

Notes de mise à jour de l'appliance virtuelle Cisco IQ v1.2.4

Introduction

Cisco IQTM offre aux clients des fonctionnalités conçues pour améliorer la visibilité des ressources et fournir des informations plus intelligentes sur l'ensemble de leurs environnements. En outre, les fonctionnalités d'IA, telles qu'AI Assistant, optimisent les résultats opérationnels et l'expérience utilisateur de Cisco IQ en fournissant une compréhension contextuelle qui permet aux utilisateurs de prendre des décisions proactives et éclairées et de rationaliser les processus pour l'engagement et la réussite des clients.

Cisco IQ On-Prem Air-Gapped est le mode de déploiement de Cisco IQ conçu pour les environnements qui ne peuvent pas se connecter au cloud. Elle est fournie sous la forme d'une machine virtuelle autonome, appelée appliance virtuelle Cisco IQ (VA), qui fonctionne entièrement dans les locaux du client en isolation complète des réseaux externes, avec des mises à jour logicielles et des packages de maintenance obtenus à partir de Cisco IQ SaaS et transférés à l'VA par le biais d'un processus manuel approuvé.

Pour les entreprises opérant dans des environnements réglementés, hautement sécurisés et souverains, la solution VA supprime le compromis entre la visibilité et le contrôle. Les clients déploient les ressources et les fonctionnalités d'évaluation de Cisco IQ sur leur propre réseau et conservent la propriété totale de leurs données, tout en obtenant les informations et les recommandations attendues de Cisco IQ. Le mode de déploiement Air-Gapped étend les fonctionnalités de Cisco IQ SaaS aux environnements isolés, permettant ainsi aux équipes stratégiques de fonctionner avec la vitesse et l'intelligence de diagnostic des entreprises connectées au cloud.

Ce document présente les nouvelles fonctionnalités, la prise en charge des modules et les problèmes connus de Cisco IQ VA v1.2.4.

Principales caractéristiques

Module de ressources

Le module Assets offre une visibilité et des fonctionnalités de gestion complètes pour les ressources Cisco et sert de base à Cisco IQ, en fournissant une liste centralisée de tous les

périphériques au sein d'une organisation. En collectant des informations auprès de plusieurs sources, il agit comme une source unique de vérité pour l'inventaire des périphériques. Il est disponible dans le cadre du programme d'installation téléchargé et peut être utilisé une fois l'appliance virtuelle installée. Principaux points saillants :

Informations sur la criticité des ressources

Les informations sur la criticité des ressources permettent au module Assets de prévoir le rôle fonctionnel et l'importance commerciale des périphériques réseau. En analysant les configurations des périphériques et les fonctionnalités activées, Asset Criticality Insights vous aide à identifier les ressources qui ont le plus d'impact sur votre réseau, vous permettant de les hiérarchiser pour la correction des problèmes de sécurité, les mises à niveau logicielles, la planification de la fin de vie/fin d'assistance et les décisions de couverture.

Contrats de service

La page Contrats de service fournit une surveillance centralisée des contrats d'assistance. Fonctionnalités clés :

- Surveillance des contrats de service : Rationalisez la planification du renouvellement et les stratégies de couverture grâce à des résumés complets des contrats et des données détaillées
- Points de vue spécifiques aux ressources : Identifiez et atténuez les vulnérabilités plus rapidement grâce à des données claires et exploitables directement liées à vos ressources

Tableau de bord LDOS

Le tableau de bord de la date de fin d'assistance (LDOS) fournit une vue centralisée des étapes de la LDOS et permet une meilleure planification des ressources et des prévisions budgétaires avant que le matériel ou les logiciels n'atteignent la fin de vie, ce qui vous permet de réduire considérablement le risque opérationnel.

Étiquetage des ressources

L'étiquetage des ressources offre un moyen flexible d'organiser, de filtrer et d'agir sur votre inventaire à l'aide d'étiquettes personnalisées. Les balises peuvent être créées, modifiées et attribuées aux ressources, avec une gestion centralisée des balises disponible pour les administrateurs de compte. Vous pouvez attribuer des balises à des ressources individuelles ou en masse, et filtrer votre inventaire par balise pour localiser rapidement les ressources souhaitées.

Module Évaluations

Le module Assessments fournit une visibilité sur votre inventaire en évaluant les ressources de votre organisation et offre une structure qui vous permet d'examiner et de limiter de manière proactive les risques liés à la sécurité, à la stabilité, à la capacité, à la conformité et au vieillissement, afin de préserver la sécurité des réseaux. Principaux points saillants :

Bulletins de renseignements de sécurité

Les avis de sécurité intégrés vous permettent de anticiper les menaces potentielles. Le système détecte de manière proactive les vulnérabilités pertinentes, ce qui vous permet d'être informé des mises à jour critiques et de prendre des mesures immédiates pour protéger votre réseau.

Renforcement de la sécurité

Le renforcement de la sécurité offre une visibilité automatisée et en temps réel sur la position de sécurité de votre infrastructure réseau en évaluant en permanence vos ressources par rapport aux guides de renforcement du système d'exploitation Cisco. Chaque règle de renforcement de la sécurité est évaluée sur l'ensemble de vos ressources couvertes afin de détecter les écarts de configuration, les conclusions étant hiérarchisées par niveau de gravité pour vous aider à combler les failles de sécurité, à améliorer la résilience et à réduire le risque opérationnel

Configuration

Évaluez vos ressources par rapport aux meilleures pratiques recommandées, basées sur l'expertise éprouvée de Cisco, afin de détecter les écarts de configuration dans votre infrastructure qui peuvent affecter la disponibilité, la sécurité ou les performances. Le système évalue chaque règle de meilleures pratiques pour l'ensemble des ressources couvertes, en hiérarchisant les conclusions par gravité pour vous aider à garantir la cohérence de la configuration, à améliorer la résilience et à réduire le risque opérationnel.

Notes de terrain

Les notifications sur site fournissent des notifications proactives et opportunes concernant les mises à jour matérielles et logicielles. En affichant les notices de champ pertinentes directement dans le tableau de bord Évaluations, cette fonctionnalité vous permet de résoudre les problèmes potentiels avant qu'ils n'affectent vos opérations.

Fonctionnalités AI-Powered

Cisco IQ VA offre des fonctionnalités optimisées par l'intelligence artificielle, qui apportent des informations de qualité SaaS directement dans votre environnement aéré. Il améliore Cisco IQ en transformant les données brutes en informations exploitables, en recommandations et en actions guidées. Les fonctionnalités optimisées par l'IA nécessitent un nœud équipé d'une unité de traitement graphique prise en charge. Ces fonctionnalités ne peuvent pas être activées sur les déploiements de CPU uniquement. Fonctionnalités :

- Ask AI Interface : accédez à des informations interactives basées sur l'IA directement dans les modules Assets et Inventory.
- LDOS : vous pouvez parcourir une liste d'invites prédéfinies pour obtenir des résumés, identifier les ressources critiques ou analyser les gammes de produits pour les ressources LDOS
- Points clés : Transformez les données des ressources et des évaluations en informations et recommandations exploitables. Intégration aux workflows pour fournir des informations et des rapports en temps réel

gestion du cycle de vie du logiciel

Vous pouvez gérer le cycle de vie du logiciel (installation et configuration) des modules opérationnels, des règles, des droits et des fonctions AI spécialisées au sein de l'appliance virtuelle. Vous pouvez les installer en téléchargeant les dernières versions de Cisco IQ (SaaS) en naviguant vers Paramètres système > Catalogue de packages.

Connecteur Cisco IQ

Cisco IQ VA est équipé d'un connecteur Cisco IQ complet, permettant une collecte flexible de données télémétriques à partir de connexions directes aux périphériques et à partir de périphériques gérés via Cisco Catalyst Center pour améliorer la visibilité et la gestion du réseau. Principaux points saillants :

Définition des périphériques

Cisco IQ VA offre des options flexibles pour définir l'étendue de votre périphérique. Vous pouvez spécifier des périphériques en téléchargeant un fichier CSV, en entrant manuellement une liste séparée par des virgules, en utilisant des plages IP ou en exploitant le CDP (Cisco Discovery Protocol) ou le LLDP (Link Layer Discovery Protocol). Cette liste peut être mise à jour à tout moment pour ajouter ou supprimer des périphériques, afin de garantir que vos groupes de périphériques restent à jour.

Planification de la détection et de la collecte

Cisco IQ VA permet une planification indépendante des processus de découverte et de collecte, prenant en charge des dates, des heures et des modèles de périodicité spécifiques. Vous pouvez configurer ces tâches séparément pour les aligner sur vos workflows opérationnels. En outre, vous pouvez effectuer une nouvelle détection à la demande pour chaque périphérique à tout moment, offrant ainsi un meilleur contrôle des cycles d'actualisation des données et des temps de réponse plus rapides pour le dépannage.

Hyperviseurs pris en charge

Cisco IQ VA prend en charge le déploiement sur les plates-formes d'hyperviseur suivantes. Avant de commencer le déploiement, assurez-vous que votre infrastructure répond à la configuration minimale requise pour la version de votre hyperviseur.

- VMware ESXi : pris en charge pour les environnements virtualisés standard
- Microsoft Hyper-V Server : pris en charge pour les piles de virtualisation Windows
- MV Red Hat basée sur le noyau : prise en charge pour les environnements de virtualisation open source

Prise en charge multinoeud non haute disponibilité

Cisco IQ VA prend en charge l'architecture multinoeud non haute disponibilité (HA), offrant ainsi une évolutivité et une flexibilité accrues pour vos environnements de déploiement. Le multinoeud offre une architecture distribuée qui sépare les fonctions de gestion et de travail, ce qui vous permet d'adapter et d'étendre votre infrastructure au-delà d'une seule appliance virtuelle pour répondre aux exigences de charges de travail plus importantes et plus complexes. Le noeud de gestion sert d'interface principale pour l'enregistrement des clusters, l'installation de la plate-forme et la surveillance post-installation.

Gestion des utilisateurs

Les fonctionnalités suivantes visent à simplifier les processus de gestion des utilisateurs, en offrant un meilleur contrôle et une meilleure sécurité pour les utilisateurs au sein du système.

Gestion des utilisateurs locaux

Les utilisateurs peuvent intégrer et gérer plusieurs utilisateurs en toute sécurité avec des privilèges d'accès distincts. Les utilisateurs locaux créés par un administrateur peuvent utiliser

l'option Sign Up lors de leur première connexion et définir en toute sécurité leurs propres mots de passe à l'aide de l'adresse e-mail configurée par l'administrateur.

Gestion de la sécurité en libre-service

Vous pouvez désormais gérer les paramètres de sécurité locaux indépendamment, ce qui vous permet de contrôler l'accès aux comptes et la récupération. Les fonctionnalités en libre-service incluent la possibilité de réinitialiser les mots de passe oubliés et de configurer les questions de sécurité, ce qui permet une expérience utilisateur plus rationalisée et plus sécurisée sans nécessiter de support externe.

Configuration SAML pour SSO sécurisé

Cisco IQ VA prend en charge les fonctionnalités d'authentification unique (SSO) en intégrant l'authentification SAML (Security Assertion Markup Language) v2.0. Cette intégration permet une fédération transparente des identités avec des fournisseurs d'identité tiers, vous permettant de vous authentifier à l'aide de vos informations d'identification d'entreprise existantes. Grâce à SAML v2.0, les entreprises peuvent améliorer la sécurité, rationaliser l'accès des utilisateurs et simplifier la gestion des identités dans leurs environnements. Un seul (1) PDI peut être actif à un moment donné. Les PDI suivants sont actuellement pris en charge :

- Okta IDP
- PDI ADFS
- PDI intra

Journaux d'activité

Tous les journaux d'exploitation sont stockés localement et peuvent être consultés par les administrateurs de compte, ce qui facilite la surveillance des activités des utilisateurs et garantit la transparence.

Prise en charge de NTP sécurisé et standard

Cisco IQ VA prend en charge le protocole NTP (Network Time Protocol) sécurisé et standard. Le protocole NTP sécurisé permet une synchronisation temporelle authentifiée et chiffrée entre Cisco IQ VA et les serveurs NTP approuvés, tandis que le protocole NTP standard offre une synchronisation pour les environnements où l'authentification n'est pas requise ou n'est pas prise en charge pour les échanges NTP chiffrés.

Prise en charge des certificats SSL personnalisés

Cisco IQ VA prend en charge l'installation et la gestion de certificats SSL personnalisés. Cette fonctionnalité permet aux administrateurs de compte de remplacer les certificats par défaut par ceux émis par l'autorité de certification de leur organisation. En utilisant des certificats personnalisés, vous pouvez garantir des communications sécurisées et fiables et assurer la conformité totale avec les stratégies de sécurité internes de votre entreprise. Actuellement, un seul (1) certificat SSL peut être installé et actif à tout moment.

Prise en charge des serveurs Syslog externes

Cisco IQ VA prend en charge l'intégration avec les serveurs Syslog externes, permettant aux administrateurs de comptes de transférer les journaux système vers une plate-forme de journalisation centralisée. Cette amélioration simplifie la surveillance, l'audit et le dépannage en fournissant une vue consolidée et permanente des événements système et des journaux de sécurité sur l'ensemble de votre infrastructure. Il est possible de configurer jusqu'à deux (2) serveurs syslog à tout moment.

Connexion et bannière personnalisée

Cisco IQ VA propose désormais une fonction de bannière configurable. Les administrateurs de compte peuvent configurer et afficher les notifications système obligatoires et les avertissements de sécurité sur l'écran de connexion. En outre, les administrateurs de compte peuvent configurer et afficher des bannières personnalisées sur l'appliance virtuelle Cisco IQ. Cette fonctionnalité permet de communiquer des informations importantes (par exemple, des notifications, des avertissements ou des alertes) directement aux utilisateurs dans Cisco IQ VA.

Gestion du système

Vous pouvez afficher et installer les dernières mises à jour de Cisco IQ VA via l'onglet System Management, ce qui vous permet d'accéder facilement aux dernières fonctionnalités, améliorations et améliorations. Cisco IQ VA prend en charge les mises à jour logicielles automatiques envoyées par Cisco IQ et les mises à jour logicielles manuelles. Pour les mises à jour manuelles, vous pouvez télécharger les packages logiciels directement à partir de Cisco IQ (SaaS) en naviguant vers System Settings > Package Catalog.

Problèmes connus

Les problèmes suivants sont activement traités dans l'évaluation des risques Cisco IQ.

Le champ Recurring Schedule affiche la syntaxe cron UNIX

Actuellement, l'entrée de planification récurrente pour les téléchargements de fichiers d'analyse réseau nécessite une expression cron UNIX avec cinq (5) champs (par exemple, "0 2 * * *"). Les utilisateurs peu familiers avec la syntaxe cron peuvent trouver ce format d'entrée peu clair. Cependant, les utilisateurs peuvent obtenir des informations plus détaillées sur la syntaxe cron et des exemples en ligne.

Échec de la collecte d'inventaire intermittent pour un petit nombre de périphériques dans des déploiements à grande échelle

Actuellement, dans les déploiements de plus de 10 000 périphériques, un petit sous-ensemble de périphériques peut ne pas effectuer la collecte d'inventaire malgré un processus de détection réussi. Pour contourner ce problème, retirez les périphériques défectueux du système et ajoutez-les à nouveau. Contactez le Centre d'assistance technique Cisco (TAC) pour obtenir de l'aide supplémentaire.

État de téléchargement des autorisations non visible pendant la collecte

Actuellement, après le téléchargement d'un fichier de droits, il n'y a aucune indication claire dans l'interface utilisateur que le droit a été chargé et traité avec succès. Le démarrage d'une collecte avant le traitement complet d'un droit peut entraîner des échecs de couverture. Pour contourner ce problème, attendez au moins une (1) heure après le téléchargement avant d'exécuter une collection.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.