



CONSEJO TÉCNICO

Diseñe un sistema de videovigilancia
enfocado en la fiabilidad

Redundancia

Introducción

Ofrecer un sistema de videovigilancia fiable es esencial cuando se trata de empresas de misión crítica, en las que cualquier fallo del sistema puede provocar pérdidas imprevisibles. Por esta razón, un sistema de videovigilancia siempre debe diseñarse siguiendo las mejores prácticas para maximizar la fiabilidad y minimizar el tiempo de inactividad.

Es necesario un plan de redundancia, pero puede dar una falsa sensación de seguridad si no se han abordado y eliminado los puntos de fallo individuales (que crean eslabones débiles en el sistema). Entre más elementos paralelos haya en un sistema, el riesgo de un fallo catastrófico será menor si alguno falla. El funcionamiento del sistema seguirá estando garantizado por los otros elementos, dando suficiente tiempo para reparar el fallo antes de que se produzca la interrupción total del sistema. En resumen, cuando se diseña un sistema de video enfocado en la fiabilidad hay que considerar que:

- Un sistema interconectado en cadena fallará cuando el elemento más débil falle. Por lo tanto, es importante que se diseñe cada elemento para que sea lo más fiable posible.
- Diseñar una ruta redundante para cada funcionalidad crítica permitirá que el sistema aguante un fallo de la rama mientras todo el sistema se mantiene en funcionamiento.
- Es fundamental realizar el monitoreo del estado de funcionamiento del sistema en tiempo real, así como la auditoría de fallos; el objetivo es repararlos con una latencia mínima.

El sistema será más predecible y requerirá menos intervenciones urgentes in situ para resolver los fallos críticos. En general, esto se traducirá en un cliente más satisfecho, siendo este el objetivo principal de cualquier despliegue a gran escala.

El resto de este documento describirá cómo tales conceptos se han incorporado en las soluciones de videovigilancia de March Networks.

Diseño centrado en la fiabilidad: el enfoque de March Networks en materia de videovigilancia

La fiabilidad comienza con los componentes

Un sistema de videovigilancia se puede dividir en:

1. Elementos in situ.

Cámaras conectadas a una grabadora local, que luego se conecta a una red corporativa para el acceso local/remoto.

2. Servicios centrales.

Estos servicios, normalmente instalados en el centro de datos de la empresa, ofrecen una plataforma unificada a los diferentes tipos de usuarios (investigadores, administradores, vigilantes, etc.) para supervisar, gestionar, dar seguimiento y agregar datos de todos los recursos del sitio.



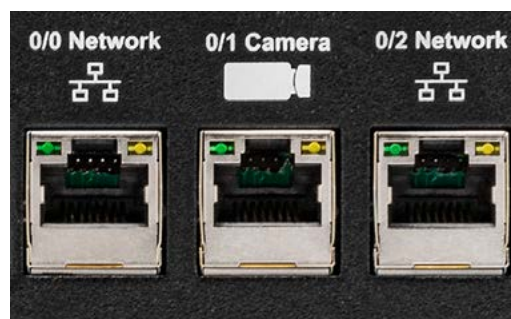
Figura 1: Detalle de la parte trasera de la grabadora de la serie X. Los tres puertos de red disponibles están diseñados para ofrecer diferentes vías de comunicación para las cámaras locales (0/1), la conectividad primaria (0/0) y la redundante (0/2) con la red corporativa.

Analicemos los distintos componentes por separado.

Grabadoras de video en red (NVR)

March Networks diseña y supervisa la fabricación de todas sus plataformas de grabación integradas. Nuestro objetivo es proporcionar componentes fiables que raramente fallen, reduciendo así las tareas de mantenimiento in situ. Por ejemplo, nuestra familia de grabadoras híbridas de la serie X ofrece un extraordinario tiempo medio entre fallos (MTBF) de más de 268,000 horas (aproximadamente 30 años). Esto representa uno de los MTBF más altos (si no el más alto) disponible en el mercado. Además, las siguientes características pueden aumentar aún más la fiabilidad:

- Fuente de alimentación redundante (disponible para ciertas familias de grabadoras)
- Ventiladores redundantes
- Interfaces de red redundantes (disponibles para ciertas familias de grabadoras)
- Batería interna para garantizar un apagado correcto y evitar la corrupción de archivos en caso de pérdida de corriente
- Configuración RAID para el almacenamiento
- Sistema operativo (OS) y aplicación en un chip flash dedicado



Cámaras

Supervisamos la fabricación de todas nuestras cámaras y personalizamos el firmware para tener un control completo de todas las funciones, y así reducir al mínimo la aparición de problemas de hardware o errores de software. Cuando lo combinamos con nuestra función de gestión masiva, podemos garantizar que todas las cámaras IP siempre ejecutarán la última versión del firmware que incluye correcciones de errores y parches de seguridad, lo que permite un funcionamiento fluido del dispositivo.

Redundancia de la capa de aplicación

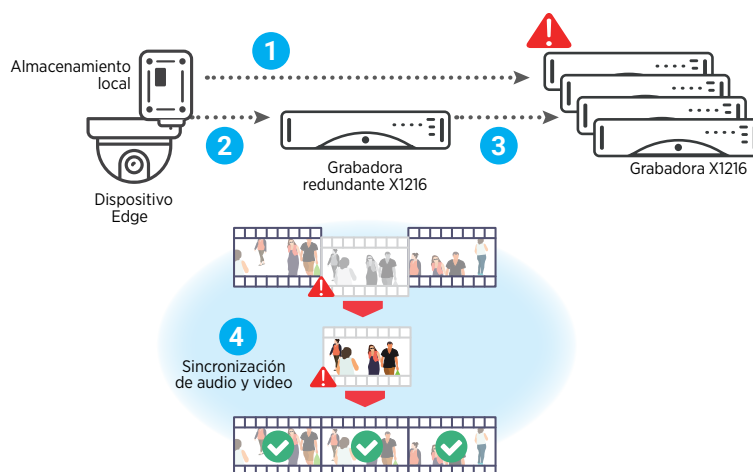
Como se señaló anteriormente, la selección de una solución fiable compuesta por un grabador, un conmutador y las cámaras es el requisito previo para reducir el tiempo de inactividad del sistema in situ. El paso siguiente es trabajar en la arquitectura del sistema para reforzar aún más la solución.

Reducir la desconexión de la cámara al grabador

En el caso de una desconexión de la red entre las cámaras y el grabador, cuando se utilizan las cámaras y el software Command de March Networks, se podrá configurar



Figura 2: Normalmente, las cámaras IP transmitirán a las respectivas NVR de producción (ruta 1). En caso de que falle una NVR, la NVR redundante sustituirá a la que falló (ruta 2), y luego enviará el video grabado a la NVR de producción una vez reestablecida (ruta 3, incluida la actividad 4 para la sincronización del video grabado). Además, el almacenamiento local de la cámara hará una copia de respaldo del video durante el proceso para evitar cualquier pérdida de información durante la grabación.



la grabación a una tarjeta SD en la cámara. Esta función de March Networks se llama Shadow Archiving. Una vez resuelta la desconexión, la grabación en la tarjeta SD de la cámara se podrá pasar al NVR. El video se puede colocar en la secuencia/intervalo de tiempo exacto para una cobertura de grabación ininterrumpida.

Para ciertos modelos de cámaras, también es posible tener una fuente de alimentación redundante [Power over Ethernet (PoE) y una fuente de alimentación externa] para mantenerla en operación en caso de que falle el conmutador.

Reducir los fallos de la grabadora

Nuestras grabadoras híbridas de la serie X y el software VMS (software Command Recording o CRS) soportan una redundancia M:N. Esto quiere decir que es posible configurar M unidades en estado de espera para supervisar de manera activa N grabadoras de producción. En el caso de que una N falle, una grabadora en estado de espera M ocupará su lugar. El escenario más común es tener una grabadora de repuesto monitoreando una o más grabadoras de producción, de esta manera se ofrece redundancia en caso de un fallo y da margen al personal de mantenimiento para reemplazarla. El software Command de March Networks puede configurarse para transferir automáticamente el archivo temporal creado en la grabadora redundante a la grabadora de producción, una vez que se haya restablecido el servicio.

Redundancia de servicios centrales

Nuestro software de gestión central (software Command Enterprise o CES) se utiliza para monitorear el estado de funcionamiento y las actividades de los usuarios de cada sitio, realizar la gestión masiva del firmware y configurar las grabadoras y las cámaras. También ofrece derechos de acceso de usuario personalizables para que los administradores del sistema puedan otorgar diferentes niveles de acceso a los diferentes usuarios. Esta solución de software de multiservidores también alberga aplicaciones adicionales, tales como nuestro software de inteligencia de negocios Searchlight. Es evidente que mantener este servicio operando en todo momento es crucial para la utilización completa del sistema.



Analicemos las opciones disponibles para reforzar la fiabilidad de los servicios CES. Estas opciones dependen del tamaño de la instalación y de los recursos informáticos disponibles. Esto nos llevará a una de las siguientes configuraciones:

CES conectado a una base de datos SQL Express que se ejecuta en el mismo servidor físico

Para las pequeñas y medianas instalaciones (hasta un máximo de 250 grabadoras/sitios), es posible instalar el software CES apoyándose en una instancia de SQL Express creada en el mismo servidor.

Durante el proceso de instalación, se puede seleccionar “Base de datos interna” para que el paquete de instalación también instale la edición de SQL Express en el mismo servidor y configure el entorno para crear la conectividad entre el servicio CES y la instancia de SQL. Esta es la forma más sencilla de instalar CES y se requiere una intervención mínima por parte del departamento de TI del cliente.

En términos de redundancia, se necesita un servidor de respaldo que sustituya el servidor primario que falló. Antes de iniciar el servicio CES en el servidor de respaldo, hay que cargar las últimas copias de respaldo de la base de datos y de la configuración a partir del servidor primario CES. Se encuentran más detalles sobre este procedimiento en la [Guía de instalación de Command Enterprise](#) en el capítulo 4 “Respaldo y restauración: conmutación por error a un servidor redundante”.

Para evitar que el servicio CES se detenga para hacer una copia de respaldo de la base de datos, una opción interesante es instalar una instancia independiente de la base de datos Microsoft SQL Express en el servidor primario y elegir “Base de datos externa” al instalar el software CES. De esta manera, el departamento de TI del cliente podrá acceder a la instancia de la base de datos y programar respaldos periódicos. Se encuentran más detalles sobre este procedimiento en la [Guía de instalación de Command Enterprise](#) en el capítulo 4 “Migración de la base de datos interna a una base de datos externa”.

CES conectado a una base de datos SQL Express ejecutado en el mismo servidor virtual

Este escenario ofrecerá las mismas opciones de instalación descritas en la sección anterior (base de datos interna o externa utilizando SQL Express en el mismo servidor — apto para un máximo de 250 servidores/sitios), pero simplificará considerablemente el procedimiento de respaldo de los datos de CES. Es generalmente fácil tomar instantáneas periódicas de la máquina virtual completa, lo que hace que la recuperación tras desastres sea bastante sencilla de implementar. Descargue simplemente la última instantánea cuando se haya detectado que el servidor primario falló (el procedimiento completo se puede gestionar de manera automática por la aplicación de gestión de la virtualización). En el caso de que el software falle, ni siquiera es necesario utilizar recursos adicionales — es suficiente con destruir la máquina virtual defectuosa y ejecutar la última instantánea.

CES en un servidor físico conectado a una base de datos SQL Profesional/ Empresarial que se ejecuta en un servidor diferente

Esta es la configuración que recomendamos para instalaciones medianas y grandes (más de 250 grabadoras/sitios). En términos de redundancia, se pueden programar la configuración de CES y las copias de respaldo de la base de datos externa como se requiera y sin ninguna limitación. Considerando que muchas empresas



Atención y soporte al cliente

Norteamérica, Sudamérica y Australia

Teléfono: 1.613.591.1441

Número gratuito (EE.UU. y Canadá):
1.800.472. 0116

Correo electrónico:
techsupport@marchnetworks.com

Europa

Teléfono: +39 0362 17935 ext. 3 (CET)

Correo electrónico:
emeatechsupport@marchnetworks.com

Medio Oriente y África

Teléfono: +00 971(0)52 818 8483

Correo electrónico:
supportmea@marchnetworks.com

cuentan con una instancia de servidor SQL como recurso informático disponible, es posible utilizar la estructura existente para conectar el servicio CES y aprovechar la programación de los respaldos de la base de datos.

En caso de que falle el servidor CES primario, será necesario iniciar un servidor redundante utilizando el último respaldo de la configuración CES primaria y, una vez en línea, éste se conectará a la instancia SQL existente.

CES en un servidor virtual conectado a una base de datos SQL Profesional/ Empresarial

Quizás este es el enfoque más flexible. Debido a que el servidor es virtual, es esencial programar instantáneas periódicas del servidor CES y restaurar la última instantánea en caso de que el software falle.

Un fallo de hardware del servidor que aloja el servicio CES no es generalmente un problema. En los grandes departamentos de TI, hay varios procedimientos para gestionar eficazmente la redundancia de hardware.

Conclusión

March Networks considera la fiabilidad en general y la ciberseguridad como dos aspectos fundamentales a la hora de diseñar una solución de videovigilancia. Hemos descrito los principales elementos de acción que forman parte de nuestra solución para garantizar que nuestros clientes no experimenten fallos catastróficos en el sistema. También hemos proporcionado algunas directrices sobre las mejores prácticas para garantizar que el video esté disponible cuando se necesite. Adoptar un sistema fiable es una inversión a largo plazo que reduce el mantenimiento del sistema y las tareas no planificadas en el sitio, disminuyendo el costo total de propiedad de la solución.

Póngase en contacto con el equipo de ingeniería de ventas de March Networks para obtener más detalles. Ellos trabajarán con usted para identificar la mejor opción dependiendo de los requisitos específicos de su negocio.

Generalidades de la compañía

March Networks® ayuda a las organizaciones a transformar el video en inteligencia de negocios a través de la integración de la videovigilancia, las analíticas, los datos de los sistemas de información del negocio y los dispositivos IoT. Las empresas de todo el mundo utilizan nuestras soluciones de software para mejorar la eficiencia y el cumplimiento normativo, reducir las pérdidas y los riesgos, mejorar el servicio al cliente y ser más competitivas. Con una presencia consolidada en la seguridad por video y redes, March Networks también es reconocida como líder en gestión de video escalable de clase empresarial y servicios alojados. Estamos orgullosos de trabajar con muchas de las instituciones financieras, comercios, operadores de cannabis y autoridades de transporte más grandes del mundo. Ofrecemos nuestro software y sistemas a través de una extensa red de distribuidores y socios en más de 70 países. Fundada en el 2000, March Networks tiene sus oficinas centrales en Ottawa, Ontario, Canadá. Para más información, por favor visite: www.marchnetworks.com.



North America 1 800 563 5564
Latin America +5255 5259 9511
Europe +39 0362 17935
Asia +65 6818 0963
Australia and New Zealand +61 1300 089 419
Middle East and Africa +971 4 399 5525

© 2022 March Networks. All rights reserved. Information in this document is subject to change without notice. MARCH NETWORKS, March Networks Command, March Networks Searchlight, March Networks RideSafe, and the MARCH NETWORKS logo are trademarks of March Networks Corporation. All other trademarks are the property of their respective owners. 060-3469-SP-A marchnetworks.com

