APPLIANCES DELL EMC VXRAIL UNE SÉCURITÉ COMPLÈTE DÈS LA CONCEPTION

Résumé

Plate-forme idéale pour l'infrastructure IT et la transformation de la sécurité, l'appliance VxRail™ offre différents niveaux de protection permettant de garantir la sécurité de vos données et de vos applications métier. Seul le groupe de sociétés Dell Technologies peut fournir les solutions de bout en bout requises pour faire face à l'évolution actuelle du paysage des menaces. Ce guide couvre à la fois les fonctions de sécurité intégrées et en option, les bonnes pratiques et les techniques éprouvées pour sécuriser votre appliance VxRail, du datacenter au Cloud, en passant par la périphérie.

Mars 2020

Table des matières

Table des matières 2
INTRODUCTION 4
LA TRANSFORMATION DE LA SÉCURITÉ COMMENCE CHEZ DELL TECHNOLOGIES 5
Vers un avenir numérique 7
UNE CONFIANCE RENFORCÉE AVEC LES PROGRAMMES DE SÉCURITÉ DES PRODUITS DELL EMC 7
Cycle de développement de la sécurité (SDL) 7
Développement sécurisé 8
Réponse aux failles de sécurité Dell EMC 9
Gestion des risques liés à la chaîne d'approvisionnement 10
Collaboration avec le secteur pour améliorer la sécurité des produits 10
Participation aux groupes de sécurité des produits du secteur 11
VxRail : une base pour la modernisation du datacenter et la transformation IT 12
Logiciel système Dell EMC VxRail HCI 13
VMware vSphere 14
VMware vCenter Server 15
Hyperviseur VMware ESXi 15
Gestion réseau virtuelle VMware 15
VMware vSAN 15
Storage Policy Based Management (SPBM) 17
VMware vRealize Log Insight 17
VMware Cloud Foundation (VCF) avec la solution NSX 17
Fonctionnalités de sécurité de l'appliance VxRail 18
SÉCURITÉ DES DONNÉES 18
Confidentialité 18
Intégrité 21
Disponibilité 21
SÉCURITÉ DU SYSTÈME 23
Authentification, autorisation et comptabilité de l'appliance VxRail 23
Sécurité de l'emplacement physique de l'appliance VxRail 24
Automatisation 25
Package de renforcement STIG VxRail 25
Sécurité intégrée à la plate-forme VxRail ACE 26
Présentation de la sécurité de la plate-forme VxRail ACE 26
Collecte de données de la plate-forme VxRail ACE 26
Données de la plate-forme VxRail ACE en transit vers Dell 27
Données VxRail ACE au repos 27

Contrôle d’accès aux données VxRail ACE 27
Accès de l’utilisateur final à la plate-forme VxRail ACE 28
Accès administratif à l’infrastructure VxRail ACE gérée par l’équipe Dell EMC IT 28
Normes et certifications compatibles 28
Le cadre de cybersécurité du NIST et l’appliance VxRail 30
Solutions et partenaires de sécurité VxRail 31
Gestion des accès et identités 31
Gestion des incidents et des événements de sécurité 32
Serveur de gestion des clés 32
Autres partenaires de sécurité 32
Conclusion 33

INTRODUCTION

Dans tous les secteurs d'activité, les organisations modernisent et transforment leur mode de fonctionnement et leur façon de fournir des produits et des services différenciés. Du datacenter au Cloud, en passant par la périphérie, tout évolue à une vitesse exponentielle : l'emplacement des données, leur mode d'accès et le nombre d'appareils. La sécurité fera toujours partie intégrante de l'IT, notamment les questions d'authentification, de pare-feu, de conformité et de cybercriminalité. Elle ne s'inscrit plus dans un ensemble de projets, mais dans un cycle continu nécessitant des révisions et des analyses constantes. Dell Technologies est convaincue que la sécurité n'est jamais un frein, mais plutôt un accélérateur de l'innovation, vous invitant à repenser la sécurité comme une opportunité stratégique.

L'appliance Dell EMC VxRail offre la voie la plus rapide et la plus simple pour entreprendre cette transformation de la sécurité, du datacenter au Cloud, en passant par la périphérie. Elle fournit une infrastructure agile avec intégrité complète de la pile et gestion du cycle de vie intégral afin d'optimiser l'efficacité opérationnelle, de réduire les risques et d'aider les équipes à se concentrer sur l'activité. Les systèmes VxRail sont des solutions qui brisent les silos opérationnels et favorisent l'innovation continue par le provisionnement et le déploiement rapides des charges applicatives. Leur adoption génère des économies considérables en termesde coûts et d'efficacité opérationnelle, ce qui permet aux départements IT de favoriser les opportunités métier plutôt que de simplement soutenir les opérations. Conçue pour VMware, avec VMware, pour améliorer les équipements VMware, l'appliance VxRail est le premier et le seul système HCI fabriqué avec VMware pour éliminer la complexité opérationnelle liée au déploiement, au provisionnement, à la gestion, à la surveillance et à la mise à jour de l'infrastructure hyperconvergée VxRail.

Elle bénéficie d'une sécurité intégrée à tous les niveaux du package technologique, du moindre processeur jusqu'au serveur PowerEdge en passant par le logiciel système VxRail HCI, y compris les logiciels VMware intégrés. Elle offre une sécurité du datacenter au Cloud, en passant par la périphérie, assurant la disponibilité, l'intégrité et la fiabilité de chaque charge applicative, qu'elle soit traditionnelle ou Cloud native.

LA TRANSFORMATION DE LA SÉCURITÉ COMMENCE CHEZ DELL TECHNOLOGIES

Chez Dell Technologies, transformer la sécurité consiste à la repenser et à accélérer l'innovation. Dell Technologies se concentre sur la sécurité à tous les niveaux, des collaborations entre les sociétés du groupe aux produits en cours de développement jusqu'à la mise en production. L'appliance VxRail ne fait pas exception : elle offre une assurance de la sécurité produit optimale et fournit des fonctionnalités de sécurité entièrement intégrée. Votre organisation peut les utiliser pour optimiser sa résilience en matière de cybersécurité, du datacenter au Cloud, en passant par la périphérie (voir figure ci-dessous), et pour accélérer l'innovation.

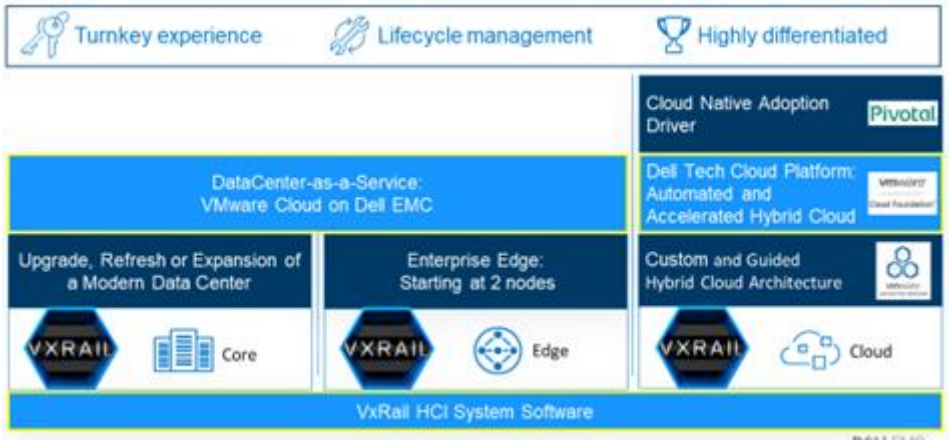

Figure 1 : Du datacenter au Cloud, en passant par la périphérie

D'après un article de Forbes qui s'appuie sur uneétude de la société Risk Based Security récemment publiée dans un rapport récapitulatif sur les violations de données de 2019, plus de 3 800 fuites de données ont été révélées publiquement au cours des six premiers mois de 2019, mettant en danger le chiffre inquiétant de 4,1 milliards d'enregistrements. Sur la base de ces chiffres, on peut supposer que les violations de données dépassent les 6 515 compromissions de données rendues publiques recensées pour l'année 2018 par la même société.

Dell Technologies permet à vos stratégies de sécurité d'évoluer avec vos initiatives de modernisation afin de réduire les risques pour l'activité.

1. Unifiez les programmes de sécurité avec les risques globaux pour l'activité, afin de connaître les risques qui valent la peine d'être pris.
2. Implémentez des opérations de sécurité avancées qui s'adaptent au paysage de menaces en constante évolution afin d'y répondre efficacement.
3. Créez une infrastructure moderne et résiliente qui protège vos points de terminaison, votre réseau, vos applications et vos données.
4. Faites appel à des services de conseils de confiance pour vous aider à concevoir et à mettre en œuvre votre programme de transformation de la sécurité. Dell Technologies est idéalement placée pour vous aider à gérer ces différents aspects.

Bien qu'une défense comptant plusieurs niveaux de sécurité soit nécessaire, il est impératif que ces différents éléments fonctionnent de concert. La transformation de la sécurité commence par une infrastructure cyber-résiliente et moderne, telle que la solution VxRail dans laquelle la sécurité a été intégrée dès les étapes de conception et de fabrication.

Aujourd'hui, l'évolution du paysage des menaces impose de changer d'approche pour prévenir ou limiter ces menaces. Une infrastructure obsolète est difficile à défendre, et le recours à des produits provenant de différents fournisseurs ajoute de la complexité et augmente le risque de failles de sécurité susceptibles d'être exploitées. Ce niveau de complexité offre plusieurs points d'entrée pour les cybercriminels.

Les normes de sécurité et la conformité doivent également être prises en compte. Des sanctions juridiques et financières importantes sont souvent prises en cas de non-conformité. Bien que coûteuses, elles peuvent avoir moins d'impact sur l'activité qu'une violation n'en aurait sur la réputation de la société. En effet, les clients sont moins enclins à traiter avec une société qui a subi une fuite de données.

- Payment Card Industry Data Security Standard (PCI DSS) : normes de protection des détenteurs de carte de crédit
- Règlement général sur la protection des données (RGPD) : réglementation de l'Union européenne sur la confidentialité des données
- Bundesdatenschutzgesetz (BDSG) : loi allemande sur la protection des données
- Sarbanes-Oxley Act (SOX) : loi américaine sur la protection des données sensibles liées aux rapports financiers dans les sociétés cotées
- Gramm-Leach-Bliley Act (GLBA) : loi américaine sur la protection des données personnelles non publiques dans le secteur des services financiers
- Health Insurance Portability & Accountability Act (HIPAA) : loi sur la protection des données et informations médicales électroniques sur les patients
- California Consumer Privacy Act (CCPA) : loi qui renforce les droits de confidentialité et la protection des consommateurs pour les résidents de Californie (promulguée le 28/06/2018)

Dell Technologies est convaincue que la transformation de la sécurité exige d'avoir un partenaire de confiance, capable de vous aider à gérer vos risques numériques et à fournir des services de sécurité gérés. Ce partenaire doit également vous apporter une expertise, des services, des solutions et des produits qui sécurisent l'intégralité de la pile, de l'infrastructure aux applications, et rationalisent les opérations, mettant la sécurité au cœur de la stratégie de l'entreprise.

Dell Technologies est votre partenaire de confiance pour la transformation de la sécurité. Qu'il s'agisse des points de terminaison, du datacenter, des développeurs, des identités, des opérations de sécurité, du Cloud ou de la virtualisation, il est nécessaire d'intégrer la sécurité de bout en bout et Dell Technologies peut vous y aider. Nous pouvons vous aider à limiter les risques de sécurité et les risques pour l'activité, à gérer les failles de sécurité, à réagir à une attaque de ransomware et à créer des applications sécurisées. Chacun appréhende la sécurité de manière différente, avec une perception positive ou négative. Au delà du ressenti individuel, Dell Technologies veut que les organisations nous embarquent dans cette transition.

Vers un avenir numérique

À l'heure actuelle, l'IT est plus que jamais sollicitée pour résoudre des problèmes métier. En effet, les organisations implémentent l'analytique des données, l'intelligence artificielle, de nouvelles applications et des appareils intelligents pour générer des quantités considérables de données. Ces données permettent de faire des découvertes et de dégager des avantages concurrentiels uniques. Malgré cela, de nombreuses organisations manquent toujours d'une vision et d'une stratégie numériques claires. Elles utilisent des technologies obsolètes, ce qui crée des contraintes et une culture de résistance au changement. Sans un plan approprié, les risques et la sécurité passent souvent au second rang ou ne sont tout simplement jamais abordés dans les discussions sur la stratégie. À notre époque marquant un tournant technologique, cette approche réactive doit être abandonnée. Pour accélérer l'innovation et concrétiser leur avenir numérique, les organisations doivent repenser la manière dont elles appréhendent la sécurité.

Dans le monde de l'IT, la sécurité est généralement perçue comme un obstacle plutôt que comme un accélérateur de changements positifs. Certaines tâches quotidiennes peuvent être ingrates et les membres de la direction ne perçoivent pas forcément la valeur qu'apportent les équipes de sécurité. Celles-ci doivent gérer un nombre croissant de menaces et des systèmes complexes, et maintenir leurs connaissances à jour sur un paysage en constante évolution. Le déluge presque quotidien de cyberattaques relayées dans les médias ne fait qu'exacerber ce stress, tout comme la sensation angoissante que votre organisation pourrait être dépouillée de ce qu'elle possède en l'espace d'une seconde. Mais la question de la sécurité n'a pas à susciter tant de peur et de frustration. L'approche de la sécurité s'est toujours voulue plus positive et proactive, mais cela n'est possible qu'avec le bon état d'esprit et les bonnes technologies. Nous ne pouvons pas continuer à appréhender la sécurité et les risques comme nous l'avons fait jusqu'à présent. Pour mieux comprendre ce tournant, pensez aux freins d'une voiture. Au départ, vous pouvez vous dire que les freins ne servent qu'à ralentir, or ils vous permettent également d'aller plus vite. En effet, ils vous donnent la confiance requise pour accélérer tout en vous préparant aux obstacles et à la voie devant vous. La sécurité et les risques doivent également être considérés comme des accélérateurs par les organisations, et non comme quelque chose qui les ralentit.

UNE CONFIANCE RENFORCÉE AVEC LES PROGRAMMES DE SÉCURITÉ DES PRODUITS DELL EMC

Dell EMC a commencé à formuler ses politiques de sécurité des produits en 2002, lorsqu'elle a amorcé son virage de fournisseur de matériel de stockage à concepteur de logiciels de niveau entreprise. La société a déployé son programme de réponse aux failles de sécurité en 2004 et mis en place une politique de sécurité des produits dans toute la société en 2005. Cette politique édicte des normes de sécurité larges mais claires, englobant la gamme complète des produits Dell EMC. Elle a été régulièrement mise à jour, puis intégrée en 2007 au nouveau cycle de développement de la sécurité (Security Development Lifecycle, SDL) de la société. Ce cycle SDL ajoutait une série de pratiques de sécurité mesurables et reproductibles à chaque étape du développement et du déploiement des produits. En 2012, Dell EMC a également officialisé un programme de gestion des risques liés à la chaîne d'approvisionnement afin d'étendre ses pratiques de sécurité à ses fournisseurs de composants de produits. Dell EMC continue à faire évoluer ses programmes de sécurité des produits en restant à la pointe des normes et des processus du secteur.

Avec l'appliance VxRail, Dell EMC poursuit son engagement vis-à-vis de la sécurité. Le cycle de développement de l'appliance VxRail suit le processus de développement de la sécurité des produits Dell EMC et la couche du cycle de développement de la sécurité. Le cycle de développement de la sécurité Dell EMC suit une approche rigoureuse pour sécuriser le développement des produits et implique que la direction étudie les risques avant la commercialisation des produits. En outre, la solution VMware vSphere joue un rôle important dans l'infrastructure hyperconvergée VxRail et a été développée suivant un cycle similaire au cycle SDL.

Cycle de développement de la sécurité (SDL)

Le cycle de développement de la sécurité Dell EMC décrit l'ensemble des activités requises tout au long du cycle de vie du produit pour intégrer une résilience de sécurité et des fonctionnalités de sécurité cohérentes dans les produits, et pour répondre rapidement aux failles de sécurité signalées en externe. Aligné sur les bonnes pratiques du secteur, le cycle Dell EMC est basé sur un ensemble de contrôles mis en œuvre par les organisations Recherche et développement produit. La figure 2 présente certaines des activités type effectuées dans le cadre du cycle SDL.

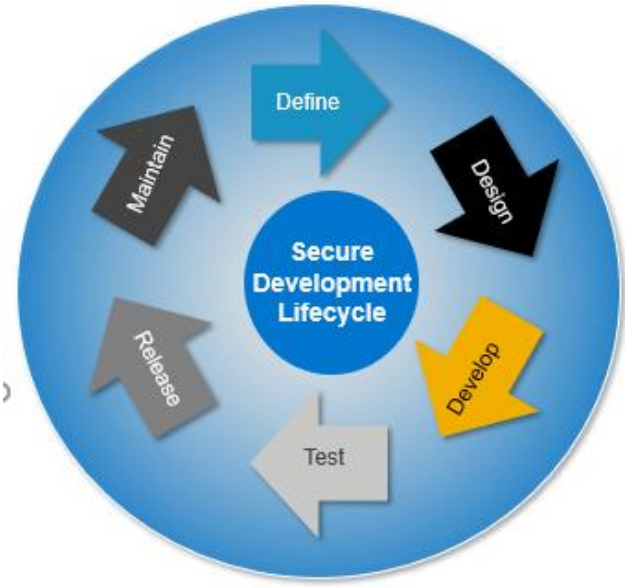

Figure 2 : Activités du cycle SDL de Dell EMC

La mise en œuvre et la validation de ces contrôles sont pilotées par des champions de la sécurité au sein des organisations R&D produit qui travaillent en étroite collaboration avec les conseillers en sécurité du Bureau de sécurité des produits (Product Security Office, PSO). La figure 3 illustre la façon dont ce cycle SDL s'inscrit dans un cycle agile classique.

Agile Development Activity		SDL Activity
High Level Planning	Requirements	• Formalize security requirements in PRD/PCD • Product Security Training
	Architecture	• **Threat Modeling** • **Security Testing** (test planning)
Sprint 1..*n*	Design	• Update **threat model**
	Develop	• **Static Analysis**
	Test	• **Security Testing**
	Release	• **Security Scanning** • **Security Configuration Guide** • Inventory of Embedded Components
General Availability	Assure	• Perform Code Signing
	Assess	• Finalize and **submit scorecard** • Have a plan for mitigating any "critical" and/or "high" issues
Post-GA	Respond	• Respond to vulnerabilities following EMC's vulnerability response policy

Figure 3 : Cycle SDL et cycle agile classique

La fiche d'évaluation est un mécanisme utilisé dans l'ensemble des activités Dell EMC pour capturer la posture de sécurité d'un produit/d'une solution lorsqu'il ou elle atteint sa date de disponibilité immédiate/générale (Direct Availability/General Availability, DA/GA).

Développement sécurisé

L'approche exhaustive de Dell EMC du développement sécurisé se concentre sur la réduction des risques liées aux failles de sécurité logicielles et aux faiblesses de conception des produits.

Cette approche exhaustive du développement logiciel sécurisé touche aussi bien la politique, les habitudes de travail, les processus et les technologies, et inclut les points suivants :

- La politique de sécurité des produits Dell EMC est une référence commune pour les organisations produit de Dell EMC permettant de comparer la sécurité des produits aux attentes du marché et aux bonnes pratiques du secteur.
- Les équipes d'ingénieurs Dell EMC forment une communauté consciente des questions de sécurité. Tous les ingénieurs assistent à un programme sur la sécurité basé sur des rôles pour se former aux bonnes pratiques en matière de sécurité et à l'utilisation des ressources appropriées. Dell EMC s'attache à instaurer une culture de la sécurité au sein de la communauté des ingénieurs.
- Le processus de développement de Dell EMC est sécurisé et reproductible. Le cycle SDL se superpose aux processus de développement standard afin d'atteindre un degré élevé de conformité à la politique de sécurité des produits Dell EMC.
- Les équipes de développement Dell EMC s'appuient sur des technologies de sécurité haut de gamme. Dell EMC a mis au point un ensemble de logiciels, de normes, de spécifications et de conceptions pour les éléments de sécurité logicielle courants, tels que l'authentification, l'autorisation, l'audit et la responsabilité, le chiffrement et la gestion des clés à l'aide de technologies RSA de pointe. Des interfaces ouvertes sont utilisées si nécessaire, ce qui permet l'intégration avec les architectures de sécurité existantes des clients.
- Le cycle SDL de Dell EMC superpose la sécurité aux processus de développement standard afin d'atteindre un niveau élevé de conformité avec la politique de sécurité des produits Dell EMC. Il suit une approche rigoureuse pour sécuriser le développement des produits et implique que la direction étudie les risques avant la commercialisation des produits.
- Le cycle SDL fait partie d'un ensemble plus large de processus qui existent au sein de la norme de conception sécurisée. La norme de conception sécurisée est le point de référence permettant d'intégrer la sécurité dans les produits Dell EMC. Elle porte sur la sécurité de toutes les fonctionnalités des produits et décrit les fonctionnalités de sécurité obligatoires qui doivent être intégrées à tout produit fourni par Dell EMC aux clients. Cette norme permet aux produits Dell EMC :
    - de répondre aux exigences de sécurité rigoureuses des clients ;
    - d'aider les clients à respecter les exigences réglementaires, telles que les normes PCI, la loi HIPAA, etc. ;
    - de réduire les risques que représentent les failles de sécurité pour les produits Dell EMC et les environnements des clients.
    - La protection du code source identifie comment sécuriser correctement les systèmes d'ingénierie Dell EMC qui contiennent du code source sur la propriété intellectuelle liée aux produits, et garantir l'intégrité des produits déployés dans les environnements des clients.

Réponse aux failles de sécurité Dell EMC

Dans tout composant système, des failles de sécurité peuvent être exploitées par des attaquants pour s'infiltrer et compromettre l'intégralité de l'infrastructure IT. Le temps entre la découverte initiale des failles de sécurité et la disponibilité d'un correctif se transforme en course contre la montre entre les attaquants et les défenseurs. L'une des priorités de Dell EMC est de minimiser ce laps de temps pour réduire les risques.

L' équipe Dell PSIRT (Product Security Incident Response Team) (équipe de réponse aux incidents de sécurité des produits) est responsable de la coordination de la réponse et de la divulgation pour toutes les failles de sécurité de produit Dell EMC identifiées en externe. L'équipe PSIRT fournit aux clients des informations en temps opportun, des conseils et des stratégies d'atténuation pour faire face aux menaces liées aux failles de sécurité.

Tout le monde peut signaler à Dell les éventuelles failles de sécurité de ses produits via le site Web de la société ou par e-mail. Chaque signalement fait l'objet d'une enquête, d'une validation, de mesures correctives et d'un compte rendu conformément aux directives du secteur.

Dell publie des informations sur les failles de sécurité des produits à tous les clients en même temps. Les conseils publiés par la société indiquent la gravité des failles de sécurité et sont diffusés à travers plusieurs systèmes de création de rapports standardisés. À l'instar du reste des pratiques Dell en matière de sécurité des produits, la politique de divulgation Dell est basée sur les bonnes pratiques du secteur.

Gestion des risques liés à la chaîne d'approvisionnement

Les programmes de sécurité des produits les plus concluants sont exhaustifs et s'étendent aux composants et logiciels externalisés. Les tests d'intégrité effectués au sein de la chaîne d'approvisionnement constituent un élément essentiel pour établir la confiance et la préserver. Dell Technologies dispose d'un programme officiel de gestion des risques liés à la chaîne d'approvisionnement qui garantit que les composants matériels utilisés dans les produits de la société proviennent de sources dûment approuvées.

La sécurité de la chaîne d'approvisionnement désigne la pratique et l'application de mesures de contrôle de prévention et de détection destinées à protéger les actifs physiques, l'inventaire, les informations, la propriété intellectuelle et les personnes. La gestion de la sécurité physique, des informations et des personnes permet d'assurer la chaîne d'approvisionnement en réduisant la probabilité que des logiciels malveillants et des composants contrefaits soient introduits dans la chaîne d'approvisionnement.

Le framework Dell de gestion des risques liés à la chaîne d'approvisionnement (voir ci-dessous) reflète le framework complet de gestion des risques du plan américain de protection des infrastructures (NIPP), qui décrit comment le gouvernement et le secteur privé américains peuvent travailler ensemble pour limiter les risques et atteindre leurs objectifs de sécurité. Le framework Dell intègre un processus ouvert et itératif d'amélioration en continu. Les plans de limitation des risques sont hiérarchisés et mis en œuvre selon les besoins tout au long du cycle de vie de la solution. La figure 4 illustre le processus de gestion des risques liés à la chaîne d'approvisionnement.

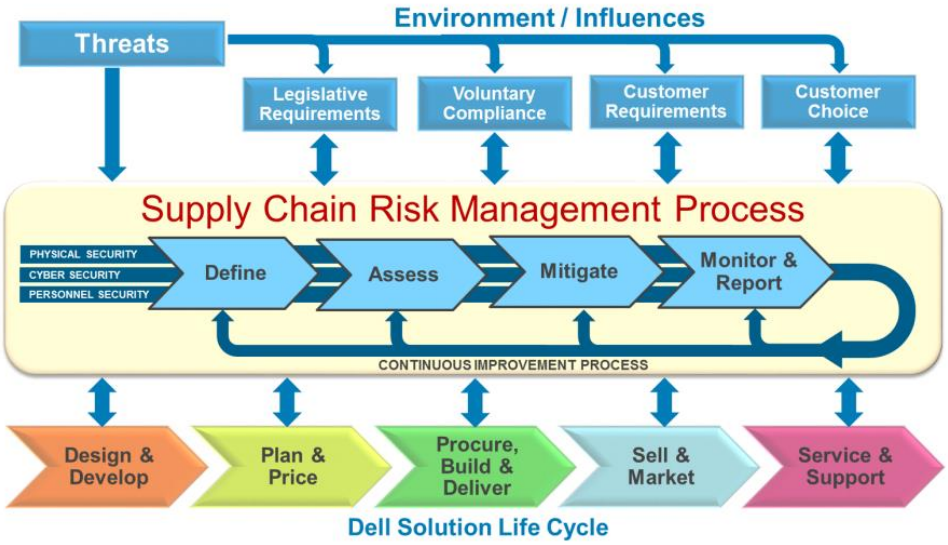

Figure 4 : Processus Dell de gestion des risques liés à la chaîne d'approvisionnement

Collaboration avec le secteur pour améliorer la sécurité des produits

Dell Technologies estime qu'une approche collaborative est la solution la plus efficace pour faire face aux menaces de sécurité qui émergent constamment et peuvent se répandre rapidement dans les organisations à travers les systèmes fortement interconnectés d'aujourd'hui.

En tenant compte des risques accrus, les fournisseurs de technologies doivent mettre de côté leurs objectifs concurrentiels sur le marché dès lors qu'il s'agit de sécurité des produits. Aucun fournisseur ne peut résoudre tous les problèmes de sécurité des produits IT par lui-même. La sécurité IT est un effort collectif et collaboratif. Dell Technologies est convaincue que la collaboration avec d'autres sociétés est essentielle pour s'assurer que les conditions du marché permettent à chacun de continuer à prospérer.

Forte de dizaines d'années d'expérience dans la sécurité des produits, Dell Technologies a su écrire une histoire riche en améliorations réussies et en analyses pertinentes, et la société partage ouvertement les enseignements qu'elle tire avec ses clients, ses homologues et de ses partenaires. Dell Technologies comprend que le système IT d'un client ne fonctionne pas uniquement sur des produits Dell Technologies. C'est pourquoi elle s'efforce d'améliorer la sécurité de l'écosystème, quel que soit l'environnement de fonctionnement. Cela implique de participer activement et d'apporter une collaboration positive dans tout le secteur.

L'engagement de longue date de Dell Technologies envers la sécurité des produits crée une obligation d'aider et de promouvoir les nouveaux acteurs du secteur. Les responsables de la sécurité des produits de la société encouragent l'échange ouvert d'idées lors de conférences, par le biais d'articles de blog et lors d'autres événements sociaux et officiels.

Participation aux groupes de sécurité des produits du secteur

Dell Technologies est active dans les groupes de sécurité des produits, où elle apprend et enseigne les bonnes pratiques progressives et cultive un sentiment de responsabilité collective en matière de sécurité des produits. Voici quelques-unes des affiliations sectorielles de Dell Technologies :

BSIMM : le modèle BSIMM (Building Security in Maturity Model) évalue les initiatives sectorielles de sécurité logicielle pour aider les organisations à comprendre le degré de pertinence de leurs propres efforts et définir la manière dont elles peuvent les faire évoluer.

The Open Group : ce consortium de 400 membres gère des programmes de certification respectés, dédiés au personnel, aux produits et aux services IT afin de concevoir et d'améliorer les normes IT. Il s'efforce de comprendre les besoins IT actuels et émergents, et d'élaborer ou de partager des bonnes pratiques pour y répondre.

SAFECode : co-fondé par Dell EMC, le SAFECode (Software Assurance Forum for Excellence in Code) est une initiative impulsée par des acteurs du marché. Son but est de définir et de promouvoir les bonnes pratiques permettant d'offrir des logiciels, des produits matériels et des services plus sécurisés et plus fiables.

CSA : l'alliance CSA (Cloud Security Alliance) est la principale organisation mondiale dédiée à la définition et à la sensibilisation aux bonnes pratiques afin de garantir un environnement de Cloud Computing sécurisé.

FIRST : le forum FIRST (Forum of Incident Response and Security Teams) est un leader mondial de la réponse aux incidents. L'équipe PSIRT de Dell est membre de l'équipe FIRST.

VxRail : une base pour la modernisation du datacenter et la transformation IT

Dans la bataille face à l'évolution constante des menaces de sécurité, l'appliance VxRail possède l'adaptabilité suffisante pour se défendre contre les menaces actuelles et futures. L'appliance VxRail repose sur la génération actuelle de serveurs Dell PowerEdge et sur les toutes dernières technologies de processeurs qui fournissent une plate-forme sécurisée et des options de configuration flexibles. vSphere fournit du stockage et une virtualisation des serveurs. À mesure que les besoins des charges applicatives augmentent, l'appliance VxRail s'adapte facilement. À mesure que les réglementations évoluent, les options de configuration flexibles de l'appliance VxRail lui permettent de s'adapter rapidement.

L'appliance VxRail peut aider votre organisation à optimiser la cyber-résilience, à gérer les risques et à répondre aux exigences de conformité, quel que soit le secteur d'activité dans lequel votre organisation opère. VxRail est la seule appliance d'infrastructure hyperconvergée entièrement intégrée, préconfigurée et testée, équipée de la technologie VMware vSAN. Qu'elle soit déployée dans le datacenter, à la périphérie ou dans le cadre d'une solution Cloud hybride, elle offre une distribution plus simple, plus efficace et plus sécurisée des applications stratégiques, de la VDI et de l'infrastructure distante. Elle permet à Dell EMC de fournir au client les fonctionnalités nécessaires à l'optimisation de la cyber-résilience sur l'ensemble de leur déploiement. La figure 5 ci-dessous illustre la sécurité intégrée à l'appliance VxRail.

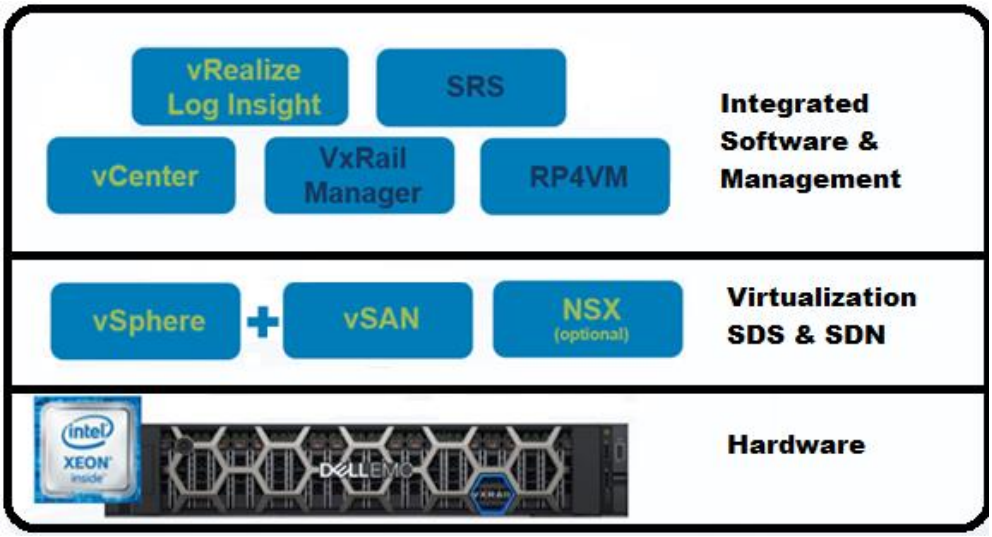

Figure 5 : Sécurité intégrée à l'appliance VxRail

Serveurs Dell EMC PowerEdge

L'appliance VxRail est construite sur la plate-forme de serveurs Dell PowerEdge avec des fonctions de sécurité intégrées au matériel et au niveau du système pour protéger l'infrastructure avec plusieurs niveaux de défense. Les violations sont rapidement détectées, ce qui permet au système de restaurer son état à une ligne de base fiable. Dans les serveurs PowerEdge, les fonctions de sécurité différenciées incluent notamment les suivantes :

- la fonctionnalité System Lockdown pour empêcher les modifications non autorisées ou accidentelles. Cette fonctionnalité, nouvelle dans le secteur, empêche les modifications de configuration qui créent des failles de sécurité et mettent en péril les données sensibles ;
- l'architecture cyber-résiliente, dotée de fonctionnalités telles que le démarrage Secure Boot UEFI, la récupération du BIOS et le firmware signé, offre une protection renforcée contre les attaques ;
- la fonctionnalité System Erase au niveau du serveur garantit la confidentialité en effaçant rapidement et en toute sécurité toutes les données utilisateur du disque dur et toute mémoire non volatile lorsqu'un serveur fait l'objet d'un retrait.

Les serveurs Dell EMC PowerEdge constituent le matériel essentiel qui compose les nœuds d'un cluster VxRail. Les ressources du processeur, de la mémoire et du disque sur chaque nœud fournissent des ressources mises en commun pour le cluster, et les interfaces réseau fournissent la connectivité. Par conséquent, les serveurs Dell EMC PowerEdge sécurisés constituent la base de la sécurité de l'appliance VxRail.

Les serveurs PowerEdge sont dotés d'un contrôleur d'accès distant intégré appelé « iDRAC ». Le contrôleur iDRAC utilise des communications sécurisées, une authentification et des contrôles d'accès basés sur les rôles pour permettre une gestion et une configuration à distance sécurisées du système physique. Avec des alertes configurables, le contrôleur iDRAC peut envoyer des informations d'événement à votre système de gestion des incidents et des événements de sécurité (SIEM) chaque fois que vous accédez au matériel ou que la configuration est modifiée. La détection des modifications non autorisées et la création de rapports à ce sujet protègent l'intégrité d'une appliance VxRail. Pour plus d'informations, cliquez sur ce lien : Sécurité cyber-résiliente dans les serveurs Dell EMC PowerEdge de 14e génération.

Les serveurs PowerEdge utilisent des firmwares signés et vérifiés de manière chiffrée pour établir un système de confiance. En utilisant des technologies de sécurité intégrées directement dans le silicium, les fonctionnalités telles que la technologie Intel TXT (Trusted Execution Technology) permettent de vérifier que le serveur n'exécute que la version prévue du firmware, du BIOS et de l'hyperviseur, tout en empêchant l'introduction non détectée de logiciels malveillants. La figure 6 ci-dessous illustre la racine de confiance matérielle.

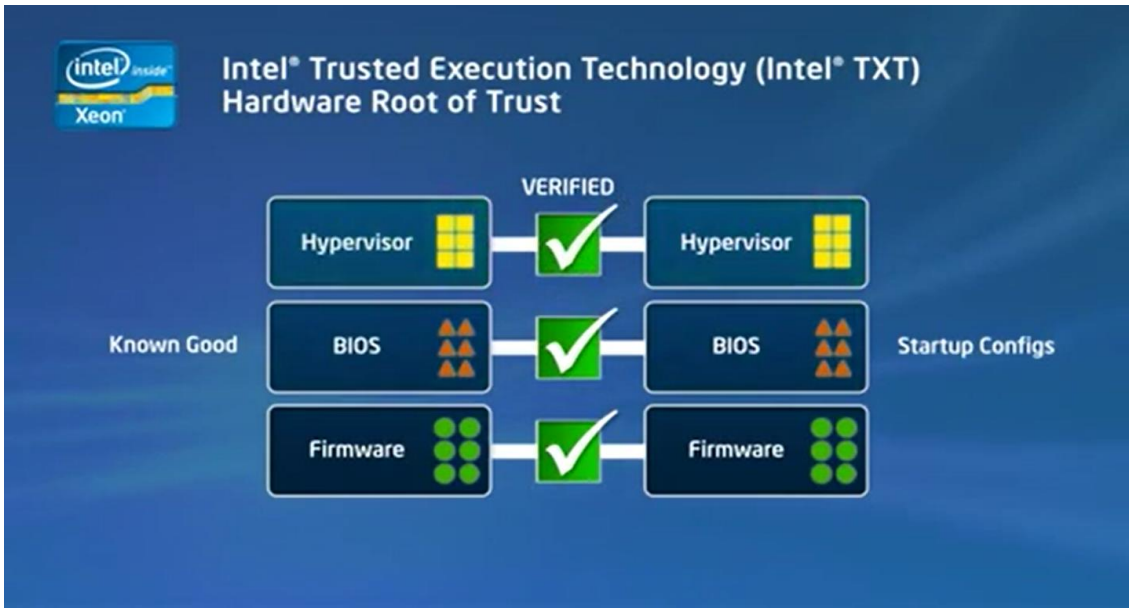

Figure 6 : Racine de confiance matérielle

L'appliance VxRail peut atteindre des niveaux de protection encore plus élevés en matière d'intégrité des serveurs en configurant les nœuds à l'aide d'un module TPM (Trusted Platform Management) en option (TPM v1.2 et v2.0). Le module TPM est une norme internationale pour les cryptoprocesseurs sécurisés, un microcontrôleur dédié conçu pour fournir un niveau de sécurité élevé pour les clés de chiffrement et une option pour tous les nœuds VxRail.

Logiciel système Dell EMC VxRail HCI

Le logiciel système VxRail HCI constitue une base pour les fonctionnalités qui font la valeur ajoutée de l'appliance VxRail. Du point de vue de la pile d'infrastructure, il s'agit du logiciel de gestion qui s'exécute sur les logiciels VMware et sur le serveur PowerEdge pour permettre à l'appliance VxRail d'agir comme un seul système unifié.

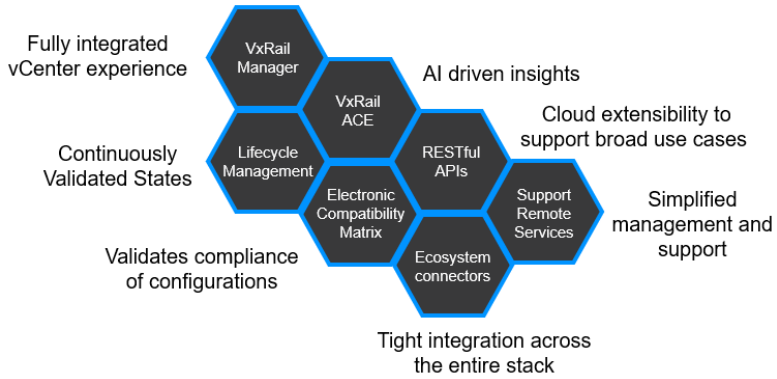

Figure 7 : Logiciel système VxRail HCI

États validés en continu : l'appliance VxRail s'exécute sur des logiciels et des firmwares prétestés et validés pour l'ensemble de la pile VxRail, y compris les logiciels VMware et les composants de serveur PowerEdge. Les fonctionnalités de gestion du cycle de vie VxRail garantissent que les clusters VxRail s'exécutent dans un état de fonctionnement connu tout au long de leur cycle de vie, au cours duquel les clusters subissent des modifications continues pour tirer profit des dernières innovations logicielles, des correctifs de sécurité ou des correctifs de bug de VMware. Le terme « États validés en continu » englobe la stabilité de la configuration fournie par les clusters VxRail.

Matrice de compatibilité électronique : face à tous les différents composants logiciels et matériels de la pile, l'équipe VxRail teste et valide constamment l'ensemble de la pile, de sorte que l'état souhaité par l'utilisateur, choisi dans le tableau de compatibilité VMware, est validé en tant qu'état validé en continu. En outre, VxRail consulte cette matrice pour s'assurer que la configuration de cluster reste conforme. Cet avantage permet de réduire considérablement les efforts et les ressources de test dont le client a besoin pour investir, tout en lui offrant la tranquillité d'esprit dont il a besoin pour faire évoluer ses clusters VxRail de façon prévisible et sécurisée sans affecter les charges applicatives.

Connecteurs de l'écosystème : afin de créer une matrice de compatibilité électronique étendue, l'appliance VxRail doit être en mesure de communiquer avec les membres de l'écosystème de la pile qui inclut vSphere, vSAN, vCenter ainsi que le serveur PowerEdge et les différents composants matériels qu'il contient. Les connecteurs permettent à l'appliance VxRail de connaître les versions des logiciels/firmwares exécutées dans chaque composant et de gérer le cycle de vie de ces composants. Les fonctionnalités d'automatisation et d'orchestration permettent à l'appliance VxRail d'être gérée comme un seul système unifié.

VxRail Manager : l'interface utilisateur de gestion principale pour l'appliance VxRail est le plug-in vCenter appelé « VxRail Manager ». Les utilisateurs VxRail peuvent effectuer tout type d'activité VxRail via cette interface, y compris la configuration initiale de cluster, la surveillance des composants matériels, l'arrêt sans échec de cluster, l'extension de cluster par ajout de nœuds et la mise à jour du logiciel système VxRail HCI. L'interface offre une expérience vCenter entièrement intégrée.

VxRail ACE : à mesure que des améliorations sont apportées à l'expérience de gestion du cycle de vie VxRail, une grande partie dépend des capacités de calcul analytique de la plate-forme VxRail ACE. L'acronyme « ACE » correspond à « Analytical Consulting Engine » (moteur de conseil analytique). Grâce à la télémétrie avancée collectée par le logiciel système HCI sur les clusters VxRail, la plate-forme ACE peut fournir des informations exploitables basées sur l'intelligence artificielle qui permettront aux utilisateurs de gérer proactivement leurs clusters afin d'améliorer les performances et la disponibilité. Les informations exploitables basées sur l'intelligence artificielle servent également à renforcer l'approche active des fonctionnalités de gestion multicluster dans la plate-forme ACE. Ce domaine remportera un intérêt croissant de la part des utilisateurs HCI à mesure qu'ils étendront leur empreinte HCI et qu'une gestion à grande échelle deviendra une nécessité.

API REST : les avantages de l'appliance VxRail en matière de gestion du cycle de vie en font une plate-forme d'infrastructure de choix. En effet, l'accent mis sur la simplification des opérations IT joue un rôle essentiel pour permettre aux équipes IT de se concentrer sur les modèles de prestation de service IT basés sur le Cloud. Les possibilités d'extension de la plate-forme VxRail rendues possibles par les API permettent aux clients de faire évoluer leur solution en s'appuyant sur des solutions d'infrastructure as-a-service. Les API permettent également une gestion à grande échelle, ce qui peut être bénéfique pour les clients disposant d'un grand nombre de clusters VxRail déployés sur différents sites et qui ont choisi des solutions scriptées internes à gérer à grande échelle.

Services distants de support : l'expérience de support peut également être un facteur crucial dans le choix d'une solution HCI. L'appliance VxRail fournit une prise en charge unique des fournisseurs pour les logiciels VMware, les serveurs PowerEdge et les logiciels VxRail via le support technique Dell. Le support VxRail inclut les services Dell EMC Secure Remote Services qui proposent des appels à distance et une connexion bidirectionnelle proactive pour la surveillance, le diagnostic et la réparation à distance tout au long du cycle de vie afin de garantir une disponibilité maximale.

VMware vSphere

La suite de logiciels VMware vSphere fournit à VxRail une infrastructure virtualisée hautement disponible, résiliente, à la demande. ESXi, vSAN et vCenter Server sont des composants centraux de la suite vSphere. La solution ESXi est un hyperviseur installé sur un nœud de serveur VxRail physique en usine qui permet à un seul serveur physique d'héberger plusieurs serveurs logiques ou machines virtuelles. vSAN est le stockage SDS utilisé par les machines virtuelles, et VMware vCenter Server est l'application de gestion des hôtes ESXi, du stockage vSAN et des machines virtuelles.

vSphere Platinum est une solution de sécurité spécialement conçue pour protéger les applications, l'infrastructure, les données et leur accès. Elle associe deux produits éprouvés : vSphere pour sécuriser l'infrastructure, les données et l'accès ; et AppDefense pour sécuriser les applications exécutées sur les machines virtuelles. La solution AppDefense protège l'intégrité des applications exécutées sur vSphere en utilisant l'apprentissage automatique pour comprendre l'état et le comportement prévus de l'application et de la machine afin de détecter et de prévenir les menaces. Les clients VxRail qui ont acheté des licences Platinum (y compris des abonnements) auprès de VMware peuvent utiliser leur licence Platinum sur une appliance VxRail qui exécute vSphere Enterprise Plus. Il est important de noter que la gestion du cycle de vie de la partie AppDefense de vSphere Platinum relève de la responsabilité du client.

À l'instar de Dell EMC, VMware suit un processus de développement logiciel sécurisé rigoureux et possède un centre de réponse de sécurité. L'appliance VxRail est développée et prise en charge conjointement avec VMware, ce qui garantit que tous les composants inclus dans la solution sont conçus, fabriqués, testés et déployés avec la sécurité en priorité absolue. Pour plus d'informations, cliquez sur le lien Sécurité des produits VMware.

VMware vCenter Server

Le serveur vCenter est le principal point de gestion pour la virtualisation des serveurs et le stockage vSAN. Une seule instance vCenter peut évoluer jusqu'aux niveaux d'une grande entreprise, en prenant en charge des centaines de nœuds VxRail et des milliers de machines virtuelles. L'appliance VxRail peut utiliser une instance vCenter déployée au sein du cluster VxRail ou utiliser une instance vCenter existante.

Le serveur vCenter fournit une hiérarchie logique de datacenters, de clusters et d'hôtes. Cette hiérarchie facilite la segmentation des ressources en fonction des cas d'utilisation ou des secteurs d'activité, et permet aux ressources d'être transférées de manière dynamique selon les besoins. Toutes ces opérations s'effectuent depuis une seule interface intuitive.

Le serveur vCenter fournit des services de machines virtuelles et de ressources, tels que le service d'inventaire, la planification des tâches, la journalisation des statistiques, la gestion des alertes et des événements, ainsi que le provisionnement et la configuration des machines virtuelles. Le serveur vCenter fournit également des fonctionnalités de disponibilité avancées, notamment :

- vSphere vMotion : permet la migration dynamique des charges applicatives des machines virtuelles sans arrêt de service.
- vSphere Distributed Resource Scheduler (DRS) : maintient l'équilibre et optimise en permanence l'allocation des ressources de calcul des machines virtuelles entre les nœuds du cluster.
- vSphere High Availability (HA) : offre des fonctionnalités de basculement et de redémarrage des machines virtuelles.

Hyperviseur VMware ESXi

Dans la solution VxRail, l'hyperviseur ESXi héberge la machine virtuelle sur les nœuds de cluster. Les machines virtuelles sont sécurisées et portables, et chaque machine virtuelle constitue un système complet avec processeurs, mémoire, gestion réseau, stockage et BIOS. Les machines virtuelles sont isolées les unes des autres. Ainsi, lorsqu'un système d'exploitation invité s'exécutant sur une machine virtuelle tombe en panne, les autres machines virtuelles sur le même hôte physique ne sont pas affectées et continuent de s'exécuter. Les machines virtuelles partagent l'accès aux processeurs, et l'hyperviseur ESXi est responsable de la planification des processeurs. En outre, l'hyperviseur ESXi attribue une zone de mémoire utilisable aux machines virtuelles et fournit un accès partagé aux cartes réseau physiques et aux contrôleurs de disque associés à l'hôte physique. Tous les systèmes d'exploitation x86 sont pris en charge, et les machines virtuelles installées sur le même matériel de serveur physique peuvent exécuter différents systèmes d'exploitation et applications.

Gestion réseau virtuelle VMware

Une des exigences de sécurité fondamentales consiste à isoler le trafic réseau. Sur l'appliance VxRail, les fonctionnalités de gestion réseau virtuelle de vSphere offrent une connectivité et des isolements flexibles. Les machines virtuelles VxRail communiquent entre elles à l'aide du commutateur VMware VDS (Virtual Distributed Switch), qui fonctionne comme un seul commutateur logique couvrant plusieurs nœuds dans le même cluster. Le commutateur VDS utilise des protocoles réseau standard et des implémentations de réseaux VLAN, et transfère les trames au niveau de la couche de liaison de données.

Il est configuré dans le serveur vCenter au niveau du datacenter, ce qui maintient une configuration réseau sécurisée et cohérente à mesure que les machines virtuelles migrent sur différents hôtes. L'appliance VxRail s'appuie sur le commutateur VDS pour son trafic, et le stockage vSAN s'appuie sur le commutateur VDS pour son accès au réseau.

De plus, l'appliance VxRail peut être configurée avec la solution NSX pour offrir une sécurité du réseau software-defined et un contrôle d'accès plus fin à l'aide de la micro-segmentation.

VMware vSAN

Les appliances VxRail sont équipées de la solution VMware vSAN pour le stockage SDS de niveau entreprise. La solution vSAN regroupe les disques connectés localement des hôtes dans un cluster vSphere afin de créer un pool de stockage partagé distribué. Pour étendre la capacité, il suffit d'ajouter d'autres disques au cluster et d'ajouter d'autres nœuds VxRail. La solution vSAN est entièrement intégrée à vSphere et fonctionne en toute transparence avec les autres fonctionnalités vSphere.

La solution vSAN se démarque par son efficacité et ses performances. Elle est auto-optimisée et ajuste l'allocation en fonction de la charge applicative, de l'utilisation et de la disponibilité des ressources. La solution vSAN offre une infrastructure HCI hautes performances, optimisée Flash et adaptée à une multitude de charges applicatives. Voici quelques-unes des fonctionnalités de stockage de niveau entreprise proposées :

- Technologie efficace de réduction des données, avec notamment la déduplication et la compression, ainsi que le codage d'effacement
- Stratégies de qualité de service pour contrôler la consommation des charges applicatives en fonction des limites définies par l'utilisateur
- Technologie d'intégrité des données et de protection des données, avec notamment les sommes de contrôle des logiciels et les domaines d'erreur
- Sécurité renforcée avec le chiffrement des données au repos vSAN

Avec la solution vSAN, les disques de chaque nœud VxRail sont automatiquement organisés en groupes de disques avec un seul disque de cache et un ou plusieurs disques de capacité. Ces groupes de disques sont utilisés pour former un seul datastore vSAN, accessible depuis tous les nœuds d'un cluster VxRail.

L'appliance VxRail propose deux options vSAN de configuration du stockage des nœuds : une configuration hybride qui utilise à la fois des disques SSD Flash et des disques durs mécaniques, et une configuration SSD All-Flash. La configuration hybride utilise des disques SSD Flash pour la mise en cache et des disques durs mécaniques pour la capacité et le stockage de données persistantes. La configuration All-Flash utilise des disques SSD Flash à la fois pour la mise en cache et pour la capacité. La figure 8 illustre les notions de base de la solution vSAN.

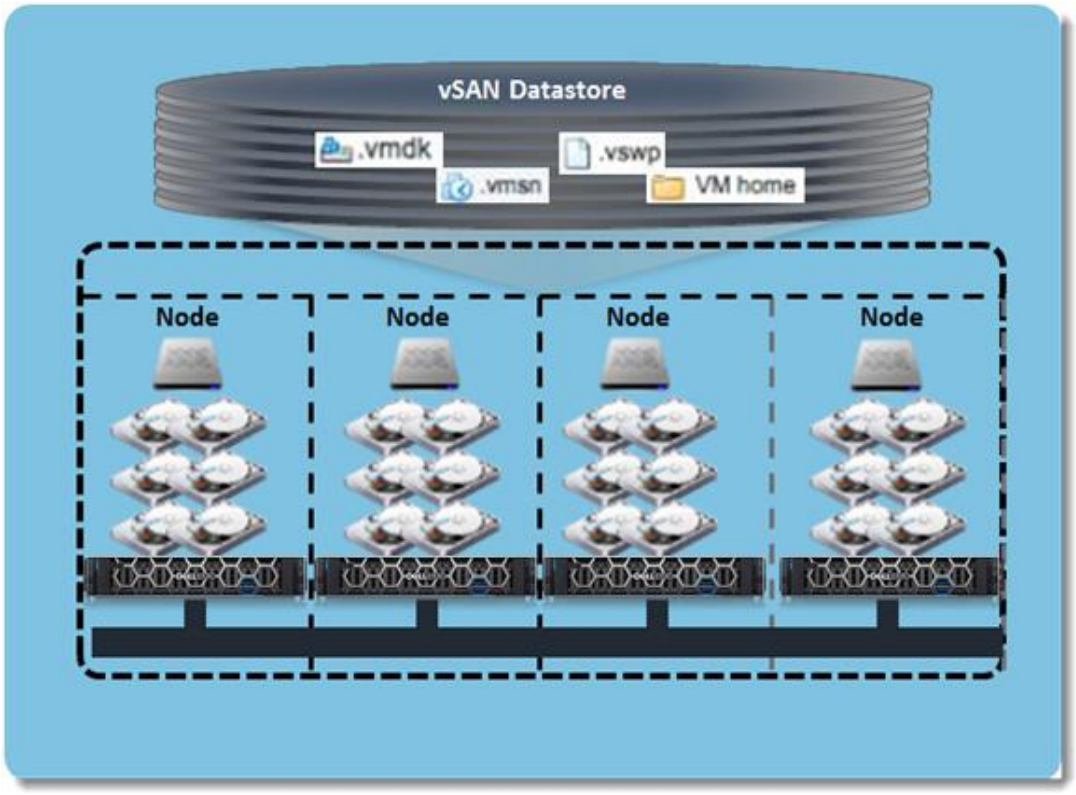

Figure 8 : Notions de base de la solution vSAN

La solution vSAN est configurée lorsque le cluster VxRail est initialisé pour la première fois et géré via la console vCenter. Au cours du processus d'initialisation de l'appliance VxRail, la solution vSAN crée un datastore partagé distribué à partir des disques connectés localement sur chaque nœud ESXi. La quantité de stockage disponible dans le datastore est un agrégat de tous les disques de capacité du cluster. La quantité de stockage utilisable dépendra du niveau de protection utilisé. La configuration et la vérification orchestrées de la solution vSAN, effectuées dans le cadre de l'initialisation du système, garantissent des performances cohérentes et prévisibles, ainsi qu'une configuration système conforme aux bonnes pratiques.

Storage Policy Based Management (SPBM)

La solution vSAN suit des règles prédéfinies et a été conçue pour simplifier le provisionnement et la gestion du stockage. Les règles de stockage vSAN sont basées sur des ensembles de règles qui définissent les exigences de stockage pour les machines virtuelles. Les administrateurs peuvent modifier de manière dynamique une règle de stockage de machine virtuelle à mesure que les besoins évoluent. Voici quelques exemples de règles SPBM : le nombre de pannes à tolérer, la technique de protection des données à utiliser et la possibilité d'activer les sommes de contrôle au niveau du stockage.

VMware vRealize Log Insight

Fourni avec l'appliance VxRail, l'outil VMware vRealize Log Insight surveille les événements système et fournit des notifications holistiques en continu concernant l'état de l'environnement virtuel et du matériel de l'appliance. Il fournit une gestion des fichiers journaux automatisée en temps réel pour l'appliance VxRail avec des fonctionnalités de surveillance des journaux, de regroupement intelligent et d'analytique permettant de simplifier le dépannage à grande échelle dans les différents environnements physiques, virtuels et Cloud de l'appliance VxRail. La journalisation centralisée est une condition fondamentale d'une infrastructure sécurisée. Pour les clients qui disposent déjà d'une fonction de journalisation ou d'un système SIEM, l'appliance VxRail s'intègre facilement à l'aide du protocole syslog de référence.

VMware Cloud Foundation (VCF) avec la solution NSX

VMware Cloud Foundation sur VxRail est une solution intégrée fabriquée conjointement par Dell EMC et VMware, dotée de fonctionnalités qui simplifient, rationalisent et automatisent les opérations de l'intégralité de votre datacenter software-defined (SDDC) du jour 0 au jour 2. La nouvelle plate-forme offre un ensemble de services software-defined pour le calcul (avec vSphere et vCenter), le stockage (avec vSAN), la gestion réseau (avec NSX), la sécurité et la gestion Cloud (avec vRealize Suite) dans les environnements privés et publics, ce qui en fait le concentrateur opérationnel de votre Cloud hybride.

VMware Cloud Foundation sur VxRail offre le chemin le plus simple vers le Cloud hybride via une plate-forme de Cloud hybride entièrement intégrée qui tire profit des fonctionnalités matérielles et logicielles VxRail natives et d'autres intégrations VxRail uniques (telles que les plug-ins vCenter et la gestion réseau Dell EMC). Ces composants fonctionnent de concert pour offrir une nouvelle expérience utilisateur de Cloud hybride clé en main, avec l'intégration de la pile complète. L'intégration de la pile complète permet de bénéficier à la fois de la couche d'infrastructure HCI et de la pile logicielle Cloud pour une expérience clé en main avec cycle de vie complet et automatisé.

Le datacenter VMware NSX est la plate-forme de virtualisation réseau et de sécurité qui fournit un réseau de Cloud virtuel. Il s'agit d'une approche software-defined de la gestion réseau qui s'étend à travers les datacenters, les Clouds, les points de terminaison et les sites périphériques. Avec le datacenter NSX, les fonctions réseau, notamment la commutation, le routage, le pare-feu et la répartition de charge, sont rapprochées de l'application et distribuées dans l'environnement. Tout comme le modèle opérationnel des machines virtuelles, les réseaux peuvent être provisionnés et gérés indépendamment du matériel sous-jacent.

Le datacenter NSX reproduit l'intégralité du modèle de réseau sous forme logicielle, de sorte que toute topologie de réseau, des réseaux simples à complexes avec plusieurs niveaux, peut être créée et provisionnée en quelques secondes. Les utilisateurs peuvent créer plusieurs réseaux virtuels avec diverses exigences, en tirant parti d'une combinaison des services proposés via la solution NSX, notamment la micro-segmentation, ou d'un vaste écosystème d'intégrations tierces, allant des pare-feu de nouvelle génération aux solutions de gestion des performances, pour créer des environnements intrinsèquement plus agiles et plus sécurisés. Ces services peuvent ensuite être étendus à plusieurs points de terminaison au sein et entre plusieurs Clouds. Pour plus d'informations, cliquez sur le lien Guide de l'architecture VMware Cloud Foundation sur VxRail.

Fonctionnalités de sécurité de l’appliance VxRail

Les fonctionnalités de sécurité sont divisées en deux catégories : sécurité des données et sécurité des systèmes. Ensuite, après la configuration et la gestion sécurisées de la solution VxRail, suivez les principes de la triade Confidentialité-Intégrité-Disponibilité (CID).

L’appliance VxRail fournit une pile entièrement préconfigurée et testée pour toutes les fonctionnalités de sécurité. Ces fonctionnalités de sécurité sont intégrées et incluses dans l’appliance.

SÉCURITÉ DES DONNÉES

La sécurité des données suit les préceptes de la triade CID afin de garantir que les données sont uniquement disponibles pour les comptes autorisés et/ou spécifiques et que la conformité et les spécifications sont respectées. Cela inclut l’accès aux données à la fois au niveau physique et au niveau utilisateur.

Confidentialité

Empêcher les données sensibles de tomber entre de mauvaises mains tout en garantissant un accès approprié et autorisé aux données d’une société est un problème fondamental qui relève du domaine de la « confidentialité ». L’appliance VxRail gère la confidentialité des données en cours d’utilisation, des données en mouvement et des données au repos de différentes manières.

Chiffrement

Le chiffrement protège la confidentialité des informations en les encodant pour qu’elles soient inintelligibles pour les destinataires non autorisés. Avec l’appliance VxRail, les datastores peuvent être chiffrés selon le chiffrement des données au repos de la solution vSAN (D@RE), qui fournit une protection validée FIPS 140-2 de niveau 1. Les machines virtuelles individuelles peuvent être chiffrées à l’aide du chiffrement vSphere, et les machines virtuelles en mouvement peuvent être chiffrées à l’aide du chiffrement vMotion. Des niveaux de chiffrement supplémentaires peuvent être configurés en fonction des exigences des applications.

Le chiffrement vSAN est le moyen le plus simple et le plus flexible de chiffrer les données au repos, car l’intégralité du datastore vSAN est chiffrée avec un seul paramètre. Ce chiffrement est à l’échelle du cluster pour toutes les machines virtuelles utilisant le datastore. En règle générale, les données chiffrées ne bénéficient pas de techniques de réduction de l’espace, telles que la déduplication ou la compression. Mais avec la solution vSAN, le chiffrement est effectué après la déduplication et la compression, ce qui permet de tirer pleinement parti de ces techniques de réduction de l’espace.

Le chiffrement des machines virtuelles offre la possibilité d’appliquer le chiffrement machine par machine, ce qui veut dire qu’un seul cluster peut compter des machines virtuelles chiffrées et non chiffrées. Le chiffrement des machines virtuelles suit la machine virtuelle où qu’elle soit hébergée. Ainsi, même si la machine virtuelle a été déplacée vers un datastore en dehors de l’appliance VxRail, elle reste chiffrée.

En outre, même si le chiffrement des machines virtuelles peut être activé et désactivé, les machines virtuelles qui sont chiffrées et migrées avec vSphere vMotion utilisent toujours vSphere vMotion chiffré. Les machines virtuelles qui ne sont pas chiffrées peuvent choisir entre les options de chiffrement Désactivé, Opportuniste et Requise en cas d’utilisation de la technologie vMotion. L’option Opportuniste est utilisée par défaut sur une machine virtuelle non chiffrée pendant une opération vMotion. La figure 9 ci-dessous récapitule la différence entre le chiffrement des machines virtuelles et le chiffrement vSAN.

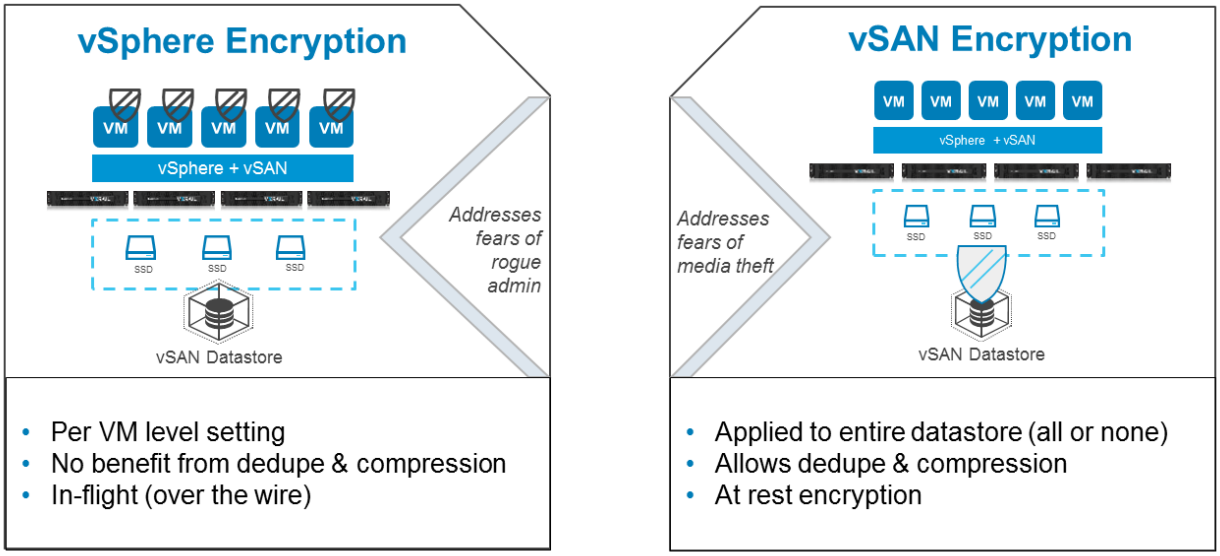

Figure 9 : Chiffrement des machines virtuelles par rapport au chiffrement vSAN

En outre, l'appliance VxRail prend en charge la fonction vMotion chiffrée si les machines virtuelles sont chiffrées lorsqu'elles sont déplacées d'un hôte à l'autre. Cela inclut les migrations vMotion au sein d'une appliance VxRail, ainsi que les migrations vMotion vers ou depuis un cluster VxRail au sein d'une instance vCenter. La migration vMotion chiffrée peut être utilisée avec le chiffrement vSAN pour disposer à la fois du chiffrement des données au repos et du chiffrement des données en cours de transfert. La migration vMotion chiffrée est appliquée aux machines virtuelles pour lesquelles le chiffrement vSphere est activé.

À l'exception du chiffrement vMotion, si vSphere fournit les clés temporaires utilisées pour chiffrer les données en mouvement, un serveur de gestion des clés (KMS) est requis pour la génération, le stockage et la distribution sécurisées des clés de chiffrement. Lorsque le chiffrement est activé, vCenter établit une relation d'approbation avec le serveur KMS, puis transmet les informations de connexion KMS aux hôtes ESXi. Les hôtes ESXi demandent les clés de chiffrement directement au serveur KMS et effectuent le chiffrement et le déchiffrement des données. La connectivité vCenter est requise pour la configuration initiale seulement.

Étant donné que le serveur KMS est un composant essentiel de l'infrastructure de sécurité, il doit disposer du même niveau de redondance et de protection que celui appliqué aux autres composants d'infrastructure critiques, tels que DNS, NTP et Active Directory. Il est important de garder à l'esprit que le serveur KMS doit être exécuté distinctement (d'un point de vue physique) des éléments qu'il chiffre. Au cours du démarrage, les hôtes ESXi demanderont les clés au serveur KMS. Si celui-ci n'est pas disponible, le système ne sera pas en mesure de procéder au démarrage.

VxRail et VMware prennent en charge les serveurs KMS compatibles avec le protocole d'interopérabilité de gestion des clés (KMIP) version 1.1 ou ultérieure, tels que Dell EMC CloudLink. VMware tient à jour un guide des serveurs KMS compatibles, dont l'utilisation avec vSphere a été validée.

Au sein de vSphere, le chiffrement est géré par un ensemble commun de modules qui sont validés FIPS 140-2. Ces modules communs sont conçus, mis en œuvre et validés par le cycle du développement sécurisé VMware. Le fait de disposer d'un ensemble de modules communs pour le chiffrement permet à l'appliance VxRail de simplifier la mise en œuvre, la gestion et la prise en charge du chiffrement.

Le chiffrement est activé sur l'appliance VxRail par le biais d'un simple paramètre de configuration dans vCenter. Les contrôles d'accès garantissent que seules les personnes autorisées peuvent activer ou désactiver le chiffrement. Un rôle nommé « No Cryptography Administrator » (Pas un administrateur du chiffrement) permet à un administrateur de procéder à des tâches d'administration normales, mais sans pouvoir modifier les paramètres de chiffrement.

Mise en réseau software-defined VxRail à l'aide de la solution NSX en option

L'environnement virtuel dynamique tel que celui de l'appliance VxRail bénéficie souvent de la flexibilité offerte par les services de réseau software-defined (SDN). Le moyen les plus simple de fournir les services SDN sur l'appliance VxRail est VMware NSX, qui est une licence logicielle en option, non incluse avec l'appliance VxRail. NSX est une plate-forme complète de virtualisation réseau et de sécurité qui permet aux administrateurs de créer des réseaux virtuels entiers, notamment des routeurs, des pare-feu et des répartiteurs de charge purement logiciels. Étant donné que cette mise en réseau software-defined est dissociée de l'infrastructure réseau physique sous-jacente, elle ne dépend pas de l'attachement de l'appliance VxRail à un fournisseur de commutateur donné.

NSX avec VxRail est une solution de sécurité intégrée qui réduit la nécessité de déployer des composants matériels ou logiciels de sécurité supplémentaires. Avec NSX, les administrateurs VxRail configurent la micro-segmentation afin de sécuriser et d'isoler différentes charges applicatives client, de contrôler les entrées et les sorties, et de fournir une sécurité renforcée pour toutes les charges applicatives, y compris les applications multiniveau traditionnelles et les machines virtuelles à usage général, ainsi que les environnements VDI. Voici quelques-uns des avantages de l'utilisation de NSX avec VxRail :

- la possibilité d'appliquer les règles de sécurité plus près de la charge applicative. Les règles de sécurité sont appliquées dans les logiciels, et les contrôles de sécurité se déplacent avec la charge applicative entre les hôtes du cluster ;
- une gestion simplifiée avec sécurité est intégrée à la pile vSphere et gérée de manière centralisée via le client Web vSphere HTML5 et le plug-in NSX Manager ;
- des contrôles de sécurité cohérents et automatiques à l'aide de groupes et de règles. Les charges applicatives sont automatiquement identifiées et placées de manière dynamique dans la bonne posture de sécurité ;
- la mise en œuvre efficace des contrôles de sécurité au niveau de l'hyperviseur réduit la latence des applications et la consommation de bande passante par rapport aux contrôles de sécurité externes ou basés sur le périmètre ;
- l'isolement de niveau DMZ permettant de contrôler les entrées et les sorties pour les clients internes et externes depuis Internet en utilisant des règles d'autorisation et de refus appropriées pour contrôler le trafic ;
- la détection et le blocage des adresses IP de machine virtuelle usurpées à l'aide de la fonctionnalité SpoofGuard (pour plus d'informations sur cette fonctionnalité, consultez la documentation Utilisation de SpoofGuard de VMware) ;
- le pare-feu d'identité permettant à un administrateur NSX de créer des règles de pare-feu distribué basées sur les utilisateurs Active Directory (pour plus d'informations sur cette fonctionnalité, consultez la documentation de VMware NSX) ;
- l'intégration à des services de sécurité tiers tels que la détection d'intrusion et la prévention contre les intrusions.

NSX améliore la posture de sécurité d'un environnement et est conforme aux certifications et normes suivantes :

- Certification Critères Communs : niveau EAL-2+
- Pare-feu certifié ICSA Labs
- Certification FIPS 140-2
- Respect de toutes les recommandations de cybersécurité du NIST concernant la protection des charges applicatives virtualisées

En tirant profit de la plate-forme VMware NSX en option pour la sécurité avec l'appliance VxRail, les règles de pare-feu et de sécurité sont intégrées. Il s'agit d'une appliance véritablement convergée, plutôt que d'une sécurité placée à l'extérieur du périmètre. Le déploiement de la solution NSX avec VxRail réduit encore le temps nécessaire au déploiement de nouvelles initiatives applicatives parce que les contrôles de sécurité sont intégrées à l'appliance, au lieu d'avoir à ajouter d'autres composants matériels ou logiciels.

Mode Verrouillage

Pour les environnements nécessitant un niveau de sécurité et de flexibilité encore plus élevé, le mode Verrouillage peut être configuré pour les hôtes ESXi. En mode Verrouillage, la possibilité d'effectuer des opérations de gestion sur les hôtes individuels est limitée, ce qui oblige à réaliser les tâches de gestion via la console vCenter.

Le verrouillage en mode « normal » permet à un groupe sélectionné d'utilisateurs d'être mis sur liste blanche, ce qui leur permet de gérer les serveurs localement plutôt que via vCenter. Cette liste blanche doit inclure certains comptes de gestion VxRail.

En mode de verrouillage strict, aucun utilisateur n'est autorisé à gérer les serveurs localement. Le verrouillage en mode « strict » n'est pas pris en charge par l'appliance VxRail.

Gestion sécurisée avec le protocole HTTPs

Le trafic de gestion non sécurisé représente un risque de sécurité important. De ce fait, l'appliance VxRail utilise les interfaces de gestion sécurisées avec le protocole TLS 1.2. vCenter, iDRAC et le logiciel système HCI désactivent tous l'interface HTTP en texte clair et nécessitent l'utilisation du protocole HTTPS, qui utilise la version TLS 1.2. En outre, l'accès à la ligne de commande des serveurs ESXi doit utiliser le protocole SSH. Le recours aux protocoles SSH et HTTPs est un élément essentiel de la commande et du contrôle sécurisés pour une appliance VxRail.

Intégrité

L'intégrité des données d'une société est une exigence fondamentale pour le bon fonctionnement de ses opérations. L'appliance VxRail garantit l'intégrité de vos données en conservant la cohérence, la précision et la fiabilité des données tout au long du cycle de vie en contrôlant l'accès utilisateur et les fonctionnalités d'intégrité intégrées, telles que les sommes de contrôle des données.

Segmentation réseau

La segmentation réseau est utilisée pour isoler le trafic réseau privé du trafic public afin de réduire la surface d'attaque. Il s'agit également d'un contrôle de sécurité efficace pour limiter les mouvements d'un attaquant d'un réseau à l'autre.

L'appliance VxRail est fabriquée avec plusieurs niveaux de segmentation réseau, notamment la segmentation physique de la mise en réseau de la gestion du matériel, la segmentation virtuelle des réseaux d'applications et d'infrastructure, et la micro-segmentation au niveau des machines virtuelles et des applications avec le logiciel NSX de VMware en option. Avec la segmentation, la visibilité des outils d'administration stratégiques est limitée, empêchant ainsi les attaquants de les utiliser contre un système. Par défaut, la segmentation réseau appropriée est automatiquement configurée dans le cadre de l'initialisation du système et l'administrateur a la possibilité de définir des niveaux supplémentaires de segmentation en fonction des besoins de l'environnement applicatif. Les bonnes pratiques en matière de configuration réseau sont présentées dans le Guide de réseau Dell EMC VxRail.

L'appliance VxRail utilise des commutateurs virtuels distribués VMware qui segmentent le trafic par défaut à l'aide de réseaux VLAN indépendants pour la gestion, vSAN, vMotion et le trafic applicatif. Les réseaux vSAN et vMotion sont des réseaux privés et non routables. Selon les applications prises en charge par un réseau VxRail, le trafic pourrait être davantage segmenté en fonction des différentes applications, de la production et du trafic hors production ou d'autres exigences.

Le commutateur virtuel distribué d'une appliance VxRail est configuré par défaut avec le contrôle vSphere Network I/O Control (NIOC). Le contrôle NIOC permet d'allouer de la bande passante physique à différents réseaux VLAN. Certaines cyberattaques, telles que les dénis de service et les vers, peuvent entraîner une utilisation abusive des ressources. Cela peut causer un déni de ressources à d'autres services qui ne sont pas directement ciblés par l'attaque. Le contrôle NIOC peut garantir que les autres services disposent de la bande passante réseau dont ils ont besoin pour maintenir leur intégrité en cas d'attaque sur un service. Les paramètres NIOC sont automatiquement configurés suivant les bonnes pratiques recommandées lors de l'initialisation du système. Le Guide de réseau Dell EMC contient des informations détaillées sur les paramètres du contrôle NIOC pour les réseaux VLAN VxRail par défaut.

Chaque nœud VxRail dispose d'un port Ethernet physique distinct pour l'interface de gestion du matériel iDRAC. La segmentation physique de ce réseau rend l'accès compliqué pour les attaquants qui voudraient accéder à la gestion du matériel. Dans le cas d'une attaque distribuée par déni de service, le réseau physiquement segmenté ne sera pas affecté, ce qui limite la portée d'une attaque potentielle.

Démarrage Secure Boot UEFI

Le démarrage Secure Boot UEFI protège le système d'exploitation contre la corruption et les attaques de rootkit. Le démarrage Secure Boot UEFI vérifie que le firmware, le chargeur de démarrage et VMkernel sont tous signés numériquement par une autorité de confiance. En outre, le démarrage Secure Boot UEFI pour ESXi vérifie que les bundles VIB (VMware Install Bundles) sont signés par chiffrement. Cela permet de s'assurer que la pile de démarrage du serveur exécute des logiciels authentiques et qu'elle n'a pas été modifiée.

Somme de contrôle logicielle

Une partie essentielle de l'intégrité des données consiste à s'assurer que les données extraites du stockage n'ont pas été modifiées depuis le moment de leur écriture. Par défaut, l'appliance VxRail utilise la somme de contrôle d'intégrité des données de bout en bout en mode bloc. La somme de contrôle est créée lorsque les données sont écrites. Elle est ensuite vérifiée lors de la lecture, et si elle montre que les données ont changé depuis leur écriture, celles-ci sont reconstruites à partir d'autres membres du groupe RAID. vSAN utilise également un mécanisme de nettoyage proactif pour détecter et corriger la corruption potentielle des données, même sur des données peu utilisées.

Disponibilité

Garder votre système IT à jour, en vous assurant que le matériel fonctionne correctement et que vous disposez d'une bande passante adéquate, est indispensable pour maintenir la disponibilité des données d'une société pour ses utilisateurs autorisés. La gestion du cycle de vie des logiciels VxRail, les fonctionnalités de disponibilité vSphere, la surveillance proactive et la récupération intégrée, ainsi que la sécurité physique du matériel et la configuration sécurisée du système garantissent une disponibilité maximale du système.

Gestion du cycle de vie des logiciels VxRail

D'un point de vue stratégique, l'une des actions essentielles qu'une organisation peut entreprendre pour maintenir la sécurité de son infrastructure IT est d'appliquer les mises à jour logicielles et les correctifs les plus récents. Outre qu'ils aident à résoudre les problèmes susceptibles de provoquer des arrêts de service ou à améliorer les performances, les mises à jour et les correctifs viennent souvent corriger les failles de sécurité. Il existe une collaboration exceptionnelle au sein de la communauté de la sécurité. L'appliance VxRail étant co-fabriquée avec VMware, nous sommes informés à l'avance des plans de correctifs de sécurité, ce qui permet à l'équipe VxRail de valider et de préparer rapidement des correctifs de sécurité préqualifiés. Mais nous ne sommes pas tous du même côté de la barrière. La situation peut tourner à l'affrontement entre les défenseurs qui s'efforcent de limiter et de corriger les menaces, et les attaquants dont l'objectif est d'exploiter les failles de sécurité. L'appliance VxRail étant co-fabriquée avec VMware, nous sommes informés à l'avance des plans de correctifs de sécurité, ce qui permet à l'équipe VxRail de valider et de préparer rapidement des correctifs de sécurité préqualifiés.

La gestion du cycle de vie des logiciels VxRail permet d'effectuer des opérations de mise à jour complexes et risquées, faciles à installer et à mettre en œuvre en toute sécurité. Le système VxRail HCI est le seul système dans lequel tous les composants logiciels sont fabriqués, testés et commercialisés sous forme de bundle. Les bundles de logiciels VxRail peuvent inclure des mises à jour du BIOS, du firmware, de l'hyperviseur, de vSphere ou de l'un des composants de gestion inclus. Si des failles de sécurité sont détectées, des correctifs sont rapidement mis au point pour limiter les menaces, quel que soit leur emplacement. Les packages de mise à jour sont rigoureusement testés sur la plate-forme matérielle VxRail et sur l'ensemble de la pile logicielle VxRail avant d'être mis à disposition des clients.

Les administrateurs sont notifiés via le logiciel système HCI lorsque des mises à jour sont disponibles. L'administrateur peut ensuite télécharger le package de mise à jour directement et lancer ou planifier un processus de mise à jour orchestrée. Les mises à jour sont exécutées par étape, tandis que le système reste en ligne et opérationnel. Si un redémarrage est nécessaire, les machines virtuelles sont automatiquement migrées vers d'autres nœuds du cluster avant de continuer.

Non seulement la gestion du cycle de vie du logiciel système HCI réduit la complexité, mais elle rend l'infrastructure plus sécurisée en réduisant le temps et les difficultés qu'il faut pour corriger les systèmes et éliminer les risques.

Fonctionnalités de disponibilité VxRail vSphere

L'appliance VxRail exploite les fonctionnalités de disponibilité vSphere intégrées, notamment VMware High Availability (HA), VMware Distributed Resource Scheduler (DRS) et les clusters étendus VMware. Ces fonctionnalités prennent en charge les logiciels automatisés VxRail et fournissent une disponibilité continue des services hébergés sur l'appliance VxRail. Par conséquent, il est recommandé aux clients d'utiliser des versions de vSphere qui incluent ces fonctionnalités.

La fonctionnalité VMware HA surveille l'exécution des machines virtuelles dans un cluster VxRail. En cas de défaillance d'une machine virtuelle ou d'un nœud, la fonctionnalité HA redémarre sur un autre nœud du cluster. Une machine virtuelle peut tomber en panne pour un certain nombre de raisons, notamment une cyberattaque, une défaillance du matériel sous-jacent ou des logiciels corrompus. Bien que la fonctionnalité VMware HA n'empêche pas les pannes, elle réduit le temps nécessaire à la restauration des services.

La fonctionnalité VMware DRS répartit la charge applicative des machines virtuelles sur tous les hôtes du cluster. À mesure que les besoins en ressources de machines virtuelles évoluent, la fonctionnalité DRS migre les charges applicatives des machines virtuelles, à l'aide de vSphere vMotion, vers d'autres hôtes du cluster. Les cyberattaques peuvent engendrer des problèmes de ressources pour les machines virtuelles qui ne sont pas ciblées par l'attaque. Les cyberattaques entraînent souvent un fort taux d'utilisation des ressources par les machines virtuelles attaquées et, par conséquent, une utilisation intensive des ressources au niveau de l'hôte, ce qui a un impact sur les ressources disponibles pour les autres machines virtuelles sur cet hôte. La fonctionnalité DRS protège les machines virtuelles en les faisant migrer sur d'autres hôtes que les hôtes limités en ressources, ce qui leur permet de continuer à fournir des services.

Le cluster étendu VMware étend le cluster VxRail d'un seul site à deux sites pour obtenir un niveau de disponibilité plus élevé. Il n'existe qu'une seule instance d'une machine virtuelle, mais des copies complètes de ses données sont conservées sur les deux sites. Si le site actuel sur lequel la machine virtuelle s'exécute devient indisponible, la machine virtuelle sera redémarrée sur l'autre site.

Protection des données

Des défenses de sécurité renforcées sont essentielles, mais un plan de récupération robuste et fiable est tout aussi important. Les sauvegardes et les réplications sont les pierres angulaires de la récupération après une violation. Afin de faciliter la récupération, le logiciel système HCI inclut une sauvegarde et une restauration basées sur les fichiers. Toutes les appliances VxRail incluent un kit de démarrage pour Dell EMC RecoverPoint for VM (RP4VM), qui fournit une réplication locale et à distance optimale et une récupération granulaire.

La sauvegarde et la restauration basées sur les fichiers du logiciel système HCI protègent contre la suppression accidentelle de l'appliance virtuelle ou la corruption interne de l'appliance. Les sauvegardes peuvent être configurées pour s'effectuer régulièrement ou en fonction des besoins. Il s'agit d'une fonctionnalité tout-en-un qui permet de sauvegarder les fichiers au sein du datastore vSAN de sorte qu'aucun matériel ou logiciel supplémentaire ne soient requis.

Avec la fonctionnalité RP4VM, si par exemple, une machine virtuelle est compromise, ou si les données sont endommagées ou sont volées et font l'objet d'une rançon, la machine virtuelle et le jeu de données sont rapidement rétablis à un état précédant l'attaque, ce qui permet une reprise d'activité rapide. Installée directement à partir de VxRail Manager, la fonctionnalité RP4VM est rapidement déployée et la surveillance quotidienne se fait via le plug-in vCenter bien connu. La récupération est simple et s'effectue dans l'interface vSphere bien connue.

Pour les organisations qui ont besoin de fonctionnalités de protection des données complètes et améliorées, l'appliance VxRail prend en charge des options telles que Dell EMC Data Protection Suite for VMware, Dell EMC Power Protect et Dell EMC Data Domain Virtual Edition.

Les sauvegardes basées sur les fichiers du logiciel système VxRail HCI permettent de garantir la continuité d'activité dans les rares cas où la machine virtuelle VxRail doit être reconstruite.

SÉCURITÉ DU SYSTÈME

Authentification, autorisation et comptabilité de l'appliance VxRail

Le cadre AAA (authentification, autorisation et comptabilité) est intégré. Il est conçu pour contrôler l'accès, ce qui permet de garantir que la bonne personne utilise le système, de fournir le niveau d'accès approprié et de consigner l'activité pour garder une trace des opérations effectuées et de leurs auteurs.

AUTHENTIFICATION

L'authentification au logiciel système HCI est gérée par authentification unique via le plug-in vCenter. VxRail vCenter prend en charge le système centralisé de gestion des identités de l'organisation conformément aux règles de sécurité d'authentification.

Les organisations centralisent souvent la gestion des identités à l'aide de services d'annuaire tels que Microsoft Active Directory (AD) en utilisant le protocole LDAP. Si l'appliance VxRail est un environnement autonome et ne fait pas partie d'un domaine, les utilisateurs et les mots de passe peuvent être gérés localement dans vSphere et iDRAC. Du point de vue des bonnes pratiques, il est recommandé d'utiliser une authentification centralisée.

Il arrive souvent que différentes personnes soient responsables des serveurs physiques, de la gestion du cycle de vie VxRail et de la gestion du serveur, du stockage et de l'environnement de virtualisation réseau. Par conséquent, l'appliance VxRail utilise des contrôles d'accès basés sur les rôles à un niveau fin pour iDRAC, le logiciel système HCI et vSphere.

AUTORISATION

En utilisant le « principe du moindre privilège » (POLP), un utilisateur se voit concéder les droits requis pour remplir son rôle, mais pas plus qu'il n'en a besoin. vSphere inclut plusieurs rôles prédéfinis qui sont utilisés pour accorder le privilège approprié. Par exemple, un utilisateur peut se voir accorder le rôle d'administrateur vSphere, le rôle de gestion HCIA ou les deux. Le rôle de gestion HCIA accorde à un utilisateur le droit d'effectuer les tâches de gestion du cycle de vie VxRail à partir du plug-in de gestion VxRail dans vCenter. Le rôle d'administrateur vSphere accorde le droit d'effectuer des tâches d'administration dans vCenter. En outre, vSphere offre un niveau de contrôle d'accès encore plus précis grâce à la création de rôles personnalisés. Par exemple, un utilisateur privilégié peut être autorisé à prendre connaissance d'une alerte ou à créer un profil de stockage, mais pas à déployer des machines virtuelles.

Les rôles sont associés à des utilisateurs et des groupes, ainsi qu'à des objets spécifiques, un objet étant une chose ou un groupe de choses. Par exemple, un utilisateur ou un groupe peut avoir l'autorisation de prendre connaissance des alertes d'une machine virtuelle ou d'un port particulier, mais pas de celles d'autres objets. En outre, des rôles restrictifs, tels que « Aucun accès », peuvent être attribués aux utilisateurs, ce qui les empêche de voir des domaines spécifiques au sein de vCenter. Plusieurs utilisateurs ou groupes peuvent bénéficier de niveaux d'accès identiques ou différents au même objet. Les autorisations accordées à un objet enfant peuvent être utilisées pour remplacer les autorisations héritées d'un objet parent.

Le contrôle d'accès basé sur les rôles vSphere prend en charge les principes de sécurité granulaires du « moindre privilège » et de la « séparation des responsabilités », et permet à l'administrateur de la sécurité d'améliorer la sécurité en définissant des autorisations précises en fonction de la structure de gestion des systèmes d'une organisation.

COMPTABILITÉ

Il est essentiel de comprendre les modifications apportées à la configuration et à l'état des composants pour assurer la sécurité et la disponibilité des systèmes. Les modifications peuvent résulter d'une correction temporaire entraînant un écart de configuration. Ces modifications peuvent également indiquer une éventuelle intrusion. La surveillance proactive de l'infrastructure est une activité de sécurité importante.

Une détection rapide dès qu'une intrusion se produit peut faire la différence entre une brève interruption où l'attaquant ne peut pas compromettre les systèmes critiques et une intrusion qui persiste pendant des mois, entraînant la compromission de plusieurs systèmes critiques. Sans maintien d'un système de journaux d'audit, il est possible que les informations disponibles sur l'attaque ne soient pas suffisantes pour déterminer sa gravité. D'après le rapport de sécurité mondial de 2019 de Trustwave (inscription requise), 57 % des incidents ayant fait l'objet d'une investigation concernaient les réseaux d'entreprise et les réseaux internes (contre 50 % simplement en 2017).

Les écarts de configuration représentent un défi qui touche tous les systèmes. Au début, un système peut fonctionner sur une configuration de base sécurisée, mais au fil du temps, des modifications peuvent survenir, rendant le système vulnérable. Ces modifications peuvent se produire pour diverses raisons, notamment une modification temporaire lors d'un dépannage ou une modification approuvée qui doit être intégrée à la configuration de base. Sans surveillance, ces changements deviennent très difficiles à détecter.

Les difficultés liées à la surveillance des informations résident dans le fait que celles-ci proviennent de nombreuses sources différentes : une machine virtuelle individuelle, un serveur physique, l'infrastructure de virtualisation, le réseau, les composants de sécurité ou encore les applications elles-mêmes. L'interprétation de ces informations nécessite une vue consolidée de l'activité et des modifications. L'appliance VxRail est équipée de l'outil vRealize Log Insight. Il compile les journaux VMware, notamment ceux des serveurs, des périphériques réseau, du stockage et des applications. Comme le montre le graphique ci-dessous, l'outil Log Insight crée un tableau de bord avec des graphiques basés sur les données contenues dans les journaux. Cela permet à l'administrateur d'effectuer rapidement une recherche verticale de la cause première du problème. La figure 9 ci-dessous présente le tableau de bord vRealize Log Insight.

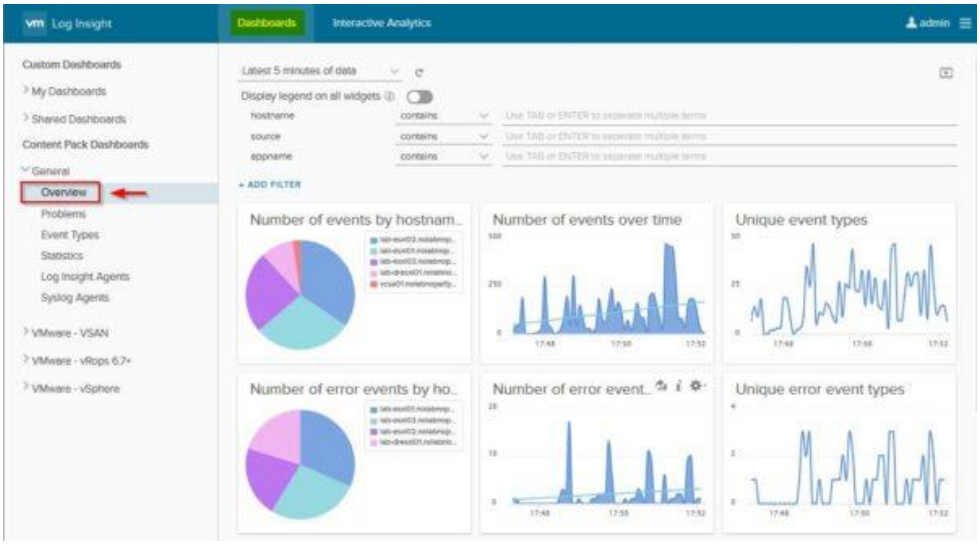

Figure 10 : vRealize Log Insight

La mise en corrélation de toutes ces informations est l'une des nombreuses raisons pour lesquelles l'appliance VxRail utilise le protocole NTP (Network Time Protocol) standard pour assurer la synchronisation de toutes les horloges de composants.

Pour les organisations qui disposent déjà d'un système de gestion des fichiers journaux ou d'un système de gestion des incidents et des événements de sécurité (SIEM), l'appliance VxRail propose une intégration facile avec le protocole syslog standard.

Sécurité de l'emplacement physique de l'appliance VxRail

La sécurité physique est un élément important de toute solution de sécurité complète. Étant donné que l'appliance VxRail peut être déployée en dehors d'un datacenter traditionnel, la sécurité physique peut prendre encore plus d'importance. Pour empêcher l'introduction de logiciels malveillants ou de logiciels infectés via une clé USB, les ports USB d'une appliance VxRail peuvent être désactivés, puis activés uniquement en cas de besoin.

Les nœuds VxRail surveillent également d'autres événements, tels que les ouvertures de châssis, les pannes ou les remplacements de pièces, les modifications du firmware et les avertissements liés à la température. Ces informations sont enregistrées dans le journal de cycle de vie iDRAC. Dans de nombreux cas, un châssis n'a plus besoin d'être ouvert une fois qu'il a été mis en production et le suivi de ce type d'activité peut révéler une tentative de compromission du système.

Automatisation

Une partie importante du maintien de la sécurité consiste à s'assurer que tous les éléments de configuration de sécurité pertinents sont implémentés sur tous les objets d'un environnement. Un cluster VxRail peut compter jusqu'à 64 nœuds physiques, et plusieurs clusters VxRail peuvent être gérés par un seul vCenter, prenant ainsi en charge des milliers de machines virtuelles. Même l'application d'une simple modification, si elle doit être configurée sur toutes les machines virtuelles, peut prendre beaucoup de temps. En outre, lorsqu'ils effectuent des tâches répétitives, les collaborateurs sont enclins à faire des erreurs. C'est là que l'automatisation devient cruciale.

L'automatisation permet à un environnement d'enregistrer moins d'erreurs de configuration et d'avoir une configuration plus homogène, tout en augmentant l'efficacité et en réduisant le temps entre le moment où une décision est prise et la date de mise en œuvre, ce qui augmente le délai de rentabilité de ces décisions.

Des outils compatibles tels que l'outil vRealize Automation permettent l'automatisation de vSphere et de vSAN. Ces outils peuvent être utilisés pour automatiser les opérations quotidiennes courantes, telles que la création de machines virtuelles ou de règles de stockage. L'outil vRealize Automation peut également être utilisé pour confirmer que la configuration de sécurité ne s'est pas éloignée des paramètres appropriés. Si la configuration a changé, l'outil vRealize Automation est en mesure de reconfigurer les serveurs ESXi, vCenter ou les machines virtuelles individuelles afin qu'ils soient à nouveau conformes à la configuration de sécurité requise. En outre, étant donné que l'outil vRealize Automation est un outil VMware standard, de nombreuses équipes de virtualisation IT savent déjà comment l'utiliser et ont créé des profils qui fonctionneront avec un cluster VxRail.

Package de renforcement STIG VxRail

La configuration de la sécurité peut être un processus complexe, sujet aux erreurs et présentant bon nombre des risques qu'elle cherche elle-même à limiter. Trois éléments différents simplifient le processus de sécurisation de l'infrastructure VxRail. Premièrement, vSphere dispose d'une approche « sécurisée par défaut » de la configuration. Deuxièmement, les guides STIG (Security Technical Implementation Guide, Guide de mise en œuvre technique de la sécurité) de l'Agence américaine DISA (Defense Information Systems Agency, Agence de défense des systèmes d'informations) offrent un blueprint pour le renforcement de la sécurité et un large éventail d'outils d'automatisation permettant de vérifier et de configurer les paramètres de sécurité en fonction des besoins. Cela permet de configurer le profil de risque approprié afin qu'il corresponde aux besoins de l'entreprise. Enfin, la possibilité d'automatiser la restauration de la configuration à un état sécurisé connu lorsque des modifications inattendues se produisent est un élément essentiel de la sécurité VxRail.

À compter de vSphere 6.0, VMware a lancé une initiative visant à faire de la sécurité le paramètre par défaut pour vSphere. Les appliances VxRail sont donc plus sécurisées dès l'installation. Dans le cadre de cette initiative, la plupart des paramètres de sécurité recommandés ont été classés comme spécifiques au site ou comme remplacés par le paramètre sécurisé par défaut. Les paramètres qui devaient auparavant être modifiés après l'installation ont été mis à jour de manière à ce que le paramètre sécurisé devienne la valeur par défaut.

Les paramètres de configuration classés comme spécifiques au site ne peuvent pas être configurés par défaut, par exemple, le nom d'hôte d'un serveur syslog ou d'un serveur NTP distant. Avec l'appliance VxRail, la plupart des paramètres que VMware classe comme étant spécifiques au site sont configurés par le logiciel système HCI pendant l'installation.

De nombreuses organisations se réfèrent aux guides STIG pour renforcer leurs systèmes. Ils fournissent une check-list au format PDF lisible par un humain et un script automatisé. Cela permet aux outils d'automatisation de lire le guide STIG et de configurer l'environnement de manière à ce qu'il corresponde à la configuration recommandée avec une intervention manuelle minimale. Bien que les guides STIG VMware existants couvrent les composants VxRail, dont vSphere, les serveurs ESXi et vSAN simplifient la mise en œuvre. L'appliance Dell VxRail exécutant le logiciel VxRail Appliance v4.5.x ou 4.7.x est conforme aux exigences des guides STIG DISA correspondants.

Au fil du temps, les configurations peuvent s'éloigner de la base et avoir des positions moins sécurisées. Pour cette raison, il est important non seulement de surveiller la configuration, mais également d'automatiser la restauration de l'environnement à l'état de sécurité initial. L'appliance VxRail prend en charge plusieurs options différentes en fonction du niveau d'automatisation requis. L'appliance VxRail dispose d'outils de renforcement automatisés qui vérifient la configuration actuelle par rapport aux recommandations d'un guide STIG. Si la configuration a changé, elle est restaurée à l'état sécurisé connu. Si vous avez besoin d'un outil d'automatisation plus complet, la solution VMware vRealize Suite fonctionne avec les environnements VxRail pour automatiser la gestion de la configuration tout en assurant gouvernance et contrôle. En outre, VMware propose la solution AppDefense, un outil plus axé sur les applications qui utilise l'apprentissage automatique pour collecter des informations sur un état de fonctionnement connu pour les machines virtuelles et les applications qu'elles prennent en charge. Avec cet outil, si une variation par rapport à l'état de fonctionnement connu est détectée, l'administrateur est averti et une réponse peut être automatisée à partir d'une bibliothèque de routines de réponse aux incidents.

Sécurité intégrée à la plate-forme VxRail ACE

La plate-forme VxRail ACE (Analytical Consulting Engine) vient compléter la simplicité opérationnelle intégrée de la solution Dell EMC VxRail avec une intelligence opérationnelle destinée aux clusters VxRail. La plate-forme VxRail ACE offre une combinaison de simplicité opérationnelle et d'intelligence opérationnelle avec une sécurité intrinsèque, ce qui permet aux sociétés de poursuivre la transformation de leur infrastructure IT.

Elle s'exécute sur une plate-forme Cloud gérée par l'équipe Dell EMC IT. En tant que Logiciel en tant que service basé sur le Cloud, la plate-forme VxRail ACE dispose de la flexibilité nécessaire pour offrir de nouvelles fonctionnalités fréquemment et sans interruption, offrant ainsi une expérience client exceptionnelle. Son réseau neuronal de Deep Learning améliore continuellement ses fonctionnalités prédictives à mesure qu'il ingère les métadonnées collectées par l'appliance VxRail sur ses clusters.

Les utilisateurs VxRail peuvent accéder à la plate-forme VxRail ACE à l'adresse https://vxrailace.emc.com à l'aide de leurs informations d'identification du support Dell EMC.

Présentation de la sécurité de la plate-forme VxRail ACE

La plate-forme VxRail ACE collecte les données de télémétrie des nœuds VxRail des différents clusters VxRail de l'organisation et transmet en toute sécurité ces données à un Logiciel en tant que service géré par l'équipe Dell EMC IT, comme illustré dans la figure 011.

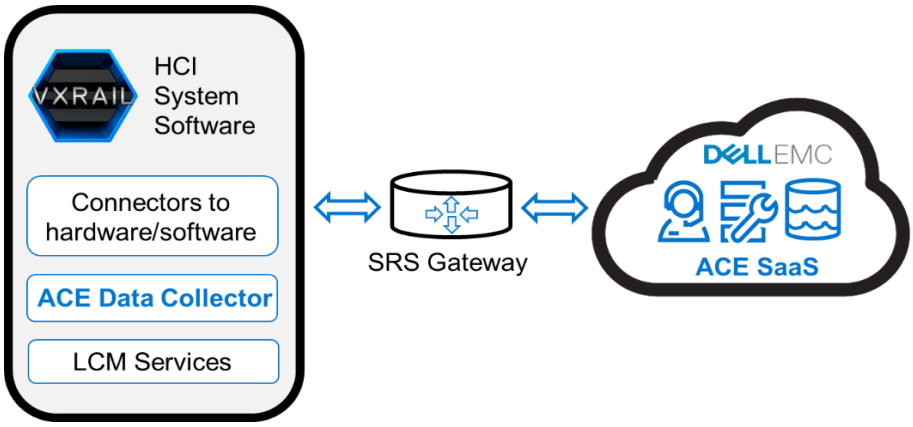

Figure 11 : Schéma de l'architecture générale de la plate-forme VxRail ACE

Dell EMC comprend les préoccupations des clients en ce qui concerne le maintien de la sécurité de leurs données. La sécurité est intrinsèque à la plate-forme VxRail ACE, de la collecte de données au transit des données et au repos. En outre, la plate-forme VxRail ACE a été développée de façon sécurisée à l'aide de contrôles architecturaux dans le cadre du cycle de développement de la sécurité standard Dell EMC. Cette norme définit les activités axées sur la sécurité que les équipes de produits Dell EMC doivent suivre lors de la création et de la mise en production de produits afin de permettre aux produits Dell EMC de minimiser les risques que représentent les failles de sécurité pour nos produits et les environnements des clients.

Collecte de données de la plate-forme VxRail ACE

Sur chaque cluster VxRail, un contrôleur de données ADC (Adaptive Data Collector) s'exécute pour récupérer les données de télémétrie du logiciel système HCI par le biais de connecteurs matériels et logiciels VxRail. L'outil de collecte ADC ne recueille aucune donnée à caractère personnel. Les données de télémétrie collectées par l'outil de collecte ADC sont indiquées dans le tableau 1.

Télémétrie de base (topologie matérielle : appliances, disques, firmware, blocs d'alimentation)	**Données de performances**	**Alertes**	**Données du capteur matériel**
• Informations sur le cluster • Informations sur l'appliance	• Cluster (processeur, mémoire, disque) • Machine virtuelle (processeur, mémoire, disque) • vSAN (disque, réseau)	• vCenter • VxRail	• Type de capteur • État • Nom • Relevé actuel

Table 1 Données de télémétrie VxRail collectées par la plate-forme ACE

Les données de télémétrie collectées par l'outil ADC ne sont pas stockées localement. Les données sont transmises en toute sécurité via la passerelle Dell EMC SRS (Secure Remote Services).

Données de la plate-forme VxRail ACE en transit vers Dell

Seules les données collectées par le contrôleur de données ADC sont transmises au serveur backend Dell EMC via la passerelle Dell EMC SRS (Secure Remote Services). La plate-forme VxRail ACE s'abonne aux notifications d'arrivée des données du système HCI via la passerelle SRS. Les clients VxRail ACE contrôlent les systèmes qui envoient les données du système HCI via la passerelle. Toutes les données transmises via la passerelle Dell EMC SRS sont protégées en transit par l'observation des bonnes pratiques du secteur. La passerelle SRS est authentifiée de manière bidirectionnelle à l'aide de certificats numériques RSA®, conjointement avec des règles d'accès contrôlées par le client et un journal d'audit détaillé. La communication point à point est établie en utilisant le chiffrement AES (Advanced Encryption Standard) 256 bits, qui garantit que toutes les données sont transportées en toute sécurité vers l'infrastructure gérée par l'équipe Dell EMC IT. En outre, la passerelle SRS fournit des fonctionnalités dédiées de VPN et d'authentification multifacteur. Une fois que les données sont arrivées chez Dell, la plate-forme VxRail ACE chiffre et stocke les données ACE dans sa propre infrastructure gérée par l'équipe Dell EMC IT.

Données VxRail ACE au repos

Les données du système HCI reçues des systèmes gérés VxRail ACE sont chiffrées et stockées sur l'infrastructure Dell gérée par l'équipe Dell EMC IT.

L'infrastructure de l'équipe Dell EMC IT :

- fournit une plate-forme sécurisée qui permet d'isoler les données de télémétrie de chaque client ;
- offre une haute disponibilité, une tolérance de panne et une reprise après sinistre ;
- localise les données de télémétrie du client (y compris les sauvegardes) aux États-Unis ;
- conserve indéfiniment les données historiques pour les systèmes qui sont activement surveillés par la plate-forme ACE, y compris les informations exploitables dérivées de l'analytique ACE ;
- permet à chaque client d'accéder à un portail indépendant et sécurisé à partir duquel chaque utilisateur ne peut voir dans VxRail ACE que les systèmes qui font partie de l'accès au site de cet utilisateur, tel qu'il est défini dans Dell EMC MyService360.

Le Bureau SRO (Security and Resiliency Office) de Dell Technologies, dirigé par le directeur de la sécurité de Dell, est responsable de la sécurité et de la protection de l'infrastructure des technologies de l'information Dell EMC qui héberge le Logiciel en tant que service VxRail ACE. Cela s'effectue selon des règles et des procédures de sécurité établies, et l'application de contrôles de sécurité des informations, lesquels incluent des mesures telles que des pare-feu multicouche, des systèmes de détection d'intrusion, des antivirus de pointe et une protection contre les logiciels malveillants. L'équipe de cybersécurité Dell EMC participe à l'exécution d'analyses continues de failles de sécurité sur l'environnement applicatif et sous-jacent. Toute mesure corrective requise est gérée par le biais d'un programme de correction des failles de sécurité, dont notamment des mises à niveaux logicielles, des correctifs ou des modifications de configuration.

Toutes les données transmises à la plate-forme VxRail ACE sont stockées sur l'infrastructure hébergée dans le datacenter Dell EMC. La politique de sécurité des informations garantit que toutes les informations et toutes les ressources Dell EMC sont correctement protégées. Les propriétaires d'informations doivent s'assurer que toutes les ressources sont prises en compte et que chaque ressource dispose d'un dépositaire attitré. Tous les composants de l'infrastructure se trouvent dans le réseau d'enclave dédié protégé par pare-feu Dell EMC qui n'est pas exposé à un accès externe. Aucune connexion directe au serveur de base de données et à la base de données n'est autorisée, à l'exception des membres des équipes d'administrateurs système et d'administrateurs de base de données. Les comptes d'applications de base de données sont gérés avec une authentification de base de données standard par mot de passe Dell EMC a mis en œuvre un processus de gestion des changements basés sur les bonnes pratiques du secteur afin de garantir que le matériel d'infrastructure Dell EMC est stable, contrôlé et protégé. La gestion des changements fournit les règles, les procédures et les outils nécessaires pour régir ces changements, afin de s'assurer qu'ils sont soumis aux révisions et approbations appropriées, et qu'ils sont communiqués efficacement aux utilisateurs.

Contrôle d'accès aux données VxRail ACE

L'accès aux données VxRail ACE peut être divisé en deux catégories :

- Accès par les clients à la plate-forme VxRail ACE pour l'affichage des données système et des informations dérivées de l'analytique ACE
- Accès par l'administrateur système informatique interne de l'équipe Dell EMC IT et l'administrateur de base de données à l'infrastructure VxRail ACE gérée par Dell EMC

Les sous-sections ci-dessous décrivent la façon dont l'accès aux données est contrôlé par ces deux catégories d'utilisateurs.

Accès de l’utilisateur final à la plate-forme VxRail ACE

Les clients utilisent leur compte de support existant pour se connecter à la plate-forme VxRail ACE. L’accès aux données VxRail ACE depuis le portail VxRail ACE requiert que chaque utilisateur final dispose d’un compte de support Dell EMC valide. L’authentification est gérée par l’infrastructure SSO (authentification unique) de Dell EMC. La plate-forme VxRail ACE utilise le profil de l’utilisateur client Dell EMC MyService360 pour le contrôle d’accès. Le profil de l’utilisateur est créé et associé à un profil client valide lorsque l’utilisateur s’inscrit pour ouvrir un compte auprès de Dell EMC. La plate-forme VxRail ACE fournit à chaque client une vue indépendante et sécurisée de ses systèmes et s’assure qu’il ne pourra voir que ses propres données via la plate-forme VxRail ACE. Dans la plate-forme VxRail ACE, chaque utilisateur peut uniquement voir les systèmes qui font partie de l’accès au site de cet utilisateur, conformément à la configuration de cet utilisateur dans Dell EMC MyService360.

Accès administratif à l’infrastructure VxRail ACE gérée par l’équipe Dell EMC IT

Dell EMC est très sensible à l’importance de la protection des informations propriétaires et confidentielles des clients. À ce titre, tous les collaborateurs Dell EMC doivent signer un contrat collaborateur, qui inclut des dispositions portant sur les informations client. Les obligations de ce contrat s’étendent à toutes les données stockées sur une machine qui sont perçues, sous quelque forme que ce soit, lors d’une mission de maintenance. Elles restent en vigueur même après la cessation de contrat avec Dell EMC.

Normes et certifications compatibles

La solution VxRail est une infrastructure hyperconvergée robuste et flexible qui peut être configurée pour permettre aux organisations de respecter des réglementations de conformité. Bien que certains fournisseurs HCI déclarent simplement que leur solution est conforme, Dell EMC cherche activement à obtenir une certification complète aux normes de sécurité importantes pour nos clients. Contactez votre responsable de compte Dell EMC pour en savoir plus sur la manière dont l’appliance VxRail répond aux exigences les plus strictes en matière d’activité et de réglementation. Vous trouverez ci-dessous une liste de quelques-unes des normes et certifications qui s’appliquent à l’appliance VxRail.

Chiffrement des données au repos FIPS 140-2 : la norme FIPS PUB 140-2 (Federal Information Processing Standard Publication 140-2) établit les exigences et les normes applicables aux composants matériels et logiciels des modules de chiffrement. La norme FIPS 140-2 est requise par le gouvernement et d’autres secteurs réglementés des États-Unis, tels que les institutions financières et de santé, qui collectent, stockent, transfèrent, partagent et diffusent des informations sensibles, mais non classifiées. Les serveurs PowerEdge utilisés par l’appliance VxRail ont été validés.

Critères Communs EAL 2+ : la norme Critères Communs pour l’évaluation de la sécurité des technologies de l’information est une norme internationale (ISO/IEC 15408) pour la certification de la sécurité informatique. Les évaluations des Critères Communs sont effectuées sur les systèmes et les produits de sécurité informatique afin d’évaluer les fonctions de sécurité du système et de fournir un niveau de confiance dans les fonctionnalités de sécurité du produit par le biais d’exigences d’assurance de sécurité ou d’un niveau d’assurance de l’évaluation. La certification Critères Communs ne peut pas garantir la sécurité, mais elle garantit que les promesses relatives aux attributs de sécurité ont été vérifiées de manière indépendante. Les serveurs PowerEdge et les composants vSphere utilisés par l’appliance VxRail sont actuellement titulaires d’une certification complète.

Cadre de cybersécurité du NIST : le cadre du NIST pour l'amélioration des infrastructures stratégiques est une directive volontaire développée pour aider les organisations à améliorer la cybersécurité, la gestion des risques et la résilience de leurs systèmes. Le NIST s'est entretenu avec un large éventail de partenaires du secteur public, de l'industrie et du milieu universitaire pendant plus d'un an pour élaborer un ensemble de recommandations et de pratiques saines qui font l'unanimité. La publication spéciale 800-131A présente des recommandations relatives à la longueur de la clé de chiffrement.

Suite B de la NSA : la Suite B est un ensemble d'algorithmes de chiffrement promulgués par la NSA (Agence de sécurité nationale américaine) dans le cadre de son programme de modernisation du chiffrement. Les versions actuelles d'ESXi et de vCenter utilisées avec l'appliance VxRail prennent en charge la suite B de la NSA.

Modèle VPAT de la section 508 : les normes de la section 508 de l'United States Access Board s'appliquent aux technologies de l'information et électroniques fournies par le gouvernement fédéral américain et définissent les exigences d'accessibilité pour les personnes souffrant de déficiences physiques, sensorielles ou cognitives. Le serveur PowerEdge et les composants logiciels vSphere utilisés par l'appliance VxRail sont conformes au modèle VPAT de la section 508.

Trade Adjustment Assistance (TAA) : le programme TAA est un programme fédéral qui offre un moyen de favoriser la croissance et les opportunités d'emploi en aidant les actifs des États-Unis ayant perdu leur emploi en raison de la concurrence du commerce extérieur. Lorsqu'elle est vendue en tant que système, l'appliance VxRail est conforme TAA.

DISA STIG : l'agence de défense des systèmes d'information (DISA) du département de la défense américain développe des normes de configuration connues sous le nom de guides STIG (Security Technical Implementation Guide) pour aider à maintenir la sécurité de l'infrastructure IT du département de la défense. Ces guides fournissent des conseils techniques pour verrouiller les systèmes d'information et/ou les logiciels susceptibles d'être vulnérables à une attaque. Dell EMC fournit des étapes manuelles et automatisées pour configurer l'appliance VxRail de sorte qu'elle soit conforme aux exigences du guide STIG relatif au réseau d'informations du département de la défense.

IPv6 : IPv6 est le protocole de nouvelle génération utilisé par Internet. En plus de résoudre les limitations d'adressage d'IPv4, IPv6 présente un certain nombre d'avantages en matière de sécurité, et de nombreux environnements l'adoptent. L'appliance VxRail a réussi le test d'interopérabilité USGv6 pour IPv6 en mode double pile, et a atteint la norme la plus élevée pour les tests compatibles IPv6.

Trusted Platform Module : le consortium Trusted Computing Group définit la spécification de Trusted Platform Module (TPM). Les modules TPM 1.2 et 2.0 sont disponibles en option avec l'appliance VxRail. Les deux sont certifiés conformes aux exigences de sécurité FIPS 140-2, TCG et Critères Communs. vSphere prend en charge les modules TPM 1.2 et TPM 2.0.

Le cadre de cybersécurité du NIST et l'appliance VxRail

Le cadre de cybersécurité du NIST (NIST CSF) fournit un cadre de conseils en matière de sécurité informatique pour expliquer comment les organisations du secteur privé peuvent évaluer et améliorer leur capacité à prévenir, détecter et réagir aux cyberattaques. Ce cadre facultatif comprend des normes, des directives et des bonnes pratiques pour gérer les risques liés à la cybersécurité. L'approche hiérarchisée, flexible et économique du cadre de cybersécurité permet de promouvoir la protection et la résilience des infrastructures stratégiques.

La partie « Core » du cadre de cybersécurité du NIST est organisée en cinq « fonctions », qui sont subdivisés en catégories, comme illustré dans la figure 12 ci-dessous.

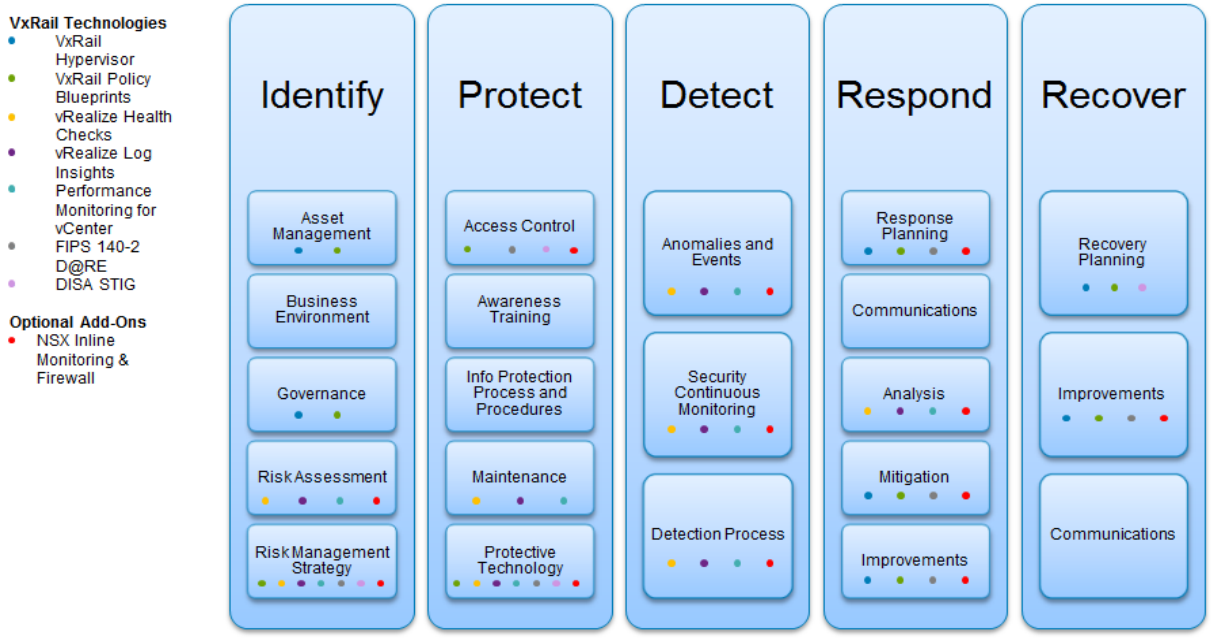

Figure 12 : Cadre de cybersécurité du NIST

Pour en savoir plus sur le cadre de cybersécurité du NIST, rendez-vous sur le site Web du NIST. Pour plus d'informations sur la façon dont l'appliance VxRail s'aligne sur le cadre de cybersécurité du NIST, lisez le document « Fonctionnalités de VxRail prenant en charge le cadre de cybersécurité NIST » disponible ici.

Solutions et partenaires de sécurité VxRail

L'appliance VxRail est conçue avec une sécurité intégrée, et déployée suivant les bonnes pratiques en matière de sécurité. Les utilisateurs bénéficient d'une authentification et d'une autorisation adaptée, offrant le niveau d'accès approprié. Les clusters VxRail sont facilement configurés avec le chiffrement des données au repos pour protéger la confidentialité des informations qu'ils contiennent, le trafic des segments de configuration réseau par défaut et des outils tels que RecoverPoint pour les machines virtuelles, afin de garantir que les applications et les services peuvent être rapidement récupérés si l'intégrité des données est compromise. Ces fonctions de sécurité sont fondamentales et inhérentes à l'appliance VxRail.

Cependant, la protection complète d'un environnement face aux menaces actuelles nécessite une « défense en profondeur » avec plusieurs niveaux de sécurité. Les réseaux qui connectent les applications et les services s'exécutant sur l'appliance VxRail aux utilisateurs qui les consomment doivent être protégés, et les applications et les services eux-mêmes doivent être sécurisés. Les pare-feu, les systèmes de prévention et de détection d'intrusion, les antivirus/protections contre les logiciels malveillants, la protection des points de terminaison, ainsi que les opérations et la gestion de la sécurité font tous partie d'une défense multicouche. Seule Dell Technologies dispose de la gamme de technologies et de services nécessaire pour vous aider à sécuriser pleinement votre environnement.

La taille de votre organisation et ses progrès dans la transformation IT qu'elle a entreprise déterminent l'approche à adopter. Certains environnements peuvent fonctionner dans des cadres de sécurité existants, tandis que d'autres organisations peuvent saisir l'occasion de transformer leurs opérations de sécurité à mesure qu'elles modifient leur infrastructure IT. Les organisations font souvent appel à de nombreux fournisseurs différents dans le cadre de leur programme de sécurité, ce qui complique les choses et accroît ainsi les risques. La famille Dell Technologies inclut RSA et SecureWorks : ces deux gammes de produits vous aident à gérer les risques et à protéger vos ressources multimédia. Seule Dell Technologies peut se poser en fournisseur unique offrant une expertise de sécurité approfondie dans le monde entier, ainsi qu'un écosystème comptant des milliers de partenaires. La figure 13 ci-dessous illustre la puissance de Dell pour la gestion des risques et la protection des données.

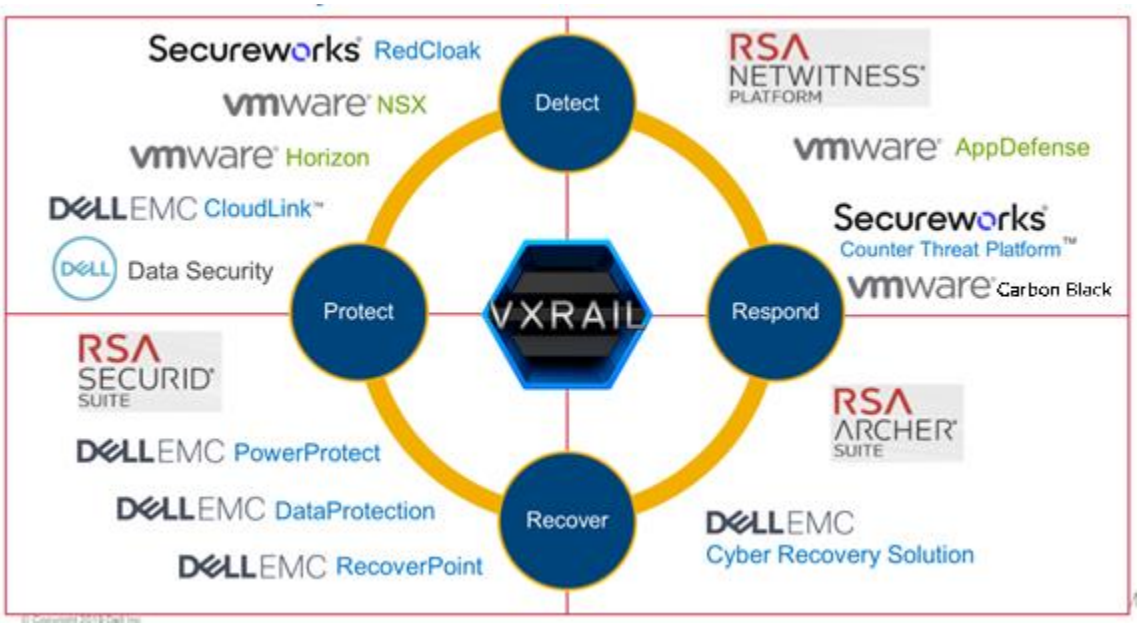

Figure 13 : La puissance de Dell pour vous aider à gérer les risques et à protéger vos données

Gestion des accès et identités

L'appliance VxRail prend en charge les comptes d'utilisateur locaux, l'intégration LDAP et l'authentification unique. Bien qu'il soit possible de disposer d'une appliance VxRail autonome, la plupart des environnements intègreront les systèmes IAM (Identity and Access Management) d'entreprise qui utilisent des services d'annuaire tels que Microsoft Active Directory.

Gestion des incidents et des événements de sécurité

L'appliance VxRail contient l'outil vRealize Log Insight permettant de centraliser la gestion des fichiers journaux pour le système. Pour les organisations qui disposent déjà d'un centre de gestion des fichiers journaux centralisé, tel que Splunk, ou d'un système SIEM (Security Incident and Event Management), l'appliance VxRail peut être facilement intégrée à l'aide de l'interface syslog de référence. La solution RSA NetWitness Suite assure la collecte des journaux et les analyses, et de nombreuses autres fonctions de sécurité qui améliorent les fonctionnalités de sécurité de l'appliance VxRail.

Pour les clients qui ne souhaitent pas gérer eux-mêmes les événements de sécurité, SecureWorks offre des services de gestion des fichiers journaux pour VxRail et pratiquement toutes les ressources d'informations ou les technologies de sécurité critiques. SecureWorks recueille et surveille les informations de sécurité dont vous avez besoin pour assurer la sécurité de votre activité. Plus important encore, les experts en sécurité hautement qualifiés de SecureWorks, basés dans des centres CTOC (Counter Threat Operation Center) intégrés, étudient toute activité malveillante 24/7 et y répondent immédiatement.

Serveur de gestion des clés

Le chiffrement est un outil puissant pour protéger la confidentialité des informations, et l'appliance VxRail possède des fonctionnalités de chiffrement intégrées pour protéger les données en cours d'utilisation, en mouvement et au repos. Toutefois, la sécurité des données fournie par le chiffrement dépend totalement de la génération, de la protection et de la gestion des clés utilisées dans le processus de chiffrement.

Les clés de chiffrement doivent être disponibles lorsqu'elles sont nécessaires, et l'accès aux clés au cours des activités de déchiffrement doit être préservé pendant toute la durée de vie des données. Par conséquent, une bonne gestion des clés de chiffrement est essentielle à l'utilisation efficace du chiffrement. De nombreuses organisations centralisent la gestion des clés à l'échelle de l'entreprise afin de simplifier la gestion, d'appliquer des règles et de fournir des rapports et des audits de conformité.

L'appliance VxRail et vSphere prennent en charge le protocole KMIP (Key Management Interoperability Protocol), ce qui leur permet de fonctionner avec de nombreux systèmes de gestion des clés d'entreprise. La solution Dell EMC CloudLink assure une gestion des clés conforme KMIP, ainsi qu'un chiffrement pour les Clouds publics, privés et hybrides. Pour les organisations qui disposent de services de gestion des clés existants, l'appliance VxRail et vSphere les intègrent facilement, fournissant un point unique de gestion des clés dans l'ensemble de l'entreprise. VMware propose une liste des serveurs de gestion des clés compatibles.

Autres partenaires de sécurité

La sécurisation des infrastructures IT et des ressources multimédia d'aujourd'hui est une entreprise complexe. Une solution unique ne peut offrir une défense suffisamment robuste. C'est pourquoi Dell Technologies propose un écosystème de partenaires qui travaillent ensemble pour résoudre les risques et les failles de sécurité propres à votre environnement. Nous sommes convaincus que l'ensemble du secteur doit travailler de concert pour aider nos clients à atteindre leurs objectifs de cybersécurité.

L'appliance Dell EMC VxRail et VMware vSphere prennent en charge les normes de sécurité ouvertes, et nos partenaires jouent un rôle essentiel dans la transition de nos clients vers un univers IT sécurisé, virtuel et multi-Cloud.

Le livre blanc « Solutions partenaires intégrées à VMware pour la gestion réseau et la sécurité » (lien fourni à l'annexe A) comprend une liste non exhaustive de solutions partenaires pour la gestion réseau, la sécurité et la conformité qui sont intégrées à VMware vSphere®, vCenter™, vShield Endpoint™ et vCloud® Networking and Security™. Il répertorie également l'ensemble des applications et logiciels pris en charge par vSphere. Outre les API EPSEC dédiées à la protection contre les virus/logiciels malveillants fournies par vShield Endpoint, le cadre de l'écosystème VMware vCloud fournit l'insertion de services au niveau vNIC et au niveau de la périphérie virtuelle. Le Guide de compatibilité VMware permet de trouver facilement le composant adapté.

Conclusion

La transformation de la sécurité commence par une infrastructure IT sécurisée. VxRail fournit une infrastructure sécurisée et moderne, du datacenter au Cloud, en passant par la périphérie. En tant qu'infrastructure hyperconvergée, VxRail est conçue, fabriquée, construite et gérée comme un produit unique pour réduire la surface d'attaque possible en réduisant le nombre de composants impliqués dans l'infrastructure. Les bundles composites VxRail de gestion du cycle de vie des logiciels VxRail peuvent inclure des mises à jour du BIOS, du firmware, de l'hyperviseur, de vSphere ou de l'un des composants de gestion inclus, ce qui simplifie considérablement la mise à jour de la pile logicielle complète et réduit le degré de vulnérabilité aux attaques.

La protection complète d'un environnement face aux menaces actuelles nécessite une « défense en profondeur » avec plusieurs niveaux de sécurité. Les réseaux qui connectent les applications et les services s'exécutant sur l'appliance VxRail aux utilisateurs qui les consomment doivent être protégés, et les applications et les services eux-mêmes doivent être sécurisés. Les pare-feu, les systèmes de prévention et de détection d'intrusion, les antivirus/protections contre les logiciels malveillants, la protection des points de terminaison, ainsi que les opérations et la gestion de la sécurité font tous partie d'une défense multicouche.

Dell Technologies comprend la sécurité et dispose d'experts dans le monde entier qui peuvent vous aider à évaluer votre environnement et à concevoir un plan de sécurité pour répondre à vos besoins spécifiques. Pour en savoir plus, contactez votre représentant Dell Technologies.

Annexe A : Références

Tous les liens et références cités dans ce livre blanc sont affichés ci-dessous.

Ressource	URL
Risk Based Security :	https://www.riskbasedsecurity.com/2019/02/13/over-6500-data-breaches-and-more-than-5-billion-records-exposed-in-2018/
Sécurité des produits EMC :	https://www.dellemc.com/fr-fr/products/security/index.htm
Le cycle du développement de la sécurité Dell EMC :	https://www.dellemc.com/fr-fr/products/security/index.htm#tab0=2
Équipe PSIRT (Product Security Incident Response Team) de Dell :	https://www.dell.com/support/contents/fr/fr/19/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy
Sécurité cyber-résiliente dans les serveurs Dell EMC PowerEdge de 14e génération :	http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download
AppDefense :	https://www.vmware.com/products/appdefense.html
Guide de l'architecture VMware Cloud Foundation sur VxRail :	https://www.dellemc.com/resources/fr-fr/asset/technical-guides-support-information/products/converged-infrastructure/vmware_cloud_foundation_on_vxrail_architecture_guide.pdf
Sécurité des produits VMware :	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf
Guide de réseau Dell EMC VxRail :	https://www.dellemc.com/resources/fr-fr/asset/technical-guides-support-information/products/converged-infrastructure/h15300-VxRail-network-guide.pdf
Guide d'utilisation de SpoofGuard VMware :	https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-06047822-8572-4711-8401-BE16C274EFD3.html
Documentation de VMware NSX :	https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-B5C70003-8194-4EC3-AB36-54C848508818.html
Sécurité pour les solutions hyperconvergées :	https://communities.vmware.com/servlet/JiveServlet/download/36084-3-183512/Security for Hyper-Converged Solutions_NSX.pdf
Rapport sur la sécurité mondiale de 2019 de Trustwave :	https://www.trustwave.com/Resources/Library/Documents/2019-Trustwave-Global-Security-Report/
*1 Rapport d'enquête sur les violations de données établi en 2017.	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
*2 Enquête PWC « 20th CEO Survey » réalisée auprès de 5 351 membres du public, dans 22 pays.	https://www.pwc.com/jg/en/publications/pwc-ceo-report-2017%20(2).pdf
Cadre de cybersécurité du NIST :	https://www.nist.gov/cyberframework
Liste des serveurs de gestion des clés compatibles :	https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details=1&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc
Solutions de partenaires intégrées à VMware pour la gestion réseau et la sécurité :	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vcns/vmware-integrated-partner-solutions-networking-security.pdf

Guide de compatibilité avec VMware :	https://www.vmware.com/resources/compatibility/search.php
TechBook sur VxRail :	https://france.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf
Fonctions de sécurité du contrôleur Dell iDRAC (Integrated Dell Remote Access Controller) :	http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download
Documentation sur vSAN :	https://docs.vmware.com/en/VMware-vSAN/index.html
Quatre transformations d'entreprise :	https://www.youtube.com/watch?v=TcKJ39_4Rwc
Certifications de chiffrement VMware :	https://www.vmware.com/security/certifications/fips.html
VMware vRealize Log Insight :	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vrealize-log-insight/vrealize-log-insight-datasheet.pdf
Certifications du NIST pour la recherche FIPS 140-2 par fournisseur pour Dell EMC et VMware :	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
Cycle du développement sécurisé VMware :	https://www.vmware.com/security/sdl.html
Gestion des clés VMware :	https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-toplogy-basics-vm-vsan-encryption.html
Guide de sécurité de vSphere 6.5 :	https://docs.vmware.com/fr/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-security-guide.pdf
Une confiance renforcée avec les programmes de sécurité des produits DELL EMC :	https://france.emc.com/products/security/index.htm
	Ressources ACE
Vidéo de démo de la plate-forme ACE	https://vxrail.is/acedemo
Vidéo de démo par étapes des bundles de mise à jour intelligents	https://vxrail.is/aceupdates
Présentation de solution	https://www.dellemc.com/resources/fr-fr/asset/offering-overview-documents/products/converged-infrastructure/vxrail-ace-solution-brief.pdf
Présentation de Dell Technologies MyService360	https://www.delltechnologies.com/en-us/services/support-deployment-technologies/my-service-360.htm
VxRail - Une sécurité complète dès la conception (livre blanc)	https://www.dellemc.com/resources/fr-fr/asset/white-papers/products/converged-infrastructure/VxRail_Comprehensive_Security_by_Design.pdf
Pratiques de sécurité des produits Dell Technologies	https://www.delltechnologies.com/fr-fr/products/security/index.htm
	YouTube - Ressources sur la sécurité
Youtube - Présentation de la sécurité de VxRail	https://www.youtube.com/watch?v=ZTNmYBgJv4s
YouTube - Renforcement de la sécurité et conformité de VxRail	https://www.youtube.com/watch?v=ZjhfCE5nq6U