CSM 3.x - IDS-sensoren en -modules aan inventaris toevoegen

Inhoud

Inleiding

Dit document bevat informatie over de manier waarop u sensoren en modules voor inbraakdetectiesysteem (IDS) kunt toevoegen (inclusief IDSM op Catalyst 6500 switches, NM-CIDS op routers en AIP-SSM op ASA) in Cisco Security Manager (CSM).

Opmerking: CSM 3.2 ondersteunt IPS 6.2 niet. Het wordt ondersteund in CSM 3.3.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat CSM- en IDS-apparaten zijn geïnstalleerd en correct werken.

Gebruikte componenten

De informatie in dit document is gebaseerd op CSM 3.0.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Apparaten aan de Security Manager-inventaris toevoegen

Wanneer u een apparaat aan Security Manager toevoegt, brengt u een reeks van identificatie informatie voor het apparaat in, zoals zijn DNS naam en IP adres. Nadat u het apparaat hebt toegevoegd, verschijnt het in de inventaris van het apparaat van Security Manager. U kunt een apparaat in Security Manager alleen beheren nadat u het aan de inventaris hebt toegevoegd.

U kunt apparaten aan de Security Manager-inventaris met deze methoden toevoegen:

- Voeg een apparaat van het netwerk toe.
- Voeg een nieuw apparaat toe dat nog niet op het netwerk is
- Voeg een of meer apparaten toe uit de Apparaat- en Credentials Repository (DCR).
- Voeg een of meer apparaten toe uit een configuratiebestand.

N.B.: Dit document concentreert zich op de methode: Voeg een nieuw apparaat toe dat nog niet op het netwerk is.

Stappen om de IDS-sensor en -modules toe te voegen

Gebruik de optie Nieuw apparaat toevoegen om één apparaat aan de inventaris van Security Manager toe te voegen. U kunt deze optie gebruiken voor pre-provisioning. U kunt het apparaat in het systeem maken, beleid aan het apparaat toewijzen en configuratiebestanden genereren voordat u de hardware van het apparaat ontvangt.

Wanneer u de hardware van het apparaat ontvangt, moet u de apparaten voorbereiden die door Security Manager worden beheerd. Raadpleeg Het apparaat voorbereiden op Security Manager om meer informatie te beheren.

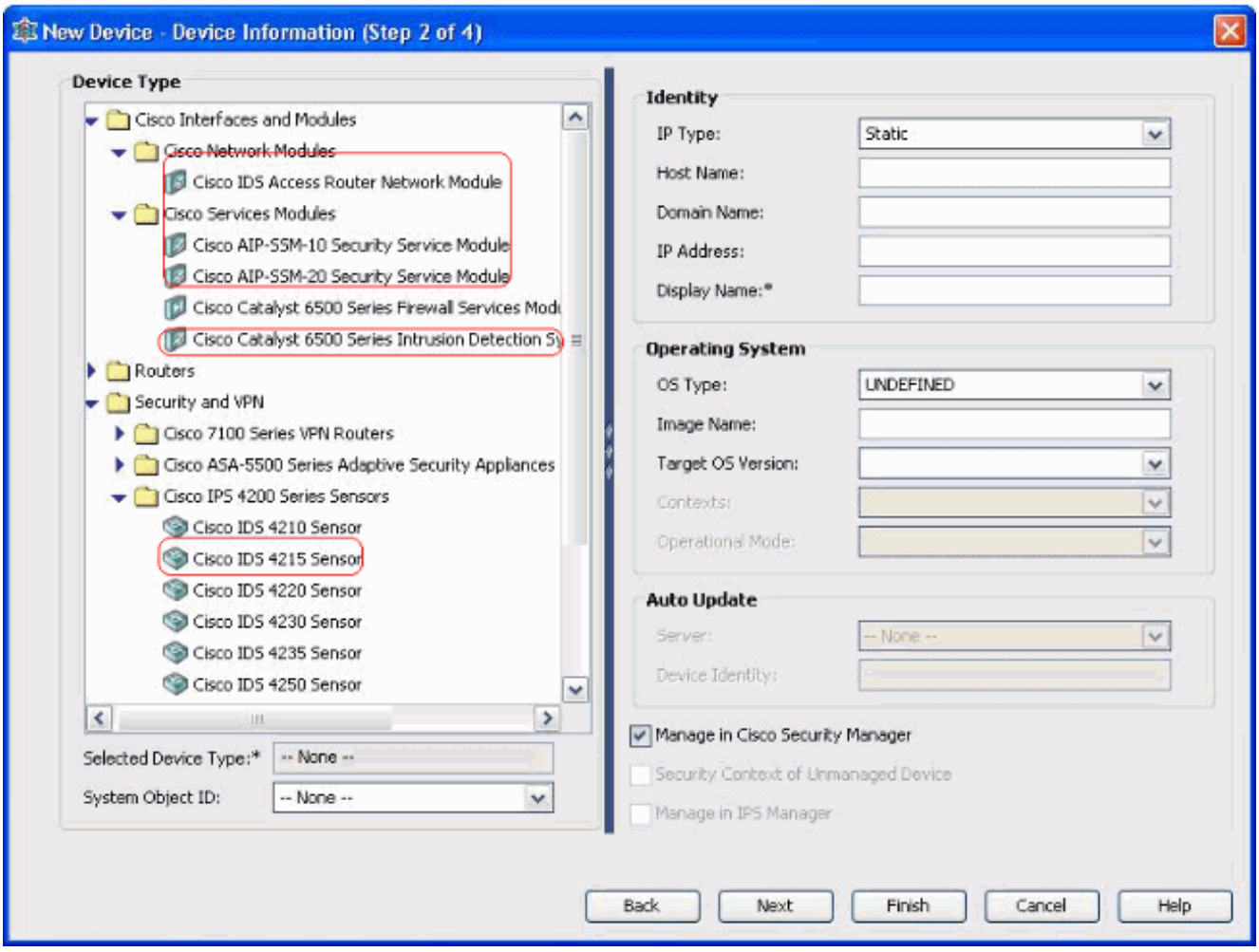
Deze procedure toont hoe een nieuwe IDS-sensor en -modules kunnen worden toegevoegd:

1. Klik de knop **Apparaatweergave** in de werkbalk aan.De pagina Apparaten verschijnt.
2. Klik op de knop **Add** in het apparaat.De pagina Nieuwe apparaat - Kies methode verschijnt met vier opties.
3. Kies **Nieuw apparaat toevoegen** en klik op **Volgende**.De pagina Informatie nieuw apparaat - apparaat verschijnt.
4. Geef de apparaatinformatie op in de juiste velden.Zie het gedeelte Apparaatinformatie verstrekken—Nieuw apparaat voor meer informatie.
5. Klik op **Voltooien**.Het systeem voert taken uit voor het valideren van hulpmiddelen:Als de gegevens niet correct zijn, genereert het systeem foutmeldingen en geeft het de pagina weer waarop de fout voorkomt met een rood foutpictogram dat gelijk is aan de fout.Als de gegevens juist zijn, wordt het apparaat aan de inventaris toegevoegd en verschijnt het in het apparaat.

Apparaatinformatie leveren — nieuw apparaat

Voer de volgende stappen uit:

1. Selecteer het type apparaat voor het nieuwe apparaat:Selecteer de map met het bovenste niveau van het apparaattype om de ondersteunde apparaatfamilies weer te geven.Selecteer de map van de apparaatfamilie om de ondersteunde apparaattypen weer te geven.Selecteer **Cisco-interfaces en -modules > Cisco-netwerkmodules** om de **netwerkmodule** voor **Cisco IDS-toegangsrouter** toe te voegen. Selecteer op dezelfde manier **Cisco-interfaces en -modules > Cisco-servicesmodules** om de weergegeven AIP-SSM- en IDSM-modules toe te voegen.Selecteer **Beveiliging en VPN > Cisco IPS 4200 Series sensoren** om de Cisco IDS 4210-sensor aan de CSM-inventaris toe te
voegen.



Selecteer het type apparaat.**Opmerking:** Nadat u een apparaat hebt toegevoegd, kunt u het type apparaat niet wijzigen.Systeemobject-ID's voor dat apparaattype worden weergegeven in het veld SysObjectID. Het eerste systeem object ID wordt standaard geselecteerd. U kunt desgewenst een andere selectie maken.

2. Voer de informatie over de identiteit van het apparaat in, zoals het IP-type (statisch of dynamisch), de hostnaam, de domeinnaam, IP-adres en de weergavenaam.
3. Voer de informatie in over het besturingssysteem van het apparaat, zoals het type besturingssysteem, de naam van de afbeelding, de doelversie van het besturingssysteem, de contexten en de operationele modus.
4. Het veld Auto Update of CNS-Configuration Engine verschijnt, dat afhankelijk is van het geselecteerde apparaattype:Auto Update-weergegeven voor PIX-firewall en ASA-apparaten.CNS-Configuration Engine-weergegeven voor Cisco IOS® routers.**Opmerking:** Dit veld is niet actief voor Catalyst 6500/7600 en FWSM-apparaten.
5. Voer de volgende stappen uit:Automatische update - klik op het pijltje om een lijst met servers weer te geven. Selecteer de server die het apparaat beheert. Als de server niet in de

lijst voorkomt, voert u de volgende stappen uit:Klik op het pijltje en selecteer vervolgens **+ Server toevoegen**... Het dialoogvenster Server Properties verschijnt.Geef de informatie in de gewenste velden op.Klik op **OK**. De nieuwe server wordt toegevoegd aan de lijst met beschikbare servers.CNS-Configuration Engine-Difference informatie wordt weergegeven. Dit is afhankelijk van de keuze van het statische of dynamische IP-type:**Statisch**-Klik op het pijltje om een lijst weer te geven van de Configuration Engines. Selecteer de Configuration Engine die het apparaat beheert. Als de Configuration Engine niet in de lijst voorkomt, voert u de volgende stappen uit:Klik op het pijltje en selecteer vervolgens **+ Configuration Engine toevoegen**... Het dialoogvenster Configuration Engine Properties wordt weergegeven.Geef de informatie in de gewenste velden op.Klik op **OK**. De nieuwe Configuration Engine wordt toegevoegd aan de lijst met beschikbare Configuration-motoren.**Dynamisch**-Klik op het pijltje om een lijst met servers weer te geven. Selecteer de server die het apparaat beheert. Als de server niet in de lijst voorkomt, voert u de volgende stappen uit:Klik op het pijltje en selecteer vervolgens **+ Server toevoegen**... Het dialoogvenster Server Properties verschijnt.Typ de informatie in het gewenste veld.Klik op **OK**. De nieuwe server wordt toegevoegd aan de lijst met beschikbare servers.

6. Voer de volgende stappen uit:Om het apparaat in Security Manager te beheren, controleert u het vakje **Manager beheren in Cisco Security Manager**. Dit is de standaard.Als de enige functie van het apparaat dat u toevoegt, als VPN-eindpunt moet dienen, **schakelt** u het vakje **Manager beheren in Cisco Security Manager uit**.Security Manager zal geen configuraties beheren of configuraties uploaden of downloaden op dit apparaat.
7. Controleer de veiligheidscontext van het onbeheerde apparaat om een veiligheidscontext te beheren, waarvan het moederapparaat (PIX Firewall, ASA of FWSM) niet door Security Manager wordt beheerd.U kunt een PIX-firewall, ASA of FWSM opdelen in meerdere beveiligingsfirewalls, ook bekend als beveiligingscontexten. Elke context is een onafhankelijk systeem, met zijn eigen configuratie en beleid. U kunt deze standalone contexten in Security Manager beheren, zelfs als de ouder (PIX Firewall, ASA, of FWSM) niet door Security Manager wordt beheerd.**Opmerking:** Dit veld is alleen actief als het apparaat dat u in de machine hebt geselecteerd een firewallapparaat is, zoals PIX-firewall, ASA of FWSM, dat de beveiligingscontext ondersteunt.
8. Controleer het aanvinkvakje **Beheer in IPS Manager** om een Cisco IOS router in IPS Manager te beheren.Dit veld is alleen actief als u een Cisco IOS-router hebt geselecteerd uit de knop Apparaatselectie.**Opmerking:** IPS Manager kan de IPS-functies alleen beheren op een Cisco IOS-router die IPS-functies heeft. Zie de IPS-documentatie voor meer informatie.Als u het aanvinkvakje Manager beheren in IPS Manager controleert, moet u ook het aanvinkvakje Manager beheren in Cisco Security Manager controleren.Als het geselecteerde apparaat IDS is, is dit veld niet actief. Het aankruisvakje wordt echter ingeschakeld omdat IPS Manager IDS-sensoren beheert.Als het geselecteerde apparaat PIX Firewall, ASA of FWSM is, is dit veld niet actief omdat IPS Manager deze apparaattypen niet beheert.
9. Klik op **Voltooien**.Het systeem voert taken uit voor het valideren van hulpmiddelen:Als de ingevoerde gegevens niet correct zijn, genereert het systeem foutmeldingen en geeft het de pagina weer waar de fout optreedt.Als de ingevoerde gegevens juist zijn, wordt het apparaat aan de inventaris toegevoegd en verschijnt het in het apparaat.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Foutmeldingen

Wanneer u IPS aan CSM toevoegt, `ongeldig apparaat: Kan SysObjID niet afleiden voor het platform type` error bericht verschijnt.

Oplossing

Voltooi deze stappen om deze foutmelding op te lossen.

1. Stop de CSM Daemon-service in Windows, en kies vervolgens **Programma's > CSCOpx > MDC > Setup > Setup > Map**, waar u `VMS-SYSObjID.xml` kunt vinden.
2. Vervang het oorspronkelijke bestand VMS-SYSObjID.xml in het CSM-systeem standaard in `C:\Program Files\CSCOpx\MDC\athena\config\directory` met het laatste bestand `VMS-SYSObjID.xml`.
3. Start de CSM Daemon Manager-service (CRMDmgtd) opnieuw en probeer de getroffen apparatuur(apparaten) opnieuw toe te voegen of te ontdekken.

Gerelateerde informatie

- Ondersteuning voor Cisco Security Manager
- Ondersteuning van Cisco-pagina voor inbraakdetectiesysteem
- Technische ondersteuning en documentatie – Cisco Systems