Cisco IQ Virtual Appliance Release Notes v1.2.4

Inleiding

Cisco IQTM biedt klanten functies die zijn ontworpen om de zichtbaarheid van bedrijfsmiddelen te verbeteren en slimmere inzichten in hun omgevingen te bieden. Bovendien optimaliseren AI-functies zoals de AI Assistant operationele resultaten en de Cisco IQ-gebruikerservaring door contextueel inzicht te bieden dat gebruikers in staat stelt proactieve, geïnformeerde beslissingen te nemen en processen voor klantbetrokkenheid en succes te stroomlijnen.

Cisco IQ On-Prem Air-Gapped is de implementatiemodus van Cisco IQ die is gebouwd voor omgevingen die geen verbinding kunnen maken met de cloud. Het wordt geleverd als een zelfstandige virtuele machine (VM), aangeduid als de Cisco IQ Virtual Appliance (VA), die volledig op het terrein van de klant draait in volledige isolatie van externe netwerken, met software-updates en onderhoudspakketten die zijn verkregen van Cisco IQ SaaS en via een goedgekeurd, handmatig proces naar de VA zijn overgebracht.

Voor organisaties die actief zijn in gereguleerde, beveiligde en soevereine omgevingen, verwijdert de VA de wisselwerking tussen inzicht en controle. Klanten implementeren Cisco IQ Assets en Assessments-mogelijkheden binnen hun eigen netwerk en behouden de volledige eigendom van hun gegevens, terwijl ze nog steeds de inzichten en aanbevelingen krijgen die ze verwachten van Cisco IQ. De Air-Gapped-implementatiemodus breidt de mogelijkheden van Cisco IQ SaaS uit naar geïsoleerde omgevingen, waardoor bedrijfskritieke teams kunnen werken met de snelheid en diagnostische intelligentie van cloudverbonden ondernemingen.

In dit document worden nieuwe functies, ondersteuning van modules en bekende problemen voor Cisco IQ VA v1.2.4 beschreven.

Belangrijkste hoogtepunten

middelenmodule

De Assets-module biedt uitgebreide zichtbaarheids- en beheermogelijkheden voor Cisco-bedrijfsmiddelen en vormt de basis van Cisco IQ en biedt een gecentraliseerde lijst van alle apparaten binnen een organisatie. Door informatie uit meerdere bronnen te verzamelen, fungeert het als een enkele bron van waarheid voor apparaatinventarisatie. Het is beschikbaar als onderdeel van het gedownloade installatieprogramma en is beschikbaar om te gebruiken zodra de VA is geïnstalleerd. Belangrijkste hoogtepunten zijn onder meer:

Inzichten in activakritiek

Met Asset Criticality Insights kan de Assets module de functionele rol en het zakelijke belang van netwerkapparaten voorspellen. Door apparaatconfiguraties en ingeschakelde functies te analyseren, helpt Asset Criticality Insights u te identificeren welke middelen de grootste impact hebben op uw netwerk, zodat u ze kunt prioriteren voor beveiligingsherstel, software-upgrades, end-of-life / end-of-support planning en dekkingsbeslissingen.

dienstencontracten

De pagina Servicecontracten biedt gecentraliseerd toezicht op supportcontracten. Belangrijkste kenmerken zijn onder meer:

- Toezicht op servicecontracten: stroomlijn vernieuwingsplanning en dekkingsstrategieën met uitgebreide contractsamenvattingen en gedetailleerde gegevens
- Asset-Specific Insights: Identificeer en verlicht kwetsbaarheden sneller met duidelijke, bruikbare gegevens die rechtstreeks aan uw bedrijfsmiddelen zijn gekoppeld

LDOS-dashboard

Het LDOS-dashboard (Last Date Of Support) biedt een gecentraliseerd overzicht van LDOS-mijlpalen en maakt verbeterde planning van bedrijfsmiddelen en budgetvoorspelling mogelijk voordat hardware of software het einde van de levenscyclus bereikt, waardoor u het operationele risico aanzienlijk kunt verminderen.

Asset Tagging

Asset tagging biedt een flexibele manier om uw inventaris te organiseren, te filteren en te handelen met behulp van aangepaste labels. Tags kunnen worden gemaakt, gewijzigd en toegewezen aan middelen, waarbij gecentraliseerd tagbeheer beschikbaar is voor accountbeheerders. U kunt tags toewijzen aan individuele activa of in bulk, evenals uw inventaris filteren op tag om snel de gewenste activa te vinden.

evaluatiemodule

De evaluatiemodule biedt inzicht in uw inventaris door de bedrijfsmiddelen van uw organisatie te evalueren en biedt een kader waarmee u proactief risico's met betrekking tot beveiliging, stabiliteit, capaciteit, naleving en veroudering kunt onderzoeken en beperken, waardoor netwerken veilig blijven. Belangrijkste hoogtepunten zijn onder meer:

Beveiligingsadviezen

Geïntegreerde beveiligingsadviezen stellen u in staat om potentiële bedreigingen voor te blijven. Het systeem brengt proactief relevante kwetsbaarheden aan het licht en zorgt ervoor dat u op de hoogte bent van kritieke updates en onmiddellijk actie kunt ondernemen om uw netwerk te beschermen.

Veiligheidshardening

Security Hardening biedt geautomatiseerd, realtime inzicht in de beveiligingspositie van uw netwerkinfrastructuur door uw bedrijfsmiddelen voortdurend te evalueren aan de hand van Cisco OS Hardening Guides. Elke regel voor het verharden van de beveiliging wordt geëvalueerd voor uw gedekte bedrijfsmiddelen om configuratieafwijkingen te detecteren, waarbij de bevindingen prioriteit krijgen op basis van de ernst om u te helpen leemten in de beveiliging aan te pakken, de veerkracht te vergroten en het operationele risico te verminderen

Configuratie

Evalueer uw bedrijfsmiddelen aan de hand van aanbevolen best practices, op basis van de bewezen expertise van Cisco, om configuratieafwijkingen in uw infrastructuur te detecteren die van invloed kunnen zijn op de beschikbaarheid, beveiliging of prestaties. Het systeem beoordeelt elke regel voor best practices voor uw gedekte bedrijfsmiddelen en geeft prioriteit aan de bevindingen op basis van de ernst om u te helpen de consistentie van de configuratie te waarborgen, de veerkracht te vergroten en het operationele risico te verminderen.

Veldkennisgevingen

Veldkennisgevingen bevatten tijdige, proactieve meldingen met betrekking tot hardware- en software-updates. Door relevante Veldberichten rechtstreeks in het Dashboard Beoordelingen te plaatsen, kunt u met deze functie potentiële problemen aanpakken voordat ze van invloed zijn op uw activiteiten.

Functies op basis van AI

Cisco IQ VA biedt AI-aangedreven functies, waardoor SaaS-grade AI-inzichten rechtstreeks in uw air-gapped omgeving worden gebracht. Het verhoogt het IQ van Cisco door ruwe gegevens om te zetten in bruikbare inzichten, aanbevelingen en begeleide acties. AI-aangedreven functies vereisen een knooppunt uitgerust met een ondersteunde Graphics Processing Unit. Deze functies kunnen niet worden ingeschakeld bij implementaties met alleen een CPU. Kenmerken zijn onder

meer:

- Ask AI Interface: Toegang tot interactieve AI-aangedreven inzichten direct binnen de Assets en Inventory modules.
- LDOS: U kunt door een lijst met vooraf gedefinieerde prompts bladeren om samenvattingen te krijgen, kritieke bedrijfsmiddelen te identificeren of productfamilies voor LDOS-bedrijfsmiddelen te analyseren
- Key Insights: Transformeer gegevens over assets en assessments in bruikbare inzichten en aanbevelingen. Geïntegreerd in de workflows om realtime inzichten en rapporten te leveren

Software Lifecycle Management

U kunt de softwarelevenscyclus (installatie en configuratie) van operationele modules, regels, rechten en gespecialiseerde AI-aangedreven functies binnen de VA beheren. U kunt ze installeren door de nieuwste versies te downloaden van Cisco IQ (SaaS) door te navigeren naar Systeeminstellingen > Pakketcatalogus.

Cisco IQ-connector

Cisco IQ VA is uitgerust met een uitgebreide Cisco IQ Connector, waardoor het mogelijk is om flexibele telemetrie-gegevens te verzamelen van directe verbindingen met apparaten en van apparaten die worden beheerd via Cisco Catalyst Center om de zichtbaarheid en het beheer van het netwerk te verbeteren. Belangrijkste hoogtepunten zijn onder meer:

Apparaten definiëren

Cisco IQ VA biedt flexibele opties voor het definiëren van het bereik van uw apparaat. U kunt apparaten opgeven door een CSV-bestand te uploaden, handmatig een door komma's gescheiden lijst in te voeren, IP-bereiken te gebruiken of gebruik te maken van CDP (Cisco Discovery Protocol) of LLDP (Link Layer Discovery Protocol). Deze lijst kan op elk moment worden bijgewerkt om apparaten toe te voegen of te verwijderen, zodat de apparaatgroepen actueel blijven.

Ontdekking en verzameling plannen

Cisco IQ VA maakt onafhankelijke planning voor detectie- en verzamelprocessen mogelijk, met ondersteuning voor specifieke datums, tijden en terugkerende patronen. U kunt deze taken afzonderlijk configureren om ze af te stemmen op uw operationele workflows. Bovendien kunt u op elk gewenst moment on-demand herdetectie uitvoeren voor afzonderlijke apparaten, waardoor u meer controle hebt over de vernieuwingscycli van gegevens en snellere responstijden voor

probleemoplossing.

Ondersteunde hypervisors

Cisco IQ VA ondersteunt implementatie op de volgende hypervisorplatforms. Zorg ervoor dat uw infrastructuur voldoet aan de minimale versievereisten voor uw specifieke hypervisor voordat u de implementatie start.

- VMware ESXi: ondersteund voor standaard gevirtualiseerde omgevingen
- Microsoft Hyper-V Server: ondersteund voor Windows-gebaseerde virtualisatiestacks
- Red Hat Kernel-gebaseerde VM: ondersteund voor open-source virtualisatieomgevingen

Niet-HA multi-node ondersteuning

Cisco IQ VA ondersteunt multi-nodearchitectuur met niet-hoge beschikbaarheid (HA), waardoor uw implementatieomgevingen schaalbaarder en flexibeler zijn. De multi-node biedt een gedistribueerde architectuur die beheer- en werknemersfuncties van elkaar scheidt, zodat u uw infrastructuur kunt aanpassen en uitbreiden tot buiten één VA om aan de eisen van grotere, complexere werklasten te voldoen. Het beheerknooppunt fungeert als de primaire interface voor clusterregistratie, platforminstallatie en monitoring na de installatie.

Gebruikersbeheer

De volgende functies zijn bedoeld om gebruikersbeheerprocessen te vereenvoudigen en gebruikers binnen het systeem betere controle en beveiliging te bieden.

Lokaal gebruikersbeheer

Gebruikers kunnen veilig aan boord gaan en meerdere gebruikers beheren met verschillende toegangsrechten. Lokale gebruikers die door een beheerder zijn gemaakt, kunnen de optie Aanmelden gebruiken tijdens hun eerste aanmelding en hun eigen wachtwoorden veilig instellen met behulp van het e-mailadres dat door de beheerder is geconfigureerd.

Self-service Beveiligingsbeheer

U kunt nu de lokale beveiligingsinstellingen onafhankelijk beheren, waardoor u controle hebt over de toegang tot en het herstel van uw account. Self-service mogelijkheden omvatten de mogelijkheid om vergeten wachtwoorden opnieuw in te stellen en beveiligingsvragen te

configureren, waardoor een meer gestroomlijnde en veilige gebruikerservaring mogelijk is zonder externe ondersteuning.

SAML-configuratie voor beveiligde SSO

Cisco IQ VA ondersteunt veilige Single Sign-On (SSO)-mogelijkheden door de integratie van Security Assertion Markup Language (SAML) v2.0-verificatie. Deze integratie maakt een naadloze identiteitsfederatie met IDP (Third-Party Identity Providers) mogelijk, zodat u uw bestaande bedrijfsreferenties kunt verifiëren. Door gebruik te maken van SAML v2.0 kunnen organisaties de beveiliging verbeteren, de gebruikerstoegang stroomlijnen en identiteitsbeheer in hun omgevingen vereenvoudigen. Slechts één (1) IDP kan op elk moment actief zijn. De volgende IDP's worden momenteel ondersteund:

- Okta IDP
- ADFS IDP
- Entra IDP

Activiteitenlogboeken

Alle operationele logs worden lokaal opgeslagen en kunnen door accountbeheerders worden bekeken, waardoor gebruikersactiviteiten eenvoudig kunnen worden gecontroleerd en transparantie wordt gewaarborgd.

Ondersteuning voor veilige en standaard NTP

Cisco IQ VA ondersteunt zowel het beveiligde als het standaard Network Time Protocol (NTP). De beveiligde NTP maakt geverifieerde en gecodeerde tijdsynchronisatie tussen Cisco IQ VA en vertrouwde NTP-servers mogelijk, terwijl standaard NTP synchronisatie biedt voor omgevingen waar verificatie niet vereist is of niet wordt ondersteund voor gecodeerde NTP-uitwisselingen.

Aangepaste SSL-certificaatondersteuning

Cisco IQ VA ondersteunt de installatie en het beheer van aangepaste SSL-certificaten. Met deze functie kunnen accountbeheerders standaardcertificaten vervangen door certificaten die zijn uitgegeven door de certificeringsautoriteit (CA) van hun organisatie. Door aangepaste certificaten te gebruiken, kunt u veilige, vertrouwde communicatie garanderen en volledige naleving van het interne beveiligingsbeleid van uw organisatie handhaven. Op dit moment kan slechts één (1) SSL-certificaat worden geïnstalleerd en actief zijn op een bepaald moment.

Ondersteuning voor externe Syslog-servers

Cisco IQ VA ondersteunt integratie met externe Syslog-servers, waardoor accountbeheerders systeemlogs kunnen doorsturen naar een gecentraliseerd logplatform. Deze verbetering vereenvoudigt de bewaking, controle en probleemoplossing door een consistent, geconsolideerd overzicht te bieden van systeemgebeurtenissen en beveiligingslogboeken in uw infrastructuur. Er kunnen op elk gewenst moment maximaal twee (2) syslog-servers worden geconfigureerd.

Aanmeldings- en aangepaste banner

Cisco IQ VA biedt nu een configureerbare bannerfunctie. Accountbeheerders kunnen verplichte systeemmeldingen en beveiligingswaarschuwingen configureren en weergeven op het aanmeldingsscherm. Daarnaast kunnen accountbeheerders aangepaste banners configureren en weergeven in Cisco IQ VA. Deze functie maakt het mogelijk om belangrijke informatie (bijvoorbeeld meldingen, disclaimers of waarschuwingen) rechtstreeks aan gebruikers binnen Cisco IQ VA door te geven.

systeembeheer

U kunt de nieuwste Cisco IQ VA-updates bekijken en installeren via het tabblad Systeembeheer, zodat u eenvoudig toegang hebt tot de nieuwste functies, verbeteringen en verbeteringen. Cisco IQ VA ondersteunt zowel automatische software-updates die vanuit Cisco IQ worden gepusht als handmatige software-updates. Voor handmatige updates kunt u de softwarepakketten rechtstreeks downloaden van Cisco IQ (SaaS) door te navigeren naar Systeeminstellingen > Pakketcatalogus.

Bekende problemen

De volgende problemen worden actief aangepakt in Cisco IQ VA.

Terugkerend planningsveld geeft UNIX Cron-syntaxis weer

Momenteel vereist de terugkerende planinvoer voor het uploaden van netwerkscanbestanden een UNIX-cron-expressie met vijf (5) velden (bijvoorbeeld "0 2 * * *"). Gebruikers die niet bekend zijn met de cron-syntaxis kunnen deze invoerindeling onduidelijk vinden. Gebruikers kunnen echter meer gedetailleerde informatie krijgen over cron-syntaxis en voorbeelden online.

Intermitterende inventarisatie mislukt voor weinig apparaten bij grootschalige

implementaties

Momenteel kan het zijn dat bij implementaties van meer dan 10.000 apparaten een kleine subset van apparaten geen inventarisverzameling uitvoert, ondanks een succesvol detectieproces. Als een tijdelijke oplossing verwijdert u de defecte apparaten uit het systeem en voegt u ze opnieuw toe. Neem contact op met het Cisco Technical Assistance Center (TAC) voor extra hulp.

Uploadstatus van rechten niet zichtbaar tijdens ophalen

Momenteel is er na het uploaden van een rechtenbestand geen duidelijke indicatie in de gebruikersinterface dat het recht met succes is geladen en verwerkt. Het starten van een inning voordat een recht volledig is verwerkt, kan leiden tot dekkingsfouten. Als een tijdelijke oplossing, wacht ten minste één (1) uur na het uploaden voordat u een verzameling uitvoert.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.