CSM 3.x - Adicionar sensores e módulos IDS ao inventário

Contents

Introdução

Este documento fornece informações sobre como adicionar sensores e módulos do Sistema de Detecção de Intrusão (IDS - Intrusion Detection System) (inclui IDSM nos switches Catalyst 6500, NM-CIDS nos roteadores e AIP-SSM no ASA) no Cisco Security Manager (CSM).

Observação: o CSM 3.2 não suporta o IPS 6.2. Ele é suportado no CSM 3.3.

Pré-requisitos

Requisitos

Este documento pressupõe que os dispositivos CSM e IDS estejam instalados e funcionando corretamente.

Componentes Utilizados

As informações neste documento são baseadas no CSM 3.0.1.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Adicionar dispositivos ao inventário do Gerenciador de segurança

Ao adicionar um dispositivo ao Gerenciador de segurança, você traz uma série de informações de identificação para o dispositivo, como seu nome DNS e endereço IP. Depois que você adicionar o dispositivo, ele aparecerá no inventário de dispositivos do Gerenciador de segurança. Você pode gerenciar um dispositivo no Gerenciador de segurança somente depois de adicioná-lo ao inventário.

Você pode adicionar dispositivos ao inventário do Gerenciador de segurança com estes métodos:

- Adicione um dispositivo da rede.
- Adicionar um novo dispositivo que ainda não esteja na rede
- Adicione um ou mais dispositivos do Repositório de dispositivos e credenciais (DCR).
- Adicione um ou mais dispositivos de um arquivo de configuração.

Observação: este documento concentra-se no método: Adicionar um novo dispositivo que ainda não esteja na rede.

Etapas para adicionar o sensor IDS e os módulos

Use a opção Adicionar novo dispositivo para adicionar um único dispositivo ao inventário do Gerenciador de segurança. Você pode usar essa opção para pré-provisionamento. Você pode criar o dispositivo no sistema, atribuir políticas ao dispositivo e gerar arquivos de configuração antes de receber o hardware do dispositivo.

Ao receber o hardware do dispositivo, você deve preparar os dispositivos para serem gerenciados pelo Security Manager. Consulte Preparação dos Dispositivos para o Gerenciador de Segurança Gerenciar para obter mais informações.

Este procedimento mostra como adicionar um novo sensor e módulos IDS:

1. Clique no botão Device View na barra de ferramentas.

   A página Dispositivos é exibida.

2. Clique no botão Adicionar no seletor de Dispositivos.

   A página Novo dispositivo - Escolher método é exibida com quatro opções.

3. Selecione Add New Device e clique em Next.

   A página Novo dispositivo - Informações do dispositivo é exibida.

4. Insira as informações do dispositivo nos campos apropriados.

   Consulte a seção Fornecimento de informações do dispositivo—Novo dispositivo para obter mais informações.

5. Clique em Finish.

   O sistema executa tarefas de validação de dispositivo:

   - Se os dados estiverem incorretos, o sistema gerará mensagens de erro e exibirá a página em que o erro ocorre com um ícone de erro vermelho correspondente.
   - Se os dados estiverem corretos, o dispositivo será adicionado ao inventário e aparecerá no seletor de dispositivos.

Fornecimento de informações do dispositivo — Novo dispositivo

Conclua estes passos:

1. Selecione o tipo de dispositivo para o novo dispositivo:

   a. Selecione a pasta de tipo de dispositivo de nível superior para exibir as famílias de dispositivos suportadas.

   b. Selecione a pasta da família de dispositivos para exibir os tipos de dispositivos suportados.

      a. Selecione Cisco Interfaces and Modules > Cisco Network Modules para adicionar o Cisco IDS Access Router Network Module. Da mesma forma, selecione Cisco Interfaces and Modules > Cisco Services Modules para adicionar os módulos AIP-SSM e IDSM mostrados.

      b. Selecione Security and VPN > Cisco IPS 4200 Series Sensors para adicionar o Cisco IDS 4210 Sensor ao inventário CSM.

   c. Selecione o tipo de dispositivo.

      Observação: depois de adicionar um dispositivo, você não poderá alterar o tipo de dispositivo.

      As IDs de objeto do sistema para esse tipo de dispositivo são exibidas no campo SysObjectId. O primeiro ID de objeto do sistema é selecionado por padrão. Você pode selecionar outro, se necessário.

2. Insira as informações de identidade do dispositivo, como o tipo de IP (estático ou dinâmico), o nome do host, o nome do domínio, o endereço IP e o nome de exibição.

3. Insira as informações do sistema operacional do dispositivo, como tipo de SO, nome da imagem, versão do SO de destino, contextos e modo operacional.

4. O campo Auto Update (Atualização automática) ou CNS-Configuration Engine (Mecanismo de configuração de CNS) será exibido, dependendo do tipo de dispositivo selecionado:

    - Atualização automática—Exibida para o PIX Firewall e dispositivos ASA.
    - CNS-Configuration Engine—Exibido para roteadores Cisco IOS®.

    Observação: este campo não está ativo para os dispositivos Catalyst 6500/7600 e FWSM.

5. Conclua estes passos:

    - Atualização automática—Clique na seta para exibir uma lista de servidores. Selecione o servidor que está gerenciando o dispositivo. Se o servidor não aparecer na lista, siga estas etapas:

        a. Clique na seta e selecione + Adicionar servidor... A caixa de diálogo Propriedades do servidor é exibida.

        b. Insira as informações nos campos obrigatórios.

        c. Click OK. O novo servidor é adicionado à lista de servidores disponíveis.

    - CNS-Configuration Engine — Informações diferentes são exibidas, dependendo da seleção do tipo de IP estático ou dinâmico:

        Estático — Clique na seta para exibir uma lista de Mecanismos de configuração. Selecione o Mecanismo de configuração que está gerenciando o dispositivo. Se o mecanismo de configuração não aparecer na lista, siga estas etapas:

        a. Clique na seta e selecione + Adicionar mecanismo de configuração... A caixa de diálogo Propriedades do mecanismo de configuração é exibida.

        b. Insira as informações nos campos obrigatórios.

        c. Click OK. O novo Configuration Engine é adicionado à lista de Configuration Engines disponíveis.

    - Dinâmico — Clique na seta para exibir uma lista de servidores. Selecione o servidor que está gerenciando o dispositivo. Se o servidor não aparecer na lista, siga estas etapas:

        a. Clique na seta e selecione + Adicionar servidor... A caixa de diálogo Propriedades do servidor é exibida.

        b. Insira as informações no campo obrigatório.

        c. Click OK. O novo servidor é adicionado à lista de servidores disponíveis.

6. Conclua estes passos:

    - Para gerenciar o dispositivo no Security Manager, marque a caixa de seleção

Gerenciar no Cisco Security Manager. Esse é o padrão.

- Se a única função do dispositivo que você está adicionando é servir como um terminal VPN, desmarque a caixa de seleção Gerenciar no Cisco Security Manager.

  O Gerenciador de Segurança não gerenciará configurações nem carregará ou baixará configurações neste dispositivo.

7. Marque a caixa de seleção Contexto de segurança de dispositivo não gerenciado para gerenciar um contexto de segurança, cujo dispositivo pai (PIX Firewall, ASA ou FWSM) não é gerenciado pelo Security Manager.

   Você pode particionar um PIX Firewall, ASA ou FWSM em vários firewalls de segurança, também conhecidos como contextos de segurança. Cada contexto é um sistema independente, com suas próprias configurações e políticas. Você pode gerenciar esses contextos independentes no Security Manager, mesmo que o pai (PIX Firewall, ASA ou FWSM) não seja gerenciado pelo Security Manager.

   Observação: este campo só estará ativo se o dispositivo selecionado no Seletor de dispositivos for um dispositivo de firewall, como PIX Firewall, ASA ou FWSM, que suporte contexto de segurança.

8. Marque a caixa de seleção Manage in IPS Manager para gerenciar um roteador Cisco IOS no IPS Manager.

   Esse campo só estará ativo se você tiver selecionado um roteador Cisco IOS no seletor de Dispositivos.

   Observação: o Gerenciador de IPS pode gerenciar os recursos de IPS apenas em um roteador Cisco IOS que tenha recursos de IPS. Para obter mais informações, consulte a documentação do IPS.

   Se você marcar a caixa de seleção Gerenciar no Gerenciador de IPS, deverá marcar a caixa de seleção Gerenciar no Cisco Security Manager também.

   Se o dispositivo selecionado for IDS, esse campo não estará ativo. No entanto, a caixa de seleção é marcada porque o IPS Manager gerencia sensores IDS.

   Se o dispositivo selecionado for PIX Firewall, ASA ou FWSM, este campo não estará ativo porque o IPS Manager não gerencia esses tipos de dispositivo.

9. Clique em Finish.

   O sistema executa tarefas de validação de dispositivo:

   - Se os dados inseridos estiverem incorretos, o sistema gerará mensagens de erro e exibirá a página onde o erro ocorre.

   - Se os dados inseridos estiverem corretos, o dispositivo será adicionado ao inventário e aparecerá no seletor de dispositivos.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Mensagens de erro

Quando você adiciona IPS ao CSM, a mensagem de erro `Dispositivo inválido: não foi possível deduzir SysObjId para o tipo de plataforma` é exibida.

Solução

Conclua estas etapas para resolver esta mensagem de erro.

1. Interrompa o serviço Daemon do CSM no Windows e escolha Program Files > CSCOpx > MDC > athena > config > Diretory, onde você pode encontrar `VMS-SysObjID.xml`.
2. No sistema CSM, substitua o arquivo VMS-SysObjID.xml original localizado por padrão em `C:\Program Files\CSCOpx\MDC\athena\config\directory` pelo arquivo `VMS-SysObjID.xml` mais recente.
3. Reinicie o serviço Gerenciador de daemon do CSM (CRMDmgtd) e tente adicionar ou descobrir novamente os dispositivos afetados.

Informações Relacionadas

- Página de suporte do Cisco Security Manager
- Página de suporte do sistema de detecção de intrusão da Cisco
- Suporte Técnico e Documentação - Cisco Systems

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.