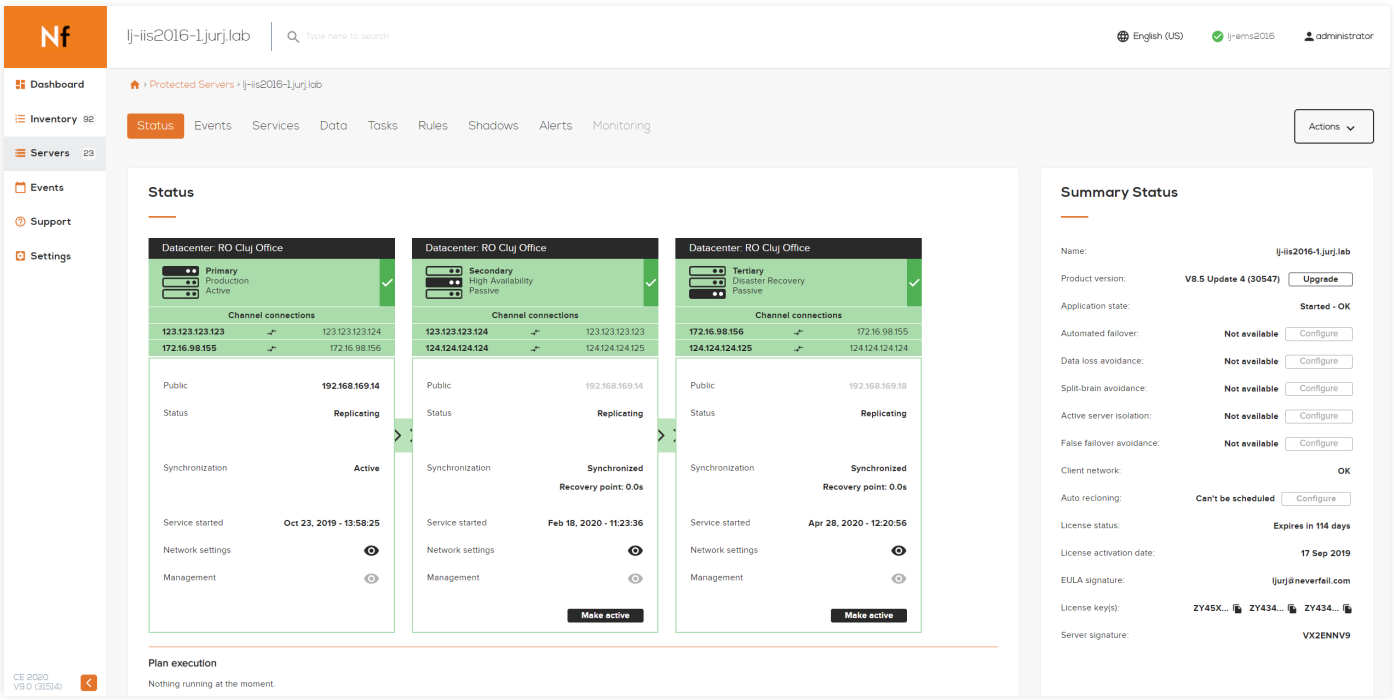


Figura 3: Consola de Gestión de Engine

Configuración de la Red

Las aplicaciones y los servidores protegidos por CE dependen de algunas estructuras de red específicas de Neverfail para garantizar la disponibilidad continua en las implementaciones de alta disponibilidad y de recuperación ante desastres. Estas incluyen:

- **Dirección IP pública o nombre público.** Esta es la dirección IP o el nombre de dominio totalmente cualificado (FQDN) asociado a un servicio de una aplicación de producción que es fundamental para la operación del sistema y que está registrado en los servidores DNS globales de la organización. Debe ser una dirección IP estática (no hay soporte para DHCP).
- **NIC público.** Este es el NIC que está configurado con un dirección IP pública/nombre público para que los clientes se comuniquen con la aplicación o el servidor protegido.
- **Dirección IP del canal Neverfail.** Esta es la dirección IP privada (generalmente interna) asignada a cada nodo del servidor en un clúster de CE que corresponde a la red del canal Neverfail en la que se produce la replicación de los datos.
- **NIC del canal Neverfail.** Este es el NIC que está configurado con una IP del canal Neverfail en cada nodo del servidor dentro de un clúster de CE para comunicarse con otros nodos a través de una red privada del canal Neverfail. Puede tratarse de un NIC dedicado y separado del NIC público (configuración de NIC dual), o bien, el canal y el público pueden ocupar el mismo NIC cuando CE se despliega en una configuración de NIC individual. Consulte las Figuras 4 y 5.

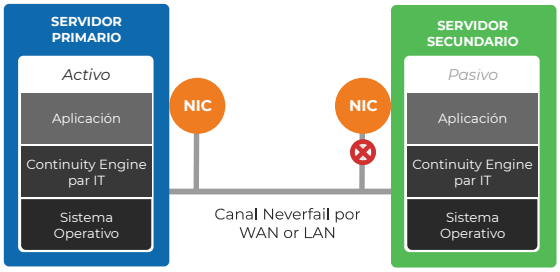


Figura 4: Configuración de NIC Individual

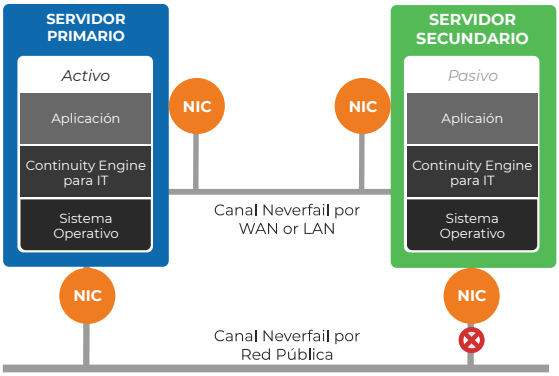


Figura 5: Configuración de NIC Dual

Al configurar un clúster de CE para HA en la red de área local (LAN), el NIC público del servidor pasivo utiliza la misma dirección IP pública del servidor activo. Sin embargo, el servidor pasivo está oculto y no puede comunicarse con la red activa mediante el sistema de filtrado de paquetes IP que se instala con CE. Este filtro de paquetes impide la transmisión del tráfico a través de la dirección IP pública. También evita que el tráfico de NetBIOS que utiliza otras direcciones IP en el NIC sea enviado a fin de prevenir un conflicto de resolución de nombres de NetBIOS.

Cuando el clúster de CE está configurado para la recuperación de desastres (DR) a un sitio remoto con una subred IP diferente, es necesario configurar CE a fin de utilizar una dirección IP pública diferente para cada uno de los servidores primarios y secundarios. Al realizarse el cambio o la conmutación por error, el servidor DNS también se actualizará automáticamente para redireccionar las conexiones del cliente a la nueva instancia del servidor activo en el sitio de recuperación ante desastres (DR). Estas actualizaciones del DNS no se requieren cuando el sitio de recuperación ante desastres (DR) utiliza la misma subred.

Tome Nota:

Neverfail ha implementado una versión mejorada de su sistema de filtrado de paquetes. La Plataforma de Filtrado de Windows (WFP) es un conjunto de interfases de programación de aplicaciones (API) y servicios del sistema que proporcionan una plataforma para crear aplicaciones de filtrado de la red.

La implementación de Engine se basa en su capacidad de filtrado de paquetes de la red, misma que evita que los nodos pasivos se comuniquen en la red. Esta nueva integración permite que Engine controle de forma dinámica el tráfico entrante y saliente de servidores con Windows 2008 R2, Windows 2012 o Windows 2012 R2 sin necesidad de complejos controladores de dispositivos diseñados para interfases de red específicas.

Ambito de Protección

CE ofrece una protección completa contra los puntos únicos de fallo para garantizar que las aplicaciones estén continuamente en funcionamiento y operación a fin de que puedan proveer los servicios críticos. Estas incluyen:

- **Protección de servidores.** CE permite la continuidad de las aplicaciones en caso de un fallo del hardware o una caída del sistema operativo. Los administradores de TI pueden tener una visibilidad total del entorno utilizando la consola de gestión de CE para conocer la salud de los servidores pertenecientes al clúster de CE. El servidor pasivo monitorea activamente al servidor activo mediante el envío frecuente de mensajes y la recepción de una respuesta a través de una conexión de red denominada el canal Neverfail. Si el servidor pasivo detecta que el servidor activo no está respondiendo, ya sea debido a un fallo del hardware o una pérdida de conectividad de la red, puede ejecutar una tarea de "conmutación por error". Durante la conmutación por error, el servidor pasivo se habilita para tomar de inmediato el rol del servidor activo. La mecánica de la conmutación por error se describe a detalle más abajo.
- **Protección de las aplicaciones.** CE monitorea continuamente las aplicaciones protegidas y los servicios relacionados que se ejecutan en el servidor activo. En caso de que alguna aplicación protegida falle repentinamente o muestre firmas de fallo que indiquen un fallo inminente, CE primero intentará reiniciar la aplicación en el servidor activo. Si el fallo no se resuelve reiniciando la aplicación, CE puede ejecutar una tarea de "cambio". La acción de cambio cierra correctamente cualquier aplicación protegida que esté siendo ejecutada en el servidor activo y la reinicia en el servidor pasivo junto con cualquier servicio dependiente necesario para que la aplicación esté disponible. La mecánica de este proceso de cambio se describe a detalle más abajo.
- **Protección de la red.** CE monitorea de manera proactiva la capacidad del servidor activo de comunicarse con el resto de la red mediante el sondeo de hasta tres nodos definidos alrededor de la red a intervalos regulares, incluyendo dispositivos como la puerta de enlace de red predeterminada, el servidor DNS primario y el servidor del Catálogo Global. En caso de que los tres nodos no respondan (debido a un fallo del NIC o del conmutador de la red, por ejemplo), CE puede cambiar los roles de los servidores activo y pasivo (lo que se denomina como un cambio), permitiendo que el servidor anteriormente pasivo asuma una identidad de red idéntica a la del servidor previamente activo. Después del cambio, el nuevo servidor activo seguirá dando servicio a los clientes.
- **Protección del desempeño.** CE monitorea de forma proactiva los indicadores de desempeño del sistema para asegurar que las aplicaciones protegidas sean verdaderamente operativas y funcionen adecuadamente para brindar la calidad de servicio esperada a los usuarios finales. Esto es posible gracias al marco tecnológico de gestión de aplicaciones (AMF) patentado por CE, el cual es modular y extensible para incluir a cualquier aplicación basada en Windows, proporcionando así una amplia cobertura de protección de las aplicaciones en las miles de aplicaciones desplegadas por las organizaciones de TI. Las siguientes secciones contienen información adicional sobre AMF.

La capacidad de expresar los indicadores clave de desempeño de una aplicación se capta a través de reglas previamente definidas y umbrales ajustables en forma de un servicio o un "plugin" de una aplicación. Estos plugins permiten que CE monitoree los atributos específicos de la aplicación para asegurar que se mantengan dentro de los rangos de operación normales. Las reglas pueden activarse o desactivarse según se desee y pueden configurarse para ejecutar acciones correctivas preventivas y específicas cuando estos atributos se encuentren fuera de sus respectivos rangos.

- **Protección de los datos.** CE asegura la disponibilidad de los datos de la aplicación y de otros datos del sistema de archivos en todos los nodos del clúster de CE. CE puede configurarse para proteger archivos, carpetas e incluso configuraciones específicas del registro en el servidor activo, reflejándolos en tiempo real en los servidores pasivos. Esto significa que en caso de producirse una conmutación por error o un cambio, todos los archivos protegidos en el servidor fallido seguirían estando disponibles en el nuevo servidor activo después del evento de cambio o conmutación por error..
- **Protección del sitio.** CE provee una disponibilidad continua de las aplicaciones y los servicios aún en caso de una interrupción a nivel de todo el sitio. Al desplegar el servidor secundario o terciario dentro de un clúster de CE en un centro de datos remoto, CE permite realizar la recuperación ante desastres con sólo presionar un botón, además de ofrecer un soporte de aceleración de la WAN para garantizar la recuperación ordenada de las aplicaciones individuales o de servicios completos siguiendo una prioridad de recuperación designada y con niveles de disponibilidad similares a los de una configuración de HA local.

Conmutación por Error y Cambio

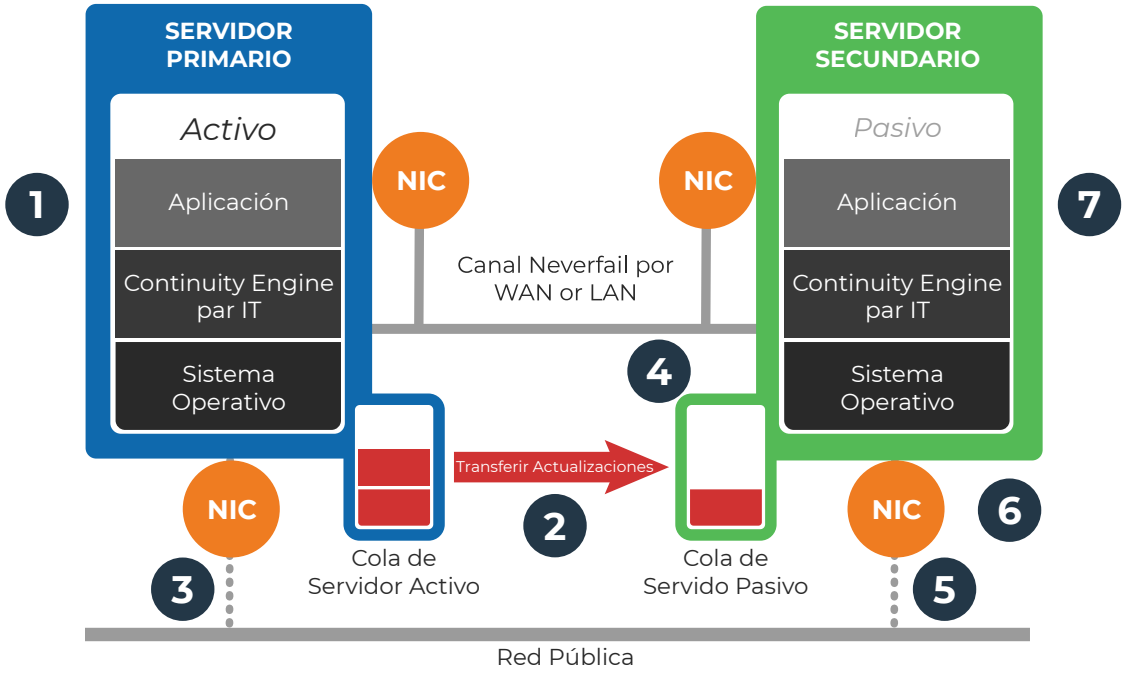
Neverfail Continuity Engine ofrece distintos procedimientos para cambiar el rol de los servidores activo y pasivo.

Los cambios se relacionan con las aplicaciones protegidas y la conmutación por error se relaciona con los servidores protegidos.

Proceso de Cambio

El proceso de cambio se inicia de manera manual o automática. En ambos casos, el resultado es que el control de la aplicación pasa de un servidor activo a uno pasivo en un clúster.

Hay siete pasos que documentan el proceso de cambio. Consulte la Figura 6 para ver una ilustración de los pasos.



1. Stop applications.
2. Transfer updates.
3. Blocked from network. Server becomes passive.
4. Applied queued updates.
5. Expose to network.
6. Start interceping updates. Server becomes active.
7. Start applications.

Figura 6: Proceso de Cambio de Engine

Cambio Gestionado. Es posible iniciar manualmente un cambio gestionado desde la interfase de gestión de CE seleccionando el botón “Activar” en el menú de Acciones o el cliente y luego eligiendo la función “Activar secundario”. Al iniciar un cambio gestionado, la operación de las aplicaciones protegidas se transfiere del servidor activo al servidor pasivo en el clúster; en otras palabras, se revierten los roles de los servidores.

Cambio Automático. Los cambios automáticos se activan de forma automática en caso de que falle una aplicación protegida que esté siendo monitoreada por el sistema.

Un cambio automático es diferente a un cambio gestionado en el sentido de que, aunque cambien los roles del servidor, el servicio CE se suspende en el servidor previamente activo para permitir que el administrador verifique la integridad de los datos en el nuevo servidor pasivo e investigue la causa del cambio automático. El cambio automático es similar a la conmutación por error (se describe a continuación) pero se inicia al ocurrir un fallo en la aplicación monitoreada. Una vez que se haya determinado y corregido la causa del cambio automático, el administrador revierte los roles de los servidores a su estado original.

Proceso de Conmutación por Error

El proceso de conmutación por error también puede iniciarse de manera manual o automática. Hay cuatro pasos que documentan el proceso de conmutación por error. Consulte la Figura 7 para ver una ilustración de los pasos.

Conmutación por Error Automática. Cuando un servidor pasivo detecta que el servidor activo ya no está funcionando o respondiendo a los mensajes, dicho servidor asume el rol del servidor activo.

Conmutación por Error Gestionada. La conmutación por error gestionada es similar a la conmutación por error automática en el sentido de que el servidor pasivo automáticamente determina que el servidor activo ha fallado y puede advertir al administrador de TI acerca del fallo; sin embargo, no se realizará la conmutación por error hasta que el administrador decida activar esta operación manualmente.

1. Procesar las actualizaciones de la cola de replicación.
2. Exponer a la red.
3. Comenzar a interceptar las actualizaciones. El servidor ahora es activo.
4. Ejecutar las aplicaciones.

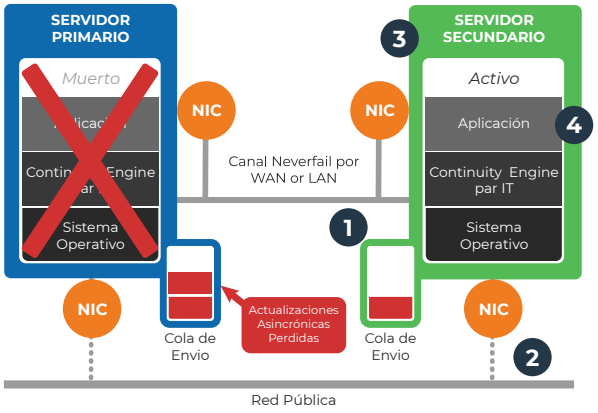


Figura 7: Proceso de Conmutación por Error de Engine

Mecanismos de Remediación Adicionales

CE ofrece opciones de remediación adicionales para la recuperación del sistema a partir de la versión CE 7.0, mismas que permiten a los administradores de VMware aprovechar la tecnología vSphere de VMware (como VMware HA, vMotion, Storage vMotion y vMotion mejorado) para la recuperación y prevención de los problemas de continuidad de las aplicaciones.

> Continuity Engine ofrece una amplia protección simultánea en todos los niveles para asegurar que todas las facetas del entorno de TI se mantengan operando en todo momento, independientemente de los escenarios de fallo que se presenten.

Integración con funciones HA de VMware

- CE puede configurarse para activar una acción de reinicio de la VM mediante el uso de funciones HA de VMware que ejecuten un apagado y reinicio limpio del SO huésped en la máquina virtual que experimente una interrupción o un problema con la aplicación.
- También es posible configurar CE para que reinicie la máquina virtual utilizando el mecanismo de monitoreo de aplicaciones HA de VMware vSphere, en vez de utilizar los mecanismos nativos de remediación de aplicaciones de CE.

Integración con vMotion de VMware

CE puede configurarse para activar VMware vMotion o Storage vMotion en respuesta a cualquier problema de degradación de la aplicación que sea detectado. Estos son dos ejemplos:

- Una aplicación podría estar funcionando incorrectamente debido a la falta de recursos de computación de la máquina virtual asociada (VM) en el equipo host ESX existente y la mejor estrategia de remediación sería trasladarla mediante vMotion a otro equipo host ESX dentro del clúster de VMware vSphere que tenga una capacidad de computación adecuada.
- Otro motivo por el cual una aplicación podría degradarse es debido a una posible latencia de I/O del disco en el equipo de almacenamiento de datos existente y el mejor mecanismo de recuperación sería reubicar el disco de la máquina virtual impactada en un equipo alternativo de almacenamiento de datos.

Las acciones de vMotion anteriormente descritas pueden configurarse aún más programando la ejecución de una tarea de reinicio por parte de CE en caso de que se desee contar con una acción de remediación más agresiva (de ser necesario).

Recuperación Ante Desastres Ampliada para Entornos VMware

CE amplía la capacidad de recuperación ante desastres de la solución Site Recovery Manager (SRM) de VMware incorporando funcionalidades de recuperación de equipos físicos con el soporte nativo para la recuperación de máquinas virtuales. Esto beneficia en gran medida a los administradores de los centros de datos de TI, quienes constantemente deben implementar y gestionar múltiples estrategias distintas para la recuperación ante desastres en sus entornos físicos y virtuales.

CE permite a los administradores de VMware crear un "paso SRM" que puede añadirse a su plan de recuperación de SRM para permitir que los equipos físicos y las máquinas virtuales protegidos por CE participen en las funciones de conmutación por error y recuperación de los sistemas a través de SRM. Este "paso SRM" crea un guion para designar cuál réplica de la máquina virtual del servidor físico será el servidor activo al ejecutar el plan de recuperación de SRM. Normalmente es necesario crear dos guiones de recuperación como parte del "paso SRM", uno para la conmutación por error y otro para la recuperación. Estos guiones deben ubicarse en el mismo servidor que el servidor SRM y se insertan en el plan de recuperación de SRM como una entrada de "paso de comando".

Una vez realizada la configuración, los administradores de VMware pueden hacer uso de todas las funciones de SRM disponibles, incluyendo las pruebas del plan de recuperación y las ejecuciones reales de dicho plan, en el contexto de los equipos físicos y las máquinas virtuales protegidos por CE.

Tome Nota:

- El instalador independiente de Neverfail Engine está disponible con Engine v6.7 (anteriormente conocido como Heartbeat) y en versiones anteriores.
- Los pares de protección P2P actualmente no son compatibles con el paquete de instalación integrado con el Servicio de Gestión de Engine en la edición empresarial o de escritorio.

Paquetes de Instalación e Implementación

CE está disponible en dos distintos paquetes de instalación, dependiendo del modo de configuración deseado. Estos incluyen:

- Paquete de instalación CE integrado con el Servicio de Gestión de CE
- Paquete de instalación CE autónomo

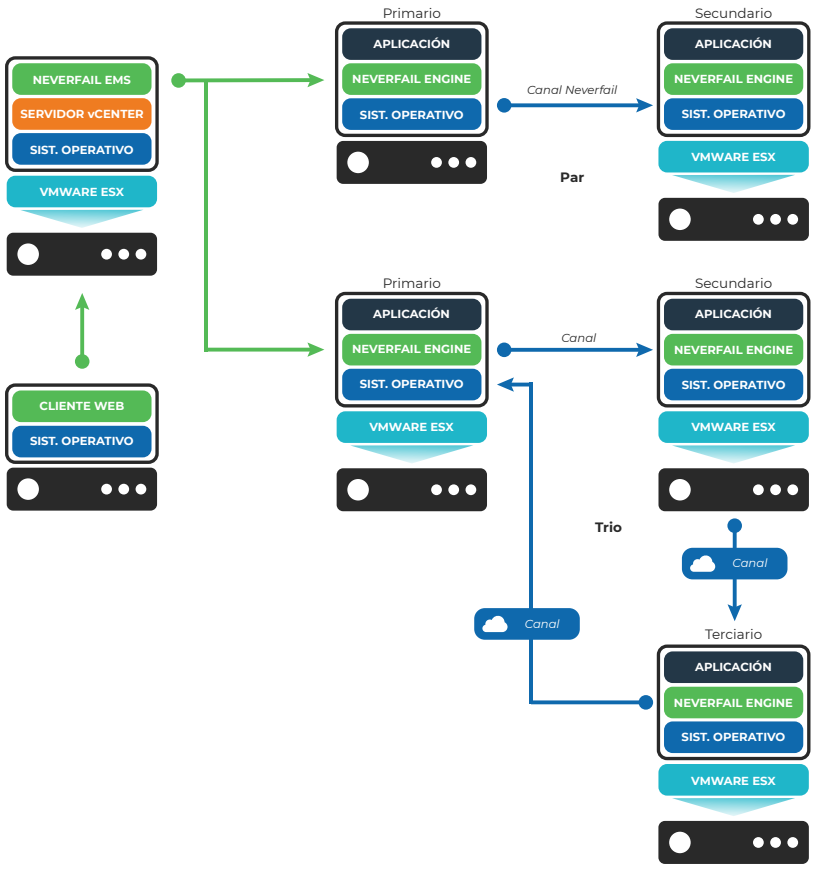


Figura 8: Marco Tecnológico del Servicio de Gestión de Engine

Paquete de Instalación Integrado con el Servicio de Gestión de VMware CE Edición Empresarial o de Escritorio

Este método de implementación se recomienda para los entornos virtuales de VMware al proteger a las aplicaciones que se ejecuten en equipos físicos o máquinas virtuales y cuando el servidor de respaldo secundario sea una máquina virtual de VMware, es decir, un par de protección físico a virtual (P2V) o virtual a virtual (V2V).

Con esta opción, el paquete de instalación de Engine v7.1 implementa el Servicio de Gestión de Engine (EMS). El EMS controla los servicios de Engine y la configuración en múltiples pares de protección remotos (o clústeres de Engine) para proveer una disponibilidad continua consciente de la aplicación. Como parte del proceso de instalación, EMS se ejecuta como un servicio web autónomo para que pueda ser gestionado por los administradores.

Es posible acceder a los servicios web de EMS con cualquier navegador web estándar. El EMS también provee un hook al cliente web de VMware vSphere para agilizar el acceso a los servicios de vSphere.

La Edición Empresarial de EMS puede instalarse como parte de una plataforma para implementar y gestionar todas las implementaciones de Engine. La Edición de Escritorio de EMS fue diseñada para implementaciones pequeñas — generalmente cinco pares o menos cuando no se requiera de una gestión de nivel empresarial. Esta versión debe instalarse en un servidor independiente con Windows que esté conectado a través de la red a una instancia remota del servidor vCenter de VMware.

Con el EMS, los administradores pueden implementar, configurar y gestionar la protección Neverfail Engine de extremo a extremo, mientras llevan a cabo la mayoría de las operaciones de disponibilidad de rutina.

Al implementar un nuevo par de protección de Engine mediante este método de instalación, Engine aprovecha su integración con VMware Converter para crear un clon del equipo físico objetivo como parte de la implementación del servidor secundario. Consulte la Figura 9.

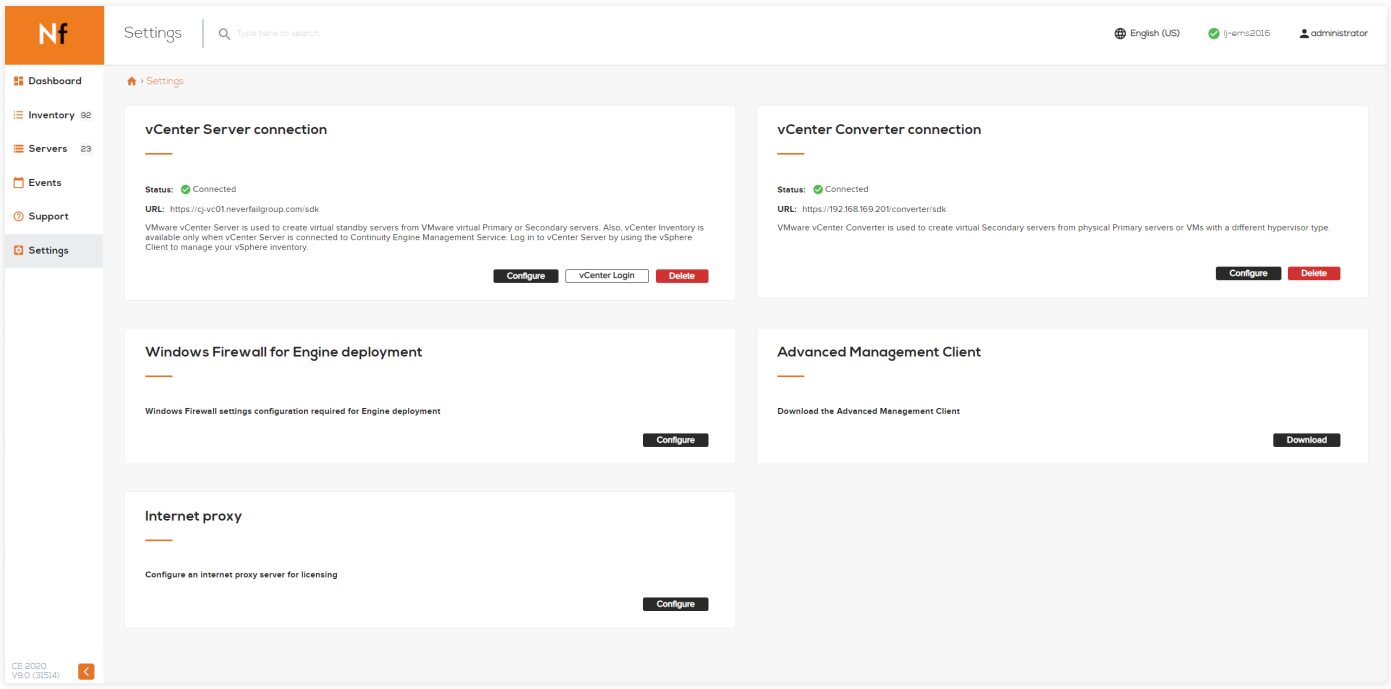


Figura 9: Integración con VMware Converter

Del mismo modo, Engine automatiza la creación de servidores secundarios para un par de protección de máquinas virtuales (V2V) aprovechando el mecanismo de clonación V2V incorporado en el servidor VMware vCenter, lo que reduce significativamente el proceso de implementación general del par de protección de Engine.

También es posible descubrir y gestionar las implementaciones existentes de los clústeres de Engine utilizando la interfase del cliente web de EMS (Heartbeat) 6.7 de Engine. Consulte las Figuras 10 y 11.

También contamos con un Cliente de Gestión CE de Escritorio autónomo para configuraciones más avanzadas en un clúster existente de Engine.

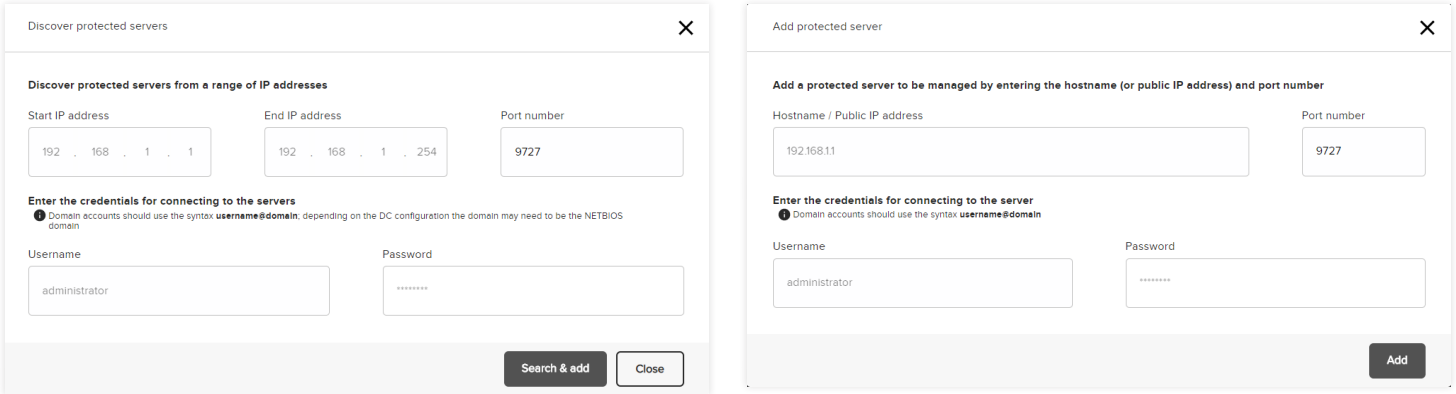


Figura 10: Gestión de Clústeres Existentes de Engine

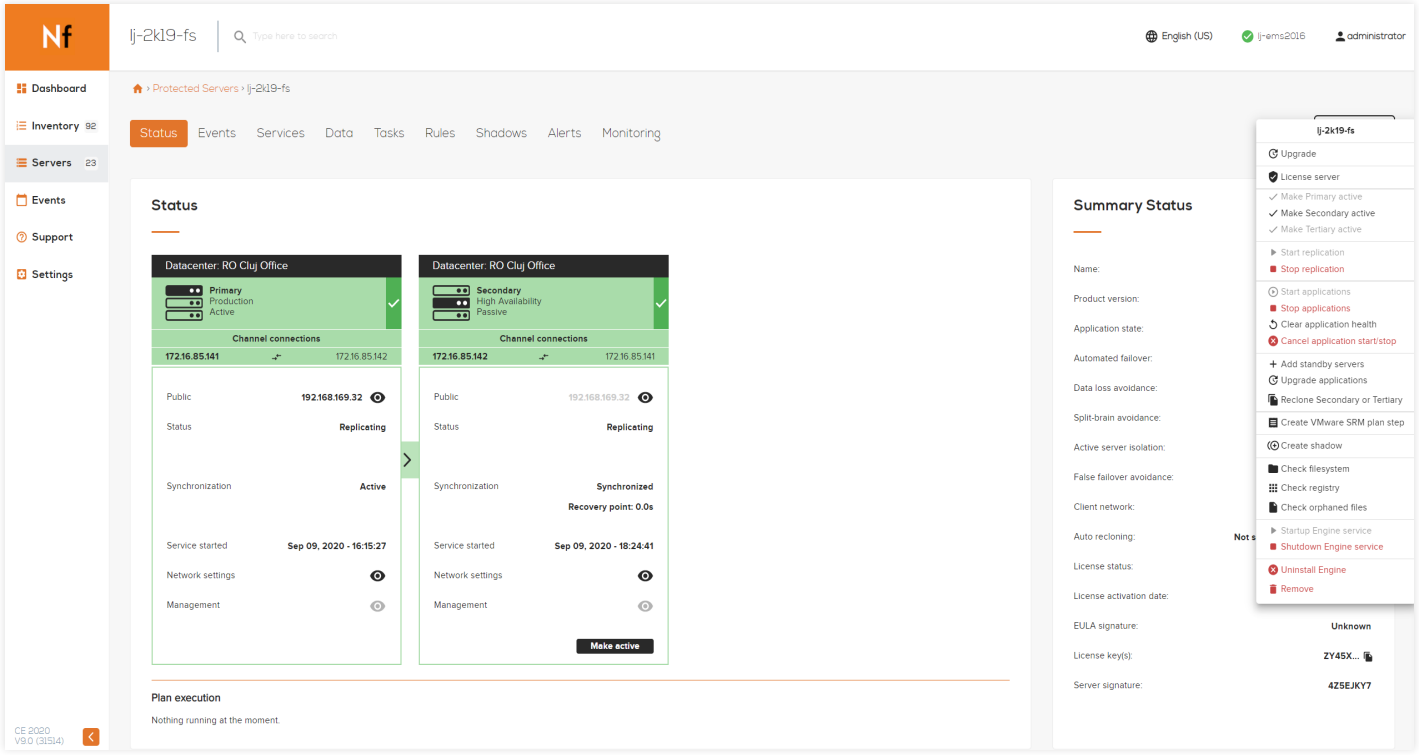


Figura 11: Administración Básica Utilizando el Servicio de Gestión de Engine

Arquitectura de los Componentes

Neverfail Continuity Engine consta de varios conceptos y componentes interrelacionados que funcionan conjuntamente para proporcionar óptimos niveles de disponibilidad continua y protección contra una amplia gama de fallos.

La arquitectura (Figura 12) detalla los componentes lógicos clave de una instancia de Neverfail Continuity Engine.

Figure 12: Engine Component Architecture

Verificación del Servidor, Optimización y Evaluación del Desempeño (SCOPE)

El primer componente a considerar es SCOPE. Este componente asegura el éxito de la implementación de Neverfail proporcionando información precisa, actualizada y completa sobre el entorno de los servidores. También provee información detallada sobre el estado operativo actual del entorno y ofrece recomendaciones para optimizar los servidores antes de instalar Neverfail Engine.

El componente está integrado en Engine 7.x y se ejecuta automáticamente como parte del proceso de implementación de Engine. Al utilizar el instalador autónomo de Neverfail Engine 6.7 como opción de implementación, SCOPE está disponible como una utilería independiente que puede ejecutarse manualmente en cada nodo del servidor que vaya a ser configurado como parte de un clúster de Engine.

Engine

El componente básico de Continuity Engine coordina las operaciones y gestiona la comunicación entre los servidores. También realiza las funciones complejas de replicar los datos hacia/desde otros servidores protegidos por Engine a nivel del núcleo de Windows mientras las aplicaciones se ejecutan en el sistema operativo.

Engine también gestiona la conmutación por error, los cambios y las reversiones entre los diversos servidores en un clúster de Continuity Engine, sincronizando la actividad según sea necesario entre las instancias activas y pasivas.

Marco Tecnológico de Gestión de las Aplicaciones

Otro de los componentes principales de Neverfail Engine es el Marco Tecnológico de Gestión de las Aplicaciones (AMF). AMF se encarga de detectar los fallos en tiempo real, descubrir los cambios en el estado de cualquier aplicación protegida, gestionar las interdependencias y realizar el registro o desregistro en tiempo real de las nuevas aplicaciones protegidas a través de módulos específicos de aplicaciones (plugins) o adaptadores de terceros.

Los plugins para aplicaciones de Neverfail permiten encapsular la información sobre la mejor manera de proteger una aplicación específica, incluyendo las interdependencias entre los servicios relacionados y las entradas del registro. Puesto que AMF conoce el estado de cada plugin o módulo de aplicación, incluyendo el estado de cualquier recurso asociado (tal como entradas de registro o servicios), es posible configurarlo para gestionar también

las interdependencias entre las aplicaciones.

Por ejemplo, el plugin de la aplicación Microsoft SQL Server pudiera detectar que a pesar de que se están ejecutando correctamente las consultas SQL (operaciones de lectura) en un servidor de producción crítico con una base de datos SQL, no se han registrado transacciones de escritura SQL durante el periodo previsto del umbral operativo. Por lo tanto, no se están cumpliendo los niveles de servicio esperados.

En este caso, se puede configurar Engine para que emita automáticamente una alerta a través de diversos métodos de notificación o incluso cambie a otra instancia de SQL Server. Sin embargo, al cambiar de SQL Server a otra instancia, se pueden afectar las comunicaciones entre SQL Server y un servicio de aplicación relacionado, tal como SharePoint.

Por lo tanto, aunque la instancia de SharePoint funcione correctamente, es posible que sea necesario cambiar esta aplicación al mismo tiempo de manera coordinada.

Por último, AMF puede personalizarse para proteger cualquier aplicación de Windows que se bloquee. Mediante el uso de un módulo genérico para las aplicaciones ("plugin"), Neverfail Engine puede monitorear y gestionar el estado de los servicios de Windows relacionados con cualquier aplicación. También se pueden implementar tareas personalizadas para realizar un monitoreo de los principales indicadores de desempeño específicos de la aplicación. Esto significa que podemos ampliar la protección de Neverfail Engine más allá de las funciones que ofrecen los módulos estándar para aplicaciones de tipo comercial (plugins), siempre y cuando las aplicaciones en cuestión cumplan con ciertas condiciones de "reiniciabilidad". Consulte la Figura 13.

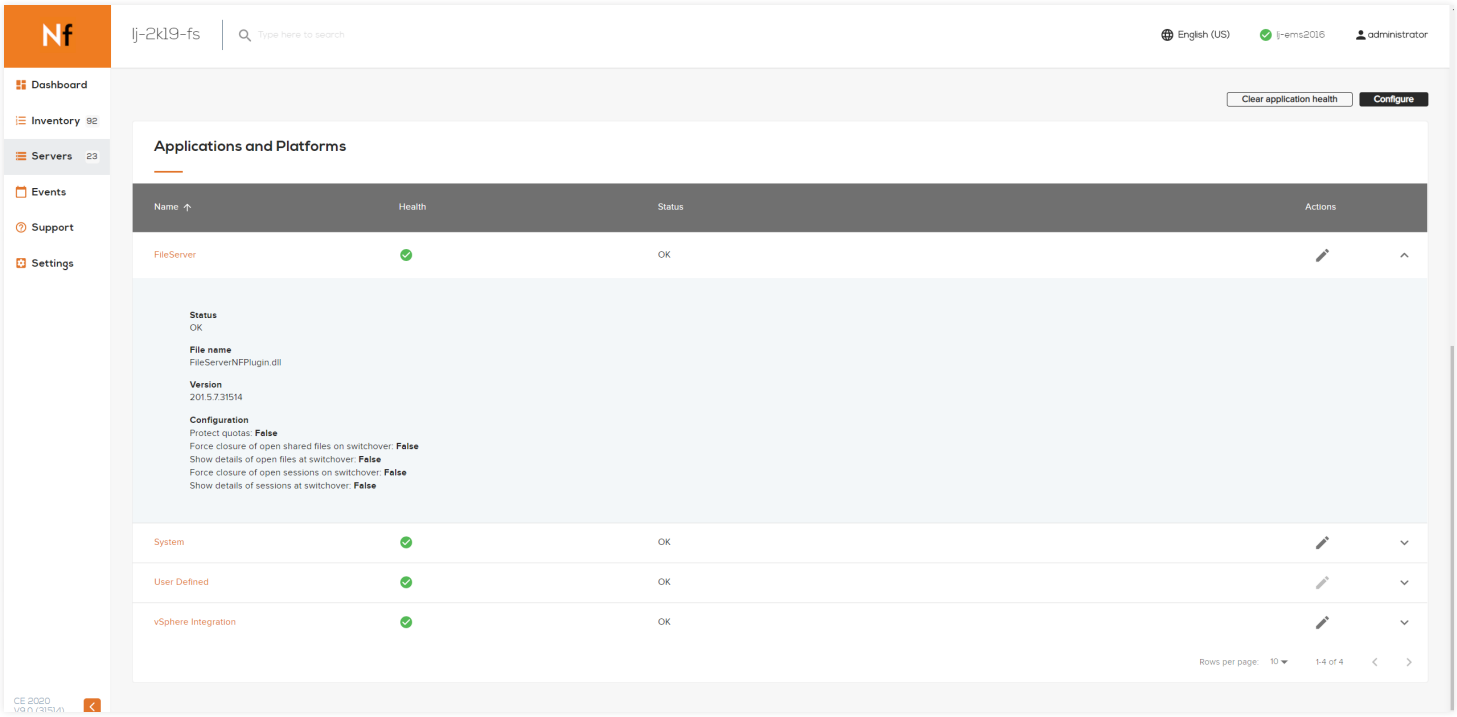


Figure 13: Application Plug-In

Consola Unificada de Gestión de Disponibilidad

La interfase de Gestión de Neverfail Engine permite monitorear y gestionar múltiples instancias de clústeres de Engine desde un mismo sitio. Esta funcionalidad actualmente está disponible en los siguientes formatos:

- Cliente de Gestión de CE Autónomo (basado en Java)
- Cliente Web del Servicio de Gestión de CE

Al asociar el nombre público (FQDN) o la dirección IP pública del servidor protegido, la interfase de gestión de Neverfail Engine se conecta a la instancia de Engine en ese servidor y permite visualizar los servidores primarios y secundarios (y terciarios, si están configurados) dentro del clúster de Neverfail Engine. El rol, el estado y la situación de cada servidor pueden consultarse fácilmente en la pantalla de resumen. Dependiendo del tipo de cliente de gestión que se utilice, las pestañas u opciones adicionales del menú de navegación permiten conocer los detalles relativos al estado de la aplicación, la red, los datos y los procesos de replicación.

Los cambios de configuración de los clústeres protegidos de Engine se pueden realizar utilizando el cliente de gestión

autónomo de Neverfail Engine sin interrumpir el proceso de replicación.

Además, es posible definir grupos de aplicaciones en la consola de gestión de Engine con el fin de supervisar y gestionar aplicaciones más complejas Al definir los grupos de aplicaciones en el cliente de gestión de Neverfail Engine, las advertencias y alertas de cualquiera de los servidores pertenecientes pasarán al nivel de grupo. El estado de todos los grupos puede consultarse simultáneamente en el cliente de gestión de Neverfail Engine a fin de identificar rápidamente cualquier problema dentro de la infraestructura protegida. Adicionalmente, se pueden configurar opcionalmente grupos de aplicaciones para cambiar a una ubicación remota de recuperación ante desastres (DR) como un contenedor lógico colectivo. Al coordinar el cambio de todo el grupo de aplicaciones, Neverfail Engine reduce la complejidad y las dependencias relacionadas con el traslado de una aplicación a un sitio de DR.

WANSmart

Continuity Engine ofrece capacidades de aceleración de la WAN (WANSmart), mismas que además de la compresión de datos predeterminada, proporcionan un algoritmo de deduplicación de datos en el momento para reducir considerablemente el ancho de banda necesario para soportar la replicación a través de una WAN. Al igual que otras soluciones de optimización de la WAN basadas en hardware que suelen ser muy costosas de adquirir e implementar, WANSmart de Continuity Engine es una implementación de software en todos los servidores que participan en el clúster de Engine, lo que reduce la cantidad de datos que deben enviarse al sitio remoto hasta en un 80%.

Cuando los servidores del clúster de Engine tienen una alta tasa de cambio de los datos protegidos, WANSmart ayuda a minimizar el costo de la conexión entre los centros de datos, además de asegurar que los cambios lleguen al sitio de recuperación ante desastres (DR) más rápido que si los datos se enviaran sin comprimir.

Resumen

Durante más de una década, Neverfail ha ayudado a más de 2,500 empresas a implementar las mejores estrategias de continuidad de las operaciones y soluciones de disponibilidad continua, desde PYMES hasta empresas que aparecen en la lista Fortune 50. Aprovechando muchos años de experiencia y un conjunto de tecnologías probadas, Neverfail Continuity Engine emplea una amplia gama de conceptos de disponibilidad para ofrecer funcionalidades de disponibilidad continua y recuperación ante desastres para todo tipo de aplicaciones y cargas de trabajo en cualquier organización de TI.

Mediante una combinación de elementos modulares de replicación de datos, clústeres de servidores, gestión de redes y monitoreo de los principales indicadores de rendimiento, Continuity Engine provee una protección total a las aplicaciones críticas, asegurando su disponibilidad las 24 horas del día y los 7 días de la semana sin importar el tipo de amenaza. Es la única solución de continuidad de TI consciente de las aplicaciones que se enfoca en eliminar el riesgo del tiempo de inactividad antes de que pueda tener un impacto en cualquier servicio o aplicación crítica de la que dependa la empresa.

Acerca de Neverfail

Neverfail permite que las empresas logren una disponibilidad del 100% en sus sistemas utilizando las soluciones de continuidad operativa y almacenamiento secundario más resilientes del mundo. Las soluciones de Neverfail fueron diseñadas para empresas con operaciones de misión crítica a fin de mitigar los riesgos del tiempo de inactividad ante cualquier posible interrupción. Al lograr una continuidad operativa libre de problemas, ayudamos a nuestros socios y clientes a desarrollar todo su potencial sin el

Honeywell vmware Mitel McKESSON citi Bank of America