Quelles sont les nouveautés de Cisco Secure Workload, version 3.8.1.1

Première publication : 2023-05-19

Nouveaux logiciels, nouveau matériel et fonctionnalités obsolètes

Nouvelles fonctionnalités logicielles

Nom de la caractéristique	Description
Facilité d'utilisation	
Amélioration de l'expérience d'accueil des nouveaux utilisateurs	L'expérience d'accueil est améliorée de bout en bout, de l'accueil à l'installation des agents logiciels à l'aide de la méthode du script ou de l'image d'installation.
Automatisation de la migration	La migration des configurations d'un détenteur à l'autre est désormais entièrement automatisée pour mettre en place des appliances virtuelles et des connecteurs.
Connecteur sécurisé	La page du connecteur sécurisé est améliorée pour afficher les mesures lorsque le protocole de ligne d'une interface de tunnel est en panne ou reprend son activité, ainsi que les journaux d'événements, ce qui offre une meilleure visibilité sur la stabilité des tunnels.
Automatisation de la migration des agents	Vous pouvez désormais utiliser la fonction de relocalisation pour déplacer des agents logiciels d'un site à un logiciel-service ou inversement.
Rapports sur l'utilisation des politiques et conformité	Vous pouvez désormais utiliser le nombre d'occurrences de la politique comme indicateur afin de : • Déterminer les polices non utilisées durant une période donnée. • Renvoyer le nombre d'occurrences pour une politique donnée dans un intervalle de temps donné, y compris le premier et le dernier comptage.
Gestion des étiquettes : Mappage étiquette-Adresse IP	Pour chaque usage d'étiquette, vous pouvez maintenant ajouter la correspondance étiquette-Adresse IP en plus d'ajouter la clé d'étiquette, le filtre d'étiquette et l'espace de travail de filtre.

Nom de la caractéristique	Description
Filtrage du trafic et analyse des politiques par type de source de flux	Vous pouvez désormais utiliser le type de capteur afin de filtrer par source de flux et la recherche de flux.
Exportation ADM	Grâce à la nouvelle fonctionnalité ADM, vous pouvez désormais télécharger une image haute résolution de la vue graphique des politiques.
Opérations du jour 2	
Licences Smart	Cisco Smart Licensing, un système unifié de gestion des licences qui gère les licences logicielles des produits Cisco, est désormais disponible pour enregistrer les grappes Cisco Secure Workload, rendre compte de l'utilisation des licences et suivre la conformité de la grappe Cisco Secure Workload sur site. Vous pouvez également synchroniser les licences intelligentes manuellement ou en planifiant la synchronisation à l'aide du Smart Software Manager sur site grâce au Smart Software Manager Portal.
Amélioration des alertes	Vous pouvez désormais configurer la gravité et le seuil d'alerte lors de la configuration de l'orchestrateur externe. Vous pouvez également afficher l'alerte générée lorsqu'un orchestrateur externe cesse de fonctionner ou en raison d'un échec de connexion à partir du connecteur respectif à Cisco Secure Workload. Pour plus de renseignements sur l'activation et l'affichage des alertes sur l'orchestrateur externe, consultez la section *External Orchestrators* (Orchestrateurs externes) dans le guide de l'utilisateur Cisco Secure Workload.
Générer une alerte de test	À des fins d'examen ou de test, utilisez le bouton Generate Test Alerts (Générer des alertes de test) pour vérifier la connectivité avec n'importe quel éditeur. Lors de la configuration des alertes, vous pouvez également configurer l'exemple d'alerte pour envoyer des alertes basées sur le type d'alerte et l'éditeur associé. Pour plus de renseignements sur la manière de générer une alerte de test, consultez *Generate a Test Alert* (Générer une alerte de test) à la section Alertes dans le guide de l'utilisateur Cisco Secure Workload.
Capacités de production de rapports	Un tableau de bord de création de rapports a été introduit, conçu pour les cadres, les administrateurs de réseau et les analystes de la sécurité. Ce tableau de bord offre des représentations visuelles de l'état critique du flux de travail, des capacités de dépannage et des fonctionnalités de création de rapports.
Amélioration de l'interface utilisateur du cadre MITRE ATT&CK	Le tableau de bord de création de rapports comprend une nouvelle présentation de la fiche Résumé de la sécurité qui correspond à la présentation de la fiche ATT&CK de MITRE. La représentation comprend les tactiques et leur décompte.

Nom de la caractéristique	Description
Extension de la mise en mémoire tampon de la télémétrie sur l'agent hôte	Les agents logiciels offrent désormais une mise en mémoire tampon portée de la télémétrie réseau sur l'hôte. La fonction peut être configurée au moyen du *Flow Disk Quota* (Quota de disque de flux) ou de la *Flow Time Window* (Fenêtre de durée du flux) dans le profil de configuration de l'agent.
Protection par mot de passe de l'agent logiciel (Windows) pour la désactivation et la désinstallation	L'agent logiciel sous Windows peut désormais être protégé contre l'arrêt/la désactivation du service et la désinstallation. Cette fonction peut être activée en utilisant la configuration de la protection du service dans la page Profil de configuration de l'agent.
Désinstallation des agents signalés à la grappe Cisco Secure Workload	Lorsque vous désinstallez un agent, vous transmettez ce renseignement à la grappe qui, à son tour, l'utilise pour mettre à jour la page de l'agent logiciel. Vous pouvez également supprimer manuellement l'agent de l'interface utilisateur sur la page Software Agent (Agent logiciel), ou l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la période de nettoyage à partir des profils de configuration d'agent. Pour plus de renseignements, reportez-vous aux sections *Supprimer un agent de visibilité approfondie ou d'application de Linux, Windows, AIX de la rubrique Suppression des agents logiciels* du guide de l'utilisateur de Cisco Secure Workload.
Intégration	
Améliorations de l'intégration du Cisco Secure Firewall Management Center	Les administrateurs réseau peuvent désormais envoyer un ensemble spécifique de règles associées à la charge de travail vers les domaines Cisco Secure Firewall Management Center et Cisco Secure Firewall Threat Defense correspondants.
Application de correctifs virtuels aux charges de travail à l'aide du Cisco Secure Firewall Management Center	Les administrateurs réseau peuvent désormais transmettre les informations CVE de Cisco Secure Workload à Cisco Secure Firewall Management Center afin d'augmenter les capacités de protection contre les menaces des pare-feux pour protéger les charges de travail contre les vulnérabilités connues et fournir des correctifs virtuels comme contrôle compensatoire en utilisant les signatures IPS sur le pare-feu.
Droits utilisateurs pour la configuration AD/LDAP sur le connecteur ISE	Pour la mise en service d'un connecteur ISE et AnyConnect NVM, vous pouvez désormais configurer LDAP sur les connecteurs avec un compte d'utilisateur de domaine standard. Pour plus de renseignements, consultez la section *LDAP Configuration* (Configuration LDAP) dans le guide de l'utilisateur Cisco Secure Workload.
Intégration d'ISE avec ISE-PIC	Le connecteur ISE dans Cisco Secure Workload se connecte désormais à ISE-PIC en utilisant le pxGRID pour récupérer les métadonnées, y compris le nom et le type de groupe ISE, à partir des terminaux signalés par l'intermédiaire d'ISE.

Nom de la caractéristique	Description
Intégration ISE : Possibilité de sélectionner/filtrer les terminaux et leurs attributs en provenance d'ISE PxGrid	Vous pouvez désormais ignorer les attributs ISE lors de la configuration du connecteur ISE si vous ne souhaitez pas ingérer toutes les informations contextuelles des terminaux signalés par l'intermédiaire d'ISE. Lorsque vous configurez le connecteur ISE, vous pouvez désormais filtrer les terminaux ISE en saisissant plusieurs sous-réseaux IPv4 ou IPv6.
Connecteur NetFlow pour afficher la liste des sources NetFlow	Vous pouvez collecter et communiquer à la grappe la liste des sources NetFlow qui envoient des flux Netflow aux connecteurs NetFlow.
Améliorations apportées à AIX/UNIX en matière de criminalistique, de vulnérabilité et d'alerte	Vous n'avez plus besoin que d'un seul moteur Tetration pour gérer la visibilité du réseau, et la visibilité au niveau des processus du système d'exploitation pour un contrôle criminalistique plus approfondi et l'application de la politique. L'agent logiciel sur AIX, Linux et Solaris est représenté uniquement par le service csw-agent.
Évolution des produits	
Capture de paquets via l'API native du système d'exploitation sous Windows	L'agent Windows utilise désormais le pilote ndiscap.sys (intégré par Microsoft) et le cadre eventstTracing using Windows (ETW) pour capturer les flux du réseau. La version de Npcap intégrée à Cisco Secure Workload n'est plus disponible sur l'hôte.
Prise en charge de la visibilité du réseau sous Solaris 11.4 x86_64	La visibilité du réseau est prise en charge sous Solaris 11.4.
Conteneurs	
Modèle de politique préconstruit pour le trafic du plan de contrôle de Kubernetes.	La découverte et la mise en œuvre de politiques sur une grappe Kubernetes sont désormais plus faciles, car des modèles de politiques sont disponibles pour l'environnement Kubernetes (eks,aks,gke,openshift), dans lesquels vous pouvez personnaliser et ajouter des politiques pour répondre aux exigences de l'application.
Prise en charge de l'équilibreur de charge de type objet de service K8s pour les nuages publics	Prend en charge l'équilibreur de charge de type objet de service pour les grappes AKS et EKS.

Nom de la caractéristique	Description
Efficacité de l'ADM pour Kubernetes ou les charges de travail conteneurisées.	Une nouvelle rubrique pour la prise en charge par Kubernetes de la découverte de politiques est ajoutée, dans laquelle la découverte de politiques utilise les renseignements sur les pods et les services de la configuration de Kubernetes pour créer des grappes à la fois pour les pods et pour les services. *L'utilisation de la fonction de mise en grappe pour la découverte de politiques* à partir de la page de l'orchestrateur externe est supprimée.
Kubernetes - Prise en charge des nœuds de travail Windows	Les agents logiciels capturent et signalent désormais la télémétrie réseau des hôtes et des pods sur les nœuds de travail Windows de Kubernetes sur AKS et les grappes Kubernetes standard utilisant des nœuds de travail Windows. **Remarque** Ne s'applique pas aux GKE ou EKS.
Charges de travail natives infonuagique	
Différencier les charges de travail sans agent dans le nuage et sur site sur l'interface utilisateur	Faire la différence entre une adresse IP normale obtenue à partir de flux et une instance de nuage sans agent comme EC2 sur l'interface utilisateur.
Évolutivité	
Évolutivité améliorée (75k) pour le logiciel-service et les appareils 39 RU	• Un seul détenteur en mode logiciel-service peut prendre en charge un maximum de 75 000 charges de travail (en mode conversation). • Un seul ou plusieurs détenteurs dans 39 RU peuvent prendre en charge un maximum de 75 000 charges de travail (en mode conversation). • Un seul ou plusieurs détenteurs dans 8 RU peuvent prendre en charge un maximum de 20 000 charges de travail (en mode conversation).
Charges de travail hybrides multinuages	
Amélioration du connecteur GCP	Le connecteur GCP prend désormais en charge de nouvelles fonctionnalités, notamment l'acquisition de balises, l'acquisition de journaux de flux VPC et la segmentation à l'aide du pare-feu intégré de GCP.
Sécurité renforcée pour le connecteur AWS	La prise en charge de l'authentification basée sur les rôles AWS IAM a été ajoutée au connecteur AWS.
Amélioration du dépannage du connecteur AWS	Un nouvel onglet Event Log (Journal des événements) a été ajouté et affiche les événements pour chaque connecteur AWS; les journaux aident à comprendre les événements significatifs qui se produisent par connecteur AWS à partir de différentes fonctionnalités.

Nom de la caractéristique	Description

Mettre à niveau le système dorsal et l'interface utilisateur pour améliorer le flux de travail	La page du connecteur AWS a été améliorée pour faciliter le flux de travail. Voici quelques-unes des améliorations apportées :
	• L'interface utilisateur améliorée affiche une vue d'ensemble de toutes les configurations créées pour chaque connecteur infonuagique.
	• La génération de modèles et la mise en route sont ajoutées dans une vue séparée.
	• L'enregistrement, la mise à jour et la suppression d'Assumer un rôle, avec ses états et ses actions de déclenchement, ont été ajoutés.
	• Les états d'enregistrement sont ajoutés d'un coup d'œil sur chaque configuration.
	• Afin de réduire l'espace occupé par l'interface utilisateur :
	  • Le flux de travail Assumer le rôle est ajouté aux paramètres.
	  • La sélection des ressources est disponible dans une structure arborescente qui permet de rechercher des ressources à chaque niveau.
	• Un onglet Inventory (Inventaire) distinct est ajouté, qui affiche les tableaux d'inventaire dans le contexte de ressource et de portée choisi, ce qui permet aux utilisateurs de comparer les différences entre elles.
	• À l'exception des paramètres, des filtres sont ajoutés à chaque vue pour faciliter la sélection des ressources et de la portée.

Amélioration du dépannage du connecteur Azure	Un nouvel onglet Event Log (Journal des événements) a été ajouté, qui affiche les événements pour chaque connecteur Azure; les journaux aident à comprendre les événements importants qui se produisent par connecteur Azure à partir de différentes fonctionnalités.
Sauvegarde et restauration des données	
État détaillé et messages d'erreur des vérifications de la configuration des compartiments S3	Lorsque vous configurez la sauvegarde des données, vous pouvez désormais afficher les contrôles d'état détaillés pour la configuration des compartiments S3.
Amélioration des rapports d'erreur pour déboguer les échecs de sauvegarde	Les rapports d'erreur sont améliorés pour afficher une vue sous forme de tableau des points de contrôle avec des options de filtrage supplémentaires sur la page d'état des sauvegardes.

Nouvelles fonctionnalités matérielles

Il n'y a pas de nouvelles fonctionnalités matérielles dans cette version.

Remarque La prise en charge de M4 est limitée à la version 3.8.1.1; M4 ne sera plus pris en charge après la version 3.8.1.1.

Fonctionnalités obsolètes

Fonctionnalités	Description de la fonctionnalité	
Les colonnes du tableau des flux sont obsolètes	Les colonnes suivantes du tableau des flux ne sont plus disponibles :	
	• Rendement du TCP • Goulot d'étranglement TCP avant • Goulot d'étranglement TCP Retour • Fenêtre de congestion Avant réduite • Fenêtre de congestion Retour réduite • MSS avant modifié • MSS avant modifié • MSS modifié Retour	• Fenêtre Récep. TCP avant à zéro? • Fenêtre TCP reçu Retour à zéro? • Chemin d'accès structure Avant • Chemin d'accès structuré Retour • Indicateur de rafale Avant • Indicateur de rafale Retour • Taille de rafale max. (Ko) Avant • Taille de rafale max. Retour (Ko) • Filtres de flux
Les fonctionnalités d'alerte sont obsolètes	Les alertes de voisinage et de structure et l'éditeur Kafka externe (Data Tap) sont obsolètes à partir de cette version.	

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.