Gerenciador de segurança 4.3: Problemas comuns e soluções IPS

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Produtos Relacionados
Não pode conectar ao IPS
Problema
Solução
Sensor AIP-SSM não reconhecido após a elevação a 7.1(6)E4
Problema
Solução
Assinaturas IPS actualizadas não automaticamente dentro do período de graça
Problema
Solução
Número grande de requisições RADIUS aos dispositivos IPS
Problema
Solução
Informações Relacionadas

Introdução

Este documento descreve problemas e solução comuns às edições do Sistema de prevenção de intrusões da Cisco (IPS) no Cisco Security Manager.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 4.3 do Cisco Security Manager.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento descreve os problemas comuns encontrados no Cisco Security Manager 4.3. Quando este documento se centrar sobre a versão 4.3 do Cisco Security Manager, é possível que os mesmos problemas e soluções se aplicam a outras versões também.

Não pode conectar ao IPS

Problema

Você pode já não conectar ao IPS através do Cisco Security Manager. Contudo, você pode conectar ao Shell Seguro (ssh) e ao gerenciador de dispositivo IPS (IDM) do server do Cisco Security Manager.

Solução

Verifique que o IPS usa um certificado X.509 atual. Execute o **comando show version no** IPS CLI a fim verificar a versão do certificado. Se o certificado expirou, execute o comando da gerar-**chave dos tls** a fim obter um certificado novo. Depois que você gerencie a chave, importe o certificado IPS.

Sensor AIP-SSM não reconhecido após a elevação a 7.1(6)E4

Problema

Depois que você promove seu módulo avançado ASA do módulo de Serviços de segurança da inspeção e da prevenção de Cisco (AIP-SSM) à versão 7.1(6)E4 na versão 4.3 do Cisco Security Manager, o Cisco Security Manager não reconhece o sensor AIP-SSM.

Solução

A fim resolver este problema, você deve instalar o pacote de serviços 1 da versão 4.3 do Cisco Security Manager, ou o pacote de serviços 2, ao server do Cisco Security Manager de modo que apoie seu AIP-SSM com os 7.1 IPS do software.

Assinaturas IPS actualizadas não automaticamente dentro do

período de graça

Problema

O Cisco Security Manager não atualiza automaticamente seu evento das assinaturas IPS embora seu IPS se realize ainda dentro do período de graça.

Solução

O Cisco Security Manager não atualiza assinaturas automaticamente se o sensor se realiza dentro do período de graça. A fim resolver este problema, escolha **ferramentas > aplicam atualizações IPS na** relação do Cisco Security Manager para atualizar manualmente as assinaturas.

Número grande de requisições RADIUS aos dispositivos IPS

Problema

Você vê um grande número requisições RADIUS do Cisco Security Manager a seus dispositivos IPS.

Solução

Esta edição ocorre quando o Cisco Security Manager vota rapidamente dispositivos monitorados. À revelia, as versões afetadas da característica do monitoramento de evento (eventing) no Cisco Security Manager podem tentar votar por segundo dispositivos monitorados diversas vezes. Se outras características da monitoração do Cisco Security Manager (saúde e monitoramento de desempenho e/ou gerente do relatório) são permitidas, as votações adicionais do dispositivo ocorrem.

A fim resolver este problema, você pode mudar o tempo de espera do padrão (intervalo do sono). O intervalo do sono do padrão entre votações do dispositivo é ajustado a 250ms à revelia. Este valor pode ser mudado manualmente a um valor maior, mais razoável. A fim mudar o valor de tempo de espera, edite o arquivo communication.properties no server do Cisco Security Manager; este arquivo é encontrado em < NMSROOT> \ *CDM* \ eventing \ configuração \ communication.properties.

No arquivo communication.properties, substitua SLEEP_INTERVAL_SYNCH_CALLS=250WITH SLEEP_INTERVAL_SYNCH_CALLS=2000.

> **Note**: O valor é especificado nos milissegundos (Senhora); consequentemente, 2000 igualam a 2 segundos.

> **Caution**: Use o cuidado quando você edita este arquivo. As mudanças a esta arquivo a não

ser esse alistado acima podem causar efeitos indesejados ao Cisco Security Manager.

Depois que você muda e salvar o arquivo, assegure-se de que todos os aplicativos do cliente do Cisco Security Manager estejam fechados, e reiniciem então o serviço do daemon manager do Cisco Security Manager (crmdmgtd).

Informações Relacionadas

- A instalação do Cisco Security Manager 4.3 e guia da elevação
- Suporte Técnico e Documentação - Cisco Systems