

Cisco IQ Virtual Appliance - Versionshinweise v1.2.0

Einleitung

Cisco IQ™ bietet Kunden Verbesserungen und Funktionen, die darauf ausgelegt sind, die Transparenz ihrer Ressourcen zu verbessern, intelligentere Einblicke in ihre Umgebungen zu liefern und das Fallmanagement zu optimieren. Darüber hinaus optimieren KI-Funktionen wie der KI-Assistent die Betriebsergebnisse und die Benutzererfahrung mit Cisco IQ, indem sie ein kontextbezogenes Verständnis bieten, das es den Benutzern ermöglicht, proaktive, fundierte Entscheidungen zu treffen und Prozesse für Kundenengagement und -erfolg zu optimieren.

Cisco IQ On-Prem Air-Gapped ist einer der Bereitstellungsmodi von Cisco IQ für Kunden in stark regulierten Branchen mit strengen Compliance-, Datenhoheit- und Sicherheitsanforderungen. In diesem Modus wird Cisco IQ als eigenständiges virtuelles System (VM) bereitgestellt, das als Cisco IQ Virtual Appliance (VA) bezeichnet wird. Die VA läuft vollständig auf dem Gelände des Kunden und ist vollständig von externen Netzwerken isoliert. Um diese Isolierung aufrecht zu erhalten, werden Software-Updates und Wartungspakete von Cisco IQ SaaS abgerufen und über einen genehmigten manuellen Prozess an die VA übertragen.

In diesem Dokument werden neue Funktionen, Modulunterstützung und bekannte Probleme im Zusammenhang mit Cisco IQ VA v1.2.0 beschrieben.

 Anmerkung: Die Cisco IQ VA ist derzeit auf Kunden beschränkt, die für das Programm "Controller Availability" registriert sind. Der Download-Zugriff für die VA-Systemsoftware und zusätzliche Betriebspakete (Module, Regeln und Berechtigungen) aus dem Cisco IQ-Portal steht ausschließlich ausgewählten Kunden zur Verfügung. Weitere Informationen erhalten Sie von Ihrem Kundenbetreuer.

Die wichtigsten Highlights

Ressourcen-Modul

Das Assets-Modul bietet umfassende Transparenz- und Managementfunktionen für Cisco Ressourcen und dient als Grundlage für den Cisco IQ. Es bietet eine zentralisierte Liste aller Geräte in einer Organisation. Durch das Sammeln von Informationen aus mehreren Quellen wird der Gerätebestand als einheitliche Datenquelle genutzt. Es ist als Teil des heruntergeladenen

Installationsprogramms verfügbar und kann nach der Installation der VA verwendet werden. Zu den wichtigsten Highlights gehören:

Einblicke in kritische Ressourcen

Mithilfe der Asset Criticality Insights kann das Assets-Modul die funktionale Rolle und die geschäftliche Bedeutung von Netzwerkgeräten vorhersagen. Durch die Analyse von Gerätekonfigurationen und aktivierten Funktionen unterstützen Asset Criticality Insights Sie dabei, die Ressourcen mit den größten Auswirkungen auf Ihr Netzwerk zu identifizieren. So können Sie sie priorisieren, um Sicherheitskorrekturen, Software-Upgrades, End-of-Life-/End-of-Support-Planung und Abdeckungsentscheidungen zu treffen.

Serviceverträge

Die Seite für Serviceverträge bietet eine zentrale Übersicht über die Supportverträge. Zu den wichtigsten Funktionen gehören:

- Überwachung von Serviceverträgen: Optimierung der Planung von Vertragsverlängerungen und der Abdeckungsstrategien durch umfassende Vertragsübersichten und detaillierte Daten
- Ressourcenspezifische Einblicke: Schnellere Identifizierung und Beseitigung von Schwachstellen durch klare, aussagekräftige Daten, die direkt mit Ihren Ressourcen verknüpft sind

LDOS-Dashboard

Das LDOS Dashboard bietet einen zentralen Überblick über die Meilensteine von LDOS und ermöglicht eine verbesserte Ressourcenplanung und Budgetplanung, bevor die Hardware oder Software das Ende ihres Lebenszyklus erreicht. Auf diese Weise können Sie betriebliche Risiken deutlich reduzieren.

Bestandskennzeichnung

Die Bestandskennzeichnung bietet eine flexible Möglichkeit, Ihren Bestand mithilfe benutzerdefinierter Etiketten zu organisieren, zu filtern und entsprechend zu agieren. Tags können erstellt, geändert und Ressourcen zugewiesen werden. Account-Administratoren können Tags zentral verwalten. Sie können einzelnen Ressourcen Tags zuweisen oder den Bestand nach Tag filtern, um schnell die gewünschten Ressourcen zu finden.

Leistungsbeurteilungsmodul

Das Analysemodul bietet Einblick in Ihren Bestand, indem es die Ressourcen Ihres Unternehmens evaluiert. Es bietet Ihnen einen Rahmen, mit dem Sie Risiken in Bezug auf Sicherheit, Stabilität, Kapazität, Compliance und Alterung proaktiv untersuchen und minimieren können, um die Sicherheit von Netzwerken zu gewährleisten. Zu den wichtigsten Highlights gehören:

Sicherheitsempfehlungen

Mit den integrierten Sicherheitsberatern sind Sie potenziellen Bedrohungen immer einen Schritt voraus. Das System deckt proaktiv relevante Schwachstellen auf und stellt sicher, dass Sie über wichtige Updates informiert sind und umgehend Maßnahmen zum Schutz Ihres Netzwerks ergreifen können.

Sichern

Die Sicherheitsfunktionen bieten einen automatisierten Einblick in den Sicherheitsstatus Ihrer Netzwerkinfrastruktur in Echtzeit, indem Sie Ihre Ressourcen fortlaufend anhand der Cisco Leitfäden zur Betriebssystemsicherung bewerten. Jede Regel zur Sicherheitshärtung wird für alle abgedeckten Ressourcen bewertet, um Konfigurationsabweichungen zu erkennen. Die Ergebnisse werden nach Schweregrad priorisiert, damit Sie Sicherheitslücken schließen, die Ausfallsicherheit verbessern und das betriebliche Risiko reduzieren können.

Konfiguration

Evaluieren Sie Ihre Ressourcen anhand von Best Practices, die auf dem bewährten Know-how von Cisco basieren. So können Sie Abweichungen in der Konfiguration in Ihrer Infrastruktur erkennen, die sich auf Verfügbarkeit, Sicherheit oder Leistung auswirken können. Das System bewertet alle Best Practice-Regeln für die abgedeckten Ressourcen und priorisiert die Ergebnisse nach Schweregrad, um die Konsistenz der Konfiguration zu gewährleisten, die Ausfallsicherheit zu erhöhen und betriebliche Risiken zu reduzieren.

Problemhinweise

Problemhinweise bieten rechtzeitige, proaktive Benachrichtigungen zu Hardware- und Software-Updates. Durch die direkte Einbindung relevanter Problemhinweise in das Leistungsbeurteilungs-Dashboard ermöglicht diese Funktion die Behebung potenzieller Probleme, bevor sie sich auf Ihre Betriebsabläufe auswirken.

Funktionen mit KI

Cisco IQ VA bietet KI-gestützte Funktionen, die SaaS-taugliche KI-Einblicke direkt in Ihre Air-Gap-Umgebung liefern. Cisco IQ wird verbessert, da Rohdaten in aussagekräftige Erkenntnisse, Empfehlungen und Aktionen umgewandelt werden. Für KI-gestützte Funktionen ist ein Knoten erforderlich, der mit einer unterstützten Grafikverarbeitungseinheit ausgestattet ist. Diese Funktionen können nicht bei reinen CPU-Bereitstellungen aktiviert werden. Zu den Funktionen gehören:

- Ask AI Interface: Greifen Sie direkt in den Asset und Inventory Modulen auf interaktive KI-gestützte Erkenntnisse zu.
- LDOS: Sie können eine Liste vordefinierter Aufforderungen durchsuchen, um Zusammenfassungen zu erhalten, wichtige Ressourcen zu identifizieren oder Produktfamilien auf LDOS-Ressourcen (Last Date Of Support) zu analysieren.
- Wichtigste Erkenntnisse: Umwandlung von Daten aus Ressourcen und Analysen in aussagekräftige Erkenntnisse und Empfehlungen Integration in die Workflows zur Bereitstellung von Einblicken und Berichten in Echtzeit

Software-Lebenszyklus-Management

Sie können den Software-Lebenszyklus (Installation und Konfiguration) von Betriebsmodulen, Regeln, Berechtigungen und speziellen KI-basierten Funktionen innerhalb der VA verwalten. Sie können sie installieren, indem Sie die neuesten Versionen von Cisco IQ (SaaS) herunterladen. Gehen Sie dazu zu System Settings > Package Catalog (Systemeinstellungen > Paketkatalog).

Cisco IQ-Connector

Cisco IQ VA ist mit einem umfassenden Cisco IQ Connector ausgestattet, der eine flexible Erfassung von Telemetriedaten ermöglicht, die von direkten Verbindungen zu Geräten und von über das Cisco Catalyst Center verwalteten Geräten erfasst werden. Auf diese Weise wird die Netzwerktransparenz und -verwaltung verbessert. Zu den wichtigsten Highlights gehören:

Definieren von Geräten

Cisco IQ VA bietet flexible Optionen zur Definition des Geräteumfangs. Sie können Geräte angeben, indem Sie eine CSV-Datei hochladen, manuell eine kommagetrennte Liste eingeben, IP-Bereiche verwenden oder CDP (Cisco Discovery Protocol) oder LLDP (Link Layer Discovery Protocol) nutzen. Diese Liste kann jederzeit aktualisiert werden, um Geräte hinzuzufügen oder zu entfernen. So wird sichergestellt, dass Ihre Gerätegruppen aktuell bleiben.

Planen der Erkennung und Erfassung

Cisco IQ VA ermöglicht eine unabhängige Planung von Erkennungs- und Erfassungsprozessen und unterstützt dabei bestimmte Daten-, Zeit- und Wiederholungsmuster. Sie können diese Aufgaben separat konfigurieren, um sie an Ihre betrieblichen Workflows anzupassen. Darüber hinaus können Sie jederzeit eine On-Demand-Neuerkennung für einzelne Geräte durchführen, um die Datenaktualisierungszyklen besser kontrollieren und die Reaktionszeiten bei der Fehlerbehebung verkürzen zu können.

Unterstützte Hypervisoren

Cisco IQ VA unterstützt die Bereitstellung auf den folgenden Hypervisor-Plattformen. Stellen Sie vor der Bereitstellung sicher, dass Ihre Infrastruktur die Mindestanforderungen für die Hypervisor-Version erfüllt.

- VMware ESXi: Unterstützt für virtualisierte Standardumgebungen
- Microsoft Hyper-V Server: Unterstützt für Windows-basierte Virtualisierungs-Stacks
- Red Hat Kernel-basiertes virtuelles System: Unterstützt für Open-Source-Virtualisierungsumgebungen

Unterstützung von mehreren Knoten (nicht HA)

Cisco IQ VA unterstützt eine Multi-Node-Architektur ohne hohe Verfügbarkeit (HA) und ermöglicht so eine höhere Skalierbarkeit und Flexibilität für Ihre Bereitstellungsumgebungen. Die Multi-Node-Architektur bietet eine verteilte Architektur, die Management- und Mitarbeiterfunktionen voneinander trennt, sodass Sie Ihre Infrastruktur auf eine einzelne VA zuschneiden und erweitern können, um die Anforderungen größerer und komplexerer Workloads zu erfüllen. Der Managementknoten dient als primäre Schnittstelle für die Cluster-Registrierung, die Plattforminstallation und die Überwachung nach der Installation.

Benutzerverwaltung

Die folgenden Funktionen sollen die Benutzerverwaltungsprozesse vereinfachen und Benutzern eine bessere Kontrolle und Sicherheit innerhalb des Systems bieten.

Lokale Benutzerverwaltung

Benutzer können mehrere Benutzer mit unterschiedlichen Zugriffsberechtigungen sicher integrieren und verwalten. Lokale Benutzer, die von einem Administrator erstellt wurden, können die Option "Sign Up" (Anmelden) bei der ersten Anmeldung verwenden und ihr eigenes Kennwort mit der vom Administrator konfigurierten E-Mail-Adresse sicher einrichten.

Self-Service-Sicherheitsmanagement

Sie können die lokalen Sicherheitseinstellungen jetzt unabhängig verwalten und damit den Zugriff auf das Konto sowie die Wiederherstellung kontrollieren. Self-Service-Funktionen umfassen die Möglichkeit, vergessene Passwörter zurückzusetzen und Sicherheitsfragen zu konfigurieren, um die Benutzerumgebung zu optimieren und zu schützen, ohne dass externe Unterstützung erforderlich ist.

SAML-Konfiguration für sicheres SSO

Cisco IQ VA unterstützt sichere Single Sign-On (SSO)-Funktionen durch die Integration der Security Assertion Markup Language (SAML) v2.0-Authentifizierung. Diese Integration ermöglicht eine nahtlose Identitätsverbundfunktion mit Identitätsanbietern von Drittanbietern (IDP), sodass Sie Ihre vorhandenen Anmeldeinformationen für das Unternehmen verwenden können. Durch den Einsatz von SAML 2.0 können Organisationen die Sicherheit erhöhen, den Benutzerzugriff optimieren und das Identitätsmanagement in ihren Umgebungen vereinfachen. Es kann jeweils nur ein (1) IDP aktiv sein. Folgende IDPs werden derzeit unterstützt:

- Okta IDP
- ADFS-IDP
- Intra-IDP

Aktivitätsprotokolle

Alle Betriebsprotokolle werden lokal gespeichert und können von den Kontoadministratoren angezeigt werden. Dadurch wird die Überwachung der Benutzeraktivitäten vereinfacht und Transparenz gewährleistet.

Unterstützung für sicheres und Standard-NTP

Cisco IQ VA unterstützt sicheres und standardmäßiges Network Time Protocol (NTP). Das sichere NTP ermöglicht die authentifizierte und verschlüsselte Zeitsynchronisierung zwischen Cisco IQ VA und vertrauenswürdigen NTP-Servern. Das Standard-NTP hingegen ermöglicht die

Synchronisierung von Umgebungen, in denen die Authentifizierung für verschlüsselte NTP-Datenaustausch nicht erforderlich ist oder nicht unterstützt wird.

Benutzerdefinierte SSL-Zertifikatunterstützung

Cisco IQ VA unterstützt die Installation und Verwaltung von benutzerdefinierten SSL-Zertifikaten. Mit dieser Funktion können Kontoadministratoren Standardzertifikate durch Zertifikate ersetzen, die von der Zertifizierungsstelle ihrer Organisation ausgestellt wurden. Durch die Verwendung benutzerdefinierter Zertifikate können Sie eine sichere und vertrauenswürdige Kommunikation sicherstellen und die vollständige Einhaltung der internen Sicherheitsrichtlinien Ihres Unternehmens gewährleisten. Derzeit kann jeweils nur ein (1) SSL-Zertifikat installiert und aktiv sein.

Unterstützung für externe Syslog-Server

Cisco IQ VA unterstützt die Integration mit externen Syslog-Servern und ermöglicht Kontoadministratoren die Weiterleitung von Systemprotokollen an eine zentralisierte Protokollierungsplattform. Diese Erweiterung vereinfacht die Überwachung, das Auditing und die Fehlerbehebung, indem eine konsistente und konsolidierte Ansicht der Systemereignisse und Sicherheitsprotokolle in der gesamten Infrastruktur bereitgestellt wird. Es können bis zu zwei (2) Syslog-Server gleichzeitig konfiguriert werden.

Anmelde- und benutzerdefiniertes Banner

Cisco IQ VA bietet jetzt eine konfigurierbare Banner-Funktion. Kontoadministratoren können erforderliche Systembenachrichtigungen und Sicherheitswarnungen auf dem Anmeldebildschirm konfigurieren und anzeigen. Darüber hinaus können Kontoadministratoren angepasste Banner in Cisco IQ VA konfigurieren und anzeigen. Diese Funktion ermöglicht die direkte Übermittlung wichtiger Informationen (z. B. Benachrichtigungen, Haftungsausschlüsse oder Warnungen) an Benutzer in Cisco IQ VA.

Systemverwaltung

Sie können die neuesten Cisco IQ VA-Updates über die Registerkarte "Systemverwaltung" anzeigen und installieren und so einfach auf die neuesten Funktionen, Verbesserungen und Verbesserungen zugreifen. Cisco IQ VA unterstützt sowohl automatische Software-Updates per Push von Cisco IQ als auch manuelle Software-Updates. Für manuelle Updates können Sie die Softwarepakete direkt von Cisco IQ (SaaS) herunterladen, indem Sie zu Systemeinstellungen > Paketkatalog navigieren.

Bekannte Probleme

Die folgenden Probleme werden derzeit aktiv in Cisco IQ VA gelöst.

Das Feld "Recurring Schedule" zeigt die UNIX-Cron-Syntax an.

Derzeit ist für die regelmäßige Zeitplaneingabe zum Hochladen von Netzwerksan-Dateien ein UNIX-Cron-Ausdruck mit fünf (5) Feldern erforderlich (z. B. "0 2 * * *"). Für Benutzer, die mit der Cron-Syntax nicht vertraut sind, ist dieses Eingabeformat möglicherweise unklar. Benutzer können jedoch detailliertere Informationen zur Cron-Syntax und Beispiele online abrufen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.