Integrazione di Security Manager con ACS

Sommario

Introduzione

In questo documento viene descritto come integrare Cisco Security Manager con Cisco Secure Access Control Server (ACS).

Cisco Secure ACS fornisce l'autorizzazione dei comandi per gli utenti che utilizzano applicazioni di gestione, ad esempio Cisco Security Manager, per configurare i dispositivi di rete gestiti. Il supporto per l'autorizzazione dei comandi è fornito da tipi di set di autorizzazioni dei comandi univoci, denominati ruoli in Cisco Security Manager, che contengono un set di autorizzazioni. Queste autorizzazioni, chiamate anche privilegi, determinano le azioni che possono eseguire gli utenti con ruoli specifici in Cisco Security Manager.

Cisco Secure ACS usa TACACS+ per comunicare con le applicazioni di gestione. Per consentire la comunicazione tra Cisco Security Manager e Cisco Secure ACS, è necessario configurare il server CiscoWorks in Cisco Secure ACS come client AAA che utilizza TACACS+. Inoltre, per accedere al server CiscoWorks sicuro, è necessario fornire il nome e la password dell'amministratore da usare. Una volta soddisfatti questi requisiti, si garantisce la validità delle

comunicazioni tra Cisco Security Manager e Cisco Secure ACS.

Quando Cisco Security Manager comunica inizialmente con Cisco Secure ACS, impone a Cisco ACS la creazione di ruoli predefiniti, visualizzati nella sezione Componenti del profilo condiviso dell'interfaccia HTML di Cisco Secure ACS. Inoltre, stabilisce che TACACS+ debba autorizzare un servizio personalizzato. Questo servizio personalizzato viene visualizzato nella pagina TACACS+ (Cisco IOS®) della sezione Configurazione interfaccia dell'interfaccia HTML. È quindi possibile modificare le autorizzazioni incluse in ogni ruolo di Cisco Security Manager e applicare questi ruoli a utenti e gruppi di utenti.

Nota: non è possibile integrare CSM con ACS 5.2 perché non è supportato.

Prerequisiti

Requisiti

Per utilizzare Cisco Secure ACS, verificare che:

- I ruoli vengono definiti che includono i comandi necessari per eseguire le funzioni necessarie in Cisco Security Manager.
- La limitazione dell'accesso alla rete (NAR) include il gruppo di dispositivi (o i dispositivi) che si desidera amministrare, se si applica un NAR al profilo.
- I nomi dei dispositivi gestiti vengono digitati e scritti in maiuscolo in modo identico in Cisco Secure ACS e Cisco Security Manager.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Security Manager versione 3.0
- Cisco Secure ACS versione 3.3

Nota: prima di eseguire l'installazione nell'ambiente di rete, accertarsi di scegliere le versioni CSM e ACS compatibili. Ad esempio, Cisco ha testato ACS 3.3 solo con CSM 3.0 e si è fermato per le versioni CSM più recenti. Si consiglia di utilizzare CSM 3.0 con ACS 3.3. Per ulteriori informazioni sulle varie versioni del software, vedere la tabella Matrice di compatibilità.

Versioni di Cisco Security Manager	Versioni ACS CS testate
3.0.0 3.0.0 SP1	Windows 3.3(3) e 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Solutions Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Solutions Engine 4.0(1) Windows 4.1(1) e 4.1(3)
3.1.1.3.0.2 SP1.3.0.2 SP2	Solutions Engine v4.0(1) Windows 4.1(2), 4.1(3) e 4.1(4)
3.1.1 SP1	Solutions Engine 4.0(1) Windows 4.1(4)

3.1.1 SP2	Solutions Engine 4.0(1) Windows 4.1(4) e 4.2(0)
3.2.0	Solutions Engine 4.1(4) Windows 4.1(4) e 4.2(0)
3.2.1	Solutions Engine 4.1(4) Windows 4.2(0)

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Integrazione di Cisco Security Manager con Cisco Secure ACS

In questa sezione vengono descritti i passaggi necessari per integrare Cisco Security Manager con Cisco Secure ACS. Alcuni passaggi contengono diversi passaggi secondari. Questi passaggi e passaggi secondari devono essere eseguiti in ordine. Questa sezione contiene anche riferimenti a procedure specifiche utilizzate per eseguire ciascun passo.

Attenersi alla seguente procedura:

1. **Pianificare l'autenticazione amministrativa e il modello di autorizzazione.**Prima di utilizzare Cisco Security Manager, è necessario decidere il modello amministrativo. Ciò include la definizione dei ruoli amministrativi e degli account che si intende utilizzare.**Suggerimento:** quando si definiscono i ruoli e le autorizzazioni dei potenziali amministratori, considerare anche se abilitare o meno Workflow. Questa selezione determina le modalità di limitazione dell'accesso.
2. **Installare Cisco Secure ACS, Cisco Security Manager e CiscoWorks Common Services.**Installare Cisco Secure ACS versione 3.3 su un server Windows 2000/2003. Installare CiscoWorks Common Services e Cisco Security Manager su un server Windows 2000/Windows 2003 diverso.Per ulteriori informazioni, fare riferimento a questi documenti:Guida all'installazione di Cisco Security Manager 3.0Guida all'installazione di Cisco Secure ACS per Windows 3.3**Nota:** prima di scegliere le versioni software CSM e ACS, vedere la tabella Matrice di compatibilità per ulteriori informazioni.
3. **Eseguire le procedure di integrazione in Cisco Secure ACS.**Definire gli utenti di Cisco Security Manager come utenti ACS e assegnarli ai gruppi di utenti in base al ruolo pianificato, aggiungere tutti i dispositivi gestiti (nonché il server CiscoWorks/Security Manager) come client AAA e creare un utente per il controllo dell'amministrazione. Per ulteriori informazioni, vedere Procedure di integrazione eseguite in Cisco Secure ACS.
4. **Eseguire le procedure di integrazione in CiscoWorks Common Services.**Configurare un utente locale che corrisponda all'amministratore definito in Cisco Secure ACS, definire lo stesso utente per l'impostazione dell'identità del sistema e configurare ACS come modalità di installazione AAA.Per ulteriori informazioni, vedere Procedure di integrazione eseguite in

CiscoWorks.

5. **Assegnare ruoli ai gruppi di utenti in Cisco Secure ACS.**Assegnare ruoli a ogni gruppo di utenti configurato in Cisco Secure ACS. La procedura da utilizzare dipende dalla configurazione dei gruppi di dispositivi di rete (NDG).Per ulteriori informazioni, vedere Assegnazione di ruoli ai gruppi di utenti in Cisco Secure ACS.

Procedure di integrazione eseguite in Cisco Secure ACS

In questa sezione viene descritta la procedura da seguire per integrare Cisco Secure ACS con Cisco Security Manager:

1. Definizione di utenti e gruppi di utenti in Cisco Secure ACS
2. Aggiunta di dispositivi gestiti come client AAA in Cisco Secure ACS
3. Creare un utente di Administration Control in Cisco Secure ACS

Definizione di utenti e gruppi di utenti in Cisco Secure ACS

Tutti gli utenti di Cisco Security Manager devono essere definiti in Cisco Secure ACS e ricevere un ruolo appropriato al loro lavoro. Il modo più semplice per eseguire questa operazione consiste nel dividere gli utenti in diversi gruppi in base a ciascun ruolo predefinito disponibile in ACS. Ad esempio, assegnare tutti gli amministratori di sistema a un gruppo, tutti gli operatori di rete a un altro gruppo e così via. Per ulteriori informazioni sui ruoli predefiniti in ACS, fare riferimento a Cisco Secure ACS Default Roles.

Èinoltre necessario creare un altro utente a cui sia assegnato il ruolo di amministratore di sistema con autorizzazioni complete. Le credenziali stabilite per questo utente verranno utilizzate successivamente nella pagina Configurazione identità di sistema in CiscoWorks. Per ulteriori informazioni, vedere Definizione dell'utente dell'identità del sistema.

In questa fase è sufficiente assegnare gli utenti a gruppi diversi. L'assegnazione effettiva dei ruoli a questi gruppi viene eseguita in un secondo momento, dopo la registrazione di CiscoWorks, Cisco Security Manager e di altre applicazioni in Cisco Secure ACS.

Suggerimento: prima di procedere, installare CiscoWorks Common Services e Cisco Security Manager su un server Windows 2000/2003. Installare Cisco Secure ACS su un server Windows 2000/2003 diverso.

1. Accedere a Cisco Secure ACS.
2. Configurare un utente con autorizzazioni complete:Fare clic su **User Setup** (Impostazioni utente) sulla barra di spostamento.Nella pagina Impostazione utente, immettere un nome per il nuovo utente, quindi fare clic su **Aggiungi/Modifica**.Selezionare un metodo di autenticazione dall'elenco Autenticazione password in Impostazione utente.Immettere e confermare la password per il nuovo utente.Selezionare **Gruppo 1** come gruppo a cui è assegnato l'utente.Per creare l'account utente, fare clic su **Submit** (Invia).
3. Ripetere il passaggio 2 per ciascun utente di Cisco Security Manager. Cisco consiglia di dividere gli utenti in gruppi in base al ruolo assegnato a ciascun utente:Gruppo 1: amministratori di sistemaGruppo 2 - Amministratori della sicurezzaGruppo 3 - Responsabili approvazione della sicurezzaGruppo 4 - Amministratori di reteGruppo 5 - ApprovatoriGruppo 6 - Operatori di reteGruppo 7 - Help DeskPer ulteriori informazioni sulle autorizzazioni

predefinite associate a ogni ruolo, vedere la tabella. Per ulteriori informazioni sulla personalizzazione dei ruoli utente, fare riferimento a Personalizzazione dei ruoli Cisco Secure ACS.**Nota:** in questa fase, i gruppi stessi sono raccolte di utenti senza definizioni di ruolo. I ruoli vengono assegnati a ogni gruppo al termine del processo di integrazione. Per ulteriori informazioni, vedere Assegnazione di ruoli ai gruppi di utenti in Cisco Secure ACS.

4. Creare un utente aggiuntivo e assegnarlo al gruppo degli amministratori di sistema. Le credenziali stabilite per questo utente verranno utilizzate successivamente nella pagina Configurazione identità di sistema in CiscoWorks. Per ulteriori informazioni, vedere Definizione dell'utente dell'identità del sistema.
5. Continuare con l'aggiunta di dispositivi gestiti come client AAA in Cisco Secure ACS.

Aggiunta di dispositivi gestiti come client AAA in Cisco Secure ACS

Prima di iniziare a importare i dispositivi in Cisco Security Manager, è necessario configurare ciascun dispositivo come client AAA nel Cisco Secure ACS. Inoltre, è necessario configurare il server CiscoWorks/Security Manager come client AAA.

Se Cisco Security Manager gestisce i contesti di sicurezza configurati sui dispositivi firewall, inclusi i contesti di sicurezza configurati sui FWSM per i dispositivi Catalyst 6500/7600, ciascun contesto deve essere aggiunto singolarmente ai Cisco Secure ACS.

Il metodo da utilizzare per aggiungere dispositivi gestiti dipende dal fatto che si desideri limitare gli utenti alla gestione di un particolare set di dispositivi con gruppi di dispositivi di rete (NDG). Vedere una delle sezioni seguenti:

- Se si desidera che gli utenti abbiano accesso a tutti i dispositivi, aggiungere i dispositivi come descritto in Aggiunta di dispositivi come client AAA senza NDG.
- Se si desidera che gli utenti abbiano accesso solo a determinati NDG, aggiungere i dispositivi come descritto in Configurazione dei gruppi di dispositivi di rete da utilizzare in Security Manager.

Aggiunta di dispositivi come client AAA senza NDG

In questa procedura viene descritto come aggiungere dispositivi come client AAA di un Cisco Secure ACS. Per informazioni complete su tutte le opzioni disponibili, consultare la sezione *Configurazione client AAA* in Configurazione di rete.

Nota: ricordare di aggiungere il server CiscoWorks/Security Manager come client AAA.

1. Fare clic su **Network Configuration** (Configurazione rete) sulla barra di navigazione di Cisco Secure ACS.
2. Fare clic su **Add Entry** (Aggiungi voce) sotto la tabella Client AAA.
3. Immettere il nome host del client AAA (fino a 32 caratteri) nella pagina Aggiungi client AAA. Il nome host del client AAA deve corrispondere al nome visualizzato che si intende utilizzare per il dispositivo in Cisco Security Manager.Ad esempio, se si intende aggiungere un nome di dominio al nome del dispositivo in Cisco Security Manager, il nome host del client AAA in ACS deve essere **<nome_dispositivo>.<nome_dominio>**.Quando si assegna un nome al server CiscoWorks, si consiglia di utilizzare il nome host completo. Accertarsi di aver digitato correttamente il nome dell'host. Il nome host non fa distinzione tra maiuscole e

minuscole.Quando si assegna un nome a un contesto di sicurezza, aggiungere il nome del contesto (_**<nome_contesto>**) al nome del dispositivo. Per gli FWSM, questa è la convenzione di denominazione:Blade FWSM—**<nome_chassis>_FW_<numero_slot>**Contesto di sicurezza—**<nome_chassis>_FW_<numero_slot>_<nome_contesto>**

4. Immettere l'indirizzo IP del dispositivo di rete nel campo AAA Client IP Address (Indirizzo IP client AAA).
5. Immettere il segreto condiviso nel campo Chiave.
6. Selezionare **TACACS+ (Cisco IOS)** dall'elenco Authenticate Using.
7. Per salvare le modifiche, fare clic su **Submit** (Invia). La periferica aggiunta viene visualizzata nella tabella Client AAA.
8. Ripetere i passaggi da 1 a 7 per aggiungere altri dispositivi.
9. Dopo aver aggiunto tutti i dispositivi, fare clic su **Submit + Restart** (Invia e riavvia).
10. Continuare con la creazione di un utente del controllo di amministrazione in Cisco Secure ACS.

Configurare i gruppi di dispositivi di rete da utilizzare in Security Manager

Cisco Secure ACS consente di configurare i gruppi di dispositivi di rete (NDG) che contengono dispositivi specifici da gestire. Ad esempio, è possibile creare i gruppi di distribuzione di servizi di rete per ogni area geografica o gruppo di distribuzione di servizi di rete corrispondente alla struttura organizzativa. Se utilizzati con Cisco Security Manager, i servizi di rete consentono di fornire agli utenti livelli di autorizzazioni diversi in base ai dispositivi che devono gestire. Ad esempio, con i servizi di rete è possibile assegnare autorizzazioni di amministratore di sistema Utente A ai dispositivi situati in Europa e autorizzazioni di Help Desk ai dispositivi situati in Asia. È quindi possibile assegnare le autorizzazioni opposte all'utente B.

I gruppi di criteri di rete non vengono assegnati direttamente agli utenti. I gruppi di criteri di rete vengono invece assegnati ai ruoli definiti per ogni gruppo di utenti. Ogni gruppo di distribuzione dei servizi di rete può essere assegnato a un solo ruolo, ma ogni ruolo può includere più gruppi di distribuzione dei servizi di rete. Queste definizioni vengono salvate come parte della configurazione per il gruppo di utenti selezionato.

In questi argomenti vengono descritti i passaggi di base necessari per configurare i gruppi di criteri di rete:

- Attivare la funzionalità NDG
- Crea gruppi di criteri di rete
- Associa gruppi di criteri di rete e ruoli a gruppi di utenti

Attivare la funzionalità NDG

Ènecessario attivare la funzionalità NDG prima di poter creare NDG e inserirvi dispositivi.

1. Fare clic su **Interface Configuration** (Configurazione interfaccia) nella barra di navigazione di Cisco Secure ACS.
2. Fare clic su **Opzioni avanzate**.
3. Scorrere verso il basso, quindi selezionare la casella di controllo **Gruppi di dispositivi di rete**.
4. Fare clic su **Invia**.

5. Continuare con la creazione di gruppi di distribuzione di rete.

Crea gruppi di criteri di rete

In questa procedura viene descritto come creare i gruppi di distribuzione di rete e inserirvi dispositivi. Ogni dispositivo può appartenere a un solo gruppo di distribuzione di rete.

Nota: Cisco consiglia di creare un NDG speciale che contenga il server CiscoWorks/Security Manager.

1. Fare clic su **Configurazione di rete** sulla barra di spostamento.Tutti i dispositivi vengono inizialmente posizionati in Non assegnato, che contiene tutti i dispositivi che non sono stati posizionati in un NDG. Tenere presente che Non assegnato non è un gruppo di distribuzione dei nomi.
2. Creazione di gruppi di criteri di rete:Fare clic su **Aggiungi voce**.Immettere un nome per NDG nella pagina Nuovo gruppo di dispositivi di rete. La lunghezza massima è 24 caratteri. Gli spazi sono consentiti.**Opzionale se con versione 4.0 o successiva:** Immettere una chiave che deve essere utilizzata da tutti i dispositivi del gruppo di distribuzione di rete. Se si definisce una chiave per il gruppo di distribuzione di rete, questa sostituirà qualsiasi chiave definita per i singoli dispositivi del gruppo.Fare clic su **Submit** (Invia) per salvare NDG.Ripetere le fasi da a a d per creare più gruppi di distribuzione non globali.
3. Popolare gli NDG con i dispositivi:Fare clic sul nome del gruppo di distribuzione di rete nell'area Gruppi di dispositivi di rete.Fare clic su **Add Entry** (Aggiungi voce) nell'area Client AAA.Definire i dettagli del dispositivo da aggiungere al gruppo di distribuzione di rete, quindi fare clic su **Invia**. Per ulteriori informazioni, vedere Aggiungere dispositivi come client AAA senza NDG.Ripetere le fasi b e c per aggiungere il resto dei dispositivi agli NDG. L'unico dispositivo che può essere lasciato nella categoria Non assegnato è il server AAA predefinito.Dopo aver configurato l'ultimo dispositivo, fare clic su **Submit + Restart** (Invia e riavvia).
4. Continuare con la creazione di un utente del controllo di amministrazione in Cisco Secure ACS.

Creare un utente di Administration Control in Cisco Secure ACS

Utilizzare la pagina Administration Control di Cisco Secure ACS per definire l'account amministratore da usare quando si definisce la modalità di installazione AAA in CiscoWorks Common Services. Per ulteriori informazioni, vedere Configurare la modalità di installazione AAA in CiscoWorks.

1. Fare clic su **Administration Control** nella barra di navigazione di Cisco Secure ACS.
2. Fare clic su **Aggiungi amministratore**.
3. Nella pagina Aggiungi amministratore immettere un nome e una password per l'amministratore.
4. Per fornire autorizzazioni amministrative complete a questo amministratore, fare clic su **Concedi tutto** nell'area Privilegi amministratore.
5. Per creare l'amministratore, fare clic su **Submit** (Invia).

Nota: fare riferimento a Amministratori e criteri amministrativi per ulteriori informazioni sulle opzioni disponibili quando si configura un amministratore.

Procedure di integrazione eseguite in CiscoWorks

In questa sezione viene descritto come completare la procedura descritta in CiscoWorks Common Services per integrarlo con Cisco Security Manager:

- Creare un utente locale in CiscoWorks
- Definisci utente identità sistema
- Configurazione della modalità di installazione AAA in CiscoWorks

Completare questi passaggi dopo aver completato le procedure di integrazione eseguite in Cisco Secure ACS. Common Services esegue la registrazione effettiva di tutte le applicazioni installate, ad esempio Cisco Security Manager, Auto-Update Server e IPS Manager, in Cisco Secure ACS.

Creare un utente locale in CiscoWorks

Utilizzare la pagina Configurazione utente locale in CiscoWorks Common Services per creare un account utente locale che duplichi l'amministratore creato in precedenza in Cisco Secure ACS. Questo account utente locale viene utilizzato successivamente per la configurazione dell'identità del sistema. Per ulteriori informazioni, vedere.

Nota: prima di procedere, creare un amministratore in Cisco Secure ACS. Per istruzioni, vedere Definizione di utenti e gruppi di utenti in Cisco Secure ACS.

1. Accedere a CiscoWorks con l'account utente **admin** predefinito.
2. Scegliere **Server > Protezione** da Servizi comuni, quindi scegliere **Configurazione utente locale** dal sommario.
3. Fare clic su **Add**.
4. Immettere lo stesso nome e la stessa password immessi al momento della creazione dell'amministratore in Cisco Secure ACS. Vedere il passaggio 4 in Definizione di utenti e gruppi di utenti in Cisco Secure ACS.
5. Selezionare tutte le caselle di controllo in Ruoli tranne Esporta dati.
6. Fare clic su **OK** per creare l'utente.

Definisci utente identità sistema

Utilizzare la pagina Configurazione dell'identità del sistema nei servizi comuni di CiscoWorks per creare un utente di trust, noto come utente dell'identità del sistema, che consenta la comunicazione tra server appartenenti allo stesso dominio e processi applicativi situati sullo stesso server. Le applicazioni utilizzano l'utente System Identity per autenticare i processi sui server CiscoWorks locali o remoti. Ciò è particolarmente utile quando le applicazioni devono essere sincronizzate prima dell'accesso di qualsiasi utente.

Inoltre, l'utente System Identity viene spesso utilizzato per eseguire una sottoattività quando l'attività principale è già autorizzata per l'utente connesso. Ad esempio, per modificare un dispositivo in Cisco Security Manager, è necessaria la comunicazione tra applicazioni tra Cisco Security Manager e Common Services DCR. Dopo che l'utente è autorizzato a eseguire l'operazione di modifica, viene utilizzato l'utente System Identity per richiamare il DCR.

L'utente di System Identity configurato in questa posizione deve essere identico all'utente con autorizzazioni amministrative (complete) configurato in ACS. In caso contrario, potrebbe non essere possibile visualizzare tutti i dispositivi e i criteri configurati in Cisco Security Manager.

Nota: prima di procedere, creare un utente locale con lo stesso nome e password dell'amministratore in CiscoWorks Common Services. Per istruzioni, vedere Creazione di un utente locale in CiscoWorks.

1. Scegliere **Server > Protezione**, quindi **Gestione trust multiserver > Impostazione identità di sistema** dal sommario.
2. Immettere il nome dell'amministratore creato per Cisco Secure ACS. Vedere il passaggio 4 in Definizione di utenti e gruppi di utenti in Cisco Secure ACS.
3. Immettere e verificare la password per questo utente.
4. Fare clic su **Apply** (Applica).

Configurazione della modalità di installazione AAA in CiscoWorks

Utilizzare la pagina Modalità di installazione AAA in CiscoWorks Common Services per definire il proprio Cisco Secure ACS come server AAA, che include la porta richiesta e la chiave privata condivisa. È inoltre possibile definire fino a due server di backup.

Questa procedura consente di eseguire la registrazione effettiva di CiscoWorks, Cisco Security Manager, IPS Manager (e, facoltativamente, Auto-Update Server) in Cisco Secure ACS.

1. Scegliere **Server > Protezione**, quindi **Configurazione modalità AAA** dal sommario.
2. Selezionare la casella di controllo **TACACS+** in Moduli di accesso disponibili.
3. Selezionare **ACS** come tipo di appliance AAA.
4. Immettere gli indirizzi IP di un massimo di tre server Cisco Secure ACS nell'area dei dettagli del server. I server secondario e terziario fungono da backup in caso di guasto del server principale.**Nota:** se tutti i server TACACS+ configurati non rispondono, è necessario accedere con l'account admin CiscoWorks Local, quindi ripristinare la modalità AAA su Non-ACS/CiscoWorks Local. Dopo aver ripristinato il servizio sui server TACACS+, ripristinare la modalità AAA su ACS.
5. Nell'area Login, immettere il nome dell'amministratore definito nella pagina Administration Control di Cisco Secure ACS. Per ulteriori informazioni, vedere Creare un utente di controllo dell'amministrazione in Cisco Secure ACS.
6. Immettere e verificare la password per l'amministratore.
7. Immettere e verificare la chiave segreta condivisa immessa quando è stato aggiunto il server Security Manager come client AAA di Cisco Secure ACS. Vedere il passaggio 5 in Aggiunta di dispositivi come client AAA senza NDG.
8. Selezionare la casella di controllo **Registra tutte le applicazioni installate con ACS** per registrare Cisco Security Manager e tutte le altre applicazioni installate con Cisco Secure ACS.
9. Per salvare le impostazioni, fare clic su **Apply** (Applica). Una barra di avanzamento visualizza lo stato della registrazione. Al termine della registrazione viene visualizzato un messaggio.
10. Se si integra Cisco Security Manager con una versione ACS, riavviare il servizio Cisco Security Manager Daemon Manager. Vedere Riavviare Daemon Manager per istruzioni.**Nota:** dopo la versione CSM 3.0.0, Cisco non esegue più i test con ACS 3.3(x) perché ha subito numerose patch ed è stata annunciata la fine del ciclo di vita. Pertanto, è necessario utilizzare la versione ACS appropriata per CSM 3.0.1 e versioni successive. Per ulteriori informazioni, vedere la tabella Matrice di compatibilità.
11. Accedere nuovamente a Cisco Secure ACS per assegnare i ruoli a ciascun gruppo di utenti. Per istruzioni, vedere Assegnare ruoli ai gruppi di utenti in Cisco Secure ACS.**Nota:**

l'installazione del server AAA configurata qui non viene mantenuta se si disinstalla CiscoWorks Common Services o Cisco Security Manager. Inoltre, non è possibile eseguire il backup e il ripristino di questa configurazione dopo la reinstallazione. Pertanto, se si esegue l'aggiornamento a una nuova versione di una delle applicazioni, è necessario riconfigurare la modalità di installazione AAA e registrare nuovamente Cisco Security Manager con ACS. Questo processo non è necessario per gli aggiornamenti incrementali. Se si installano ulteriori applicazioni, ad esempio AUS, su CiscoWorks, è necessario registrare nuovamente le nuove applicazioni e Cisco Security Manager.

Riavviare Gestione daemon

In questa procedura viene descritto come riavviare Daemon Manager del server Cisco Security Manager. Affinché le impostazioni AAA configurate abbiano effetto, è necessario eseguire questa operazione. È quindi possibile accedere nuovamente a CiscoWorks con le credenziali definite in Cisco Secure ACS.

1. Accedere al computer in cui è installato il server Cisco Security Manager.
2. Scegliere **Start > Programmi > Strumenti di amministrazione > Servizi** per aprire la finestra Servizi.
3. Dall'elenco dei servizi visualizzati nel riquadro di destra, selezionare **Cisco Security Manager Daemon Manager**.
4. Fare clic sul pulsante **Riavvia servizio** sulla barra degli strumenti.
5. Continuare con l'assegnazione di ruoli ai gruppi di utenti in Cisco Secure ACS.

Assegnazione di ruoli ai gruppi di utenti in Cisco Secure ACS

Dopo aver registrato CiscoWorks, Cisco Security Manager e altre applicazioni installate in Cisco Secure ACS, è possibile assegnare ruoli a ciascuno dei gruppi di utenti configurati in precedenza in Cisco Secure ACS. Questi ruoli determinano le azioni che gli utenti di ogni gruppo possono eseguire in Cisco Security Manager.

La procedura da utilizzare per assegnare i ruoli ai gruppi di utenti dipende dall'utilizzo o meno dei gruppi di distribuzione dei nomi (NDG):

- Assegnazione di ruoli a gruppi di utenti senza gruppi di criteri di rete
- Associa gruppi di criteri di rete e ruoli a gruppi di utenti

Assegnazione di ruoli a gruppi di utenti senza gruppi di criteri di rete

In questa procedura viene descritto come assegnare i ruoli predefiniti ai gruppi di utenti quando non sono definiti i gruppi di distribuzione di rete. per ulteriori informazioni, fare riferimento a Ruoli predefiniti di Cisco Secure ACS.

Nota: prima di procedere:

- Creare un gruppo di utenti per ogni ruolo predefinito. Per istruzioni, vedere Definizione di utenti e gruppi di utenti in Cisco Secure ACS.
- Completare le procedure descritte in Procedure di integrazione eseguite in Cisco Secure ACS e Procedure di integrazione eseguite in CiscoWorks.

Attenersi alla seguente procedura:

1. Accedere a Cisco Secure ACS.
2. Fare clic su **Imposta gruppo** sulla barra di spostamento.
3. Selezionare il gruppo di utenti per gli amministratori di sistema dall'elenco. Vedere il passaggio 2 di Definizione di utenti e gruppi di utenti in Cisco Secure ACS, quindi fare clic su **Modifica impostazioni**.

Associa gruppi di criteri di rete e ruoli a gruppi di utenti

Quando si associano i gruppi di distribuzione di rete ai ruoli da utilizzare in Cisco Security Manager, è necessario creare le definizioni in due punti della pagina Impostazione gruppo:

- Area CiscoWorks
- Area Cisco Security Manager

Le definizioni in ciascuna zona devono corrispondere il più possibile. Quando si associano ruoli personalizzati o ruoli ACS che non esistono in CiscoWorks Common Services, provare a definire un equivalente il più simile possibile in base alle autorizzazioni assegnate a tale ruolo.

Ènecessario creare associazioni per ogni gruppo di utenti da utilizzare con Cisco Security Manager. Ad esempio, se si dispone di un gruppo di utenti che contiene personale di supporto per l'area occidentale, è possibile selezionare tale gruppo di utenti, quindi associare il gruppo NDG che contiene i dispositivi di tale area al ruolo Help Desk.

Nota: prima di procedere, attivare la funzione NDG e creare gli NDG. Per ulteriori informazioni, vedere Configurare i gruppi di dispositivi di rete da utilizzare in Security Manager.

1. Fare clic su **Imposta gruppo** sulla barra di spostamento.
2. Selezionare un gruppo di utenti dall'elenco Gruppo, quindi fare clic su **Modifica impostazioni**.
3. Mappare i gruppi di criteri di rete e i ruoli da utilizzare in CiscoWorks:Nella pagina Configurazione gruppo, scorrere verso il basso fino all'area CiscoWorks in TACACS+ Settings.Selezionare **Assegna CiscoWorks per gruppo di dispositivi di rete**.Selezionare un NDG dall'elenco Gruppo dispositivi.Selezionare il ruolo a cui questo gruppo di distribuzione dei nomi deve essere associato dal secondo elenco.Fare clic su **Aggiungi associazione**. L'associazione viene visualizzata nella casella Gruppo dispositivi.Ripetere i passaggi da c a e per creare ulteriori associazioni.**Nota:** per rimuovere un'associazione, selezionarla dal gruppo di dispositivi e fare clic su Rimuovi associazione.
4. Scorrere l'area Cisco Security Manager e creare associazioni che corrispondano il più possibile alle associazioni definite nel passaggio 3.**Nota:** quando si selezionano i ruoli Security Approver o Security Administrator in Cisco Secure ACS, si consiglia di selezionare Network Administrator come ruolo CiscoWorks equivalente più vicino.
5. Per salvare le impostazioni, fare clic su **Submit** (Invia).
6. Ripetere i passaggi da 2 a 5 per definire i gruppi di indirizzi di rete per i restanti gruppi di utenti.
7. Dopo aver associato i gruppi di criteri di rete e i ruoli a ogni gruppo di utenti, fare clic su **Invia + Riavvia**.

Risoluzione dei problemi

1. Prima di iniziare a importare i dispositivi in Cisco Security Manager, è necessario configurare ciascun dispositivo come client AAA nel Cisco Secure ACS. Inoltre, è necessario configurare il server CiscoWorks/Security Manager come client AAA.
2. Se si riceve un log dei tentativi non riusciti, l'autore ha restituito un errore in Cisco Secure ACS.
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   Per risolvere il problema, verificare che il nome del dispositivo in ACS sia un nome di dominio completo.

Informazioni correlate

- Pagina di supporto di Cisco Security Access Control Server per Windows
- Pagina di supporto di Cisco Security Manager
- Cisco Secure Access Control Server per Windows
- Guida alla configurazione di Cisco Secure ACS 4.1
- Guida alla risoluzione dei problemi online di Cisco Secure ACS, 4.1
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure ACS per Windows)
- Documentazione e supporto tecnico – Cisco Systems