GDPR
OFICIÁLNÍ ZPRÁVA

QNAP

Nové evropské nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR): Společnost QNAP nabízí podnikům komplexní podporu nejen při provádění úprav požadovaných tímto nařízením.

Co je to GDPR?

GDPR (General Data Protection Regulation) je nařízení Evropské unie 2016/679, které se týká ochrany fyzických osob s ohledem na zpracování osobních údajů a volný pohyb takových údajů. Toto nařízení nahrazuje směrnici Evropské unie o ochraně osobních údajů (směrnice 95/46/ES) přijatou v roce 1995 a zruší odporující si předpisy zavedené v kodexu o ochraně osobních údajů (legislativní nařízení č. 196/2003). Nařízení bylo přijato 27. dubna 2016 a bude plně zavedeno v zemích EU od 25. května 2018 po dvouletém přechodném období a na rozdíl od směrnic nevyžaduje od členských států žádný prováděcí předpis.

Cílem GDPR je sjednotit a standardizovat v rámci Evropské unie odlišné předpisy, které řídí zpracování osobních údajů, a definitivně určit způsoby, jakými se mají údaje a informace společnostmi uchovávat, chránit a zpřístupňovat. GDPR se vztahuje také na společnosti mimo EU, které poskytují zboží a služby jednotlivcům s bydlištěm na území Evropské unie.

Je třeba zdůraznit, že předpisy v GDPR jsou všeobecně použitelné a nepředpokládají specifické nebo odlišné požadavky v závislosti na velikosti a typu společnosti či na tom, kde společnost působí.

Podle Evropské komise jsou osobní údaje jakékoli informace o jednotlivci, které se vztahují na jeho soukromý, profesní nebo veřejný život. Mohou se týkat jakýchkoli informací: jmen, fotografií, emailových adres, bankovních údajů, příspěvků na webových stránkách sociálních sítí, lékařských záznamů nebo počítačových adres IP.

Kroky, které je třeba podniknout: od záznamu o činnostech zpracování po adaptační plán za účelem dosažení shody

Hlavním účelem GDPR je zajistit, že osobní údaje nebudou zveřejněny a že budou chráněny a sledovány. Změny představené v GDPR, které mohou zahrnovat změny ve způsobu, jakým jsou organizovány procesy, od společností vyžadují důkladné plánování v průběhu velmi krátkého časového období, protože lhůta pro zavedení se rychle přibližuje (přibližně šest měsíců).

Společnosti musí zavést adaptační plán, který odpovídá požadavkům v GDPR. V tomto kroku je třeba zhodnotit současný model organizace, aby se mohl definovat plán s podrobnými kroky, které musí společnost učinit.

Adaptační plán, zaváděný strukturovaným přístupem, musí vzít v úvahu dvě důležité oblasti v technologiích a IT:

• Oblast procesů a předpisů. To je bezpochyby oblast, která je adaptačními požadavky v GDPR významně ovlivněna. Například přenositelnost údajů, řízení narušení bezpečnosti údajů, záznam činností zpracování a práva subjektů údajů. Ochrana soukromí již při návrhu je dalším důležitým aspektem. Jinými slovy se jedná o nový přístup vyžadovaný předpisy v GDPR, který společnosti zavazuje, aby již při zahájení projektu plánovali nástroje k ochraně osobních údajů.

• Oblast technologií a nástrojů. Jedná se o klíčovou oblast, která také zvažuje zahrnutí investic do rozpočtu adaptačního plánu. Bezpečnostní opatření v oblasti IT (antiviry, obnova po havárii, firewall, pseudonymizace osobních údajů, šifrování osobních údajů, předcházení a detekce narušení bezpečnosti údajů, správa identity apod.), fyzická bezpečnost (např. kontrola přístupu), IT nástroje v oblasti kontroly, rizik a dodržování předpisů.

GDPR zavádí právní rámec zaměřený na úkoly a odpovědnosti správce údajů. Nové předpisy vyžadují, aby správce zajistil dodržování zásad zavedených v tomto nařízení a také aby byl schopen takové dodržování prokázat, a to přijetím řady nástrojů určených v GDPR.

Jak společnost QNAP pomáhá chránit Vaše údaje

Datové úložiště QNAP NAS Vám umožňuje zašifrovat všechny data nebo jednotlivé složky pomocí 256bitového šifrování AES. K dalším mechanismům ochrany dat patří konfigurace RAID, snímky a monitorovací systém S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology).

• Flexibilní konfigurace RAID

Úložiště QNAP NAS podporuje komplexní typy RAID včetně RAID 1/5/6/10/50/60 a hot spare 5+, 6+ a 10+. Použijte tu nejvhodnější konfiguraci RAID, abyste efektivně snížili riziko ztráty dat způsobené neočekávanou poruchou pevného disku a zároveň zachovali optimální výkon systému.

• Ochrana pomocí snímků

Snímky umožňují úložišti QNAP NAS kdykoli zaznamenat stav systému. Pokud na vašem systému dojde k neočekávané situaci, můžete obnovit předchozí stav, který zaznamenal snímek. Storage Manager vám dodává snadno použitelný webový snímkovací nástroj, pomocí kterého můžete snadno zálohovat a obnovovat svá data zpět do jakéhokoli bodu a zabránit tak ztrátě důležitých dat.

• Kontrola pevného disku technologií S.M.A.R.T.

Monitorovací systém S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology) zobrazuje stav pevných disků instalovaných na úložišti QNAP NAS, což vám umožňuje vykonat včasná opatření, pokud je kterákoli hodnota S.M.A.R.T. označena jako abnormální, a zmírnit riziko ztráty dat způsobené fyzickou poruchou pevného disku.

• 256 bitové šifrování AES celého úložiště NAS

Úložiště QNAP NAS podporuje šifrování svazků za účelem ochrany citlivých údajů. Pro připojení šifrovaného svazku při spuštění úložiště QNAP NAS je zapotřebí bezpečnostní kód a heslo. Bez šifrovacího klíče, který chrání před neoprávněným přístupem a narušením citlivých údajů na úložišti QNAP NAS, není možný přístup ke všem údajům, a to i v případě, že dojde k odcizení pevných disků a zařízení NAS. Některé modely NAS podporují hardwarově akcelerované šifrování, které odstraňuje šifrovaná data z pracovní zátěže procesoru, a poskytují tak rychlejší výkon a zároveň zajišťují ochranu údajů.

• Šifrování externích disků

Zařízení QNAP NAS také dokáže zašifrovat externí úložná zařízení, aby je chránila před neoprávněným přístupem. Pracovníci oddělení IT mají možnost zašifrovat diskové svazky na konkrétním oddílu externího zařízení pomocí šifrování AES-128, AES-192 nebo AES-256.

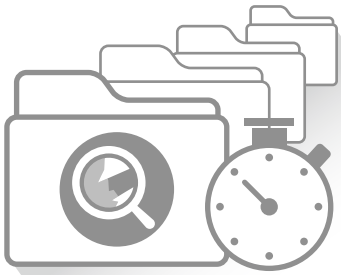
• Ochrana na vojenské úrovni

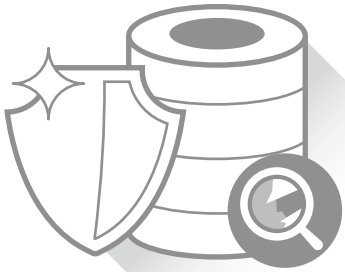
Pro šifrování interních a externích úložných jednotek se používá 256bitová metoda šifrování AES na vojenské úrovni. Tato metoda disponuje ověřením FIPS 140-2 CAVP (program pro ověřování kryptografických algoritmů) a pomáhá předcházet neoprávněnému přístupu k citlivým obchodním datům, když dojde k odcizení pevných disků nebo celého systému.

Jak společnost QNAP pomáhá spravovat Vaše údaje

• Výkonný vyhledávací nástroj Qsirch na zařízení NAS

Pro společnosti představuje bezpočet výhod, například možnost získávání dokumentů a souborů pro vytváření návrhů, zpráv či smluv. Nástroj Qsirch může výrazně zvýšit produktivitu a efektivitu.

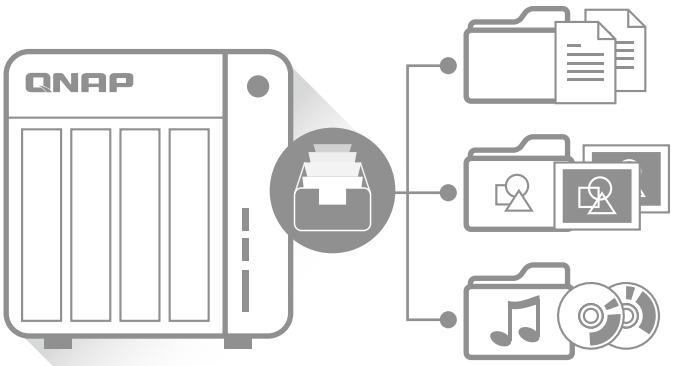




Nástroj Qsirch funguje tak, že sleduje přístupová práva pro sdílené složky a uživatelské účty. Nástroj Qsirch účinně chrání soukromí dat a výsledky vyhledávání uvádějí pouze soubory, ke kterým má daný uživatel přístup. Správci mohou pro nástroj Qsirch snadno přidat a odstranit specifické sdílené složky. Sdílené složky lze selektivně vyloučit z indexování, aby se zajistilo zabezpečení dat.

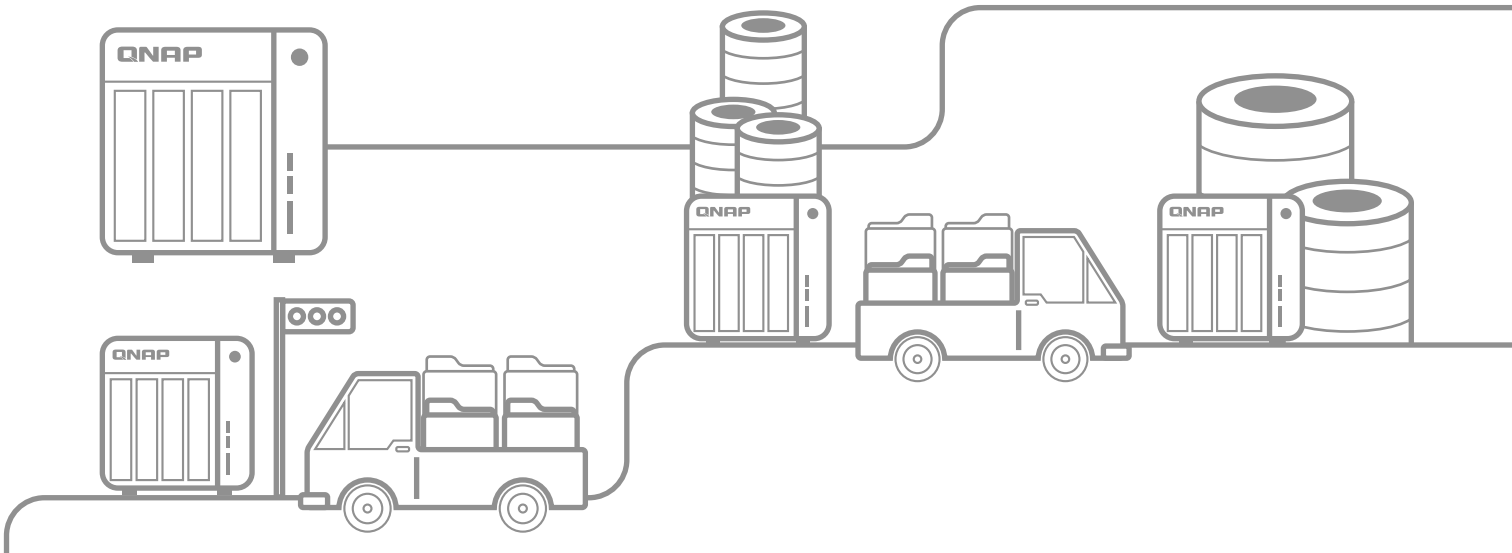
• Qfiling účinně automatizuje uspořádání souborů

Při používání QNAP NAS v roli centrálního souborového centra je schopnost efektivního uspořádání souborů klíčovým principem správy a používání souborů. Když se však musíme zabývat rozsáhlým množstvím souborů rozmístěných v mnoha složkách, jejich klasifikace a ukládání bývá časově náročné a únavné. S programem Qfiling probíhá uspořádání souborů automaticky a efektivně.



Hlavní funkce programu Qfiling:

- Rychlost ▶ Program Qfiling lze nastavit několika málo kliknutími.
- Organizace ▶ Soubory jsou uspořádány podle uživatelského nastavení.
- Zvýšená produktivita ▶ Uspořádání souborů probíhá automaticky a v pravidelných intervalech, aniž by se mrhalo časem nebo silami.
- Optimalizovaná správa ▶ Udržuje soubory uspořádané, aby je mohli uživatelé snadno vyhledat.



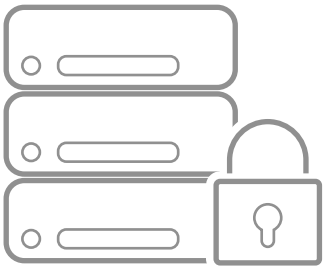
Jak společnost QNAP pomáhá spravovat Vaše uživatele

Pokud jde o systém, přístup k datům a uložené soubory podporuje zařízení QNAP NAS několik bezpečnostních funkcí. Šifrovaný přístup chrání systém a komunikační spojení, blokování adres IP zabraňuje v přístupu podezřelým uživatelům a šifrování externích úložných zařízení snižuje riziko, že se data zneužijí v případě odcizení pevných disků. Jsou podporována pokročilá nastavení práv, jako je Windows ACL, Windows Active Directory (AD) a adresářové služby LDAP, aby se zjednodušila správa kontroly přístupu. Rovněž jsou podporována antivirová řešení. Všechna tato opatření dělají ze zařízení QNAP NAS bezpečné místo pro Vaše důležité soubory.

Ochrana síťového přístupu

Správci IT mohou sestavit seznam autorizovaných a neautorizovaných spojení, aby pomocí adresy IP umožnili řadě uživatelů přístup do úložiště QNAP NAS. Ten funguje jako automatický blok adres IP založený na kritériích a chrání síťový přístup. Tento příkaz lze nastavit například jako„ po 5 neúspěšných pokusech za 1 minutu, blokovat adresu IP 1 hodinu, 1 den nebo vždy“.
Pokud je adresa IP odmítnuta, host se již nemůže k serveru připojit, a to bez ohledu na to, který připojovací port používá.

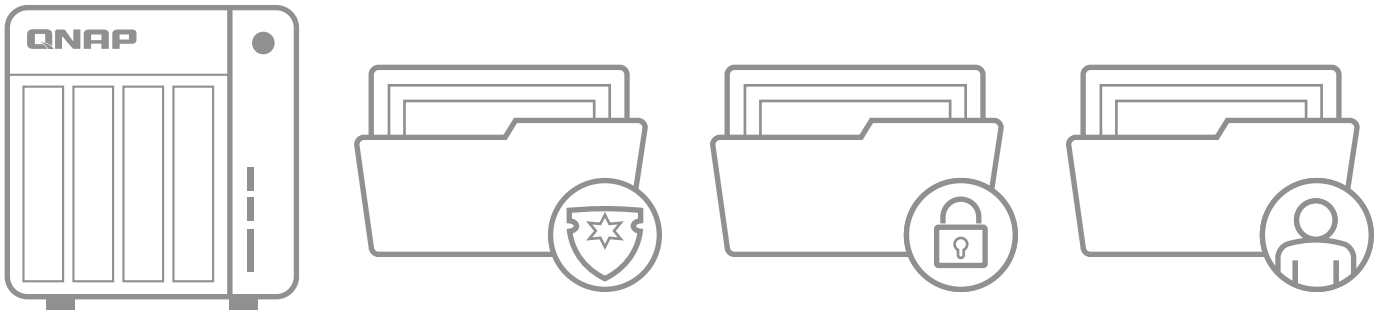
Ochrana ve smíšeném prostředí



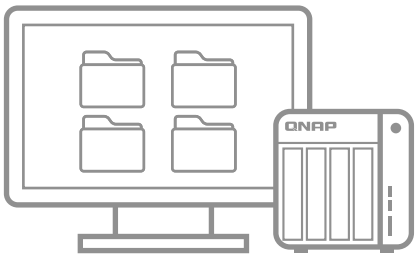
Podnikoví uživatelé obvykle používají vhodný antivirus. Není však možné předvídat vývoj virů a není možné zastavit záměrné pokusy uživatelů připojit se na nebezpečné internetové stránky. Vzhledem k tomu, že infikované soubory mohou ve smíšeném prostředí způsobit podstatnou škodu, je důležité mít na úložišti QNAP NAS antivirové řešení, které nabízí sdílení souborů mezi platformami.
Chytrá detekce: Integrované antivirové řešení pro QNAP NAS zajišťuje bezproblémový provoz podnikových činností prostřednictvím detekce nejnovějších virů, malwaru, červů a trojských koňů díky nepřetržité, bezplatné aktualizaci databáze virů. Skenování na přítomnost virů lze přizpůsobit a nastavit tak, aby probíhalo podle daného rozvrhu a v případě detekce viru zasílalo e-mailová upozornění.

Lepší ochrana systému

Úložiště NAS s několika porty LAN obvykle umožňuje, aby měly všechny povolené síťové služby přístup k obsahu na serveru přes všechny porty LAN. Ochrana dat je omezena. Ve společnostech by měly mít přístup k důležitým datům pouze vybrané osoby, a to prostřednictvím určeného síťového protokolu, který je interní adresou IP. Přiřazování služby QNAP NAS nabízí správcům IT možnost povolit nebo blokovat vybrané služby z určeného síťového rozhraní, aby se zajistila ochrana systému.



Nastavení práv pro Windows ACL



Úložiště QNAP NAS podporuje Windows ACL a umožňuje Vám snadno využít nastavení práv ke sdíleným složkám a kontrolu přístupu v systému Windows na zařízení NAS. Ze systému Windows lze nastavit základní práva a 13 pokročilých práv a synchronizovat je do nastavení práv ke sdíleným složkám zařízení NAS. Podporována jsou také práva k podsložkám a nastavení práv na úrovni souborů. Ta samá práva lze použít na AFP, FTP, aplikaci File Station a Samba, když jsou povolena pokročilá práva ke složkám, aby se zavedla přísnější kontrola přístupu za účelem lepšího zabezpečení dat.

Windows Active Directory (AD)

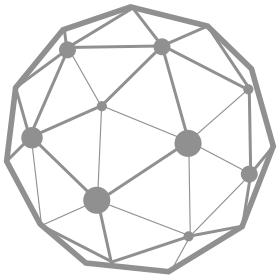
Úložiště QNAP NAS lze snadno propojit se službou Windows AD pro efektivní správu uživatelského účtu. Správci IT mají užitek z centralizovaného ověření přístupových práv, takže se zjednodušuje složité nastavování práv a uživatelé domény mohou zároveň snadno používat svůj účet a heslo ke službě Windows AD, aby se připojili k jinému úložišti QNAP NAS v místní síti. QNAP NAS podporuje velkoformátové zavedení s až 200 000 uživateli a skupinami služby AD.

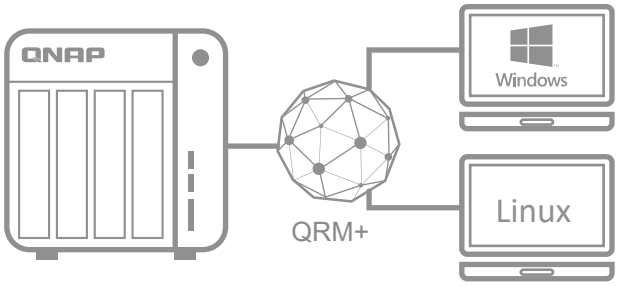
Adresářová služba LDAP

Podpora služby LDAP umožňuje přidání úložiště NAS k adresářovým službám LDAP, jako je například OpenLDAP. Uživatelé jsou pak centrálně ověřeni serverem LDAP a mohou použít stejný název účtu a heslo pro přístup ke kterémukoli úložišti QNAP NAS s přidaným serverem LDAP. S integrovaným a snadno použitelným serverem LDAP lze úložiště QNAP NAS použít také jako server LDAP k centrálnímu ověřování uživatelů a skupin u všech ostatních zařízení a aplikací s LDAP. Zjednodušuje se tím správa a zároveň se posiluje bezpečnost dat.

Jak společnost QNAP pomáhá spravovat Vaše systémy

QNAP QRM+ (QNAP Remote Manager Plus) a Q'center představují centralizované řešení správy s jedním rozhraním pro IT týmy pro centrální detekci, mapování, sledování a správu síťových zařízení, jako jsou počítače, servery, tencí klienti a úložiště QNAP NAS. Úložiště QNAP NAS také poskytuje webové protokoly pro efektivní sledování a lze jej použít jako server Syslog k centrálnímu uložení systémových protokolů pro všechna síťová zařízení.



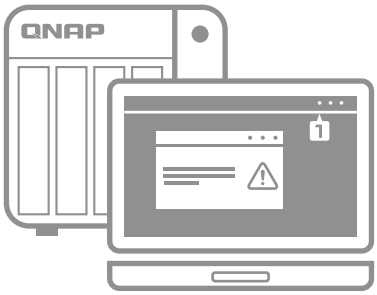


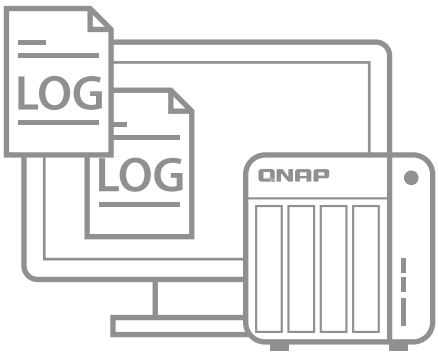
QRM+: Centralizované sledování a správa síťových zařízení

Aplikace QRM+ dokáže pro správce vytvořit seznam připojených zařízení, aby mohli rychle monitorovat jejich stav – včetně zařízení IPMI. Aplikaci QRM+ je možné použít pro sledování v reálném čase, pro přístup ke stavu zařízení (včetně teploty, rychlosti ventilátoru, napájení a oznamování událostí rozhraní IPMI) kteréhokoli koncového bodu, kdykoli je to třeba. S QRM+ je vzdálená správa zařízení IT bezpečná, rychlá a snadná.

Upozornění a oznámení: Přijímejte upozornění s předstihem, než dojde k havárii

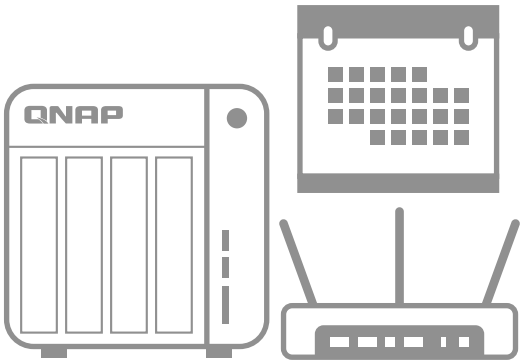
QRM+ obsahuje výstrahy, které pomáhají pracovníkům IT vyřešit problémy s výkonem předtím, než jsou jimi postiženi uživatelé, aplikace a společnost.





Komplexní protokolový systém

Zařízení QNAP NAS pomáhá správcům IT při efektivním sledování systému prostřednictvím webových protokolů: protokolární záznamy systémových událostí správcům IT sdělují informace, varování a chyby zařízení QNAP NAS; protokoly systémových připojení správcům IT umožňují zobrazit přístupovou historii u každého souboru (kdo a kdy vykonal jakou akci). Pro sledování uživatelského přístupu je navíc k dispozici online seznam uživatelů. Pokud se zjistí podezřelé připojení, správci mohou kliknout pravým tlačítkem myši na daného uživatele a ihned ho přidat na seznam zablokovaných nebo odpojených uživatelů.

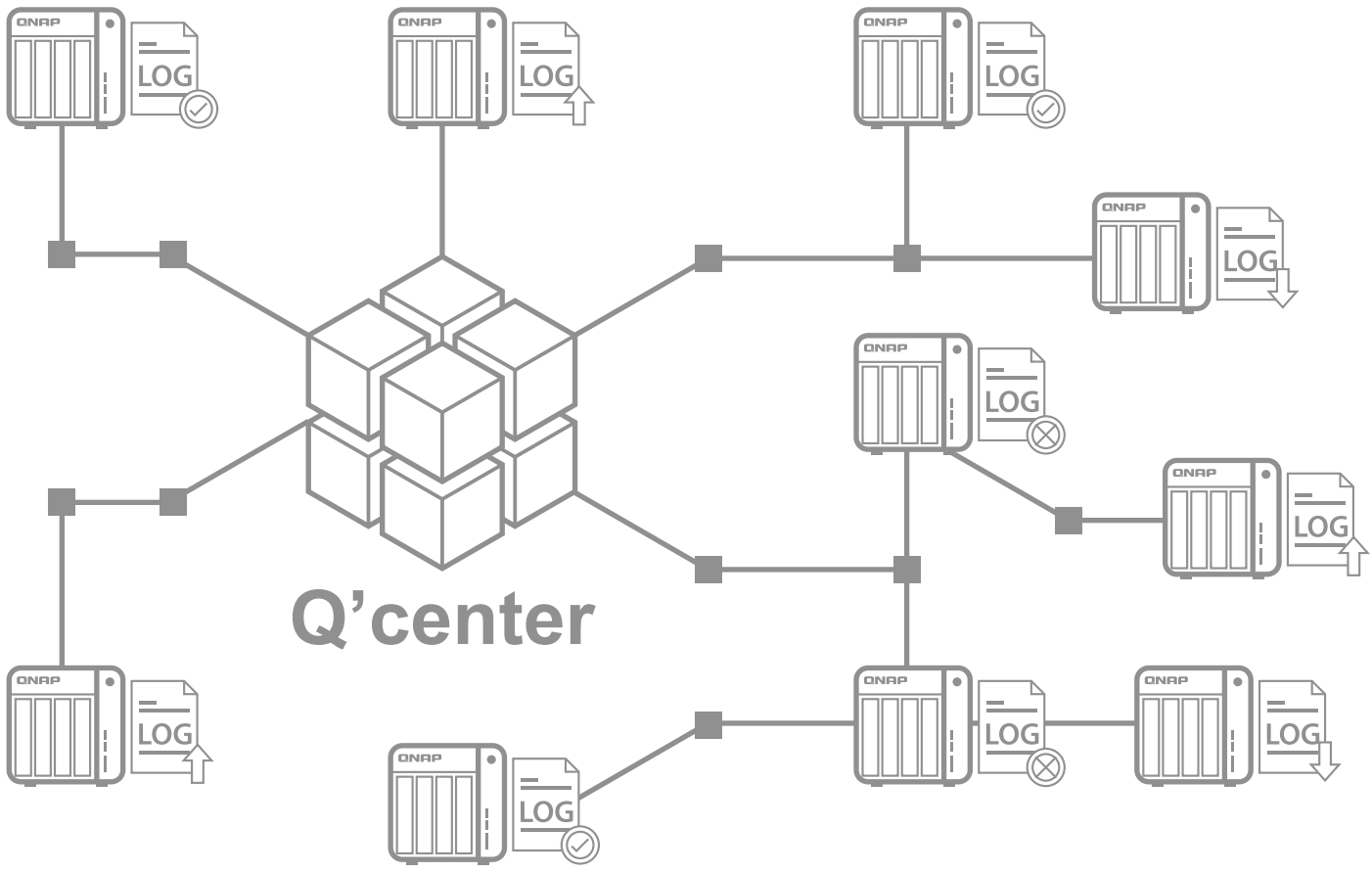


Zařízení QNAP NAS jako server Syslog

Centrální depozitář dat protokolů z různých síťových zařízení umožňuje v podnicích efektivní kontrolu správy a bezpečnosti. Zařízení QNAP NAS podporuje protokoly UDP a TCP, takže může sloužit jako server Syslog a umožnit správcům IT snadno shromažďovat a uchovávat protokoly z jiných síťových zařízení na úložiště QNAP NAS, aby se zlepšila efektivita při správě a řešení potíží, když je to zapotřebí. Pokročilé filtry a e-mailová upozornění pomáhají rychle identifikovat poruchy nebo bezpečnostní hrozby.
Kromě toho, že zařízení QNAP NAS plní úlohu serveru pro shromažďování protokolů z dalších zařízení, může se chovat také jako klient, který zasílá své vlastní protokoly na server Syslog.

Q’center: Centrální sledování a správa všech vašich zařízení NAS

Platforma Q’center dokáže současně spravovat a sledovat několik klientských zařízení NAS a plnit tak potřeby jak centrální správy, tak segmentované kontroly. Informace, jako jsou teploty systému a rychlosti ventilátoru, vám umožňují snížit rizika spojená se selháním systému pomocí řízení podmínek v místnosti. Můžete také najednou zapnout či vypnout více NAS pomocí přednastavených možností napájení pro vylepšení přístupnosti a účinnosti vašich zařízení NAS. Platforma Q’center také umožňuje centrální sledování systémových protokolů a řídí aktualizace firmwaru a údržbu u všech zařízení QNAP NAS, a to s minimálním úsilím.

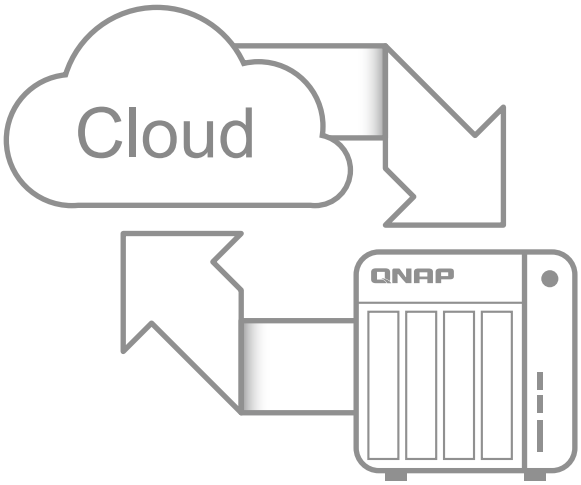


QNAP NAS: Účinný plán obnovy po havárii

Zařízení QNAP NAS podporuje několik metod zálohování, synchronizace a obnovy dat.

Hybrid Backup Sync

Hybrid Backup Sync společnosti QNAP konsoliduje funkce zálohování, obnovení a synchronizace do jedné aplikace, aby mohli uživatelé snadno přenášet data na místní, vzdálená i cloudová úložiště pomocí služeb RTRR (Real-Time Remote Replication), rsync, FTP a CIFS/SMB.



Cloudové zálohování:

Zařízení QNAP NAS nabízí cloudová řešení, která jsou bezpečná, snadno použitelná a nabitá funkcemi pro zálohování dat na veřejných cloudových úložištích podnikové třídy, jako jsou Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, Dropbox* a IBM SoftLayer. Podporována jsou také cloudová úložiště kompatibilní se službami OpenStack Swift a WebDAV.

Při vytváření adaptačního plánu pro GDPR si mohou společnosti zvolit, zda pouze dodrží požadavky aktuálního nařízení nebo zda tuto příležitost využijí k vytvoření hodnoty pro svou organizaci. Mohou přispět k šíření nové kultury v oblasti zpracování osobních údajů a způsobit skutečnou digitální transformaci podnikových procesů, které spravují data klientů a zaměstnanců.

Kriminálníci ze sféry IT neustále pátrají po slabinách a vymýšlejí stále cílenější útoky. Udržitelná bezpečnostní řešení se musí rozvíjet a přizpůsobovat – prostřednictvím četných aktualizací a využitím informací o hrozbách, jakmile jsou k dispozici. Zabezpečení je užitečné pouze v případě, že detekuje hrozby, vyvolává reakci a zaručuje globální ochranu v rámci celé struktury – od koncových bodů po sítě a hybridní cloudové služby.