CSM 3.x - Aggiunta di sensori e moduli IDS all'inventario

Sommario

Introduzione

Questo documento offre informazioni su come aggiungere sensori e moduli Intrusion Detection System (IDS) (include IDSM sugli switch Catalyst 6500, NM-CIDS sui router e AIP-SSM sull'appliance ASA) in Cisco Security Manager (CSM).

Nota: CSM 3.2 non supporta IPS 6.2. È supportato in CSM 3.3.

Prerequisiti

Requisiti

in questo documento si presume che i dispositivi CSM e IDS siano installati e funzionino correttamente.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il CSM 3.0.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Aggiungi dispositivi all'inventario di Security Manager

Quando si aggiunge un dispositivo a Security Manager, viene inserito un intervallo di informazioni di identificazione per il dispositivo, ad esempio il nome DNS e l'indirizzo IP. Dopo l'aggiunta, il dispositivo viene visualizzato nell'inventario dei dispositivi di Security Manager. È possibile gestire un dispositivo in Security Manager solo dopo averlo aggiunto all'inventario.

Èpossibile aggiungere dispositivi all'inventario di Security Manager utilizzando i seguenti metodi:

- Aggiungere un dispositivo dalla rete.
- Aggiungi un nuovo dispositivo non ancora connesso alla rete
- Aggiungere uno o più dispositivi dal repository dei dispositivi e delle credenziali (DCR).
- Aggiungere uno o più dispositivi da un file di configurazione.

Nota: in questo documento viene illustrato il metodo Aggiungere un nuovo dispositivo non ancora connesso alla rete.

Procedura per aggiungere il sensore IDS e i moduli

Utilizzare l'opzione Add New Device (Aggiungi nuovo dispositivo) per aggiungere un singolo dispositivo all'inventario di Security Manager. È possibile utilizzare questa opzione per il preprovisioning. È possibile creare il dispositivo nel sistema, assegnare criteri al dispositivo e generare file di configurazione prima di ricevere l'hardware del dispositivo.

Quando si riceve l'hardware del dispositivo, è necessario preparare i dispositivi da gestire con Security Manager. per ulteriori informazioni, fare riferimento a Preparazione dei dispositivi da gestire per Security Manager.

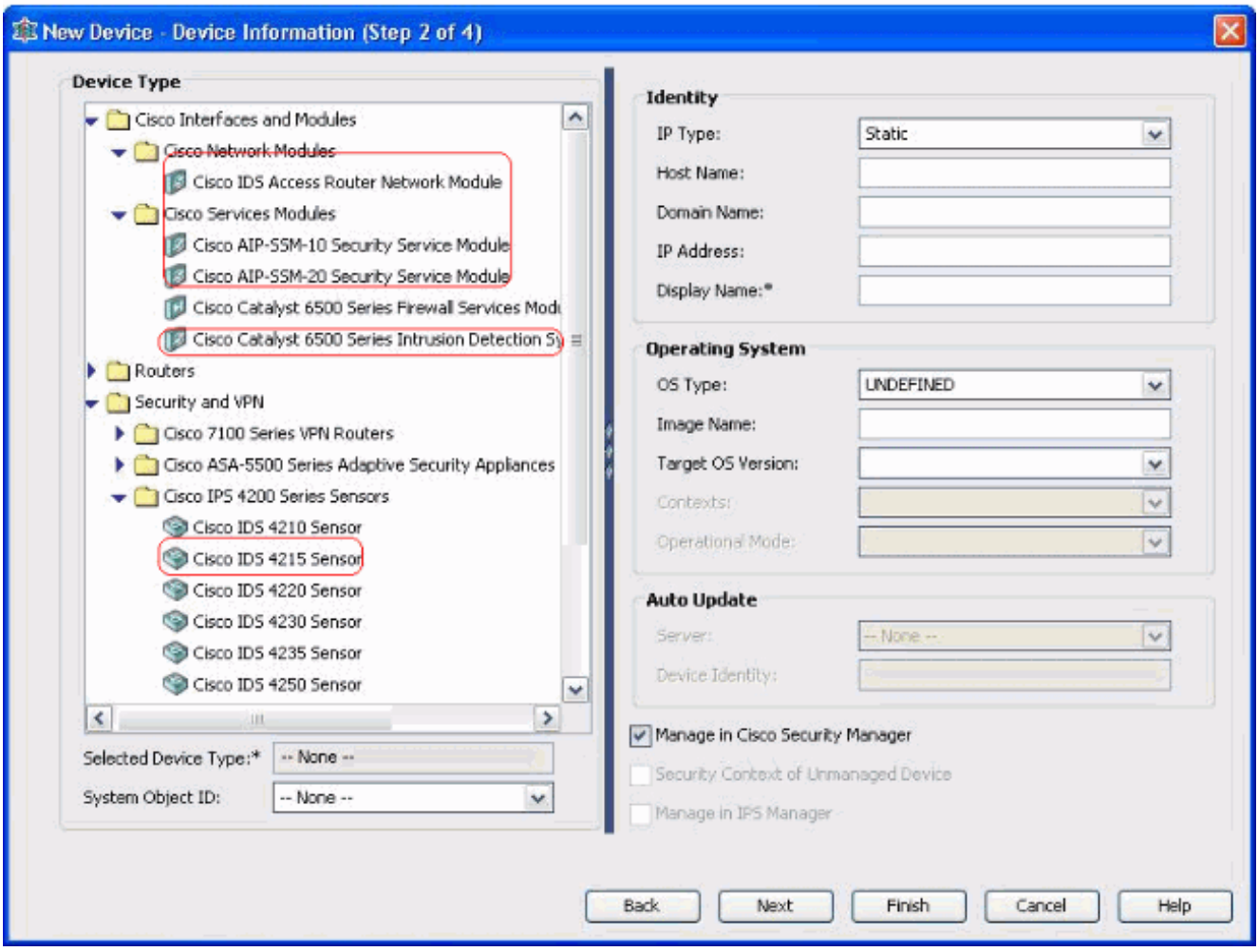
In questa procedura viene illustrato come aggiungere un nuovo sensore IDS e i relativi moduli:

1. Fare clic sul pulsante **Visualizzazione periferica** nella barra degli strumenti.Viene visualizzata la pagina Dispositivi.
2. Fare clic sul pulsante **Add** (Aggiungi) nel selettore di periferiche.Viene visualizzata la pagina Nuova periferica - Scegli metodo con quattro opzioni.
3. Scegliere **Aggiungi nuova periferica**, quindi fare clic su **Avanti**.Viene visualizzata la pagina Nuova periferica - Informazioni periferica.
4. Immettere le informazioni sul dispositivo nei campi appropriati.Per ulteriori informazioni, vedere la sezione Fornitura delle informazioni sui dispositivi -Nuovo dispositivo.
5. Fare clic su **Finish** (Fine).Il sistema esegue le operazioni di convalida dei dispositivi:Se i dati non sono corretti, il sistema genera messaggi di errore e visualizza la pagina in cui si è verificato l'errore con un'icona di errore rossa corrispondente.Se i dati sono corretti, il dispositivo viene aggiunto all'inventario e visualizzato nel selettore Dispositivo.

Informazioni sul dispositivo - Nuovo dispositivo

Attenersi alla seguente procedura:

1. Selezionare il tipo di dispositivo per il nuovo dispositivo:Selezionare la cartella dei tipi di dispositivo di primo livello per visualizzare le famiglie di dispositivi supportate.Selezionare la cartella della famiglia di dispositivi per visualizzare i tipi di dispositivi supportati.Selezionare **Cisco Interfaces and Modules > Cisco Network Module** per aggiungere il **Cisco IDS Access Router Network Module**. Analogamente, selezionare **Cisco Interfaces and Modules > Cisco Services Module** per aggiungere i moduli AIP-SSM e IDSM mostrati.Selezionare **Security and VPN > Cisco IPS serie 4200 Sensor** per aggiungere il sensore Cisco IDS 4210 all'inventario
CSM.



Selezionare il tipo di dispositivo.**Nota:** dopo aver aggiunto una periferica, non è possibile modificarne il tipo.Gli ID degli oggetti di sistema per il tipo di dispositivo vengono visualizzati nel campo SysObjectId. Il primo ID oggetto di sistema è selezionato per default. Se necessario, potete selezionarne un altro.
2. Immettere le informazioni sull'identità del dispositivo, ad esempio il tipo IP (statico o dinamico), il nome host, il nome di dominio, l'indirizzo IP e il nome visualizzato.
3. Immettere le informazioni sul sistema operativo del dispositivo, ad esempio tipo di sistema operativo, nome dell'immagine, versione del sistema operativo di destinazione, contesti e modalità operativa.
4. Viene visualizzato il campo Auto Update (Aggiornamento automatico) o CNS-Configuration Engine (Motore di configurazione CNS), che dipende dal tipo di dispositivo selezionato:Auto Update - Visualizzato per i dispositivi PIX Firewall e ASA.CNS-Configuration Engine - Visualizzato per i router Cisco IOS®.**Nota:** questo campo non è attivo per i dispositivi Catalyst 6500/7600 e FWSM.
5. Attenersi alla seguente procedura:Aggiornamento automatico: fare clic sulla freccia per

visualizzare un elenco di server. Selezionare il server che gestisce il dispositivo. Se il server non è presente nell'elenco, procedere come segue:Fare clic sulla freccia, quindi selezionare **+ Aggiungi server**... Verrà visualizzata la finestra di dialogo Proprietà server.Immettere le informazioni nei campi obbligatori.Fare clic su **OK**. Il nuovo server viene aggiunto all'elenco dei server disponibili.CNS-Configuration Engine - Vengono visualizzate informazioni diverse a seconda che venga selezionato il tipo di IP statico o dinamico:**Statico (Static**) - Fate clic sulla freccia per visualizzare un elenco dei motori di configurazione. Selezionare il Configuration Engine che gestisce il dispositivo. Se il motore di configurazione non è presente nell'elenco, attenersi alla seguente procedura:Fare clic sulla freccia, quindi selezionare **+ Aggiungi motore di configurazione**... Viene visualizzata la finestra di dialogo Proprietà motore di configurazione.Immettere le informazioni nei campi obbligatori.Fare clic su **OK**. Il nuovo motore di configurazione viene aggiunto all'elenco dei motori di configurazione disponibili.**Dinamico**: fare clic sulla freccia per visualizzare un elenco di server. Selezionare il server che gestisce il dispositivo. Se il server non è presente nell'elenco, procedere come segue:Fare clic sulla freccia, quindi selezionare **+ Aggiungi server**... Verrà visualizzata la finestra di dialogo Proprietà server.Immettere le informazioni nel campo obbligatorio.Fare clic su **OK**. Il nuovo server viene aggiunto all'elenco dei server disponibili.

6. Attenersi alla seguente procedura:Per gestire il dispositivo in Security Manager, selezionare la casella di controllo **Gestisci in Cisco Security Manager**. Questa è l'impostazione predefinita.Se l'unica funzione del dispositivo che si sta aggiungendo è quella di fungere da endpoint VPN, deselezionare la casella di controllo **Gestisci in Cisco Security Manager**.Security Manager non gestirà le configurazioni, né le caricherà o scaricherà sul dispositivo.
7. Per gestire un contesto di sicurezza, selezionare la casella di controllo Contesto di sicurezza del dispositivo non gestito il cui dispositivo padre (PIX Firewall, ASA o FWSM) non è gestito da Security Manager.Èpossibile partizionare un firewall PIX, un'ASA o un FWSM in più firewall di sicurezza, noti anche come contesti di sicurezza. Ogni contesto è un sistema indipendente, con la propria configurazione e le proprie regole. È possibile gestire questi contesti autonomi in Security Manager, anche se l'elemento padre (PIX Firewall, ASA o FWSM) non è gestito da Security Manager.**Nota:** questo campo è attivo solo se il dispositivo selezionato nel selettore di dispositivi è un dispositivo firewall, ad esempio PIX Firewall, ASA o FWSM, che supporta il contesto di sicurezza.
8. Per gestire un router Cisco IOS in IPS Manager, selezionare la casella di controllo **Gestisci in IPS Manager**.Questo campo è attivo solo se è stato selezionato un router Cisco IOS dal selettore di dispositivi.**Nota:** IPS Manager può gestire le funzionalità IPS solo su un router Cisco IOS con funzionalità IPS. Per ulteriori informazioni, vedere la documentazione di IPS.Se si seleziona la casella di controllo Gestione in Gestione IPS, è necessario selezionare anche la casella di controllo Gestione in Cisco Security Manager.Se il dispositivo selezionato è IDS, questo campo non è attivo. Tuttavia, la casella di controllo è selezionata perché IPS Manager gestisce i sensori IDS.Se il dispositivo selezionato è PIX Firewall, ASA o FWSM, questo campo non è attivo perché IPS Manager non gestisce questi tipi di dispositivo.
9. Fare clic su **Finish** (Fine).Il sistema esegue le operazioni di convalida dei dispositivi:Se i dati immessi non sono corretti, il sistema genera messaggi di errore e visualizza la pagina in cui si è verificato l'errore.Se i dati immessi sono corretti, il dispositivo viene aggiunto all'inventario e visualizzato nel selettore Dispositivo.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Messaggi di errore

Quando si aggiunge un IPS al CSM, viene visualizzata la finestra di dialogo `Periferica non valida: Impossibile dedurre il SysObjId per il tipo di piattaforma` che viene visualizzato come messaggio di errore.

Soluzione

Per risolvere questo messaggio di errore, completare la procedura seguente.

1. Arrestare il servizio Daemon di CSM in Windows, quindi scegliere **Programmi > CSCOpx > MDC > athena > config > Directory**, dove è possibile trovare `VMS-SysObjID.xml`.
2. Sul sistema CSM, sostituire il file VMS-SysObjID.xml originale, che per impostazione predefinita si trova in `C:\Program Files\CSCOpx\MDC\athena\config\directory`, con il file `VMS-SysObjID.xml` più recente.
3. Riavviare il servizio Gestione daemon CSM (CRMDmgtd) e riprovare ad aggiungere o individuare i dispositivi interessati.

Informazioni correlate

- Pagina di supporto di Cisco Security Manager
- Pagina di supporto per Cisco Intrusion Detection System
- Documentazione e supporto tecnico – Cisco Systems