Installazione, rinnovo e risoluzione dei problemi di certificati digitali SSL su Cisco ISE

Introduzione

In questo documento vengono illustrati i passaggi necessari per l'installazione, il rinnovo e la risoluzione dei certificati SSL più comuni rilevati in un Identity Services Engine. In questo documento viene descritto come procedere e viene fornita una lista di controllo dei problemi comuni da verificare e risolvere prima di iniziare a risolvere il problema e contattare il supporto tecnico Cisco.

Queste soluzioni provengono direttamente dalle richieste di assistenza risolte dal supporto tecnico Cisco. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dalle operazioni eseguite per risolvere i problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GUI Identity Service Engine

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

- Cisco Identity Service Engine 2.7

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.

Premesse

Un certificato è un documento elettronico che identifica un individuo, un server, una società o un'altra entità e associa tale entità a una chiave pubblica. Un certificato autofirmato è firmato dal proprio creatore. I certificati possono essere autofirmati o firmati digitalmente da un'Autorità di certificazione (CA) esterna. Un certificato digitale firmato dalla CA è considerato uno standard del settore e più sicuro.

I certificati vengono utilizzati in una rete per fornire un accesso sicuro. Cisco ISE utilizza i certificati per la comunicazione tra nodi e per la comunicazione con server esterni, quali il server Syslog, il server di feed e tutti i portali degli utenti finali (guest, sponsor e dispositivi personali). I certificati

identificano un nodo Cisco ISE per un endpoint e proteggono la comunicazione tra tale endpoint e il nodo Cisco ISE. I certificati vengono utilizzati per tutte le comunicazioni HTTPS e EAP (Extensible Authentication Protocol).

Configurazione

Le guide seguenti illustrano come importare e sostituire i certificati:

Importazione di un certificato di sistema

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

Sostituzione di un certificato scaduto

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

Problemi comuni

Scenario 1: Impossibile sostituire un certificato portale in scadenza su un nodo ISE

Errore

Durante l'associazione del nuovo certificato del portale al CSR, il processo di associazione del certificato non riesce con l'errore riportato di seguito:

Errore interno. Per ulteriori informazioni, rivolgersi all'amministratore ISE

Le cause più comuni di questo errore sono:

- Il nuovo certificato ha lo stesso nome soggetto del certificato esistente

- Importa un certificato rinnovato che utilizza la stessa chiave privata di un certificato esistente

Soluzione

1. Assegna temporaneamente l'utilizzo del portale a un altro certificato nello stesso nodo
2. Elimina certificato portale in scadenza
3. Installare il nuovo certificato portale, quindi assegnare l'utilizzo del portale

Ad esempio, se si desidera assegnare temporaneamente l'utilizzo del portale a un certificato esistente con utilizzo dell'autenticazione EAP, eseguire la procedura seguente:

Passaggio 1. Selezionare e modificare il certificato con l'utilizzo dell'autenticazione EAP, aggiungere il ruolo del portale in Utilizzo e salvare

Passaggio 2. Eliminare il certificato del portale in scadenza

Passaggio 3. Caricare il nuovo certificato del portale senza selezionare alcun ruolo (in Utilizzo) e Inviare

Passaggio 4. Selezionare e modificare il nuovo certificato del portale, assegnare il ruolo del portale in Utilizzo e salvataggio

Scenario 2: Impossibile generare due CSR per lo stesso nodo ISE con utilizzo multiuso

Errore

La creazione di un nuovo CSR per lo stesso nodo con utilizzo multiuso non riesce con l'errore: *Esiste già un altro certificato con lo stesso nome descrittivo. I nomi descrittivi devono essere univoci.*

Soluzione

I nomi descrittivi CSR sono hardcoded per ogni nodo ISE, pertanto non consente la creazione di 2 CSR per lo stesso nodo con utilizzo multiuso. Lo Use Case si trova in un nodo specifico, sono presenti un certificato firmato dalla CA utilizzato per l'autenticazione Admin e EAP e un altro certificato firmato dalla CA utilizzato per l'utilizzo di SAML e Portal ed entrambi i certificati scadranno.

In questo scenario:

Passaggio 1. Generare il primo CSR con utilizzo multiuso

Passaggio 2. Associare il certificato firmato dalla CA al primo CSR e assegnare il ruolo di autenticazione Admin e EAP

Passaggio 3. Generare un secondo CSR con utilizzo multiuso

Passaggio 4. Associare il certificato firmato dalla CA al secondo CSR e assegnare il ruolo SAML e portale

Scenario 3: Impossibile associare il certificato firmato dall'autorità di certificazione per l'utilizzo del portale oppure impossibile assegnare il tag del portale al certificato e ottenere un errore

Errore

Il binding del certificato firmato dalla CA per l'utilizzo del portale genera l'errore:

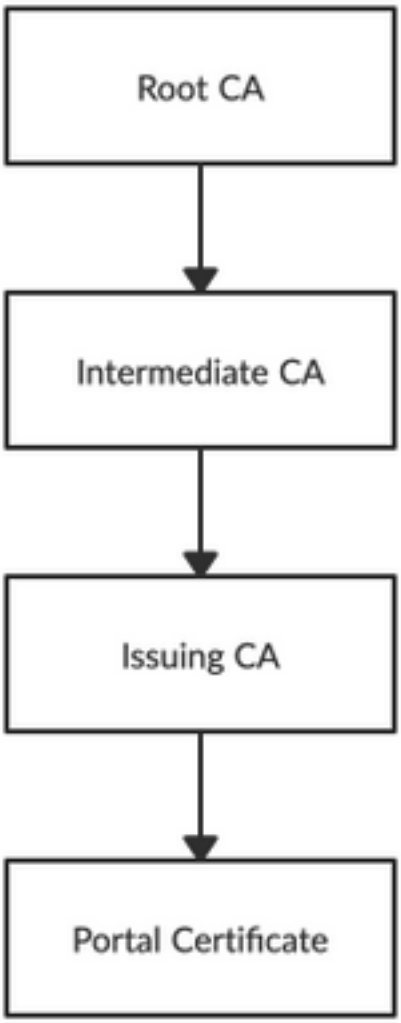
Sono presenti uno o più certificati attendibili che fanno parte della catena di certificati del sistema del portale o sono selezionati con il ruolo di autorizzazione amministratore basato su certificati con lo stesso nome soggetto ma con un numero di serie diverso. Importazione/aggiornamento interrotto. Per eseguire correttamente l'importazione o l'aggiornamento, è necessario disabilitare il ruolo di autorizzazione amministratore basato sul carrello da un certificato attendibile duplicato oppure modificare il ruolo del portale dal certificato di sistema che contiene il certificato attendibile

duplicato nella catena.

Soluzione

Passaggio 1. Controllare la catena di certificati del certificato firmato dall'autorità di certificazione (per l'utilizzo con il portale) e verificare se sono presenti certificati duplicati della catena nell'archivio Certificati attendibili.
Passaggio 2. Rimuovere il certificato duplicato o deselezionare la casella di controllo **Considera attendibile l'autenticazione dell'amministratore basata sui certificati** dal certificato duplicato.

Ad esempio, il certificato del portale firmato dalla CA presenta la catena di certificati seguente:



Verificare se sono presenti certificati duplicati per uno qualsiasi dei 3 certificati CA nella catena di certificati (potrebbe essere un certificato scaduto) e rimuovere il certificato duplicato dall'archivio dei certificati protetti.

Scenario 4: Impossibile eliminare il certificato autofirmato predefinito scaduto dall'archivio certificati attendibili

Errore

L'eliminazione del certificato autofirmato predefinito scaduto dall'archivio certificati attendibili

genera l'errore seguente:
Disabilitazione, eliminazione o attendibilità del certificato non consentita perché vi viene fatto riferimento da in Certificati di sistema E/O Destinazione syslog sicura in Destinazioni di registrazione remota.

Soluzione

1. Verificare che il certificato autofirmato predefinito scaduto non sia associato ad alcuna destinazione di registrazione remota esistente. È possibile verificare questa condizione in *Amministrazione > Sistema > Registrazione > Destinazioni registrazione remota > Seleziona e modifica SecureSyslogCollector(s)*
2. Verificare che il certificato autofirmato predefinito scaduto non sia associato ad alcun ruolo specifico (utilizzo). è possibile verificare questa condizione in *Amministrazione > Sistema > Certificati > Certificati di sistema*.

Se il problema persiste, contattare TAC.

Scenario 5: Impossibile associare il certificato PXGrid firmato dalla CA al CSR su un nodo ISE

Errore

Durante l'associazione del nuovo certificato pxGrid con CSR, il processo di associazione del certificato ha esito negativo e genera l'errore seguente:

Il certificato per pxGrid deve contenere sia l'autenticazione client che quella server nell'estensione per l'utilizzo chiavi esteso (EKU).

Soluzione

Verificare che il certificato pxGrid con firma CA disponga sia dell'autenticazione server Web TLS (1.3.6.1.5.5.7.3.1) che dell'utilizzo esteso delle chiavi TLS (1.3.6.1.5.5.7.3.2), in quanto viene utilizzato sia per l'autenticazione client che per l'autenticazione server (per proteggere la comunicazione tra il client pxGrid e il server)

Link di riferimento: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

Scenario 6: Impossibile eliminare il certificato autofirmato predefinito scaduto dall'archivio certificati attendibili a causa della configurazione esistente del profilo RA LDAP o SCEP

Errore

L'eliminazione del certificato autofirmato predefinito scaduto dall'archivio certificati attendibili genera l'errore seguente:

Impossibile eliminare il certificato di attendibilità perché vi viene fatto riferimento altrove,

probabilmente da un profilo RA SCEP o da un'origine identità LDAP

* Certificato server predefinito autofirmato

Per eliminare i certificati, eliminare il profilo RA SCEP o modificare l'origine dell'identità LDAP in modo da non utilizzare questo certificato.

Soluzione

1. Selezionare ***Amministrazione > Gestione identità > Origini identità esterne > LDAP > Nome server > Connessione***
2. Verificare che la CA radice del server LDAP non utilizzi il "Certificato server autofirmato predefinito"
3. Se il server LDAP non utilizza il certificato richiesto per una connessione protetta, selezionare ***Amministrazione > Sistema > Certificati > Autorità di certificazione > Impostazioni CA esterne > Profili RA SCEP***
4. Verificare che i profili RA SCEP non utilizzino il certificato autofirmato predefinito

Ulteriori risorse

Installazione di un certificato con caratteri jolly
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

Gestisci certificati ISE
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

Installare un certificato CA di terze parti su ISE
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html