Installation, Verlängerung und Fehlerbehebung von digitalen SSL-Zertifikaten auf der Cisco ISE

Einführung

Dieses Dokument enthält die erforderlichen Schritte für die Installation, Erneuerung und Behebung der häufigsten Zertifikatprobleme, die bei einer Identity Services Engine beobachtet wurden. Dieses Dokument enthält die empfohlenen Schritte und eine Checkliste für häufige Probleme, die überprüft und behoben werden müssen, bevor Sie mit der Fehlerbehebung beginnen und den technischen Support von Cisco anrufen.

Diese Lösungen resultieren direkt aus Serviceanfragen, die der technische Support von Cisco bearbeitet hat. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen der Schritte zur Behebung des Problems verstehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Benutzeroberfläche der Identity Service Engine

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- Cisco Identity Service Engine 2.7

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ein Zertifikat ist ein elektronisches Dokument, das eine Person, einen Server, ein Unternehmen oder eine andere Körperschaft identifiziert und dieser Körperschaft einen öffentlichen Schlüssel zuordnet. Ein selbstsigniertes Zertifikat wird vom eigenen Ersteller signiert. Zertifikate können selbstsigniert oder digital von einer externen Zertifizierungsstelle (Certificate Authority, CA) signiert werden. Ein digitales Zertifikat mit CA-Signatur gilt als Branchenstandard und sicherer.

Zertifikate werden in einem Netzwerk verwendet, um einen sicheren Zugriff bereitzustellen. Die Cisco ISE verwendet Zertifikate für die Kommunikation zwischen Knoten und für die Kommunikation mit externen Servern wie Syslog-Server, Feed-Server und allen

Endbenutzerportalen (Gast-, Sponsor- und Portale für private Geräte). Zertifikate identifizieren einen Cisco ISE-Knoten mit einem Endpunkt und sichern die Kommunikation zwischen diesem Endpunkt und dem Cisco ISE-Knoten. Zertifikate werden für die gesamte HTTPS-Kommunikation und die EAP-Kommunikation (Extensible Authentication Protocol) verwendet.

Konfigurieren

In den folgenden Leitfäden wird das Importieren und Ersetzen von Zertifikaten erläutert:

Importieren eines Systemzertifikats

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

Ersetzen eines abgelaufenen Zertifikats

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

Häufige Probleme

Szenario 1: Kein Austausch eines ablaufenden Portalzertifikats auf einem ISE-Knoten möglich

Fehler

Beim Binden des neuen Portalzertifikats an den CSR schlägt der Zertifikatbindungsprozess fehl, wenn der folgende Fehler angezeigt wird:

Interner Fehler. Bitten Sie Ihren ISE-Administrator, die Protokolle auf weitere Details zu überprüfen.

Die häufigsten Gründe für diesen Fehler sind:

- Das neue Zertifikat hat den gleichen Betreffnamen wie das vorhandene Zertifikat.

- Importieren eines erneuerten Zertifikats, das den gleichen privaten Schlüssel eines vorhandenen Zertifikats verwendet

Lösung

1. Weisen Sie die Portalnutzung vorübergehend einem anderen Zertifikat auf demselben Knoten zu.
2. Löschen des ablaufenden Portalzertifikats
3. Installieren Sie das neue Portal-Zertifikat, und weisen Sie dann die Portalnutzung zu.

Wenn Sie beispielsweise die Portalnutzung vorübergehend einem vorhandenen Zertifikat mit EAP-Authentifizierungsverwendung zuweisen möchten, gehen Sie wie folgt vor:

Schritt 1: Zertifikat mit EAP-Authentifizierungsverwendung auswählen und bearbeiten, Portalrolle unter Nutzung hinzufügen und speichern

Schritt 2: Löschen Sie das ablaufende Portalzertifikat.

Schritt 3: Laden Sie das neue Portal-Zertifikat hoch, ohne eine Rolle auszuwählen (unter Verwendung), und senden Sie es ein.

Schritt 4: Wählen und bearbeiten Sie das neue Portal-Zertifikat, weisen Sie unter Nutzung die Portalrolle zu und speichern

Szenario 2: Es können keine zwei CSR für denselben ISE-Knoten mit Multi-Use-Funktion generiert werden.

Fehler

Die Erstellung neuer CSR für denselben Knoten mit Mehrfachverwendung schlägt fehl und es wird folgender Fehler angezeigt:
Es existiert bereits ein anderes Zertifikat mit dem gleichen freundlichen Namen. Freundesnamen müssen eindeutig sein.

Lösung

CSR-freundliche Namen sind für jeden ISE-Knoten hardcodiert, sodass nicht zwei CSRs für denselben Knoten mit Mehrfachverwendung erstellt werden können. Der Anwendungsfall befindet sich auf einem bestimmten Knoten. Es gibt ein von einer Zertifizierungsstelle signiertes Zertifikat, das für die Verwendung der Admin- und EAP-Authentifizierung verwendet wird, und ein anderes von einer Zertifizierungsstelle signiertes Zertifikat, das für die Verwendung von SAML und Portal verwendet wird. Beide Zertifikate laufen ab.

In diesem Szenario:

Schritt 1: Erster CSR mit Multi-Use-Funktion erstellen

Schritt 2: Binden des Zertifikats der Zertifizierungsstelle an den ersten CSR und Zuweisen der Authentifizierungsrolle "Admin" und "EAP"

Schritt 3: Generieren eines zweiten CSR mit Mehrfachverwendung

Schritt 4: Binden des Zertifizierungsstellen-signierten Zertifikats an den zweiten CSR und Zuweisen der SAML- und Portalrolle

Szenario 3: Das Zertifikat, das die Zertifizierungsstelle signiert hat, kann nicht für die Portalnutzung gebunden werden oder das Portal-Tag kann dem Zertifikat nicht zugewiesen werden, und es wird ein Fehler ausgegeben.

Fehler

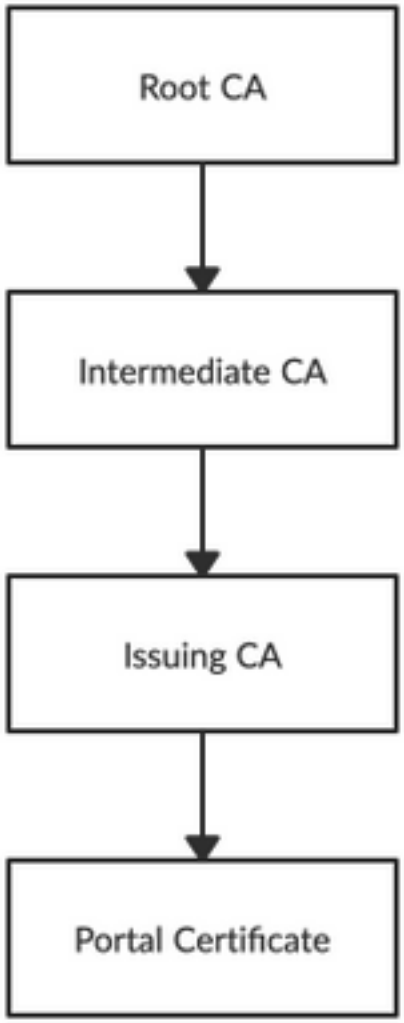
Das Binden eines von einer CA signierten Zertifikats für die Portalnutzung löst den Fehler aus:

Es gibt ein oder mehrere vertrauenswürdige Zertifikate, die Teil der Zertifikatskette des Portalsystems sind oder die mit einer cert-basierten admin-Autorenrolle mit demselben Betreffnamen, aber mit einer anderen Seriennummer ausgewählt wurden. Import/Update wurde abgebrochen. Für einen erfolgreichen Import/eine erfolgreiche Aktualisierung müssen Sie entweder die cart-basierte admin-Autorenrolle aus einem doppelten vertrauenswürdigen Zertifikat deaktivieren oder die Portalfunktion aus dem Systemzertifikat ändern, das das doppelte vertrauenswürdige Zertifikat in seiner Kette enthält.

Lösung

Schritt 1: Überprüfen Sie die Zertifikatskette des Zertifikats mit CA-Vorzeichen (zur Portalnutzung) und im Speicher für vertrauenswürdige Zertifikate, ob doppelte Zertifikate aus der Zertifikatskette vorliegen.
Schritt 2: Entfernen Sie das doppelte Zertifikat, oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdig für zertifikatbasierte Admin-Authentifizierung** aus dem doppelten Zertifikat.

Das CA-signierte Portalzertifikat weist beispielsweise die folgende Zertifikatkette auf:



Überprüfen Sie, ob ein Duplikat eines Zertifikats für eines der drei Zertifizierungsstellen in der Zertifikatkette vorhanden ist (möglicherweise ein abgelaufenes Zertifikat), und entfernen Sie das Duplikat des Zertifikats aus dem Speicher für vertrauenswürdige Zertifikate.

Szenario 4: Das abgelaufene selbstsignierte Standardzertifikat kann nicht aus dem Trusted Certificate Store gelöscht werden.

Fehler

Wenn Sie das abgelaufene, selbstsignierte Standardzertifikat aus dem Speicher für vertrauenswürdige Zertifikate löschen, tritt der Fehler auf:
Das Deaktivieren oder Löschen bzw. Verlässlichen eines Zertifikats ist nicht zulässig, da auf das Zertifikat in den Systemzertifikaten UND/ODER in Secure Syslog Target unter Remote Logging Targets verwiesen wird.

Lösung

1. Stellen Sie sicher, dass das abgelaufene selbstsignierte Standardzertifikat keinem vorhandenen Remote Logging Target zugeordnet ist. Dies kann unter ***Administration > System > Logging > Remote Logging Targets > Select and Edit SecureSyslogCollector(s) überprüft werden.***
2. Stellen Sie sicher, dass das abgelaufene selbstsignierte Standardzertifikat keiner bestimmten Rolle zugeordnet ist (Verwendung). Dies kann unter ***Administration > System > Certificates > System Certificates (Verwaltung > System > Zertifikate > Systemzertifikate)*** überprüft werden.

Wenn das Problem weiterhin besteht, wenden Sie sich an das TAC.

Szenario 5: CA signiertes pxGrid-Zertifikat kann nicht an den CSR eines ISE-Knotens gebunden werden.

Fehler

Beim Binden des neuen pxGrid-Zertifikats an den CSR schlägt der Prozess der Zertifikatsbindung mit dem Fehler fehl:

Das Zertifikat für pxGrid muss sowohl die Client- als auch die Serverauthentifizierung in der EKU-Erweiterung (Extended Key Usage) enthalten.

Lösung

Stellen Sie sicher, dass das CA-signierte pxGrid-Zertifikat sowohl über TLS-Webserver-Authentifizierung (1.3.6.1.5.5.7.3.1) als auch über TLS-Webclient-Authentifizierung (1.3.6.1.5.7.3.2) mit erweiterter Schlüsselverwendung verfügt, da es sowohl für die Client- als auch die Serverauthentifizierung (zur Sicherung der Kommunikation zwischen dem pxGrid-Client und Server) verwendet wird.

Referenzlink: 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

Szenario 6: Das abgelaufene, selbstsignierte Standardzertifikat kann aufgrund der

vorhandenen LDAP- oder SCEP RA-Profilkonfiguration nicht aus dem Trusted Certificate Store gelöscht werden.

Fehler

Wenn Sie das abgelaufene, selbstsignierte Standardzertifikat aus dem Speicher für vertrauenswürdige Zertifikate löschen, tritt der Fehler auf:

Das Vertrauenszertifikat konnte nicht gelöscht werden, da es an anderer Stelle referenziert wird, möglicherweise aus einem SCEP-RA-Profil oder einer LDAP-Identitätsquelle.

* Standard-selbstsigniertes Serverzertifikat

Um die Zertifikate zu löschen, löschen Sie das SCEP RA-Profil, oder bearbeiten Sie die LDAP-Identitätsquelle, um dieses Zertifikat nicht zu verwenden.

Lösung

1. Navigieren Sie zu ***Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connection.***
2. Stellen Sie sicher, dass die LDAP-Server-Root-CA nicht das "Standard-selbstsigniertes Serverzertifikat" verwendet.
3. Wenn der LDAP-Server das erforderliche Zertifikat für eine sichere Verbindung nicht verwendet, navigieren Sie zu ***Administration > System > Certificates > Certificate Authority > External CA Settings > SCEP RA Profiles.***
4. Vergewissern Sie sich, dass eines der SCEP RA-Profile kein selbstsigniertes Standardzertifikat verwendet.

Weitere Ressourcen

Installieren eines Wildcard-Zertifikats
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

Verwalten von ISE-Zertifikaten
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

Installieren eines Zertifizierungsstellenzertifikats eines Drittanbieters auf der 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