Plateforme Cisco Intersight et sécurité

Une gestion sécurisée des logiciels en tant que service (SaaS)

Une gestion sécurisée et fiable

Si votre infrastructure informatique se trouve dans un centre de données d'entreprise, à la périphérie du réseau et dans des bureaux distants et des succursales, vous constaterez que la gestion des différents outils utilisés dans chaque emplacement est complexe. La plateforme Cisco Intersight™ unifie et simplifie la gestion de vos serveurs Cisco Unified Computing System™ (Cisco UCS®) et des systèmes Cisco HyperFlex™. Que vous accédiez au logiciel Intersight à partir d'un portail de SaaS en nuage ou d'un appareil que vous hébergez dans votre centre de données, nous facilitons le déploiement, l'exploitation et la gestion sécurisés de vos technologies de l'information.

Table des matières

Plateforme Cisco Intersight

La plateforme de logiciel en tant que service (SaaS) Cisco Intersight vous permet de transformer vos intentions et ce que vous souhaitez accomplir en configuration d'infrastructures, en gestion continue et en optimisation proactive. Grâce à cette solution infonuagique nécessitant un abonnement, vous n'avez qu'à revendiquer vos serveurs, vos infrastructures hyperconvergentes et vos interconnexions de trame dans l'interface utilisateur; à obtenir une autorisation de service; à regrouper vos ressources de façon logique (comme dans des bureaux distants, des succursales ou des grappes de virtualisation); et à utiliser des interfaces fondées sur les rôles et les politiques, afin de configurer et de gérer vos ressources où qu'elles se trouvent.

Sécurité intégrée

La plateforme Cisco Intersight utilise une architecture de sécurité multicouche qui repose sur les technologies de sécurité selon les normes de l'industrie. Elle chiffre également les données, en plus de respecter les normes de sécurité et de traitement des données strictes de Cisco, et de gérer séparément la gestion et la production informatique du trafic réseau pour une isolation supplémentaire. Par conséquent, votre plateforme de gestion de systèmes infonuagiques vous offre assurément la sécurité renforcée dont vous avez besoin.

Un environnement de gestion en évolution

Les outils conventionnels de gestion d'infrastructures informatiques se servent de produits isolés et de plusieurs gestionnaires d'éléments. Grâce à Cisco UCS, les infrastructures informatiques et la méthode de gestion des systèmes ont connu un nouvel essor. Cisco UCS simplifie et automatise l'informatique en combinant des infrastructures convergées et une gestion intégrée fondée sur des modèles, ce qui facilite les opérations quotidiennes et en optimise l'efficacité. Grâce aux logiciels en tant que service (SaaS) et aux appareils de gestion virtuelle Cisco sur site de Cisco Intersight, nous avons franchi l'étape nous permettant d'étendre notre cadre de gestion aux systèmes Cisco UCS et Cisco HyperFlex, peu importe où ils se trouvent.

Présentation de Cisco Intersight

Que vous utilisiez le portail en nuage ou un appareil local, Cisco Intersight combine les avantages de la gestion en nuage avec une sécurité semblable à celle des systèmes sur site. Cette plateforme de gestion et d'automatisation est renforcée par des techniques d'analyse et d'apprentissage automatique qui font croître votre efficacité et vous permettent de maintenir une évolution constante. Ainsi, vous pouvez gérer votre infrastructure informatique, malgré sa complexité croissante.

Le logiciel surveille l'état des éléments d'infrastructures qui utilisent la gestion Cisco UCS ou HyperFlex et leurs relations entre eux. Les informations de télémétrie et de configuration sont recueillies et conservées conformément aux exigences de sécurité de l'information de Cisco. Vos données sont isolées, puis affichées sur une interface utilisateur intuitive. Étant donné que le logiciel évolue rapidement et que des mises à jour sont fréquemment effectuées sans entraîner de conséquences, cette approche de gestion des infrastructures simplifiée et cohérente permet d'éliminer les difficultés liées à la prise en charge des outils et des appareils courants (voir l'illustration 1).

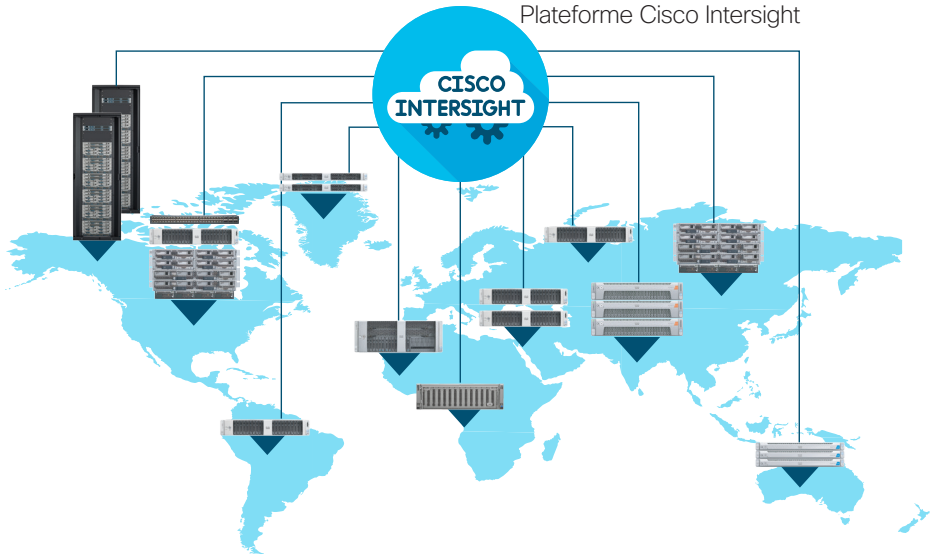

Figure 1. Cisco Intersight simplifie la gestion des infrastructures, peu importe où vos ressources informatiques se trouvent

« Les clients s'attendent à être constamment en mesure de surveiller les charges de travail, d'optimiser les performances et d'orchestrer le fonctionnement des infrastructures à l'aide de solutions de gestion intégrées et propulsées par l'API, qui sont prises en charge par des interfaces utilisateur graphiques personnalisables et des analyses d'activités informatiques basées sur le traitement massif de données. »

IDC : Worldwide Cloud Systems Management Software Forecast, 2017-2021, février 2017, no US41374417.

L'importance de la sécurité

Votre entreprise doit faire face à un contexte de cybersécurité en constante évolution dans lequel les attaques sont de plus en plus sophistiquées et fréquentes. Déjà à l'étape de conception de la plateforme Cisco Intersight, nous savions que la sécurité était d'une importance cruciale. Nous avons donc créé une plateforme de gestion SaaS en nuage qui offre la sécurité renforcée dont vous avez besoin. Certaines entreprises préfèrent toutefois héberger un serveur de gestion local, donc nous offrons également l'appareil virtuel Cisco Intersight qui fournit les mêmes services. Ces deux produits sont des SaaS qui sont mis à jour grâce à notre processus d'intégration continue.

Plateforme Cisco Intersight et sécurité

Le développement, l'intégration et la vérification de la plateforme Intersight sont effectués en fonction des directives relatives aux cycles de développement Cisco Secure. Cette pratique de développement et de déploiement de produits sécurisés comporte plusieurs éléments, dont les pratiques de conception et de développement inhérentes, les tests de mise en œuvre et les formulations d'ensembles de recommandations en matière de déploiement avec une sécurité maximale. Les processus de développement de Cisco sont certifiés ISO 27001. De plus, la certification propre au développement d'Intersight est actuellement en examen.

Une protection intégrée assure ainsi la sécurité des appareils, des systèmes, des infrastructures et des services. La plateforme Cisco Intersight utilise une architecture de sécurité multicouche et repose sur les mêmes technologies de sécurité qui sont utilisées largement dans le commerce Internet et qui respectent les normes de l'industrie. Elle chiffre également les données, en plus de respecter les normes strictes en matière de sécurité et de traitement des données de Cisco, et de gérer séparément la gestion et la production informatique du trafic réseau pour fournir une isolation supplémentaire.

Authentification unique (SSO)

L'authentification unique (SSO) vous permet d'utiliser un ensemble unique d'identifiants pour vous connecter à plusieurs applications. Grâce à cette méthode, vous pouvez vous connecter à Intersight en utilisant vos identifiants d'entreprise au lieu de vos identifiants Cisco. Intersight prend en charge l'authentification unique par le biais de SAML 2.0, agit en tant que fournisseur de services (SP), et permet l'intégration des fournisseurs d'identité (IdP) pour l'authentification SSO.

Authentification de l'utilisateur et contrôle d'accès fondé sur les rôles

Les comptes Intersight constituent le domaine d'authentification des utilisateurs. Les comptes contrôlent tous les accès aux ressources, et les utilisateurs authentifiés ne peuvent voir les données que dans les comptes pour lesquels ils sont autorisés. Sur la plateforme SaaS, les identifiants de connexion Cisco peuvent être utilisés pour l'authentification avec le fournisseur d'identité sur la page Cisco.com qui comprend la prise en charge de l'authentification multifactorielle. La mise en œuvre de SaaS et d'Intersight sur site permet l'intégration des systèmes de gestion d'identités externes dans le but de répondre aux exigences d'authentification des clients actuels.

La structure Cisco Intersight utilise un contrôle d'accès granulaire et des privilèges gérés par des ressources. Le logiciel Intersight permet de configurer les utilisateurs et les groupes en fonction de plusieurs rôles, et chaque utilisateur ou groupe peut occuper plusieurs rôles. Les rôles tenus obtiennent les privilèges suivants :

- **Administrateur de compte :** capacité à gérer et à contrôler entièrement le compte Cisco Intersight et les appareils dans le cadre de ce compte
- **Lecture seule :** visibilité en lecture seule des ressources dans le cadre d'un compte
- **Technicien d'appareils :** actions administratives en lien avec les appareils, dont la revendication d'un appareil à un compte Cisco Intersight
- **Administrateur d'appareils :** actions administratives en lien avec les appareils, dont la suppression d'un appareil à un compte Cisco Intersight
- **Administrateur de grappes HyperFlex :** gestion du cycle de vie des grappes et de la politique HyperFlex
- **Administrateur de serveurs :** gestion du cycle de vie du serveur et des politiques
- **Administrateur d'accès utilisateur :** configuration d'utilisateurs, de groupes et de fournisseurs d'identité

Veuillez consulter les pages d'aide Intersight pour obtenir des détails sur les rôles de gestion et les ressources.

Connexion d'appareils

Les systèmes Cisco UCS et HyperFlex sont connectés à la plateforme Intersight SaaS ou aux appareils virtuels sur site, grâce à un connecteur d'appareils qui est intégré au contrôleur de gestion de chaque système

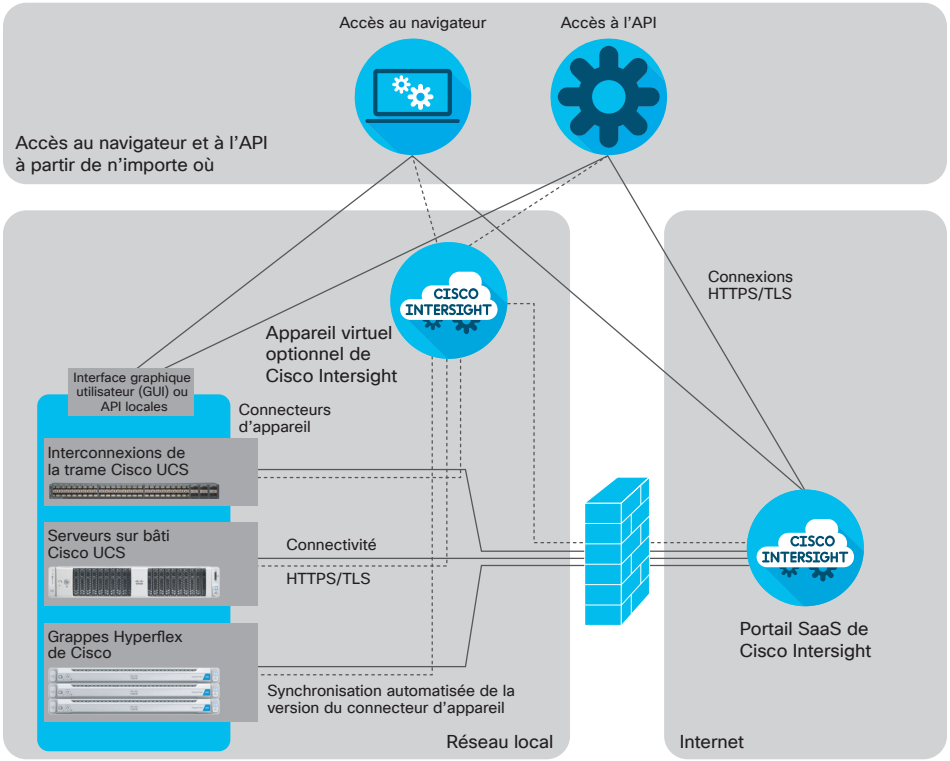

Figure 2. La plateforme Intersight sépare le trafic entre les utilisateurs et les appareils et communique à l'aide des protocoles HTTPS et TLS standard de l'industrie.

Infrastructure du portail

La gestion Intersight est accessible sur un portail en nuage. Le personnel de Cisco est disponible 24 h sur 24, 7 jours sur 7, pour offrir de l'assistance en ce qui concerne la sécurité logistique, les opérations et la gestion du changement. Tous les services sont reproduits dans de nombreux centres de données indépendants afin que les services aux utilisateurs basculent rapidement en cas de défaillance du centre de données.

Fiabilité et accessibilité du centre de données

- Procédures de signalisation progressive rapide entre plusieurs équipes opérationnelles
- Système indépendant d'alerte en cas de panne
- Reproduction de toutes les données (y compris les mesures et les configurations d'appareils) dans les centres de données
- Reproduction en temps réel des données entre les centres de données
- Basculement rapide des services Intersight en cas de défaillance matérielle ou d'un autre type de pannes dans le centre de données
- Conservation des fonctions du réseau de l'utilisateur final, et ce, même si la connectivité du portail est interrompue, grâce à une architecture hors bande
- Vérification fréquente des procédures de basculement

Architecture hors bande sécurisée

- Aucune interruption de votre réseau de production ou de gestion informatique, même si la connexion est interrompue
- Stockage des données du réseau de gestion seulement
- Chiffrement des données sensibles lorsqu'elles sont stockées
- Tests d'intrusion fréquents des centres de données

Certification et conformité du centre de données

- Communiquez avec l'équipe de sécurité et de confidentialité des données de Cisco Intersight pour en savoir plus au sujet des rapports de conformité et des certifications au sein des centres de données.

(voir l'illustration 2). Le connecteur de périphérique prend en charge une connexion chiffrée permettant aux appareils d'envoyer des informations et de recevoir des instructions de contrôle envoyées par la plateforme Intersight.

Chiffrement de données et connexions sécurisées

Toutes les données échangées entre des appareils et la plateforme Intersight adhèrent à des protocoles de chiffrement et de sécurité conformes aux normes du secteur. Les appareils connectés utilisent le protocole de sécurité de la couche de transport (TLS) avec chiffrement restreint et HTTPS sur le port standard 443 HTTPS. Toutes les données envoyées à Intersight sont chiffrées au moyen du Standard de cryptage avancé (AES) et d'une clé de 256 bits générée au hasard et distribuée avec un mécanisme de clé publique. De plus, chaque connexion d'appareil au portail est authentifiée par un jeton cryptographique permettant uniquement aux appareils légitimes d'être gérés, ce qui élimine les risques de différents vecteurs d'attaques d'un cheval de Troie.

Toutes les connexions sont établies à partir de l'appareil. Ainsi, les pare-feu peuvent bloquer toutes les demandes de connexion entrantes, et seul le port 443 HTTPS doit être activé pour permettre les connexions sortantes. Par conséquent, les pare-feu ne nécessitent aucune autre configuration particulière pour activer la connectivité Intersight. Les périphériques peuvent être configurés pour que les serveurs mandataires HTTPS soient utilisés et qu'une couche de sécurité supplémentaire soit ajoutée au moyen de la non-direction.

Afin d'assurer la sécurité des connexions et de prévenir les attaques d'intercepteurs, les appareils Cisco UCS et Cisco HyperFlex qui se connectent directement à la plateforme Intersight utilisent une URL HTTPS à destination unique. La plateforme fournit un certificat signé par une autorité de certification (CA). Cependant, si un certificat n'est pas signé, les appareils ne pourront pas se connecter au portail. Le logiciel Intersight et le connecteur d'appareil créent un cadre de gestion sécurisé qui fournit des renseignements en temps réel liés à la sécurité des appareils. Cette approche permet également aux appareils connectés et au logiciel Intersight de synchroniser les dernières mises à jour de sécurité en matière de connexion.

Revendication sécurisée des appareils grâce à l'authentification à deux facteurs

Pour surveiller et gérer les appareils avec la plateforme Intersight, ces appareils doivent d'abord être revendiqués à partir d'un compte Intersight. Vous devez accéder au portail SaaS ou au portail d'appareils virtuels pour revendiquer des appareils à partir d'un navigateur, puis cliquer sur l'onglet **Revendiquer les appareils**. Les identifiants d'appareils et les codes de revendication, tous deux uniques à chaque appareil, sont extraits de l'appareil. Vous pouvez trouver l'identifiant et le code dans l'interface de gestion locale de l'appareil. Le code de revendication est actualisé toutes les dix minutes à titre de protection supplémentaire, ce qui permet de confirmer que l'administrateur qui revendique l'appareil y a un accès physique.

« Notre objectif est d'être dignes de confiance, transparents et responsables. Cela signifie que nous ne devons rien négliger dans nos recherches contre les menaces qui pourraient s'en prendre à nos infrastructures ou nos données. »

Michele Guel, ingénieure et architecte en chef de renom dans le domaine de la sécurité, Cisco

L'authentification à deux facteurs est utilisée pour vérifier l'identité et l'authenticité de chaque appareil revendiqué. Ce mécanisme d'authentification ajoute une protection supplémentaire au processus de revendication d'un appareil. Il nécessite un accès à l'appareil et à ses données d'identification qui sont validées dans votre compte Intersight. Dans le cas où un utilisateur non autorisé devine ou découvre les données d'identification de l'appareil, il ne peut pas le revendiquer sans y avoir un accès physique.

Le processus de revendication d'un appareil permet à un utilisateur de configurer un appareil en lecture seule ou avec autorisation de contrôle, à partir de la plateforme Intersight. Les appareils configurés en lecture seule ne peuvent pas être modifiés au moyen du logiciel Intersight, quels que soient les privilèges de l'utilisateur du compte Intersight. Il est également possible que des appareils ne soient pas revendiqués ou qu'ils soient retirés d'un compte Cisco Intersight à partir du portail.

Respect des normes de sécurité de l'industrie

La plateforme Intersight répond aux exigences d'InfoSec qui sont conformes à de nombreuses normes du secteur et les surpasse même :

- **Normes FIPS 140-2 :** Intersight utilise des modules cryptographiques conformes à la norme FIPS 140-2. Les certifications font l'objet d'une planification.

L'architecture de gestion hors bande de la plateforme la rend hors de portée pour certaines normes/vérifications :

- **Norme PCIDSS (Payment Card Industry Data Security Standard) :** le trafic des clients (y compris les données des titulaires de cartes) ne circule pas par la plateforme Intersight.
- **Loi HIPAA (Health Insurance Portability and Accountability Act) :** aucune information sur la santé identifiable individuellement sur le réseau n'est envoyée au portail Intersight.

Collecte de données et chiffrement pendant le stockage

La plateforme Intersight, tout comme l'accès local aux API, offre une visibilité et un contrôle complets sur les systèmes gérés. Les données recueillies à partir de connecteurs d'appareils de systèmes gérés peuvent comprendre les éléments suivants :

- **Données d'inventaire et de configuration** pour les interconnexions de la trame et pour tous les serveurs et les nœuds, dont les contrôleurs de stockage, les adaptateurs réseau, les modules d'E/S et les CPU.
- **Données opérationnelles du serveur** (par exemple, les défaillances) qui, en étant utilisées sur la plateforme Intersight, fournissent des recommandations automatisées.
- **Fichiers d'assistance technique** pouvant être créés à la demande du Centre d'assistance technique de Cisco (Cisco TAC).

Veuillez noter que les connecteurs d'appareils ne recueillent pas les données sensibles qui peuvent être conservées au sein des systèmes connectés, comme les mots de passe.

Si vous utilisez l'appareil virtuel Cisco Intersight, vous pouvez choisir de transmettre ou non les données présentées ci-dessus dans le portail en nuage. Si vous désactivez la collecte de données supplémentaires, les renseignements ci-dessus seront conservés localement. Veuillez consulter les pages d'aide Intersight pour obtenir de plus amples renseignements sur les données recueillies par l'appareil virtuel Cisco Intersight sur site.

Pour toutes les données recueillies, les pratiques de sécurité supplémentaires suivantes sont mises en œuvre :

- **Les données d'un client** sont séparées des autres données de clients grâce à la ségrégation virtuelle des données. Les demandes de données des services Cisco Intersight renvoient uniquement des données propres au compte d'un client. Les clés de chiffrement par client sont utilisées pour y donner accès.
- **Les données persistantes à long terme** sont chiffrées pendant le stockage. Le stockage en bloc ou le chiffrement à volume similaire est activé pour toutes les données et tous les fichiers détenteurs.
- **L'accès de tiers** aux données n'est pas autorisé.

Respect des normes de sécurité et de traitement des données de Cisco

La protection des infrastructures et des données nécessite un partenariat étroit entre les services informatiques et les services de sécurité de l'information (InfoSec) de Cisco. Faisant partie de l'Organisme de la confiance et de la sécurité (STO) de Cisco, InfoSec collabore avec le service informatique de Cisco pour assurer la sécurité des produits que nous concevons et des infrastructures que nous exploitons. Ces services travaillent de pair pour soutenir la productivité au sein des entreprises tout en protégeant nos systèmes et nos données contre les menaces internes et externes. Au lieu de nous concentrer uniquement sur le matériel et les logiciels de sécurité, nous adoptons une approche holistique et généralisée de la sécurité en :

- développant, intégrant et vérifiant Intersight à l'aide des lignes directrices du cycle de développement Cisco Secure;
- intégrant plusieurs éléments de développement et de déploiement de produits dans notre méthodologie, dont les pratiques de conception et de développement inhérentes, les tests de mise en œuvre, et enfin, les formulations d'ensembles de recommandations en matière de déploiement pour optimiser la sécurité du système;
- favorisant une culture soucieuse de la sécurité dans le but de réduire la surface d'attaque et d'offrir une posture de sécurité robuste;
- mettant en œuvre des politiques et des processus axés sur la sécurité;
- intégrant la sécurité dans l'ensemble de nos infrastructures.

Parallèlement à l'importance que nous accordons aux personnes et aux processus, nous adoptons des politiques axées sur la sécurité pour les éléments suivants :

- **Gestion des accès :** nous respectons les exigences relatives à la gestion de l'accès des utilisateurs et des administrateurs aux ressources et aux systèmes d'information, grâce à des mesures de contrôle appropriées pour l'authentification, l'autorisation et la vérification.

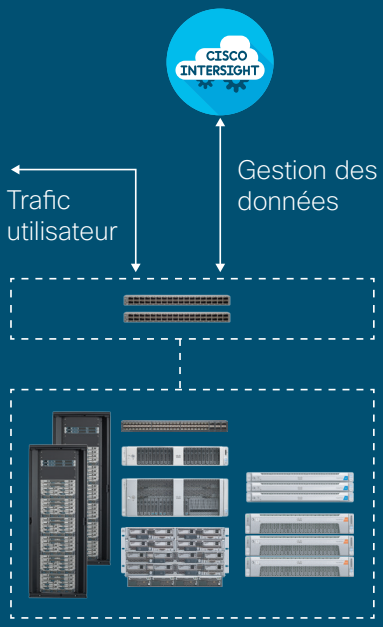

Figure 4. Séparation du trafic

- **Vérification et évaluation des risques :** nous respectons les politiques de sécurité et d'intégrité des données, en plus d'enquêter sur les incidents et de surveiller les activités des utilisateurs et des systèmes, le cas échéant.
- **Sécurité du nuage :** le service est basé sur le nuage et les services que nous utilisons doivent respecter nos exigences en matière de sécurité.
- **Contrôles cryptographiques :** nous utilisons des contrôles cryptographiques pour protéger la confidentialité, l'intégrité et la disponibilité des ressources d'information.
- **Protection des données :** nous formulons des exigences en matière de classification, d'étiquetage et de protection des données. Ces politiques définissent la sensibilité relative des renseignements, en plus de déterminer la façon dont ces renseignements sont traités et divulgués aux employés de Cisco et à des tiers.
- **Sécurité de l'information :** nous adhérons à des politiques dans lesquelles la confidentialité, l'intégrité et la disponibilité des ressources d'information sont précisées.
- **Accès au réseau :** nous déterminons les utilisateurs et les appareils autorisés à accéder à nos réseaux.

Séparation du réseau de gestion

Le plan de commande hors bande de la plateforme Intersight sépare les données de gestion des données informatiques de production et d'application (voir l'illustration 4). Les données de gestion, comme la configuration et les informations et les statistiques de surveillance, circulent à partir des appareils vers le portail Intersight (voir l'illustration 3). Les données de production et d'application des TI sont envoyées directement sur votre réseau de données de production pour atteindre leur destination.

En utilisant une architecture hors bande, les utilisateurs ne sont pas touchés lorsque les appareils sont incapables de communiquer avec le logiciel Intersight en raison de perturbations Internet ou de perturbations liées à d'autres services. Les utilisateurs peuvent toujours accéder aux réseaux locaux de gestion et de production. De plus, toutes les politiques et tous les paramètres de Cisco UCS et Cisco HyperFlex continuent d'être respectés. En outre, les mesures d'authentification locale de l'utilisateur restent inchangées, et les outils locaux de configuration comme Cisco UCS Manager demeurent accessibles.

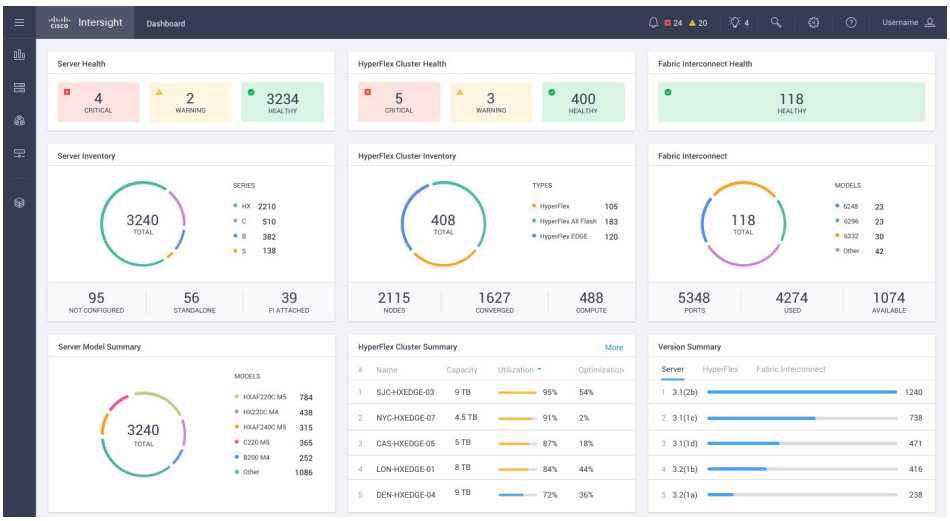

Figure 3. Tableau de bord Cisco Intersight

Pour en apprendre davantage

Pour en savoir plus sur la plateforme Cisco Intersight, rendez-vous à l'adresse http://www.cisco.com/go/intersight

Pour en savoir plus sur l'approche de Cisco en matière de sécurité opérationnelle, rendez-vous à l'adresse http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/cs-sec-03232016-operational-security.html

Pour en savoir plus sur la solution Cisco UCS, rendez-vous à l'adresse http://www.cisco.com/go/ucs

Pour en savoir plus sur les systèmes Cisco HyperFlex, rendez-vous à l'adresse http://www.cisco.com/go/hyperflex

Avantages en matière de sécurité

L'approche de gestion de la plateforme Cisco Intersight offre de nombreux avantages en matière de sécurité lorsqu'on la compare aux outils de surveillance et de gestion classiques :

- **Efficacité :** la plateforme Intersight s'occupe de la gestion au sein de la plateforme, ce qui permet aux experts en informatique de se concentrer sur d'autres tâches et priorités.
- **Connectivité des appareils :** les appareils gérés par Intersight se connectent automatiquement et indiquent l'état de leur configuration et de leur fonctionnement, y compris celui de leurs versions de micrologiciels et de logiciels.
- **Autonomie :** une fois que la connexion initiale est établie, aucune interaction humaine n'est requise sur l'appareil. Aucun agent ni autre logiciel ne doit être installé ou entretenu.
- **Synchronisation :** grâce aux connecteurs d'appareil qui se mettent à jour automatiquement, chaque appareil se synchronise automatiquement sur la plateforme Intersight. Au besoin, les correctifs et les mises à jour de sécurité peuvent être transmis au connecteur de l'appareil, sans intervention requise par l'utilisateur.
- **Analyse :** en fonction des données recueillies automatiquement, Cisco Intersight émet des recommandations pour les mises à jour de l'infrastructure qui sont nécessaires pour assurer la conformité de votre matériel, de vos micrologiciels et de vos logiciels aux dernières combinaisons testées de Cisco.
- **Simplicité :** Cisco Intersight offre un emplacement unique pour le suivi et la production de rapports sur la sécurité et la conformité des terminaux.

Offrir des avantages en matière de sécurité

L'approche de gestion SaaS de la plateforme Cisco Intersight offre de nombreux avantages en matière de sécurité lorsqu'on la compare aux outils locaux de surveillance et de gestion basés sur l'agent :

- **Efficacité :** le portail Cisco Intersight s'occupe de la gestion au sein de la plateforme, ce qui permet aux experts en informatique de se concentrer sur d'autres tâches et priorités.
- **Connectivité des appareils :** les appareils gérés par Cisco Intersight se connectent automatiquement et indiquent l'état de leur configuration et de leur fonctionnement, y compris celui de leurs versions de micrologiciels et de logiciels.
- **Autonomie :** une fois que la connexion initiale est établie, aucune interaction n'est requise par l'utilisateur sur l'appareil. Aucun agent ni autre logiciel ne doit être installé ou entretenu.
- **Synchronisation :** grâce aux connecteurs d'appareil qui se mettent à jour automatiquement, chaque appareil se synchronise automatiquement avec Cisco Intersight. Au besoin, les correctifs et les mises à jour de sécurité peuvent être transmis au connecteur de l'appareil, sans intervention requise de l'utilisateur.
- **Analyse :** en fonction des données recueillies automatiquement, Cisco Intersight émet des recommandations pour les mises à jour de l'infrastructure qui sont nécessaires pour assurer la conformité de votre matériel, de vos micrologiciels et de vos logiciels aux dernières combinaisons testées de Cisco.
- **Simplicité :** Cisco Intersight offre un emplacement unique pour le suivi et la production de rapports sur la sécurité et la conformité des terminaux.

LE-63304-01 19/04