

Note sulla release di Cisco IQ Virtual Appliance v1.2.0

Introduzione

Cisco IQTM offre ai clienti miglioramenti e funzionalità progettate per migliorare la visibilità degli asset, offrire informazioni più dettagliate negli ambienti e semplificare la gestione dei casi. Inoltre, le funzioni di AI, come l'Assistente AI, ottimizzano i risultati operativi e l'esperienza utente di Cisco IQ fornendo una comprensione contestuale che consente agli utenti di prendere decisioni proattive e informate e di semplificare i processi per il coinvolgimento e il successo del cliente.

Cisco IQ On-Prem Air-Gapped è una delle modalità di implementazione di Cisco IQ, progettata per i clienti in settori altamente regolamentati con rigorosi requisiti di conformità, sovranità sui dati e sicurezza. In questa modalità, Cisco IQ viene fornito come macchina virtuale (VM) indipendente, nota come Cisco IQ Virtual Appliance (VA). Il VA viene eseguito interamente presso la sede del cliente e funziona in totale isolamento dalle reti esterne. Per mantenere questo isolamento, gli aggiornamenti software e i pacchetti di manutenzione vengono ottenuti da Cisco IQ SaaS e trasferiti all'appliance VA tramite un processo manuale approvato.

Questo documento descrive nuove funzionalità, il supporto di moduli e i problemi noti di Cisco IQ VA v1.2.0.

 Nota: Cisco IQ VA è attualmente limitato ai clienti iscritti al programma Controlled Availability. L'accesso per il download del software di sistema VA e di pacchetti operativi aggiuntivi (moduli, regole e autorizzazioni) dal portale Cisco IQ è disponibile esclusivamente per determinati clienti. Per ulteriori informazioni, contattare il rappresentante commerciale.

Caratteristiche principali

Modulo Assets

Il modulo Assets offre visibilità e funzionalità di gestione complete per gli asset Cisco e costituisce la base di Cisco IQ, fornendo un elenco centralizzato di tutti i dispositivi all'interno di un'organizzazione. Raccogliendo informazioni da più fonti, funge da fonte unica di informazioni per l'inventario dei dispositivi. È disponibile come parte del programma di installazione scaricato ed è disponibile per l'utilizzo una volta installato VA. I punti salienti includono:

Asset Criticality Insights

Asset Criticality Insights consente al modulo Assets di prevedere il ruolo funzionale e l'importanza aziendale dei dispositivi di rete. Analizzando le configurazioni dei dispositivi e le funzionalità abilitate, Asset Criticality Insights consente di identificare quali risorse hanno il maggiore impatto sulla rete, consentendo di assegnare loro una priorità per il monitoraggio e l'aggiornamento del software, la pianificazione di fine ciclo di vita/fine supporto e le decisioni di copertura.

Contratti di assistenza

La pagina Contratti di assistenza fornisce la supervisione centralizzata dei contratti di supporto. Le caratteristiche principali includono:

- Supervisione del contratto di assistenza: Semplificazione della pianificazione del rinnovo e delle strategie di copertura con riepiloghi completi dei contratti e dati dettagliati
- Informazioni specifiche sugli asset: Identificazione e mitigazione più rapida delle vulnerabilità grazie a dati chiari e utilizzabili collegati direttamente alle risorse

Dashboard LDOS

Il dashboard LDOS fornisce una vista centralizzata delle fasi cardine di LDOS e consente una migliore pianificazione degli asset e una previsione del budget prima che l'hardware o il software raggiunga la fine del ciclo di vita, consentendo di ridurre significativamente il rischio operativo.

Etichettatura degli asset

L'etichettatura degli asset offre un modo flessibile per organizzare, filtrare ed eseguire operazioni sull'inventario utilizzando etichette personalizzate. Le etichette possono essere create, modificate e assegnate alle risorse, con la gestione centralizzata delle etichette disponibile per gli amministratori degli account. È possibile assegnare cartellini a singole risorse o in grandi quantità, nonché filtrare il magazzino in base al cartellino per individuare rapidamente le risorse desiderate.

Modulo di valutazione

Il modulo Valutazioni fornisce visibilità sull'inventario valutando le risorse dell'organizzazione e offre una struttura che consente di analizzare in modo proattivo e ridurre i rischi correlati a sicurezza, stabilità, capacità, conformità e invecchiamento, contribuendo a mantenere sicure le reti. I punti salienti includono:

Consulenze sulla sicurezza

Gli avvisi di sicurezza integrati consentono di stare al passo con le minacce potenziali. Il sistema rileva in modo proattivo le vulnerabilità rilevanti, assicurando che l'utente sia informato degli aggiornamenti critici e possa intraprendere azioni immediate per proteggere la rete.

Protezione avanzata

La protezione avanzata offre una visibilità automatizzata in tempo reale sulla postura di sicurezza dell'infrastruttura di rete attraverso una valutazione continua degli asset rispetto alle guide alla protezione avanzata del sistema operativo Cisco. Ciascuna regola di protezione avanzata viene valutata a livello delle risorse coperte per rilevare le deviazioni dalla configurazione, con risultati con priorità per gravità che consentono di colmare le lacune di sicurezza, migliorare la resilienza e ridurre il rischio operativo

Configurazione

Valutare le risorse in base alle best practice consigliate, sulla base della comprovata esperienza di Cisco, per rilevare le deviazioni della configurazione nell'infrastruttura che possono influire su disponibilità, sicurezza o prestazioni. Il sistema valuta ogni regola delle procedure ottimali per le risorse coperte, assegnando priorità ai risultati in base alla gravità per garantire la coerenza della configurazione, migliorare la resilienza e ridurre il rischio operativo.

Notifiche sul campo

Gli avvisi sui prodotti forniscono notifiche tempestive e proattive sugli aggiornamenti hardware e software. Visualizzando gli avvisi sui prodotti pertinenti direttamente nel pannello di controllo Valutazioni, questa funzione consente di risolvere i potenziali problemi prima che influiscano sulle operazioni.

Caratteristiche con tecnologia AI

Cisco IQ VA offre funzionalità basate sull'intelligenza artificiale, offrendo informazioni approfondite sull'intelligenza artificiale di livello SaaS direttamente nell'ambiente con air-gapped. Eleva il QI di Cisco trasformando i dati raw in informazioni, consigli e azioni guidate utilizzabili. Le funzionalità basate su AI richiedono un nodo dotato di un'unità di elaborazione grafica supportata. Queste funzionalità non possono essere abilitate nelle distribuzioni basate solo sulla CPU. Le caratteristiche includono:

- Interfaccia Ask AI: accesso diretto a informazioni interattive basate sull'intelligenza artificiale nei moduli Assets e Inventory.
- LDOS: è possibile sfogliare un elenco di prompt predefiniti per ottenere riepiloghi, identificare le risorse critiche o analizzare le famiglie di prodotti per le risorse LDOS (Last Date Of Support)
- Informazioni principali: Trasformare i dati relativi alle risorse e alle valutazioni in informazioni e consigli utili. Integrazione nei flussi di lavoro per fornire informazioni dettagliate e report in tempo reale

Gestione del ciclo di vita del software

È possibile gestire il ciclo di vita del software (installazione e configurazione) di moduli operativi, regole, diritti e funzionalità specializzate basate su IA all'interno di VA. Per installarli, è possibile scaricare le versioni più recenti da Cisco IQ (SaaS) selezionando Impostazioni di sistema > Catalogo pacchetti.

Cisco IQ Connector

Cisco IQ VA è dotato di un connettore Cisco IQ completo, che consente la raccolta flessibile dei dati di telemetria da connessioni dirette ai dispositivi e da dispositivi gestiti tramite Cisco Catalyst Center per migliorare la visibilità e la gestione della rete. I punti salienti includono:

Definizione dei dispositivi

Cisco IQ VA offre opzioni flessibili per definire l'ambito del dispositivo. È possibile specificare i dispositivi caricando un file CSV, inserendo manualmente un elenco separato da virgole, utilizzando intervalli IP o utilizzando il protocollo CDP (Cisco Discovery Protocol) o LLDP (Link Layer Discovery Protocol). L'elenco può essere aggiornato in qualsiasi momento per aggiungere o rimuovere dispositivi, assicurando che i gruppi di dispositivi rimangano aggiornati.

Pianificazione individuazione e raccolta

Cisco IQ VA consente la pianificazione indipendente dei processi di rilevamento e raccolta, supportando date, ore e criteri di ricorrenza specifici. È possibile configurare queste attività separatamente per allinearle ai flussi di lavoro operativi. È inoltre possibile eseguire in qualsiasi momento il re-discovery su richiesta dei singoli dispositivi, garantendo un maggiore controllo sui cicli di aggiornamento dei dati e tempi di risposta più rapidi per la risoluzione dei problemi.

Hypervisor supportati

Cisco IQ VA supporta l'installazione sulle seguenti piattaforme hypervisor. Prima di avviare l'installazione, verificare che l'infrastruttura soddisfi i requisiti minimi di versione per l'hypervisor in uso.

- VMware ESXi: supportato per ambienti virtualizzati standard
- Microsoft Hyper-V Server: supportato per stack di virtualizzazione basati su Windows
- VM basata su kernel Red Hat: supportata per ambienti di virtualizzazione open-source

Supporto multi-nodo non HA

Cisco IQ VA supporta l'architettura a più nodi non ad alta disponibilità (HA, Non-High Availability), consentendo una maggiore scalabilità e flessibilità per gli ambienti di implementazione. L'architettura a più nodi offre un'architettura distribuita che separa le funzioni di gestione da quelle di lavoro, consentendo di personalizzare ed estendere l'infrastruttura oltre un singolo VA per soddisfare le esigenze di carichi di lavoro più grandi e complessi. Il nodo di gestione funge da interfaccia primaria per la registrazione del cluster, l'installazione della piattaforma e il monitoraggio successivo all'installazione.

Gestione utenti

Le funzionalità seguenti consentono di semplificare i processi di gestione degli utenti, offrendo un maggiore controllo e una maggiore sicurezza per gli utenti all'interno del sistema.

Gestione utente locale

Gli utenti possono incorporare e gestire in modo sicuro più utenti con privilegi di accesso distinti. Gli utenti locali creati da un amministratore possono usare l'opzione "Iscriviti" durante il primo accesso e impostare in modo sicuro le proprie password usando l'indirizzo e-mail configurato dall'amministratore.

Gestione della sicurezza in modalità self-service

È ora possibile gestire le impostazioni di protezione locali in modo indipendente, garantendo il controllo dell'accesso e del ripristino dell'account. Le funzionalità self-service includono la possibilità di reimpostare le password dimenticate e configurare le domande di sicurezza,

consentendo un'esperienza utente più semplice e sicura senza richiedere supporto esterno.

Configurazione SAML per Secure SSO

Cisco IQ VA supporta funzionalità SSO (Single Sign-On) sicure tramite l'integrazione dell'autenticazione SAML (Security Assertion Markup Language) v2.0. Questa integrazione consente la perfetta federazione delle identità con provider di identità di terze parti (IDP, Identity Provider), consentendo l'autenticazione tramite le credenziali aziendali esistenti. Sfruttando SAML v2.0, le organizzazioni possono migliorare la sicurezza, semplificare l'accesso degli utenti e semplificare la gestione delle identità all'interno dei propri ambienti. Può essere attivo un solo (1) IDP alla volta. I seguenti IDP sono attualmente supportati:

- Okta IDP
- IDP ADFS
- IDP Entra

Log attività

Tutti i registri operativi sono archiviati localmente e possono essere visualizzati dagli amministratori degli account, consentendo un facile monitoraggio delle attività degli utenti e garantendo la trasparenza.

Supporto per NTP sicuro e standard

Cisco IQ VA supporta il protocollo NTP (Network Time Protocol) sia sicuro che standard. Il protocollo NTP sicuro consente la sincronizzazione dell'ora autenticata e crittografata tra Cisco IQ VA e server NTP attendibili, mentre il protocollo NTP standard offre la sincronizzazione per ambienti in cui l'autenticazione non è richiesta o non è supportata per gli scambi NTP crittografati.

Supporto certificato SSL personalizzato

Cisco IQ VA supporta l'installazione e la gestione di certificati SSL personalizzati. Questa funzionalità consente agli amministratori degli account di sostituire i certificati predefiniti con quelli rilasciati dall'Autorità di certificazione (CA) dell'organizzazione. L'utilizzo di certificati personalizzati consente di garantire comunicazioni sicure e affidabili e di mantenere la piena conformità con i criteri di sicurezza interni dell'organizzazione. Attualmente è possibile installare e attivare un solo (1) certificato SSL alla volta.

Supporto per server syslog esterni

Cisco IQ VA supporta l'integrazione con server Syslog esterni, consentendo agli amministratori degli account di inoltrare i log di sistema a una piattaforma di registrazione centralizzata. Questo miglioramento semplifica il monitoraggio, l'auditing e la risoluzione dei problemi fornendo una vista consolidata e permanente degli eventi di sistema e dei registri di protezione nell'intera infrastruttura. È possibile configurare fino a due (2) server syslog in qualsiasi momento.

Banner di accesso e personalizzato

Cisco IQ VA offre ora una funzionalità di banner configurabile. Gli amministratori degli account possono configurare e visualizzare notifiche di sistema obbligatorie e avvisi di protezione nella schermata di accesso. Inoltre, gli amministratori degli account possono configurare e visualizzare banner personalizzati in Cisco IQ VA. Questa funzione consente la comunicazione di informazioni importanti (ad esempio, notifiche, declinazioni di responsabilità o avvisi) direttamente agli utenti all'interno di Cisco IQ VA.

Gestione del sistema

È possibile visualizzare e installare gli ultimi aggiornamenti di Cisco IQ VA dalla scheda Gestione sistema, fornendo un facile accesso alle funzionalità, ai miglioramenti e alle migliorie più recenti. Cisco IQ VA supporta sia gli aggiornamenti software automatici inviati da Cisco IQ sia gli aggiornamenti software manuali. Per gli aggiornamenti manuali, è possibile scaricare i pacchetti software direttamente da Cisco IQ (SaaS) selezionando Impostazioni di sistema > Catalogo pacchetti.

Problemi noti

In Cisco IQ VA vengono attivamente affrontati i seguenti problemi.

Nel Campo Pianificazione Ricorrente Viene Visualizzata La Sintassi Cron Di UNIX

Al momento, l'input di pianificazione ricorrente per il caricamento dei file di analisi della rete richiede un'espressione cron UNIX con cinque (5) campi (ad esempio, "0 2 * * *"). Per gli utenti che non hanno familiarità con la sintassi cron, questo formato di input potrebbe non essere chiaro. Tuttavia, gli utenti possono ottenere informazioni più dettagliate sulla sintassi del cron e sugli esempi online.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).