

Notas de versão do Cisco IQ Virtual Appliance v1.2.0

Introdução

O Cisco IQTM oferece aos clientes aprimoramentos e recursos projetados para melhorar a visibilidade de ativos, fornecer insights mais inteligentes em seus ambientes e simplificar o gerenciamento de casos. Além disso, os recursos de IA, como o AI Assistant, otimizam os resultados operacionais e a experiência do usuário do Cisco IQ, fornecendo entendimento contextual que capacita os usuários a tomar decisões proativas e informadas e simplifica os processos para o envolvimento e o sucesso do cliente.

O Cisco IQ On-Prem Air-Gapped é um dos modos de implantação do Cisco IQ, projetado para clientes em setores altamente regulamentados com requisitos rigorosos de conformidade, domínio sobre dados e segurança. Nesse modo, o Cisco IQ é fornecido como uma máquina virtual (VM) independente, conhecida como Cisco IQ Virtual Appliance (VA). O VA é executado inteiramente nas instalações do cliente e opera em total isolamento de redes externas. Para manter esse isolamento, as atualizações de software e os pacotes de manutenção são obtidos do Cisco IQ SaaS e transferidos para o VA por meio de um processo aprovado e manual.

Este documento descreve novos recursos, suporte a módulos e problemas conhecidos do Cisco IQ VA v1.2.0.

 **Note:** O Cisco IQ VA está atualmente limitado a clientes inscritos no programa de disponibilidade controlada. O acesso de download para o software do sistema VA e pacotes operacionais adicionais (módulos, regras e direitos) do portal Cisco IQ está disponível exclusivamente para clientes selecionados. Entre em contato com seu representante de conta para obter mais informações.

Principais destaques

Módulo Ativos

O módulo Ativos oferece visibilidade abrangente e recursos de gerenciamento para ativos da Cisco e serve como base do Cisco IQ, fornecendo uma lista centralizada de todos os dispositivos em uma organização. Coletando informações de várias fontes, ele atua como uma única fonte verdadeira para o inventário de dispositivos. Ele está disponível como parte do instalador baixado

e estará disponível para uso depois que o VA for instalado. Os principais destaques incluem:

Insights sobre a importância dos ativos

Os Asset Criticality Insights permitem que o módulo Ativos preveja a função funcional e a importância comercial dos dispositivos de rede. Analisando as configurações de dispositivos e os recursos ativados, os Asset Criticality Insights ajudam a identificar quais ativos têm o maior impacto na rede, permitindo que você priorize-os para correção de segurança, atualizações de software, planejamento de fim da vida útil/fim do suporte e decisões de cobertura.

Contratos de serviço

A página Contratos de serviço oferece supervisão centralizada dos contratos de suporte. Os principais recursos incluem:

- Supervisão do contrato de serviço: Simplificar o planejamento de renovação e as estratégias de cobertura com resumos de contrato abrangentes e dados detalhados
- Informações específicas do ativo: Identifique e reduza vulnerabilidades mais rapidamente com dados claros e acionáveis vinculados diretamente aos seus ativos

Painel LDOS

O painel do LDOS oferece uma visão centralizada dos marcos do LDOS e permite um melhor planejamento de ativos e previsão de orçamento antes que o hardware ou software chegue ao fim da vida útil, permitindo que você reduza significativamente o risco operacional.

Marcação de ativos

A marcação de ativos oferece uma maneira flexível de organizar, filtrar e atuar em seu inventário usando rótulos personalizados. As marcas podem ser criadas, modificadas e atribuídas a ativos, com o gerenciamento centralizado de marcas disponível para administradores de conta. Você pode atribuir etiquetas a ativos individuais ou em massa, bem como filtrar seu inventário por etiqueta para localizar rapidamente os ativos desejados.

Módulo de avaliações

O módulo de avaliações oferece visibilidade do inventário avaliando os ativos da empresa e

oferece uma estrutura que permite investigar e reduzir proativamente os riscos relacionados à segurança, estabilidade, capacidade, conformidade e envelhecimento, ajudando a manter as redes seguras. Os principais destaques incluem:

Orientações de Segurança

As Recomendações de Segurança Integradas permitem que você fique à frente de possíveis ameaças. O sistema detecta proativamente vulnerabilidades relevantes, garantindo que você seja informado sobre atualizações críticas e possa tomar medidas imediatas para proteger sua rede.

Fortalecimento da segurança

O Security Hardening fornece visibilidade automatizada e em tempo real da postura de segurança da sua infraestrutura de rede, avaliando continuamente seus ativos em relação aos Guias de proteção do SO da Cisco. Cada regra de proteção de segurança é avaliada em todos os ativos cobertos para detectar desvios de configuração, com descobertas priorizadas por gravidade para ajudá-lo a lidar com falhas de segurança, aumentar a resiliência e reduzir o risco operacional

Configuração

Avalie seus ativos em relação às práticas recomendadas, com base na experiência comprovada da Cisco, para detectar desvios de configuração em sua infraestrutura que possam afetar a disponibilidade, a segurança ou o desempenho. O sistema avalia cada regra de prática recomendada nos ativos cobertos, priorizando as descobertas por gravidade para ajudar a garantir a consistência da configuração, aumentar a resiliência e reduzir o risco operacional.

Field Notices

Os avisos de campo fornecem notificações oportunas e proativas com relação a atualizações de hardware e software. Ao exibir avisos de campo relevantes diretamente no painel de avaliação, esse recurso permite que você resolva possíveis problemas antes que eles afetem suas operações.

Recursos acionados por IA

O Cisco IQ VA oferece recursos ativados por IA, trazendo insights de IA de nível SaaS diretamente para seu ambiente totalmente isolado. Ele eleva o Cisco IQ transformando dados brutos em insights práticos, recomendações e ações guiadas. Os recursos com IA exigem um nó equipado com uma unidade de processamento gráfico suportada. Esses recursos não podem ser

habilitados em implantações somente de CPU. Os recursos incluem:

- Pergunte à interface de IA: acesse informações interativas baseadas em IA diretamente nos módulos Ativos e Inventário.
- LDOS: você pode procurar uma lista de solicitações predefinidas para obter resumos, identificar ativos críticos ou analisar famílias de produtos para ativos LDOS (Última data de suporte)
- Principais insights: Transforme os dados de ativos e avaliações em percepções e recomendações acionáveis. Integrado aos fluxos de trabalho para fornecer informações e relatórios em tempo real

Gerenciamento do ciclo de vida do software

Você pode gerenciar o ciclo de vida do software (instalação e configuração) de módulos operacionais, regras, direitos e recursos especializados com IA dentro do VA. Você pode instalá-los fazendo o download das versões mais recentes do Cisco IQ (SaaS) navegando até Configurações do sistema > Catálogo de pacotes.

Conector Cisco IQ

O Cisco IQ VA é equipado com um Cisco IQ Connector abrangente, permitindo a coleta flexível de dados de telemetria de conexões diretas para dispositivos e de dispositivos gerenciados através do Cisco Catalyst Center para aprimorar a visibilidade e o gerenciamento da rede. Os principais destaques incluem:

Definindo dispositivos

O Cisco IQ VA oferece opções flexíveis para definir o escopo do seu dispositivo. Você pode especificar dispositivos carregando um arquivo CSV, inserindo manualmente uma lista separada por vírgulas, usando intervalos de IP ou aproveitando o CDP (Cisco Discovery Protocol) ou o LLDP (Link Layer Discovery Protocol). Essa lista pode ser atualizada a qualquer momento para adicionar ou remover dispositivos, garantindo que seus grupos de dispositivos permaneçam atualizados.

Agendamento de descoberta e coleta

O Cisco IQ VA permite o agendamento independente para processos de descoberta e coleta, suportando datas, horas e padrões de recorrência específicos. Você pode configurar essas

tarefas separadamente para alinhá-las aos fluxos de trabalho operacionais. Além disso, você pode executar a redetecção sob demanda para dispositivos individuais a qualquer momento, fornecendo maior controle sobre os ciclos de atualização de dados e tempos de resposta mais rápidos para a solução de problemas.

Hipervisores compatíveis

O Cisco IQ VA suporta a implantação nas seguintes plataformas de hipervisor. Certifique-se de que sua infraestrutura atenda aos requisitos mínimos de versão para seu hipervisor específico antes de iniciar a implantação.

- VMware ESXi: compatível com ambientes virtualizados padrão
- Microsoft Hyper-V Server: compatível com pilhas de virtualização baseadas em Windows
- VM baseada em Kernel da Red Hat: compatível com ambientes de virtualização de código aberto

Suporte a vários nós sem alta disponibilidade

O Cisco IQ VA suporta arquitetura de vários nós sem alta disponibilidade (HA), permitindo maior escalabilidade e flexibilidade para seus ambientes de implantação. O multi-nó oferece uma arquitetura distribuída que separa as funções de gerenciamento e de funcionário, permitindo que você adapte e estenda sua infraestrutura além de um único VA para atender às demandas de cargas de trabalho maiores e mais complexas. O nó de gerenciamento serve como a interface principal para registro de cluster, instalação de plataforma e monitoramento pós-instalação.

Gerenciamento de usuários

Os recursos a seguir têm como objetivo simplificar os processos de gerenciamento de usuários, fornecendo melhor controle e segurança para os usuários no sistema.

Gerenciamento de usuários locais

Os usuários podem integrar e gerenciar vários usuários com privilégios de acesso distintos com segurança. Os usuários locais criados por um administrador podem usar a opção "Inscrever-se" durante o primeiro login e definir suas próprias senhas com segurança usando o endereço de e-mail configurado pelo administrador.

Gerenciamento de segurança self-service

Agora você pode gerenciar as configurações de segurança locais de forma independente, fornecendo controle sobre o acesso e a recuperação da conta. Os recursos de autoatendimento incluem a capacidade de redefinir senhas esquecidas e configurar perguntas de segurança, permitindo uma experiência de usuário mais simplificada e segura sem exigir suporte externo.

Configuração SAML para SSO Seguro

O Cisco IQ VA suporta recursos seguros de Single Sign-On (SSO) integrando a autenticação Security Assertion Markup Language (SAML) v2.0. Essa integração permite a federação de identidade transparente com Provedores de Identidade de terceiros (IDP), permitindo que você se autentique usando suas credenciais corporativas existentes. Aproveitando o SAML v2.0, as organizações podem aprimorar a segurança, simplificar o acesso do usuário e simplificar o gerenciamento de identidades em seus ambientes. Apenas um (1) IDP pode estar ativo em um determinado momento. Os seguintes IDPs são suportados atualmente:

- IDP Okta
- IDP ADFS
- Entra IDP

Logs de atividade

Todos os registros operacionais são armazenados localmente e podem ser visualizados pelos administradores de contas, permitindo o fácil monitoramento das atividades dos usuários e garantindo a transparência.

Suporte para NTP padrão e seguro

O Cisco IQ VA suporta Network Time Protocol (NTP) seguro e padrão. O NTP seguro permite a sincronização de tempo autenticada e criptografada entre o Cisco IQ VA e servidores NTP confiáveis, enquanto o NTP padrão oferece sincronização para ambientes onde a autenticação não é necessária ou não é suportada para trocas de NTP criptografado.

Suporte ao certificado SSL personalizado

O Cisco IQ VA suporta a instalação e o gerenciamento de certificados SSL personalizados. Este

recurso permite que os administradores de conta substituam os certificados padrão pelos certificados emitidos pela autoridade de certificação (CA) de sua organização. Ao usar certificados personalizados, você pode garantir uma comunicação segura e confiável e manter total conformidade com as políticas de segurança internas da sua empresa. Atualmente, apenas um (1) certificado SSL pode ser instalado e ativo em um determinado momento.

Suporte para servidores syslog externos

O Cisco IQ VA suporta integração com servidores Syslog externos, permitindo que os administradores de conta encaminhem logs do sistema para uma plataforma de registro centralizada. Esse aprimoramento simplifica o monitoramento, a auditoria e a solução de problemas, fornecendo uma visualização consolidada e persistente dos eventos do sistema e registros de segurança em toda a infraestrutura. Até dois (2) servidores syslog podem ser configurados a qualquer momento.

Login e banner personalizado

O Cisco IQ VA agora oferece um recurso de banner configurável. Os administradores de conta podem configurar e exibir notificações de sistema obrigatórias e avisos de segurança na tela de login. Além disso, os administradores de conta podem configurar e exibir banners personalizados no Cisco IQ VA. Esse recurso permite a comunicação de informações importantes (por exemplo, notificações, avisos de isenção de responsabilidade ou alertas) diretamente para usuários no Cisco IQ VA.

Gerenciamento do sistema

Você pode visualizar e instalar as atualizações mais recentes do Cisco IQ VA através da guia System Management, fornecendo acesso fácil aos recursos mais recentes, melhorias e aprimoramentos. O Cisco IQ VA suporta atualizações de software automáticas enviadas do Cisco IQ e atualizações de software manuais. Para atualizações manuais, você pode baixar os pacotes de software diretamente do Cisco IQ (SaaS) navegando para Configurações do sistema > Catálogo de pacotes.

Problemas conhecidos

Os problemas a seguir estão sendo tratados ativamente no Cisco IQ VA.

Campo Programação Recorrente Exibe Sintaxe Cron UNIX

Atualmente, a entrada de agendamento recorrente para carregamentos de arquivos de verificação de rede requer uma expressão cron UNIX com cinco (5) campos (por exemplo, "0 2 * * *"). Usuários não familiarizados com a sintaxe cron podem achar este formato de entrada incerto. No entanto, os usuários podem obter informações mais detalhadas sobre a sintaxe cron e exemplos on-line.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.