GDPR

WHITE PAPER

QNAP

Nuevo Reglamento Europeo sobre Protección de Datos Personales (GDPR - Reglamento General de Protección de Datos): toda la oferta de QNAP para apoyar a las empresas durante y después de las adaptaciones necesarias para cumplir con el Reglamento.

¿Qué es el RGPD?

El RGPD (Reglamento General de Protección de datos) es el Reglamento Europeo 2016/679 que cubre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos. Este Reglamento sustituye a la Directiva europea sobre protección de datos personales (Directiva 95/46/CE) adoptada en 1995 y derogará las normas contradictorias establecidas en el Código sobre protección de datos personales (Decreto Legislativo nº 196/2003). El Reglamento fue adoptado el 27 de abril de 2016 y se implementará completamente en los países de la UE a partir del 25 de mayo de 2018 después de un período de transición de dos años y, a diferencia de las Directivas, no se requiere una ley de solicitud de los estados miembros.

El RGPD tiene como objetivo unificar y estandarizar, dentro de la Unión Europea, las diferentes reglas que rigen el procesamiento de datos personales, definiendo de manera definitiva las formas en que los datos y la información deben ser almacenados, protegidos y accedidos por parte de las empresas. El RGPD es aplicable a compañías no pertenecientes a la UE si proporcionan bienes o servicios a personas residentes dentro de la Unión Europea.

Debe subrayarse que las reglas en el RGPD serán de aplicación general y no prevén requisitos específicos o diferentes dependiendo del tamaño, tipo o sector en que opera la Compañía.

Según la Comisión Europea, los datos personales representan cualquier información sobre un individuo relacionada tanto con su vida privada, profesional o pública. Pueden referirse a cualquier información: nombres, fotos, direcciones de correo electrónico, datos bancarios, publicaciones en sitios web de redes sociales, registros médicos o direcciones IP informáticas.

Los pasos a llevar a cabo: del registro de actividades de procesamiento al plan de adaptación para lograr el cumplimiento

El principal objetivo del RGPD es garantizar que los datos personales no se divulguen, se protejan y se controlen. Los cambios introducidos por el RGPD, que pueden implicar cambios en la forma en que se organizan los procesos de gestión de datos, requieren que las compañías planifiquen cuidadosamente durante un período de tiempo muy limitado, dado que el periodo para la adaptación está ya muy cerca (aproximadamente seis meses).

Las empresas deben establecer un Plan de Adaptación para cumplir con los requisitos del RGPD. En este paso, se evaluará el modelo actual de la organización, para definir un plan con acciones detalladas a implementar en la Compañía.

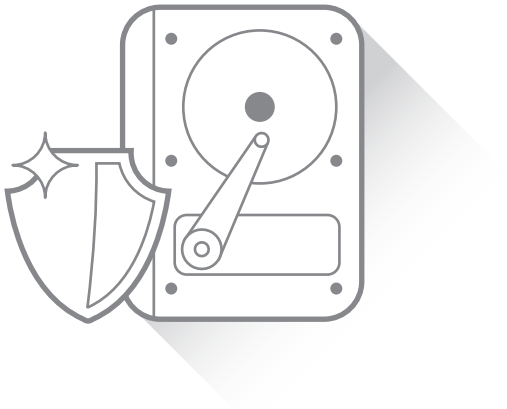
El Plan de Adaptación, que se implementará siguiendo un enfoque estructurado, debe tener en cuenta dos áreas importantes en la Tecnología y la Informática:

• El Área de Procesos y Reglas. Sin duda, esta es una de las áreas más afectadas por los requisitos de adaptación en el RGPD. A destacar por ejemplo la portabilidad de datos, la gestión de violación de los datos, el registro de actividades de procesamiento y los derechos de los datos de los interesados. La privacidad por diseño es también otro aspecto crucial, en otras palabras el RGPD requiere un nuevo enfoque que establece la obligación de las empresas de comenzar un proyecto, planificando desde el inicio las herramientas para proteger los datos personales.

• El Área de Tecnología y Herramientas. Esta es un área crucial, incluso considerando la inversión presupuestada en el Plan de Adaptación. Incluye medidas de seguridad informática (antivirus, recuperación de desastres, firewall, seudónimización de datos, criptografía de datos, prevención y detección de violaciones de datos, gestión de identidades, etc.), seguridad física (por ejemplo controles de acceso), adopción de herramientas GRC de TI (gobernanza, riesgos y cumplimiento).

El RGPD establece un marco legal centrado en las tareas y la responsabilidad del controlador de datos. Las nuevas reglas requieren que el Controlador garantice el cumplimiento de los principios establecidos en el Reglamento, y también que sea capaz de demostrar tal cumplimiento, adoptando una serie de herramientas especificadas en el RGPD.

Cómo puede ayudarle QNAP a proteger sus datos



El NAS de QNAP le permite encriptar todos sus datos o carpetas individuales, usando el cifrado AES de 256 bits. Otros mecanismos de protección de datos incluyen configuraciones de RAID, instantáneas y S.M.A.R.T. (Tecnología de informes y análisis de autocontrol).

• Configuración RAID flexible

El NAS de QNAP admite tipos de RAID completos, incluidos RAID 1/5/6/10/50/60, 5+ repuesto en caliente, 6+ repuesto en caliente y 10+ repuesto en caliente. Puede habilitar la configuración RAID más adecuada para reducir de forma efectiva el riesgo de pérdida de datos provocada por fallos inesperados en el disco duro y, al mismo tiempo, mantener el rendimiento óptimo del sistema.

• Protección de instantáneas

Las instantáneas permiten que su NAS de QNAP registre el estado del sistema en cualquier momento. Si surge una situación inesperada en su sistema, siempre puede volver a un estado anterior que la instantánea haya grabado. Storage Manager incorpora una herramienta de instantánea fácil de usar y basada en la web, para que pueda hacer copias de seguridad y restaurar datos fácilmente en cualquier momento para evitar la pérdida de datos importantes.

• S.M.A.R.T. diagnóstico del disco duro

El sistema S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology) muestra el estado de los discos duros instalados en el NAS de QNAP, lo que le permite tomar medidas tempranas si el resultado de alguno de los valores del S.M.A.R.T. se considera anormal, mitigando así el riesgo de pérdida de datos causada por el fallo físico del disco duro.

• Cifrado AES de 256-bit del NAS completo

El NAS de QNAP admite el cifrado basado en volúmenes para proteger los datos confidenciales. Se necesita un código de seguridad y una contraseña para montar un volumen codificado al iniciar el NAS de QNAP. En el NAS de QNAP no se puede acceder a todos los datos sin la clave de cifrado que lo protege contra el acceso no autorizado y la violación de datos confidenciales, incluso en el caso de que los discos duros y el NAS fueran robados. Algunos modelos NAS admiten el cifrado acelerado por hardware que elimina los datos codificados de la carga de trabajo de la CPU, lo que proporciona un rendimiento más rápido al tiempo que garantiza una protección de datos segura.

• Cifrado de discos externos

El NAS de QNAP también puede encriptar dispositivos de almacenamiento externos para proteger contra el acceso no autorizado. El personal de TI tiene la opción de encriptar los volúmenes de disco en una partición específica del dispositivo externo usando AES-128, AES-192 o AES-256.

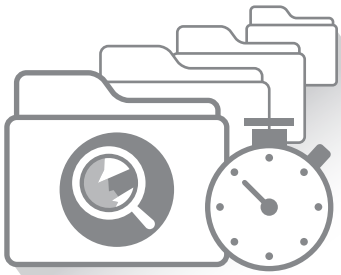
• Protección de grado militar

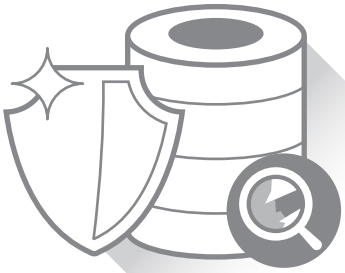
Para cifrar unidades de almacenamiento internas y externas, se utiliza el método de encriptación AES de 256 bits de grado militar. Este método es validado mediante FIPS 140-2 CAVP (Programa de Validación de Algoritmos Criptográficos) y ayuda a evitar que se acceda a datos comerciales confidenciales en el caso de que los discos duros o todo el sistema NAS fueron robados.

Cómo puede ayudarle QNAP a gestionar sus datos

• Qsirch es un potente motor de búsqueda del NAS

Existen muchas ventajas para las empresas, en particular la posibilidad de recuperar documentos y archivos para crear propuestas, informes, contratos y más. Tanto la productividad como la efectividad pueden aumentar considerablemente con Qsirch

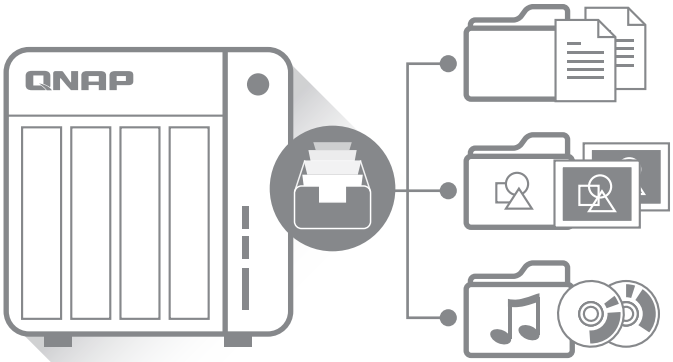




Qsirch funciona siguiendo los derechos de acceso para carpetas compartidas y cuentas de usuario. Qsirch protege eficazmente la privacidad de los datos y los resultados de las búsquedas proporcionan acceso solo a los archivos a los que el usuario tiene permiso a acceder. Los administradores pueden agregar y eliminar fácilmente carpetas compartidas específicas para Qsirch. Las carpetas compartidas se pueden excluir selectivamente de la indexación para garantizar la seguridad de los datos.

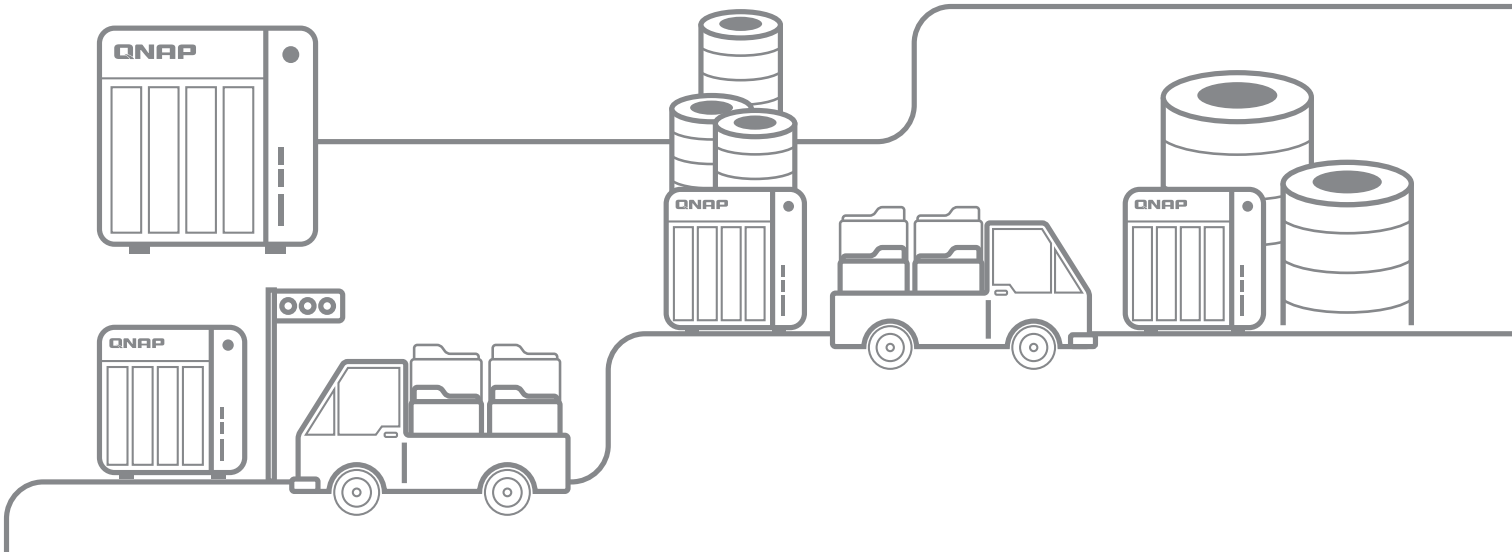
• Qfiling automatiza eficazmente la organización de archivos

Cuando el NAS de QNAP se utiliza como almacenamiento central de archivos, la posibilidad de organizar archivos de manera eficiente es un punto clave para administrar y usar archivos. Sin embargo, cuando se enfrentan a una gran cantidad de archivos distribuidos en muchas carpetas, clasificarlos y almacenarlos puede ser difícil, lento y agotador. Con Qfiling, la organización de archivos es automatizada y eficiente.



Las principales características de Qfiling son:

- Velocidad ▶ Qfiling se puede configurar con tan solo unos clics.
- Organización ▶ Los archivos se organizan según la configuración de los usuarios
- Aumento de la productividad ▶ La organización de los archivos es automática y en intervalos regulares, sin perder tiempo ni esfuerzo.
- Gestión optimizada ▶ Mantiene los archivos organizados para que los usuarios los localicen fácilmente.



Cómo puede ayudarle QNAP a gestionar sus usuarios

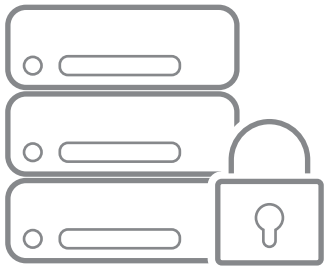
El NAS de QNAP admite varias funciones de seguridad para el sistema, el acceso a los datos y los archivos almacenados. El acceso cifrado protege las conexiones del sistema y de la comunicación, el bloqueo de IP impide el acceso a usuarios sospechosos, y el cifrado de los dispositivos de almacenamiento externo reduce el riesgo de que los datos sean usurpados si se sustraen los discos duros. La configuración avanzada de privilegios como Windows ACL, Windows Active Directory (AD) y LDAP Directory Service son también compatibles para simplificar la administración de controles de acceso. Las soluciones antivirus también son compatibles. Todas estas medidas hacen que el NAS de QNAP sea un espacio seguro para los archivos importantes.

Protección de acceso a la red

Los administradores de TI pueden definir una lista de conexiones autorizadas y no autorizadas para permitir el acceso de varios usuarios al NAS de QNAP utilizando una dirección IP. Funciona como un bloque automático de IP basado en criterios y protege el acceso a la red. Por ejemplo, este comando se puede configurar como "en 1 minuto, después de 5 intentos fallidos, bloquear la dirección IP durante 1 hora, 1 día o para siempre".

Si se rechaza una dirección IP, el host ya no puede conectarse al servidor, independientemente de los puertos de conexión que se utilicen.

Protección en entornos mixtos



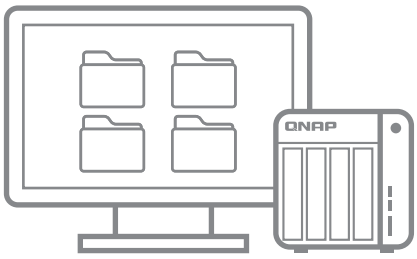
Por lo general, todos los usuarios profesionales usan un antivirus adecuado. Sin embargo, no es posible predecir el desarrollo de un virus y no es posible detener los intentos voluntarios de los usuarios de conectarse a páginas web peligrosas. Debido a que los archivos infectados en un entorno mixto pueden causar daños sustanciales, es importante tener una solución antivirus en el NAS de QNAP que ofrezca el acceso compartido de archivos multiplataforma.

Detección inteligente: la solución antivirus integrada en el NAS de QNAP garantiza un funcionamiento ininterrumpido de las actividades profesionales mediante la detección de los últimos virus, malware, gusanos y troyanos, con continuas y gratuitas actualizaciones de la base de datos de virus. Los análisis de virus se pueden personalizar y configurar para que se ejecuten según un programa, y con alertas por mail en caso de detección.

Mejor protección del sistema

Por lo general, un NAS con varios puertos LAN permite que todos los servicios de red habilitados accedan al contenido en el servidor a través de cada puerto LAN. La protección de datos se reduce. En las empresas, solo las personas seleccionadas deben poder acceder a datos importantes utilizando un protocolo de red establecido que es una dirección IP interna. La combinación del servicio de NAS de QNAP ofrece a los administradores de TI la opción de permitir o bloquear servicios seleccionados de interfaces de red definidas para garantizar la protección del sistema.

onfiguración de permisos de Windows ACL



El NAS de QNAP es compatible con Windows ACL, lo que le permite aprovechar fácilmente la configuración de permisos de carpetas compartidas del sistema de Windows y los controles de acceso al NAS. Se pueden configurar permisos básicos y 13 permisos avanzados desde Windows y sincronizarlos con las configuraciones de permisos de la carpeta compartida del NAS. También son compatibles los permisos de subcarpetas y las configuraciones de privilegios de nivel de archivo. Los mismos permisos se pueden aplicar a AFP, FTP, File Station y Samba cuando se habilitan los permisos avanzados de carpetas para hacer cumplir el estricto control de acceso para una mayor seguridad de los datos.

Windows Active Directory (AD)

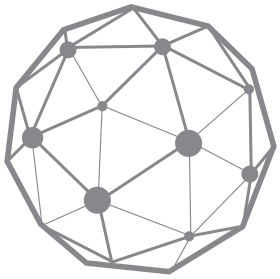
El NAS de QNAP se puede unir fácilmente a Windows AD para una eficiente administración de cuentas de usuario. Los administradores de TI pueden beneficiarse de la verificación de derechos de acceso centralizada para reducir las complejas configuraciones de privilegios, mientras que los usuarios de dominio pueden usar fácilmente su nombre de usuario y contraseña de Windows AD para conectarse a diferentes NAS de QNAP en la red local. El NAS de QNAP admite la implementación AD a gran escala de hasta 200.000 usuarios y grupos de AD.

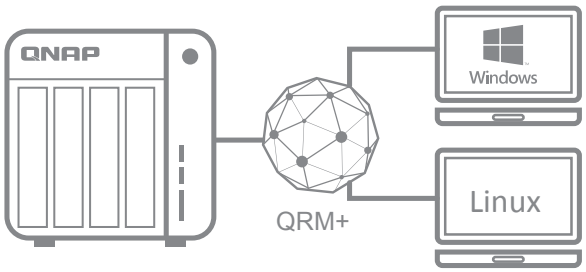
LDAP Directory Service

El soporte LDAP de QNAP permite que el NAS se agregue a los servicios de directorio basados en LDAP, como OpenLDAP. El servidor LDAP autentifica de forma centralizada a los usuarios y pueden usar el mismo nombre de cuenta y contraseña LDAP para acceder a cualquier NAS de QNAP que se haya agregado al servidor LDAP. Con un servidor LDAP incorporado y fácil de usar, el NAS de QNAP también se puede utilizar como un servidor LDAP para autentificar centralmente a usuarios y grupos en todos los demás dispositivos y aplicaciones habilitados para LDAP, para así ahorrar esfuerzos en la gestión y al mismo tiempo mejorar los datos seguridad.

Cómo puede ayudarle QNAP a gestionar sus sistemas

El QRM+ de QNAP (Remote Manager Plus de QNAP) y el Q'center son soluciones de gestión centralizadas y de interfaz única para que los equipos de TI detecten, mapeen, monitoricen y administren dispositivos en red de forma centralizada, como PC, servidores, thin clients y NAS de QNAP. El NAS de QNAP también proporciona registros de visualización basados en la web para un seguimiento eficiente y se puede utilizar como un servidor Syslog para almacenar centralmente los registros del sistema de todos los dispositivos en red.



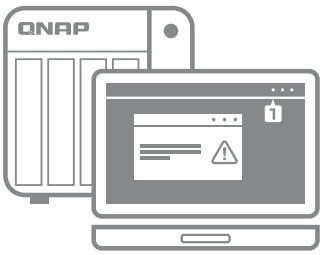


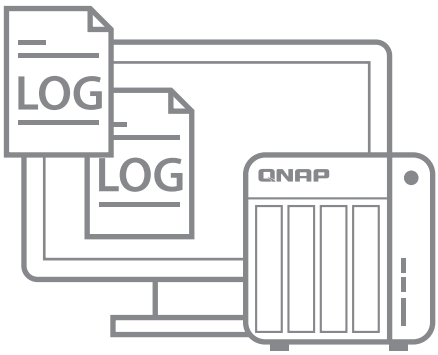
QRM+: Monitorización y gestión centralizada de dispositivos en red

QRM+ puede crear una lista de dispositivos conectados para que los administradores puedan monitorizar rápidamente su estado, incluidos los dispositivos compatibles con IPMI. QRM+ se puede utilizar para la supervisión en tiempo real, para evaluar el estado del dispositivo (incluida la temperatura, la velocidad del ventilador, los sensores, la fuente de alimentación y las notificaciones de eventos IPMI) de cada punto final siempre que sea necesario. Con QRM+, la administración remota de dispositivos de TI es segura, rápida y fácil.

Alertas y notificaciones: reciba alertas por adelantado antes de que ocurra un desastre

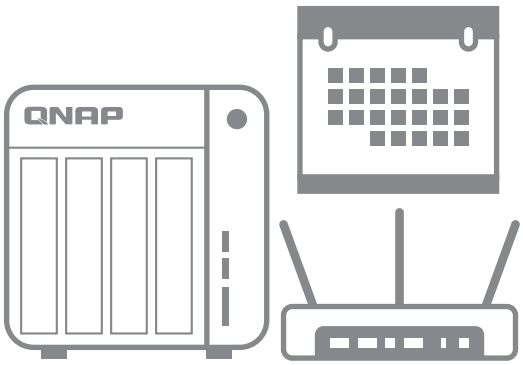
QRM+ cuenta con alertas para ayudar al personal de TI a corregir los problemas de rendimiento antes de que los usuarios, las aplicaciones y la empresa se vean afectados.





Sistema de registro completo

El NAS de QNAP ayuda a los administradores de TI a realizar un seguimiento eficaz del sistema al proporcionar registros de visualización basados en la web: los registros de eventos del sistema mantienen informados a los administradores de TI sobre la información, la advertencia y los eventos de error del NAS de QNAP; los registros de conexión del sistema permiten a los administradores de TI ver el historial de acceso de cada archivo (quién, cuándo y qué acciones se realizaron). Además, hay una lista de usuarios en línea disponible para monitorizar el acceso de los usuarios. Si se detecta una conexión sospechosa, los administradores pueden hacer clic con el botón derecho sobre el usuario para agregarle inmediatamente a la lista de usuarios bloqueados o a la lista de desconexión.



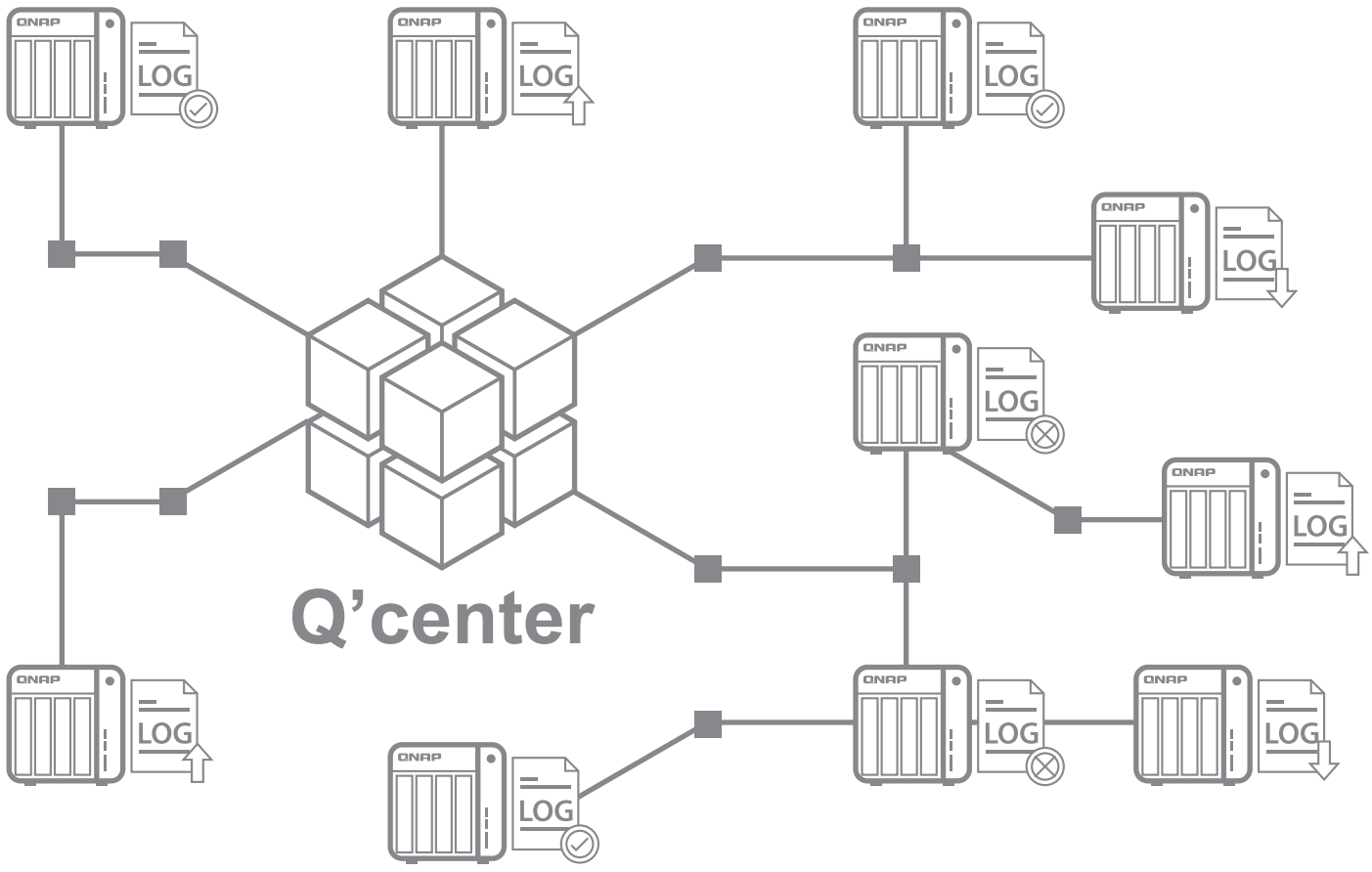
NAS de QNAP como un servidor Syslog

Un repositorio central de datos de registro de varios dispositivos de red permite una gestión eficiente y una auditoría de seguridad en las empresas. Al admitir protocolos UDP y TCP, el NAS de QNAP puede servir como un servidor Syslog, lo que permite a los administradores de TI recopilar y almacenar fácilmente registros de otros dispositivos en red en el NAS de QNAP para mejorar la eficiencia en la administración y la solución de problemas cuando sea necesario. Se proporcionan filtros avanzados y notificaciones por correo electrónico para ayudar a identificar rápidamente los fallos o amenazas de seguridad.

Además de jugar el rol de un servidor para recopilar registros de otros dispositivos, el NAS de QNAP también puede actuar como un cliente para enviar sus propios registros al servidor Syslog.

Q’center: Monitorice y administre centralmente todos sus NAS

Q'center puede administrar y monitorizar varios NAS clientes, satisfaciendo al mismo tiempo las necesidades de administración central y los objetivos de control de segmentos. La información, como la temperatura de los sistemas y la velocidad de los ventiladores, le permite reducir los riesgos de fallo de sistemas al utilizar las condiciones de la sala de control. También puede encender/apagar varios NAS a la vez con opciones de encendido preestablecidas para mejorar la accesibilidad y la eficiencia de sus NAS. Q'center también permite la supervisión central de los registros del sistema y puede gestionar las actualizaciones del firmware y el mantenimiento de todos los NAS de QNAP con un mínimo esfuerzo.

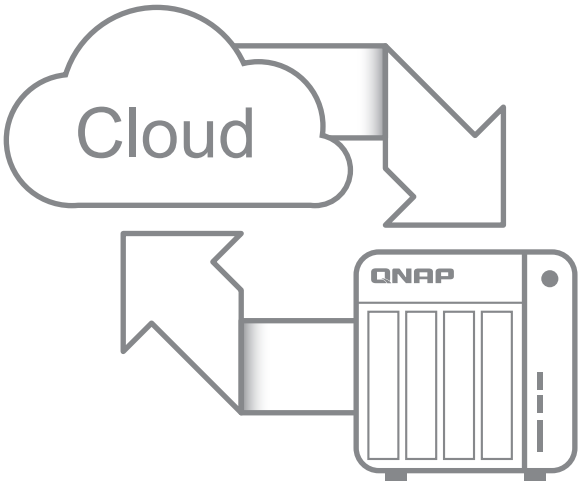


NAS de QNAP: Una eficiente solución de recuperación ante desastres

El NAS de QNAP admite varios métodos para realizar copias de seguridad, sincronizar y recuperar datos.

Hybrid backup sync

El Hybrid Backup Sync de QNAP concentra las funciones de copia de seguridad, restauración y sincronización en una única aplicación para que los usuarios transfieran datos fácilmente a espacios de almacenamiento locales, remotos y en la nube mediante RTRR (replicación remota en tiempo real), rsync, FTP y CIFS / SMB.



Copias de seguridad en la nube:

El NAS de QNAP ofrece soluciones de copia de seguridad en la nube seguras, fáciles de usar y repletas de características para respaldar datos en los servicios de almacenamiento disponibles en nubes públicas de tipo profesional como Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, Dropbox* y IBM SoftLayer. Incluso se admiten soluciones de nube de almacenamiento privado compatibles con OpenStack Swift y WebDAV.

Al diseñar un Plan de Adaptación para el RGPD, las compañías pueden optar por cumplir solo con los requisitos de la regulación actual o convertir esto en una oportunidad para crear valor en su organización, contribuyendo así a difundir una nueva cultura en el procesamiento de datos personales y crear una transformación digital real de los procesos de la empresa que gestionan los datos de clientes y empleados.

Los delincuentes informáticos están constantemente buscando los puntos débiles y están desarrollando ataques cada vez más dirigidos. Las soluciones de seguridad sostenibles deben evolucionar y adaptarse con actualizaciones frecuentes y el uso de información sobre amenazas tan pronto como esté disponible. La seguridad solo es útil si detecta amenazas, desencadena una reacción y garantiza la protección global de toda la estructura, desde los puntos finales hasta las redes y la nube híbrida.

¿Necesita realizar un backup remoto en territorio nacional?

La máxima de la implementación de esta ley es que siempre debe existir un modo confiable de poder borrar los datos personales a petición del propietario de los mismos. De este modo, se garantiza que la información personal, que es privada, no es utilizada por terceros sin el consentimiento expreso de la persona. Esto obliga a los integradores de sistemas y empresas relacionadas con el campo de la tecnología a disponer de un método efectivo de borrado de estos datos.

Los proveedores internacionales de almacenamiento en nube son una solución generalmente económica, eficiente y que provee de una gran disponibilidad de los datos. Sin embargo, no es siempre posible establecer compromisos legales vinculantes que aseguren el cumplimiento de la GDPR y sus posibles actualizaciones en determinados casos. Los proveedores de almacenamiento en data center nacionales, además de una disponer de soluciones más flexibles ante desastres (envío de discos duros por correo express certificado, requerimientos personalizados, etc), cuentan un ancho de banda dedicado a sus clientes para optimizar las velocidades de transferencia.

En lo que concierne a la GDPR, los data center locales hacen posible cumplir la ley de protección de datos mediante requerimientos de privacidad vinculantes específicos, que se pueden confirmar directamente con la empresa receptora de los datos. En España, QNAP ya cuenta con un primer data center de backup remoto certificado por QNAP, que cumple con el protocolo de transferencia remota RTRR de QNAP, certificación Tier II y asegura las máximas garantías de seguridad y redundancia con un 99.749% de disponibilidad, redundancia en alimentación, refrigeración y conexión, y con un máximo de 22 horas de downtime por año. Los datos almacenados en este data-center cuentan con una encriptación end-to-end, por la cual el cliente puede disponer de una clave única de desencriptación de los datos, lo cual le confiere un acceso exclusivo sin que el data center pueda acceder a esta información o transferirla a terceros para su distribución.

Big SAFEBOX Data

Más información sobre esta solución en www.bsbdata.com
Consulte y contacte con QNAP en https://www.qnap.com/es-es/before_buy para más información sobre la gestión de backups remotos