CS 3.x: Adicionar sensors de IDS e módulos ao inventário do gerenciador de segurança

Índice

Introdução

Este documento fornece a informação em como adicionar sensores e módulos do sistema de detecção de intrusões (IDS) (inclui o IDSM em Catalyst 6500 Switch, o NM-CIDS no Roteadores e o AIP-SSM no ASA) no Cisco Security Manager (CS).

Note: O CS 3.2 não apoia IPS 6.2. É apoiado em CS 3.3.

Pré-requisitos

Requisitos

Este documento supõe que os dispositivos CS e IDS estão instalados e trabalham corretamente.

Componentes Utilizados

A informação neste documento é baseada no CS 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.

Convenções

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

Adicionar dispositivos ao inventário do gerenciador de segurança

Quando você adiciona um dispositivo ao gerenciador de segurança, você traz em uma escala de identificar a informação para o dispositivo, tal como seus nome de DNS e endereço IP de Um ou Mais Servidores Cisco ICM NT. Depois que você adiciona o dispositivo, aparece no inventário de dispositivo do gerenciador de segurança. Você pode controlar um dispositivo no gerenciador de segurança somente depois que você o adiciona ao inventário.

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

- Adicionar um dispositivo da rede.
- Adicionar um dispositivo novo que não esteja ainda na rede
- Adicionar uns ou vários dispositivos do dispositivo e do repositório das credenciais (RCI).
- Adicionar uns ou vários dispositivos de um arquivo de configuração.

Note: Este documento centra-se sobre o método: Adicionar um dispositivo novo que não esteja ainda na rede.

Etapas para adicionar o sensor de IDS e os módulos

Use a opção nova do dispositivo adicionar a fim adicionar um dispositivo único ao inventário do gerenciador de segurança. Você pode usar esta opção para o PRE-abastecimento. Você pode criar o dispositivo no sistema, atribuir políticas ao dispositivo, e gerar arquivos de configuração antes que você receba o hardware do dispositivo.

Quando você recebe o hardware do dispositivo, você deve preparar os dispositivos para ser controlado pelo gerenciador de segurança. Refira a preparação dos dispositivos para que o gerenciador de segurança controle para mais informação.

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

1. Clique o botão da **vista do dispositivo na** barra de ferramentas.A página dos dispositivos publica-se.
2. Clique o **botão Add no** seletor de dispositivo.O dispositivo novo - Escolha a página do método aparece com quatro opções.
3. Escolha **adicionam o dispositivo novo**, a seguir clicam-no **em seguida**.O dispositivo novo - A página da informação do dispositivo publica-se.
4. Incorpore a informação do dispositivo aos campos apropriados.Veja a informação do dispositivo de fornecimento — Seção nova do dispositivo para mais informação.
5. Clique em Finish.O sistema executa tarefas da validação do dispositivo:Se os dados estão incorretos, o sistema gerencie Mensagens de Erro e indica a página em que o erro ocorre com um ícone vermelho do erro que lhe corresponda.Se os dados estão corretos, o dispositivo está adicionado ao inventário e aparece no seletor de dispositivo.

Fornecendo a informação do dispositivo — Dispositivo novo

Conclua estes passos:

1. Selecione o tipo de dispositivo para o dispositivo novo:Selecione o dobrador nível mais alto do tipo de dispositivo a fim indicar as famílias do dispositivo suportado.Selecione o dobrador da família de dispositivo a fim indicar os tipos de dispositivo suportado.Selecione o **Cisco Interfaces and Modules > os Módulos de rede da Cisco** a fim adicionar o **Módulo de rede por roteador de acesso Cisco IDS**. Igualmente, **Cisco Interfaces and Modules > Cisco Services Modules** seletos a fim adicionar os módulos AIP-SSM e IDSM mostrados.Selecione a **Segurança e VPN > o Sensores Cisco IPS série 4200** a fim adicionar o Sensor Cisco IDS 4210 ao inventário CS.Selecione o tipo de dispositivo.**Note**: Depois que você adiciona um dispositivo, você não pode mudar o tipo de dispositivo.As identificações de objeto do sistema para esse tipo de dispositivo são indicadas no campo do sysObjectID. A primeira identificação de objeto do sistema é selecionada à revelia. Você pode selecionar outro se necessário.
2. Incorpore a informação de identidade do dispositivo, tal como o tipo IP (estático ou dinâmico), o hostname, o Domain Name, o endereço IP de Um ou Mais Servidores Cisco ICM NT, e o nome do indicador.
3. Incorpore a informação do sistema operacional do dispositivo, tal como o tipo do OS, o nome da imagem, a versão de OS do alvo, os contextos, e o modo operacional.
4. O auto campo do motor da atualização ou da CNS-configuração aparece, que depende do tipo de dispositivo que você seleciona:Auto atualização — Indicado para o PIX Firewall e os dispositivos ASA.Motor da CNS-configuração — Indicado para o Roteadores de Cisco IOS®.**Note**: Este campo não é ativo para o catalizador 6500/7600 e os dispositivos FWSM.
5. Conclua estes passos:Auto atualização — Clique a seta para indicar uma lista de server. Selecione o server que está controlando o dispositivo. Se o server não aparece na lista, termine estas etapas:Clique a seta, a seguir selecione **+ adicionar o server**… A caixa de diálogo das propriedades de servidor aparece.Incorpore a informação aos campos requerido.Click **OK**. O server novo é adicionado à lista de server disponíveis.Motor da CNS-configuração — A informação diferente é indicada, que depende sobre se você seleciona o tipo da estática ou do IP dinâmico:**Estático** — Clique a seta para indicar uma lista de motores da configuração. Selecione o motor da configuração que está controlando o dispositivo. Se o motor da configuração não aparece na lista, termine estas etapas:Clique a seta, a seguir selecione **+ adicionar o motor da configuração**… A caixa de diálogo das propriedades do motor da configuração aparece.Incorpore a informação aos campos requerido.Click **OK**. O motor novo da configuração é adicionado à lista de motores disponíveis da configuração.**Dinâmico** — Clique a seta para indicar uma lista de server. Selecione o server que está controlando o dispositivo. Se o server não aparece na lista, termine estas etapas:Clique a seta, a seguir selecione **+ adicionar o server**… A caixa de diálogo das propriedades de servidor aparece.Incorpore a informação ao campo requerido.Click **OK**. O server novo é adicionado à lista de server disponíveis.
6. Conclua estes passos:A fim controlar o dispositivo no gerenciador de segurança, verifique o **controlo na** caixa de verificação do **Cisco Security Manager**. Esse é o padrão.Se a única função do dispositivo que você está adicionando é servir como um ponto final VPN, desmarca o **controlo na** caixa de verificação do **Cisco Security Manager**.O gerenciador de segurança não controlará configurações nem transferirá arquivos pela rede ou transferirá configurações neste dispositivo.
7. Verifique o contexto de segurança de caixa de verificação Unmanaged do dispositivo a fim controlar um contexto de segurança, cujo o dispositivo do pai (PIX Firewall, ASA, ou FWSM) não seja controlado pelo gerenciador de segurança.Você pode dividir um PIX Firewall, um ASA, ou um FWSM nos Firewall múltiplos da Segurança, igualmente conhecidos como

contextos de segurança. Cada contexto é um sistema independente, com suas próprias configuração e políticas. Você pode controlar estes contextos autônomos no gerenciador de segurança, mesmo que o pai (PIX Firewall, ASA, ou FWSM) não seja controlado pelo gerenciador de segurança.**Note**: Este campo é ativo somente se o dispositivo que você selecionou no seletor de dispositivo é um dispositivo de firewall, tal como o PIX Firewall, o ASA, ou o FWSM, que apoia o contexto de segurança.

8. Verifique o **controlo na caixa de verificação de gerenciador IPS** a fim controlar um roteador do Cisco IOS no gerente IPS.Este campo é ativo somente se você selecionou um roteador do Cisco IOS do seletor de dispositivo.**Note**: O gerente IPS pode controlar as características IPS somente em um roteador do Cisco IOS que tenha capacidades IPS. Para mais informação, veja a documentação IPS.Se você verifica o controlo na caixa de verificação de gerenciador IPS, você deve verificar o controlo na caixa de verificação do Cisco Security Manager igualmente.Se o dispositivo selecionado é IDS, este campo não é ativo. Contudo, a caixa de verificação é verificada porque o gerente IPS controla sensors de IDS.Se o dispositivo selecionado é PIX Firewall, ASA, ou FWSM, este campo não é ativo porque o gerente IPS não controla estes tipos de dispositivo.
9. Clique em Finish.O sistema executa tarefas da validação do dispositivo:Se os dados que você incorporou estão incorretos, o sistema gerencie Mensagens de Erro e indica a página onde o erro ocorre.Se os dados que você incorporou estão corretos, o dispositivo está adicionado ao inventário e aparece no seletor de dispositivo.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Mensagens de erro

Quando você adicionar o IPS ao CS, o `dispositivo inválido: Não podia deduzir o SysObjId para o` Mensagem de Erro do `tipo de plataforma` aparece.

Solução

Termine estas etapas a fim resolver este Mensagem de Erro.

1. Pare o serviço de demônio CS em Windows, e escolha então **arquivos de programa > CSCOpx > CDM > athena > configuração > diretório**, onde você pode encontrar `VMS-SysObjID.xml.`
2. No sistema CS, substitua o arquivo original VMS-SysObjID.xml situado à revelia em C:\Program Files\CSCOpx\MDC\athena\config\directory `com o arquivo` o mais atrasado VMS-SysObjID.xml.
3. Reinicie o serviço do daemon manager CS (crmdmgtd), e experimente-o de novo para adicionar outra vez ou descobrir 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