

Cisco IQ Virtual Appliance 릴리스 노트 v1.2.4

소개

Cisco IQ™은 고객에게 자산 가시성을 개선하고 환경 전반에서 더 스마트한 통찰력을 제공하도록 설계된 기능을 제공합니다. 또한 AI Assistant와 같은 AI 기능은 사용자가 사전 대응적이고 정보에 입각한 결정을 내리고 고객 참여와 성공을 위한 프로세스를 간소화하는 상황 인식 기능을 제공하여 운영 성과와 Cisco IQ 사용자 경험을 최적화합니다.

Cisco IQ On-Prem Air-Gapped는 클라우드에 연결할 수 없는 환경을 위해 설계된 Cisco IQ의 구축 모드입니다. Cisco IQ SaaS에서 가져온 소프트웨어 업데이트 및 유지 보수 패키지를 사용하여, 외부 네트워크와 완전히 격리된 상태로 고객의 프레미스 내에서 실행되는 Cisco IQ VA(Virtual Appliance)라고 하는 일체형 VM(Virtual Machine)으로 제공되며, 승인된 수동 프로세스를 통해 VA로 전송됩니다.

VA는 규정 준수, 높은 보안, 주권 환경에서 운영되는 조직의 경우 통찰력과 통제력 사이의 상충점을 제거합니다. 고객은 자체 네트워크 내에 Cisco IQ 자산 및 평가 기능을 구축하고 데이터에 대한 완전한 소유권을 유지하는 동시에, Cisco IQ에서 기대하는 통찰력과 권장 사항을 얻을 수 있습니다. Air-Gapped 구축 모드는 Cisco IQ SaaS의 기능을 격리된 환경으로 확장하여 미션 크리티컬 팀이 클라우드에 연결된 엔터프라이즈의 속도 및 진단 인텔리전스를 사용하여 운영할 수 있도록 합니다.

이 문서에서는 Cisco IQ VA v1.2.4의 새로운 기능, 모듈 지원 및 알려진 문제에 대해 간략하게 설명합니다.

주요 특징

Assets 모듈

Assets 모듈은 Cisco 자산에 대한 포괄적인 가시성 및 관리 기능을 제공하며 Cisco IQ의 기반으로 조직 내 모든 장치에 대한 중앙 집중식 목록을 제공합니다. 여러 소스에서 정보를 수집하므로 디바이스 인벤토리에 대한 단일 정보 소스 역할을 합니다. 다운로드 설치 프로그램의 일부로 제공되며 VA가 설치되면 사용할 수 있습니다. 주요 내용은 다음과 같습니다.

자산 중요도 인사이트

Asset Criticality Insights를 통해 Assets 모듈은 네트워크 장치의 기능적 역할과 비즈니스 중요성을 예측할 수 있습니다. Asset Criticality Insights는 디바이스 컨피그레이션 및 활성화된 기능을 분석하

여 네트워크에 가장 큰 영향을 미치는 자산을 식별함으로써 보안 개선, 소프트웨어 업그레이드, EoL/EoS 계획 및 커버리지 결정에 우선 순위를 지정할 수 있도록 합니다.

서비스 계약

Service Contracts(서비스 계약) 페이지에서는 지원 계약에 대한 중앙 집중식 관리 기능을 제공합니다. 주요 기능은 다음과 같습니다.

- 서비스 계약 감독: 포괄적인 계약 요약과 세부 데이터로 갱신 계획 및 커버리지 전략을 간소화
- 자산별 통찰력: 자산에 직접 연결된 명확하고 실행 가능한 데이터를 통해 취약성을 더 빠르게 식별 및 완화

LDOS 대시보드

LDOS(Last Date Of Support) 대시보드는 LDOS 주요 시점을 중앙에서 볼 수 있으며 하드웨어 또는 소프트웨어가 단종되기 전에 자산 계획 및 예산 예측을 향상시켜 운영 위험을 크게 줄일 수 있습니다.

자산 태깅

자산 태깅은 사용자 지정 레이블을 사용하여 인벤토리를 구성, 필터링 및 수행할 수 있는 유연한 방법을 제공합니다. 어카운트 관리자가 중앙 집중식 태그 관리를 사용하여 태그를 만들고 수정하고 자산에 할당할 수 있습니다. 개별 자산에 태그를 할당하거나 대량으로 할당할 수 있으며, 원하는 자산을 신속하게 찾기 위해 인벤토리를 태그별로 필터링할 수 있습니다.

평가 모듈

평가 모듈은 조직의 자산을 평가하여 인벤토리에 대한 가시성을 제공하고 보안, 안정성, 용량, 규정 준수, 노후화와 관련된 위험을 사전에 조사하고 완화할 수 있는 프레임워크를 제공하여 네트워크의 보안을 유지합니다. 주요 내용은 다음과 같습니다.

보안 자문

Integrated Security Advisories를 통해 잠재적 위협에 한발 앞서 대처할 수 있습니다. 시스템에서 사전에 관련 취약성을 찾아내 중요 업데이트에 대한 정보를 얻고 네트워크를 보호하기 위한 즉각적인 조치를 취할 수 있도록 합니다.

보안 강화

Security Hardening은 Cisco OS Hardening Guides를 기준으로 자산을 지속적으로 평가하여 네트워크 인프라의 보안 상태에 대한 자동화된 실시간 가시성을 제공합니다. 각 보안 강화 규칙은 지원되는 자산 전반에서 평가되어 구성 편차를 탐지하고 심각도별로 우선 순위를 지정하여 보안 허점을 해결하고 복원력을 향상하며 운영 위험을 줄이는 데 도움이 됩니다.

설정

Cisco의 검증된 전문성을 기반으로 권장 모범 사례와 비교하여 자산을 평가하여 가용성, 보안 또는 성능에 영향을 미칠 수 있는 인프라 전반의 컨피그레이션 편차를 탐지합니다. 시스템은 지원 대상 자산의 전 범위에서 각 모범 사례 규칙을 평가하고, 심각도별로 검색 결과의 우선 순위를 지정하여 구성 일관성을 보장하고, 탄력성을 강화하고, 운영 위험을 줄일 수 있도록 지원합니다.

필드 알림

Field Notice는 하드웨어 및 소프트웨어 업데이트에 대한 사전 대응적 알림을 적시에 제공합니다. Assessments(평가) 대시보드 내에서 관련 Field Notice(필드 알림)를 직접 표시하면 잠재적인 문제가 운영에 영향을 미치기 전에 해결할 수 있습니다.

AI 기반 기능

Cisco IQ VA는 AI로 구동되는 기능을 제공하여 SaaS급 AI 인사이트를 에어 갭(air-gapped) 환경에 직접 제공합니다. 원시 데이터를 실행 가능한 통찰력, 권장 사항 및 안내 작업으로 변환하여 Cisco IQ를 향상합니다. AI로 구동되는 기능에는 지원되는 그래픽 처리 장치가 장착된 노드가 필요합니다. 이러한 기능은 CPU 전용 구축에서 활성화할 수 없습니다. 다음과 같은 기능을 제공합니다.

- Ask AI Interface: Assets and Inventory 모듈 내에서 직접 대화형 AI로 통찰력을 얻으십시오.
- LDOS: 미리 정의된 프롬프트 목록을 탐색하여 요약물 얻거나, 중요한 자산을 식별하거나, LDOS 자산에 대한 제품군을 분석할 수 있습니다
- 주요 정보: 자산 및 평가 데이터를 실행 가능한 통찰력 및 권장 사항으로 변환합니다. 워크플로에 통합되어 실시간 통찰력 및 보고서 제공

소프트웨어 라이프사이클 관리

VA 내에서 운영 모듈, 규칙, 자격, AI로 구동되는 특수 기능의 소프트웨어 라이프사이클(설치 및 구성)을 관리할 수 있습니다. 시스템 설정 > 패키지 카탈로그로 이동하여 Cisco IQ(SaaS)에서 최신 버전을 다운로드하여 설치할 수 있습니다.

Cisco IQ 커넥터

Cisco IQ VA에는 포괄적인 Cisco IQ Connector가 장착되어 있으므로, 장치에 직접 연결하고 Cisco Catalyst Center를 통해 관리되는 장치에서 유연한 텔레메트리 데이터 수집을 통해 네트워크 가시성 및 관리를 개선할 수 있습니다. 주요 내용은 다음과 같습니다.

디바이스 정의

Cisco IQ VA는 디바이스 범위를 정의하기 위한 유연한 옵션을 제공합니다. CSV 파일을 업로드하고, 쉼표로 구분된 목록을 수동으로 입력하고, IP 범위를 사용하거나 CDP(Cisco Discovery Protocol) 또는 LLDP(Link Layer Discovery Protocol)를 활용하여 디바이스를 지정할 수 있습니다. 이 목록은 언제든지 업데이트하여 디바이스를 추가 또는 제거할 수 있으므로 디바이스 그룹이 최신 상태를 유지하도록 합니다.

검색 및 수집 예약

Cisco IQ VA는 검색 및 수집 프로세스를 위한 독립적인 스케줄링을 활성화하여 특정 날짜, 시간 및 반복 패턴을 지원합니다. 이러한 작업을 별도로 구성하여 운영 워크플로에 맞출 수 있습니다. 또한 언제든지 개별 디바이스에 대한 온디맨드 재검색을 수행하여 데이터 갱신 주기를 보다 효과적으로 제어하고 문제 해결을 위한 응답 시간을 단축할 수 있습니다.

지원되는 하이퍼바이저

Cisco IQ VA는 다음과 같은 하이퍼바이저 플랫폼에서 구축을 지원합니다. 구축을 시작하기 전에 인프라가 특정 하이퍼바이저의 최소 버전 요구 사항을 충족하는지 확인하십시오.

- VMware ESXi: 표준 가상 환경에서 지원됨
- Microsoft Hyper-V Server: Windows 기반 가상화 스택에서 지원됨
- Red Hat Kernel 기반 VM: 오픈 소스 가상화 환경에서 지원

비HA 다중 노드 지원

Cisco IQ VA는 Non-High Availability(HA) 멀티 노드 아키텍처를 지원하여 구축 환경에 더 우수한 확장성과 유연성을 제공합니다. 멀티 노드는 관리 기능과 작업자 기능을 분리하는 분산형 아키텍처를 제공하여 더 크고 복잡한 워크로드 요구 사항에 맞게 인프라를 단일 VA 이상으로 맞춤화하고 확장할 수 있습니다. 관리 노드는 클러스터 등록, 플랫폼 설치 및 설치 후 모니터링을 위한 기본 인터페이스 역할을 합니다.

사용자 관리

다음 기능은 사용자 관리 프로세스를 간소화하여 시스템 내에서 사용자를 더 효과적으로 제어하고 보호하는 데 목적이 있습니다.

로컬 사용자 관리

사용자는 고유한 액세스 권한을 가진 여러 사용자를 안전하게 온보딩하고 관리할 수 있습니다. 관리자가 생성한 로컬 사용자는 첫 번째 로그인 시 Sign Up(등록) 옵션을 사용하고 관리자가 구성된 이메일 주소를 사용하여 비밀번호를 안전하게 설정할 수 있습니다.

셀프 서비스 보안 관리

이제 로컬 보안 설정을 독립적으로 관리하여 계정 액세스 및 복구를 제어할 수 있습니다. 셀프 서비스 기능에는 잊어버린 비밀번호를 재설정하고 보안 질문을 구성할 수 있는 기능이 포함되어 있어 외부 지원 없이도 더욱 간소화되고 안전한 사용자 경험을 제공할 수 있습니다.

보안 SSO를 위한 SAML 컨피그레이션

Cisco IQ VA는 SAML(Security Assertion Markup Language) v2.0 인증을 통합하여 보안 SSO(Single Sign-On) 기능을 지원합니다. 이러한 통합을 통해 타사 IDP(Identity Providers)와의 원활한 ID 페더레이션을 지원하므로 기존 엔터프라이즈 자격 증명을 사용하여 인증할 수 있습니다. SAML v2.0을 활용하여 보안을 강화하고 사용자 액세스를 간소화하며 환경 전반의 ID 관리를 간소화할 수 있습니다. 지정된 시간에 하나의 IDP만 활성화할 수 있습니다. 다음 IDP가 현재 지원됩니다.

- 옥타
- AD FS IDP
- 엔트라 IDP

작업 로그

모든 운영 로그는 로컬에 저장되며 계정 관리자가 볼 수 있으므로 사용자 활동을 손쉽게 모니터링하고 투명성을 보장할 수 있습니다.

보안 및 표준 NTP 지원

Cisco IQ VA는 보안 및 표준 NTP(Network Time Protocol)를 모두 지원합니다. 보안 NTP는 Cisco IQ VA와 신뢰할 수 있는 NTP 서버 간의 인증 및 암호화된 시간 동기화를 지원하는 반면, 표준 NTP는 암호화된 NTP 교환에 인증이 필요하지 않거나 지원되지 않는 환경에 대한 동기화를 제공합니다.

맞춤형 SSL 인증서 지원

Cisco IQ VA는 맞춤형 SSL 인증서의 설치 및 관리를 지원합니다. 이 기능을 통해 계정 관리자는 기본 인증서를 조직의 CA(Certificate Authority)에서 발급한 인증서로 교체할 수 있습니다. 사용자 지정 인증서를 사용하면 안전하고 신뢰할 수 있는 통신을 보장하고 조직의 내부 보안 정책을 완벽하게 준수할 수 있습니다. 현재 SSL 인증서는 한 번에 하나만 설치하고 활성화할 수 있습니다.

외부 Syslog 서버 지원

Cisco IQ VA는 외부 Syslog 서버와의 통합을 지원하므로 계정 관리자가 중앙 집중식 로깅 플랫폼에 시스템 로그를 전달할 수 있습니다. 이러한 기능 향상은 인프라 전반의 시스템 이벤트 및 보안 로그에 대한 지속적이고 통합된 보기를 제공함으로써 모니터링, 감사 및 문제 해결을 간소화합니다. 지정된 시간에 최대 2개의 syslog 서버를 구성할 수 있습니다.

로그인 및 사용자 지정 배너

Cisco IQ VA는 이제 구성 가능한 배너 기능을 제공합니다. 계정 관리자는 로그인 화면에서 필수 시스템 알림 및 보안 경고를 구성하고 표시할 수 있습니다. 또한 어카운트 관리자는 Cisco IQ VA에서 맞춤형 배너를 구성하고 표시할 수 있습니다. 이 기능을 사용하면 Cisco IQ VA 내의 사용자에게 중요한 정보(예: 알림, 면책조항 또는 알림)를 직접 전달할 수 있습니다.

시스템 관리

System Management(시스템 관리) 탭을 통해 최신 Cisco IQ VA 업데이트를 보고 설치할 수 있으며, 이를 통해 최신 기능, 개선 사항 및 개선 사항에 쉽게 액세스할 수 있습니다. Cisco IQ VA는 Cisco IQ에서 푸시되는 자동 소프트웨어 업데이트와 수동 소프트웨어 업데이트를 모두 지원합니다. 수동 업데이트의 경우 시스템 설정 > 패키지 카탈로그로 이동하여 Cisco IQ(SaaS)에서 소프트웨어 패키지를 직접 다운로드할 수 있습니다.

알려진 문제

Cisco IQ VA에서는 다음과 같은 문제를 적극적으로 다루고 있습니다.

반복 일정 필드에 UNIX Cron 구문이 표시됩니다.

현재 네트워크 스캔 파일 업로드를 위해 반복되는 일정 입력을 위해서는 5개의 필드가 있는 UNIX cron 식이 필요합니다(예: "0 2 * * *"). cron 구문에 익숙하지 않은 사용자는 이 입력 포맷이 불분명하다는 것을 발견할 수 있다. 그러나 사용자는 온라인에서 cron 구문 및 예제에 대한 자세한 정보를 얻을 수 있습니다.

대규모 구축의 일부 장비에 대한 간헐적인 인벤토리 수집 실패

현재 디바이스 수가 10,000개를 초과하는 구축에서는 성공적인 검색 프로세스에도 불구하고 일부 디바이스가 인벤토리 수집을 수행하지 못할 수 있습니다. 이를 해결하려면 시스템에서 장애가 발생한 디바이스를 제거한 다음 다시 추가합니다. 추가 도움말은 Cisco TAC(Technical Assistance Center)에 문의하십시오.

수집 중에 자격 업로드 상태가 표시되지 않음

현재, 엔타이틀먼트 파일을 업로드한 후, UI에 엔타이틀먼트가 성공적으로 로드 및 처리되었음을 나타내는 명확한 표시가 없습니다. 자격이 완전히 처리되기 전에 수집을 시작하면 검사 실패가 발생할 수 있습니다. 이를 해결하려면, 업로드가 끝난 후 최소 1시간 동안 기다렸다가 수집을 실행합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.