Integrazione di Cisco ACS 5.X con RSA SecurID Token Server

Sommario

[Introduzione](#)
[Premesse](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazioni](#)
[Server RSA](#)
[ACS versione 5.X Server](#)
[Verifica](#)
[ACS versione 5.X Server](#)
[Server RSA](#)
[Risoluzione dei problemi](#)
[Creare un record agente (sdconf.rec)](#)
[Reimposta segreto nodo (securid)](#)
[Sostituisci bilanciamento automatico del carico](#)
[Intervenire manualmente per rimuovere un server RSA SecurID inattivo](#)

Introduzione

In questo documento viene descritto come integrare un Cisco Access Control System (ACS) versione 5.x con la tecnologia di autenticazione RSA SecurID.

Premesse

Cisco Secure ACS supporta il server RSA SecurID come database esterno.

L'autenticazione a due fattori RSA SecurID è costituita dal PIN dell'utente e da un token RSA SecurID registrato singolarmente che genera codici token monouso basati su un algoritmo di codice temporale.

A intervalli fissi viene generato un codice token diverso, in genere ogni 30 o 60 secondi. Il server RSA SecurID convalida questo codice di autenticazione dinamica. Ogni token RSA SecurID è univoco e non è possibile prevedere il valore di un token futuro in base ai token passati.

Pertanto, quando insieme al PIN viene fornito un codice token corretto, esiste un elevato grado di certezza che la persona sia un utente valido. Pertanto, i server RSA SecurID forniscono un

meccanismo di autenticazione più affidabile rispetto alle password riutilizzabili convenzionali.

Èpossibile integrare Cisco ACS 5.x con la tecnologia di autenticazione RSA SecurID nei modi seguenti:

- Agente RSA SecurID: gli utenti vengono autenticati con nome utente e passcode tramite il protocollo RSA nativo.
- Protocollo RADIUS: gli utenti vengono autenticati con il nome utente e il passcode tramite il protocollo RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Sicurezza RSA
- Cisco Secure Access Control System (ACS)

Componenti usati

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

- Cisco Secure Access Control System (ACS) versione 5.x
- Server token RSA SecurID

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.

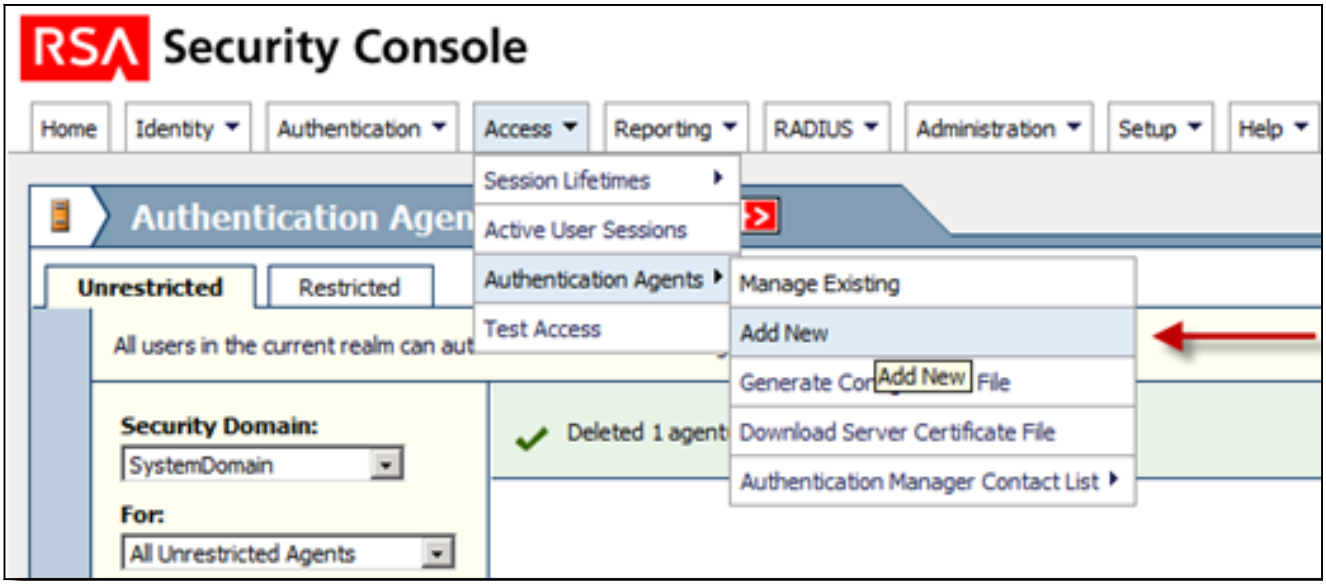
Configurazioni

Server RSA

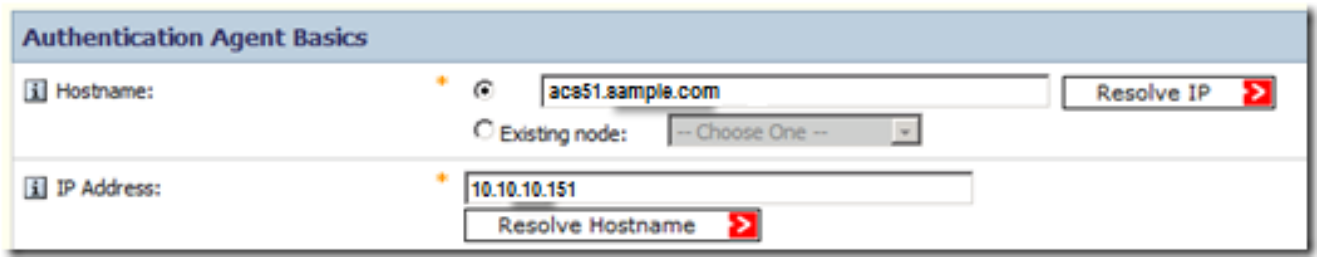
In questa procedura viene descritto come l'amministratore del server RSA SecurID crea gli agenti di autenticazione e un file di configurazione. Un agente di autenticazione è fondamentalmente un nome DNS (Domain Name Server) e un indirizzo IP di un dispositivo, software o servizio che dispone dei diritti per accedere al database RSA. Il file di configurazione descrive la topologia e la comunicazione RSA.

Nell'esempio, l'amministratore RSA deve creare due agenti per le due istanze di ACS.

1. In RSA Security Console, selezionare **Access > Authentication Agents > Add New** (Aggiungi nuovo):

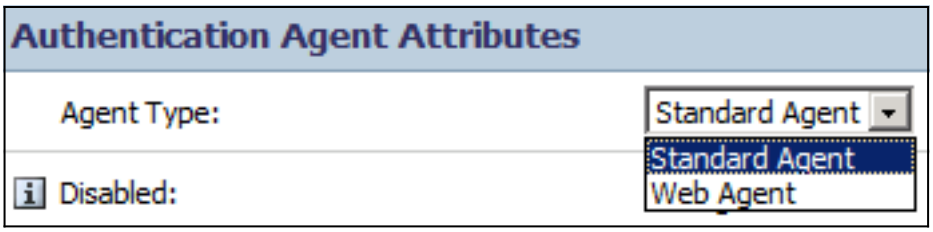


2. Nella finestra Aggiungi nuovo agente di autenticazione, definire un nome host e un indirizzo IP per ciascuno dei due agenti:

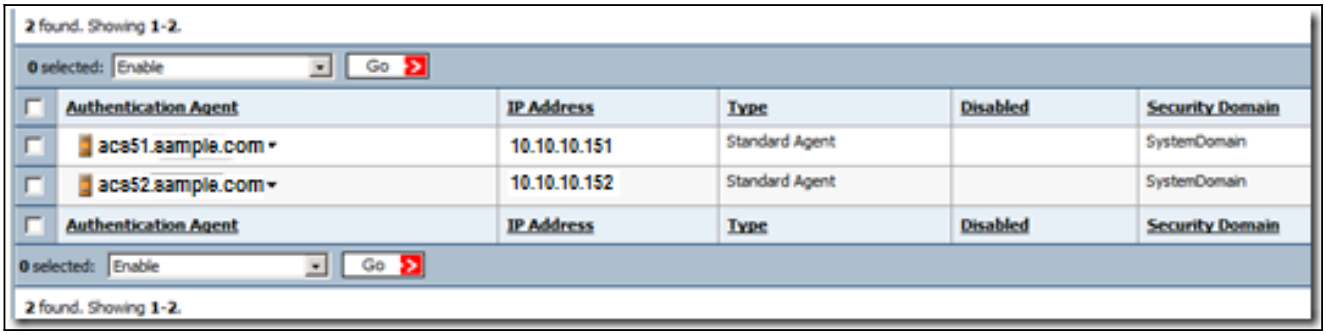


È consigliabile eseguire ricerche DNS dirette e inverse per gli agenti ACS.

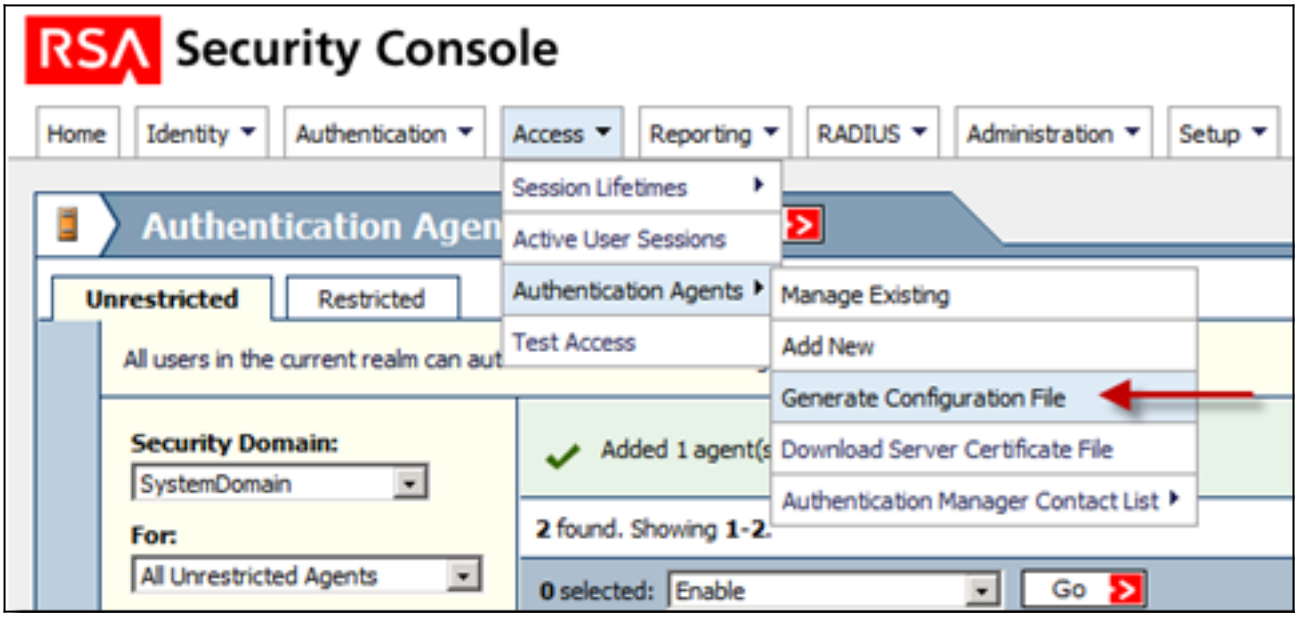
3. Definire il tipo di agente come agente standard:



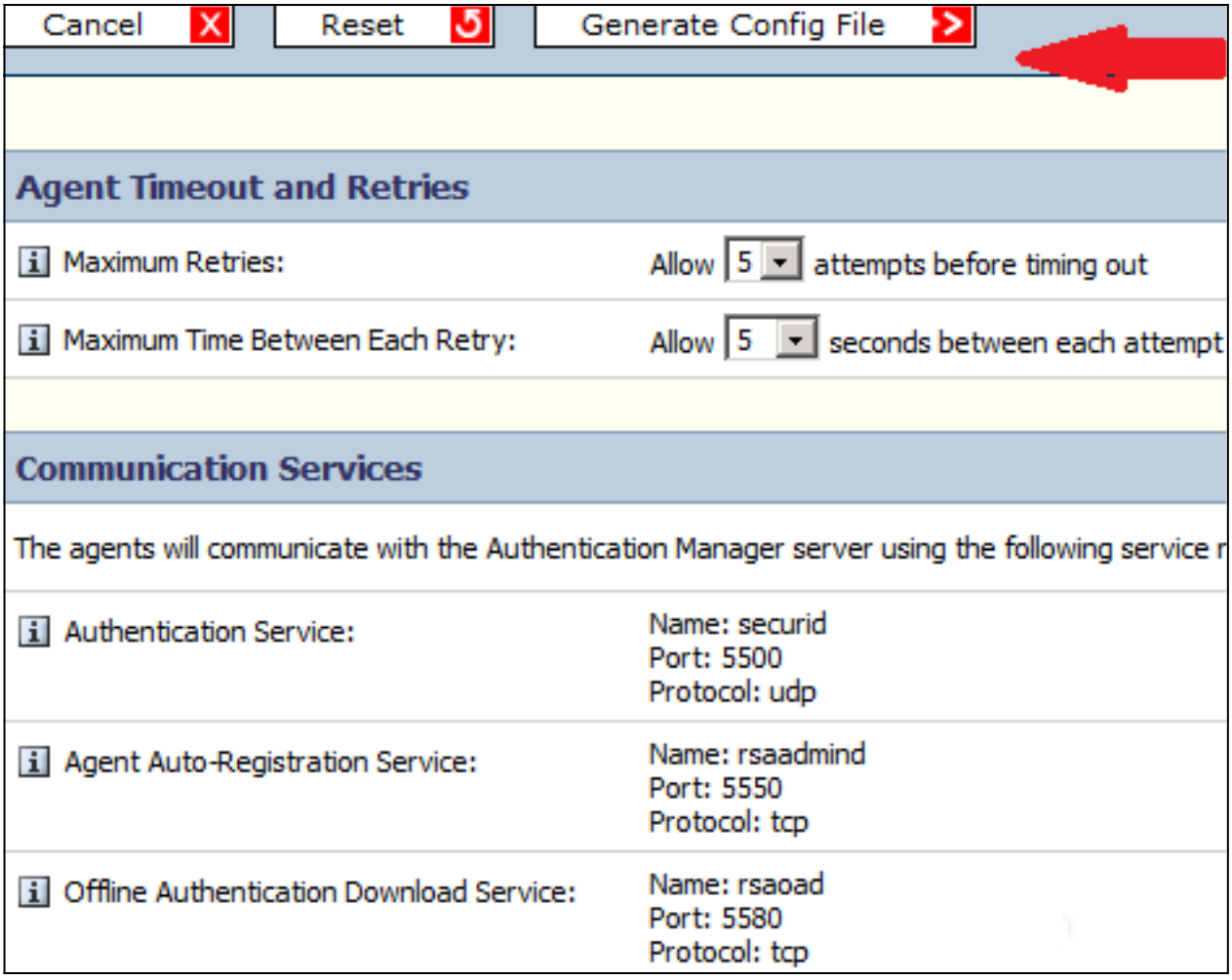
Questo è un esempio delle informazioni visualizzate dopo l'aggiunta degli agenti:



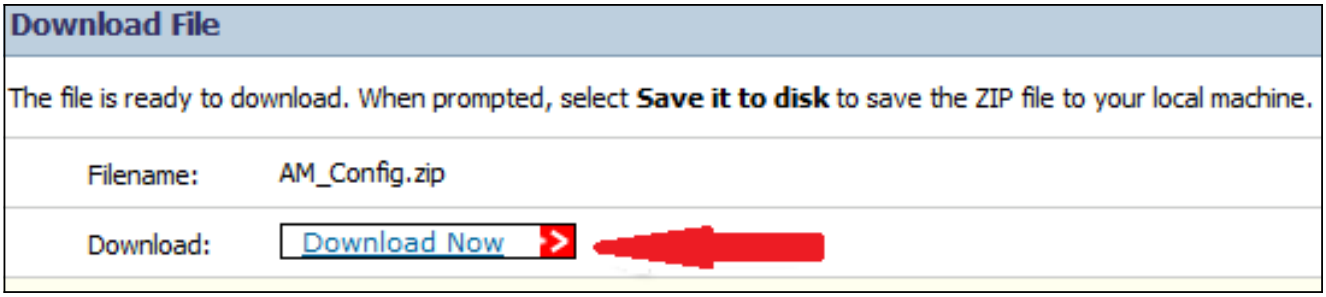
4. Nella console di sicurezza RSA, selezionare **Access > Authentication Agents > Generate Configuration File** per generare il file di configurazione sdconf.rec:



5. Utilizzare i valori predefiniti per Numero massimo di tentativi e Tempo massimo tra ogni tentativo:



6. Scaricare il file di configurazione:

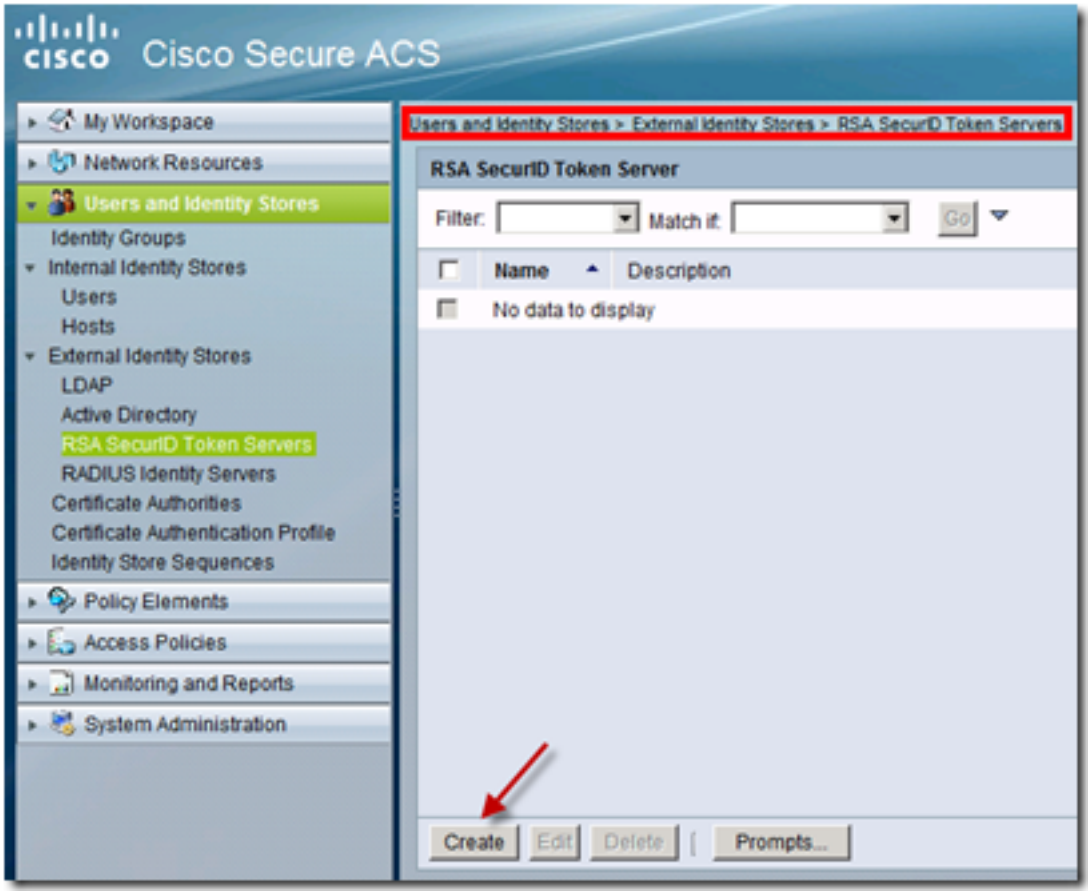


Il file .zip contiene il file di configurazione sdconf.rec necessario all'amministratore ACS per completare le attività di configurazione.

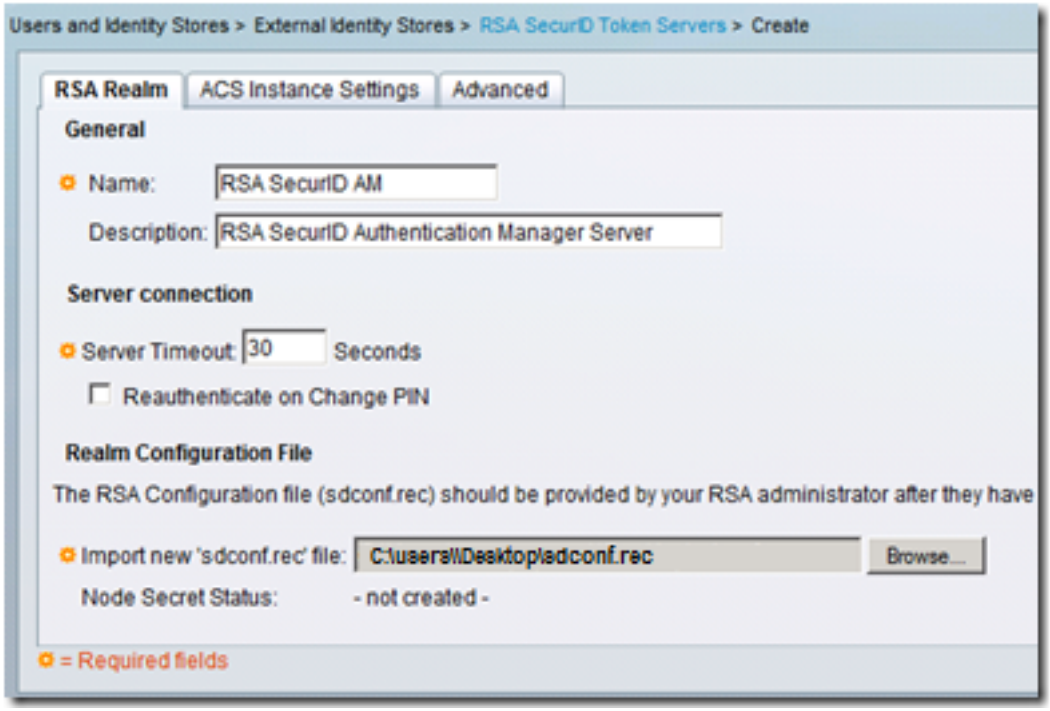
ACS versione 5.X Server

In questa procedura viene descritto come l'amministratore ACS recupera e invia il file di configurazione.

1. Nella console Cisco Secure ACS versione 5.x, selezionare **Users and Identity Stores > External Identity Stores > RSA SecurID Token Server**, quindi fare clic su **Crea**:



2. Immettere il nome del server RSA e individuare il file sdconf.rec scaricato dal server RSA:



3. Selezionare il file e fare clic su **Invia**.

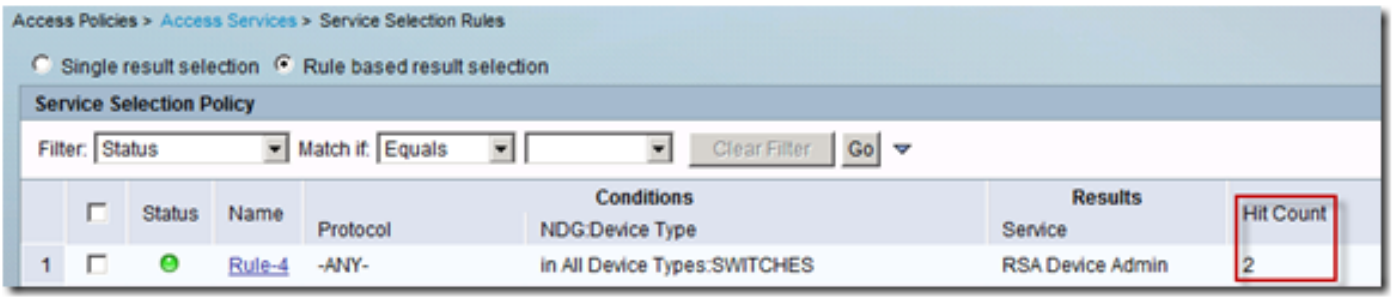
   Nota: La prima volta che ACS contatta il server di token, viene creato un altro file, denominato file segreto del nodo, per l'agente ACS in RSA Authentication Manager e viene scaricato in ACS. Questo file viene utilizzato per le comunicazioni crittografate.

Verifica

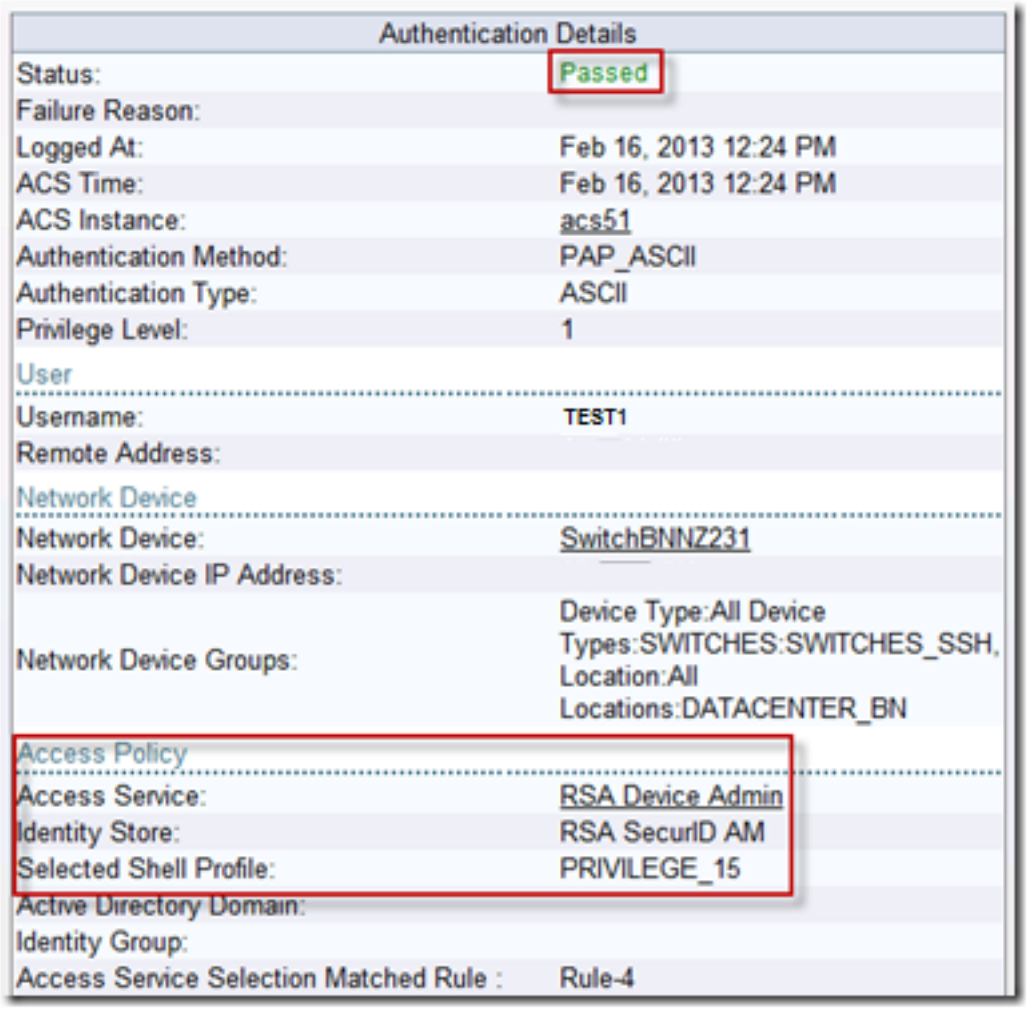
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

ACS versione 5.X Server

Per verificare che l'accesso sia riuscito, andare alla console ACS e rivedere il numero di accessi:



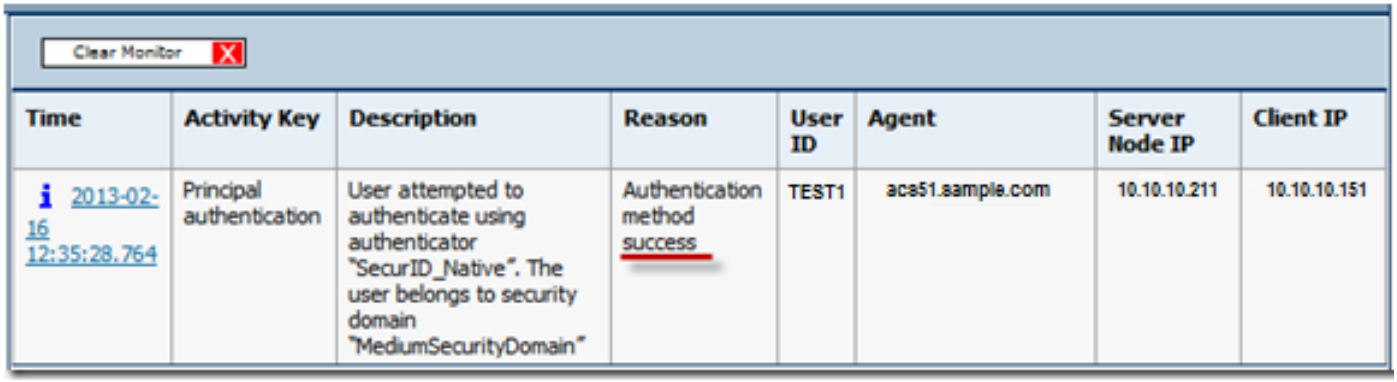
È inoltre possibile esaminare i dettagli di autenticazione dai log ACS:



Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	acs51
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	TEST1
Remote Address:	
Network Device	
Network Device:	SwitchBNNZ231
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
Access Policy	
Access Service:	RSA Device Admin
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

Server RSA

Per verificare la corretta autenticazione, accedere alla console RSA ed esaminare i registri:



Clear Monitor

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	Authentication method success	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Creare un record agente (sdconf.rec)

Per configurare un server token RSA SecurID in ACS versione 5.3, l'amministratore ACS deve disporre del file sdconf.rec. Il file sdconf.rec è un file di record di configurazione che specifica la modalità di comunicazione dell'agente RSA con l'area di autenticazione del server SecurID RSA.

Per creare il file sdconf.rec, l'amministratore RSA deve aggiungere l'host ACS come host agente sul server RSA SecurID e generare un file di configurazione per l'host agente.

Reimposta segreto nodo (securid)

Dopo la comunicazione iniziale dell'agente con il server RSA SecurID, il server fornisce all'agente un file segreto del nodo denominato securid. Le successive comunicazioni tra il server e l'agente si basano sullo scambio del segreto del nodo per verificare l'autenticità dell'altro.

In alcuni casi, gli amministratori potrebbero dover reimpostare il segreto del nodo:

1. L'amministratore RSA deve deselezionare la casella di controllo Segreto nodo creato sul record Host agente nel server RSA SecurID.
2. L'amministratore ACS deve rimuovere il file securid da ACS.

Sostituisci bilanciamento automatico del carico

L'agente RSA SecurID bilancia automaticamente i carichi richiesti sui server RSA SecurID del realm. Tuttavia, è possibile bilanciare manualmente il carico. È possibile specificare il server utilizzato da ciascun host agente. È possibile assegnare una priorità a ogni server in modo che l'host dell'agente indirizzi le richieste di autenticazione ad alcuni server con una frequenza maggiore rispetto ad altri.

È necessario specificare le impostazioni di priorità in un file di testo, salvarlo come sdopts.rec e caricarlo nel server ACS.

Intervenire manualmente per rimuovere un server RSA SecurID inattivo

Quando un server RSA SecurID è inattivo, il meccanismo di esclusione automatica non sempre funziona rapidamente. Rimuovere il file sdstatus.12 da ACS per velocizzare il processo.