Fiche produit

Fonctions de sécurité d'E-Series SANtricity OS

Sécurisation des ressources les plus importantes : les données

Principaux avantages

Amélioration de la confidentialité, l'intégrité et la disponibilité des données
Exploitation des fonctions de sécurité et des contrôles associés de NetApp E-Series SANtricity pour renforcer la confidentialité, l'intégrité et la disponibilité des ressources les plus importantes de l'entreprise : les données.

Création d'un environnement sûr
L'environnement Data Fabric de l'entreprise bénéficie d'un socle sûr et solide, et vous bénéficiez de la visibilité et des fonctionnalités permettant d'obtenir une infrastructure vraiment sécurisée.

Exploitation des bonnes pratiques du secteur et de NetApp en matière de sécurité
Mise en place d'une culture avancée de la sécurité grâce aux experts de NetApp, à leurs connaissances du secteur et aux pratiques communes.

Satisfaction des exigences de gouvernance et de conformité
Valorisation des bonnes pratiques établies en matière de sécurité pour respecter et soutenir la réglementation du secteur et les règles de sécurité.

Le logiciel de gestion du stockage NetApp® SANtricity® continue d'évoluer, et la sécurité fait partie intégrante de la solution. Les nombreuses caractéristiques et fonctions de sécurité de la solution E-Series SANtricity sont précieuses pour protéger la stratégie de sécurité de l'entreprise et appliquer les bonnes pratiques du secteur. Ces nouvelles fonctions donnent la priorité à la confidentialité, à l'intégrité et à la disponibilité des données.

Consulter plus d'informations sur la certification Critères communs de SANtricity OS 11.50 E-Series pour le profil de protection collaborative pour les appareils en réseau (Network Device Collaborative Protection Profile, NDcPP).

Pour en savoir plus sur les solutions NetApp de sécurité des disques et de gestion, consultez les rapports techniques TR-4474 : Sécurité des disques NetApp SANtricity et TR-4712 : Sécurité de gestion NetApp SANtricity.

Le challenge

Chaque jour, les menaces gagnent du terrain et sont plus sophistiquées, et les enjeux augmentent. En tant qu'administrateurs et opérateurs de ressources d'informations et de données, les ingénieurs du stockage doivent gérer les données de manière sécurisée tout au long de leur cycle de vie.

La solution

Cette fiche produit présente les fonctionnalités de sécurité de SANtricity 11.50 et versions ultérieures. Vous y découvrirez tous les éléments à connaître pour établir une stratégie de sécurité visant à protéger vos ressources les plus importantes : les données.

NetApp®

Sécurité de la révocation de certificats

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Revocation Checking Using Online Certificate Status Protocol (OCSP) (Vérification de la révocation au moyen du protocole de vérification de certificat en ligne)	OCSP permet aux applications E-Series qui utilisent le protocole TLS ou LDAP de recevoir le statut du certificat numérique. L'application reçoit une réponse signée indiquant le statut du certificat demandé : bon, révoqué ou inconnu. Paramètre privilégié pour le mode Critères communs : OCSP activé.	Une fois OCSP activé, la vérification de révocation est effectuée et les certificats sont validés.

Sécurité cryptographique

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Transport Layer Security for Management Interface (Sécurité de la couche de transport pour l'interface de gestion)	E-Series exploite le protocole TLS v1.2 pour sécuriser les fonctions de communication et d'administration dans l'interface graphique d'administration, l'interface de ligne de commandes et l'API REST.	NetApp déconseille d'utiliser les versions TLS v1.0 ou TLS v1.1, car leur vulnérabilité les rend incompatibles avec certaines normes de conformité telles que PCI-DSS. NetApp privilégie plutôt l'utilisation de TLS v1.2 en raison de sa robustesse et de son intégrité.
FIPS Compliant Encryption (Chiffrement conforme à la norme FIPS)	Pour toutes les données chiffrées, E-Series utilise Bouncy Castle, un ensemble d'API employées en cryptographie, conforme à la norme FIPS 140-2 de niveau 1.	La norme FIPS 140-2 de niveau 1 est la norme du secteur pour les produits et solutions de cryptographie.

Sécurité des données

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Full Disk Encryption, FDE (Chiffrement de disque intégral)	Le chiffrement de disque intégral est une méthode de chiffrement matériel pour les données sur disques autochiffrés. Avec des disques compatibles FDE certifiés FIPS140-2, les données sont chiffrées par le disque à l'aide d'algorithmes de cryptographie conformes à la norme FIPS140-2.	Le chiffrement des données au repos demeure une priorité dans le secteur. La fonctionnalité FDE répond à cette priorité tout en assurant une sécurité forte au niveau du sous-système grâce à d'autres fonctions liées à la sécurité.
FDE Internal Key Management (Gestion interne des clés FDE)	La fonction de gestion interne des clés FDE est une solution de chiffrement autonome pour les données au repos. Elle fonctionne avec le chiffrement de disque intégral (FDE) qui est effectué avec les disques autochiffrés.	Il s'agit d'une solution autonome proposée aux entreprises qui ne souhaitent pas investir dans des serveurs de gestion externe des clés, leur permettant ainsi de réduire le coût total de possession. Cette fonction permet également à l'utilisateur de sécuriser les données au repos, un point essentiel.
FDE External Key Management (Gestion externe des clés FDE)	La gestion externe des clés FDE est assurée par un système tiers dans l'environnement de stockage qui gère les clés d'authentification de manière sécurisée au sein du système de stockage grâce à des fonctionnalités de chiffrement, notamment FDE. Le système de stockage utilise une connexion SSL pour contacter le serveur de gestion externe des clés (par exemple, Gemalto SafeNet KeySecure). Il stocke et récupère les clés d'authentification au moyen du protocole standard KMIP (Key Management Interoperability Protocol).	La gestion externe des clés FDE permet de centraliser les fonctions de gestion des clés d'une entreprise tout en veillant à ce que les clés ne soient pas stockées près des ressources, réduisant ainsi le risque pour la sécurité.
Secure Erase for FDE-Capable Drives (Effacement sécurisé pour les disques compatibles FDE)	La fonction Secure Erase assure le nettoyage des disques en effaçant les données sur un ou plusieurs disques compatibles FDE de sorte qu'elles ne puissent jamais être restaurées.	Les protocoles de sécurité pour désactiver ou requalifier les disques exigent généralement que les données soient irrécupérables.

Sécurité de journalisation des messages

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Login and Message of the Day (MOTD) Banners (Bannières de connexion et MOTD) - SANtricity OS 11.40.1 et versions ultérieures	Les bannières de connexion sont affichées à l'écran avant l'authentification. Elles permettent aux entreprises et aux administrateurs de communiquer avec les utilisateurs du système.	Les bannières de connexion permettent aux entreprises de présenter aux opérateurs, administrateurs, voire aux utilisateurs malveillants, les conditions d'utilisation d'un système. Elles indiquent également qui est autorisé à accéder au système.
Secure Log Forwarding (Syslog over Transport Layer Security [TLS]) (Transfert de journaux sécurisé Syslog via TLS) - SANtricity OS 11.40.1 et versions ultérieures	La fonction de transfert de journaux permet aux administrateurs de provisionner des cibles ou destinations de manière à ce qu'elles puissent recevoir des informations d'audit ou syslog. Compte tenu du caractère sensible des informations d'audit et syslog, E-Series peut les envoyer de manière sécurisée via TLS à l'aide du paramètre TCP chiffré.	Les informations d'audit et de journalisation sont extrêmement précieuses pour le support et la disponibilité. En outre, les informations figurant dans les journaux (syslog) ainsi que dans les rapports et résultats d'audit sont généralement sensibles. Pour préserver les contrôles et le niveau de sécurité, les données de journalisation et d'audit doivent être gérées de manière sécurisée.
Simple Network Management Protocol (Protocole simple de gestion de réseau) SNMP v2c	SNMP est un protocole standard qui permet aux appareils connectés au réseau (baies E-Series) de signaler leur statut. E-Series prend en charge le protocole SNMP v2c, dont la sécurité a été améliorée (authentification basée sur la communauté). Paramètre privilégié pour le mode Critères communs : SNMP désactivé.	Cette fonction permet à une application de gestion SNMP des fonctionnalités simples de surveillance pour les baies de stockage NetApp E-Series.

Authentification de l'OS

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Digitally Signed SANtricity OS Firmware (Firmware SANtricity OS avec signature numérique) - SANtricity OS 11.40.2 et versions ultérieures	Un firmware de contrôleur avec signature numérique est requis dans la version 8.42 et les versions ultérieures. Si le firmware n'a pas de signature, les tentatives de téléchargement seront rejetées. De plus, un test automatique est effectué lors du démarrage de la baie pour vérifier que le firmware est intact.	Cela permet d'empêcher les utilisateurs non autorisés ou malveillants de télécharger des bundles de code modifiés ou non-NetApp.

Sécurité du contrôle d'accès utilisateur

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Contrôle d'accès basé sur des rôles (RBAC)	La fonction RBAC dans E-Series permet aux administrateurs de limiter l'accès administratif des utilisateurs au niveau correspondant à leur rôle. Les administrateurs peuvent ainsi gérer les utilisateurs par le biais du rôle qui leur a été attribué.	Le contrôle d'accès est un élément fondamental pour obtenir le niveau de sécurité requis. Les fonctions telles que le RBAC permettent aux entreprises de définir qui peut accéder aux données et dans quelle mesure. Cela réduit les vulnérabilités et les abus, y compris les fuites de données et l'escalade de privilèges.
Lightweight Directory Access Protocol (LDAP)	Il est essentiel de pouvoir authentifier et autoriser les utilisateurs du répertoire pour le déploiement du stockage dans les environnements IT d'entreprise.	Prise en charge de la configuration et de l'attribution des utilisateurs à partir de LDAP pour exécuter des fonctions de gestion du stockage sur les baies E-Series.
Secure Lightweight Directory Access Protocol (LDAPS) pour les interactions avec les services de répertoire	E-Series prend en charge le protocole sécurisé LDAPS lors des interactions avec un serveur LDAP.	Le protocole LDAPS évite de transmettre des données sensibles en clair.
Authentification multifacteur (MFA) avec la technologie SAML 2.0	L'interface graphique SANtricity System Manager intégrée à E-Series prend en charge le langage SAML. L'authentification peut être gérée au moyen d'un fournisseur d'identités qui utilise la norme SAML. Un administrateur établit la communication entre le système du fournisseur d'identités et la baie de stockage, puis il mappe les utilisateurs de ce fournisseur aux rôles des utilisateurs locaux intégrés dans la baie de stockage.	La prise en charge de la norme SAML permet d'implémenter des solutions d'authentification multifacteur, et ainsi de respecter les directives relatives à la gestion des identités.
Stratégie de mot de passe	Cette fonctionnalité permet à l'administrateur de fixer le nombre de tentatives de connexion à SANtricity System Manager pour chaque contrôleur avant que l'utilisateur ne soit bloqué pendant un certain temps. L'administrateur peut paramétrer deux modes de blocage : un basé sur l'adresse IP (par défaut) et un basé sur le compte de l'utilisateur. Méthode privilégiée pour le mode Critères communs : blocage basé sur le compte de l'utilisateur. E-Series permet de configurer le mot de passe pour exiger un minimum de 15 caractères. La longueur maximale est de 30 caractères.	Cela permet de réduire les attaques par déni de service, car le nombre de tentatives d'accès aux baies de stockage est limité. L'augmentation du nombre minimal de caractères pour les mots de passe rend le piratage plus difficile et assure le respect des exigences de sécurité.

Sécurité de l'interface utilisateur

LOGICIEL OU FONCTIONNALITÉ	FONCTION	IMPACT
Accès à la console via SSH	Avec E-Series, l'utilisateur peut se connecter à la console de la baie via SSH. Paramètre privilégié pour le mode Critères communs : accès via SSH désactivé.	L'accès à la console via SSH est généralement utilisé pour résoudre des problèmes avec la baie de stockage. Cette tâche est réalisée avec l'aide de l'équipe NetApp de support client.
Sécurisation des protocoles et des ports pour l'accès à l'API REST via le protocole sécurisé HTTPS	Les systèmes E-Series prennent en charge l'API REST qui propose une interface de communication sécurisée entre la baie de stockage et le client de gestion via le protocole sécurisé HTTPS. Paramètre privilégié pour le mode Critères communs : SYMbol (une interface de communication propriétaire) désactivé.	L'interface de gestion chiffrée de l'API REST renforce la confidentialité des communications entre la baie de stockage et le client de gestion.
Secure Command-Line Access (Accès par ligne de commande sécurisée)	E-Series met en œuvre la ligne de commande SMcli pour communiquer avec la baie de stockage. Cette fonction offre un canal de communication sécurisé utilisé pour les communications par ligne de commande entre le client et le serveur via le protocole TLS.	L'établissement d'un accès sécurisé aux systèmes est primordial pour le maintien de la sécurité de la solution.

À propos de NetApp

NetApp est la référence en matière de gestion des données dans le cloud hybride. Nous fournissons une gamme complète de services qui simplifient la gestion des applications et des données dans les environnements cloud et sur site afin d'accélérer la transformation digitale. Avec ses partenaires, NetApp donne les moyens aux entreprises d'envergure mondiale d'exploiter tout le potentiel de leurs données afin de multiplier les points de contact avec les clients, de favoriser l'innovation et d'optimiser leurs opérations. Pour en savoir plus, visitez le site **www.netapp.com/fr**. #DataDriven