Konfigurieren des SAML SSO-Setups mit Kerberos-Authentifizierung

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Konfigurieren von AD FS Browser konfigurieren Microsoft Internet Explorer Mozilla Firefox Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Active Directory und Active Directory Federation Service (AD FS) Version 2.0 konfiguriert werden, um die Verwendung der Kerberos-Authentifizierung durch Jabber-Clients (nur Microsoft Windows) zu ermöglichen. Dadurch können sich Benutzer bei ihrer Microsoft Windows-Anmeldung anmelden und nicht zur Eingabe von Anmeldeinformationen aufgefordert werden.

Vorsicht: Dieses Dokument basiert auf einer Laborumgebung und geht davon aus, dass Sie sich der Auswirkungen der vorgenommenen Änderungen bewusst sind. Lesen Sie die entsprechende Produktdokumentation, um die Auswirkungen der vorgenommenen Änderungen zu verstehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt Folgendes:

- Installation und Konfiguration von AD FS Version 2.0 mit Cisco Collaboration-Produkten als Relying Party Trust
- Collaboration-Produkte wie Cisco Unified Communications Manager (CUCM) IM und Presence, Cisco Unity Connection (UCXN) und CUCM-fähig zur Verwendung von Single

Sign-on (SSO) für Security Assertion Markup Language (SAML)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Active Directory 2008 (Hostname: ADFS1.ciscolive.com)
- AD FS Version 2.0 (Hostname: ADFS1.ciscolive.com)
- CUCM (Hostname: CUCM1.ciscolive.com)
- Microsoft Internet Explorer Version 10
- Mozilla Firefox Version 34
- Telerik Fiddler Version 4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Konfigurieren von AD FS

1. Konfigurieren Sie AD FS Version 2.0 mit Service Principal Name (SPN), um den Client-Computer, auf dem Jabber installiert ist, für die Anforderung von Tickets zu aktivieren. Dadurch kann der Client-Computer wiederum mit einem AD FS-Dienst kommunizieren.



Siehe <u>AD FS 2.0: Konfigurieren des SPN (servicePrincipalName) für das Dienstkonto</u> für weitere Informationen

 Stellen Sie sicher, dass die Standardauthentifizierungskonfiguration f
ür den AD FS-Dienst (in C:\inetpub\adfs\ls\web.config) Integrierte Windows-Authentifizierung ist. Vergewissern Sie sich, dass die Option nicht in Form-basierte Authentifizierung ge
ändert wurde.

| <microsoft.identityserver.web></microsoft.identityserver.web> |
|---|
| <localauthenticationtypes></localauthenticationtypes> |
| <add name="Integrated" page="auth/integrated/"></add> |
| <add name="Forms" page="FormsSignIn.aspx"></add> |
| <pre><add name="TlsClient" page="auth/sslclient/"></add></pre> |
| <add name="Basic" page="auth/basic/"></add> |
| |
| <commondomaincookie reader="" writer=""></commondomaincookie> |
| <context hidden="true"></context> |
| <error page="Error.aspx"></error> |
| <pre><acceptedfederationprotocols saml="true" wsfederation="true"></acceptedfederationprotocols></pre> |
| <pre><homerealmdiscovery page="HomeRealmDiscovery.aspx"></homerealmdiscovery></pre> |
| <pre><pre><pre><pre>content</pre><pre>persistIdentityProviderInformation enabled="true" lifetimeInDays="30" /></pre></pre></pre></pre> |
| <singlesignon_enabled="true"></singlesignon_enabled="true"> |
| |

3. Wählen Sie Windows-Authentifizierung aus, und klicken Sie im rechten Bereich auf Erweiterte Einstellungen. Deaktivieren Sie unter Erweiterte Einstellungen die Option Kernel-Modus-Authentifizierung aktivieren, stellen Sie sicher, dass der erweiterte Schutz deaktiviert ist, und klicken Sie auf OK.



4. Stellen Sie sicher, dass AD FS Version 2.0 sowohl das Kerberos-Protokoll als auch das NT LAN Manager-Protokoll (NTLM) unterstützt, da alle Nicht-Windows-Clients Kerberos nicht verwenden können und sich auf NTLM verlassen.

Wählen Sie im rechten Teilfenster **Provider** aus, und stellen Sie sicher, dass **Negotiate** und **NTLM** unter Enabled Providers (Aktivierte Anbieter) vorhanden sind:



Anmerkung: AD FS übergibt den Negotiate Security-Header, wenn zur Authentifizierung von Client-Anforderungen eine integrierte Windows-Authentifizierung verwendet wird. Mit dem Sicherheitsheader "Negotiate" können Clients zwischen der Kerberos-Authentifizierung und der NTLM-Authentifizierung wählen. Beim Verhandlungsprozess wird die Kerberos-Authentifizierung ausgewählt, es sei denn, eine der folgenden Bedingungen ist zutreffend:

- Eines der Systeme, das an der Authentifizierung beteiligt ist, kann die Kerberos-Authentifizierung nicht verwenden.

- Die aufrufende Anwendung stellt keine ausreichenden Informationen bereit, um die Kerberos-Authentifizierung zu verwenden.

- Damit der Verhandlungsprozess das Kerberos-Protokoll für die Netzwerkauthentifizierung auswählen kann, muss die Client-Anwendung als Zielname ein SPN, einen User Principal Name (UPN) oder einen Network Basic Input/Output System (NetBIOS)-Kontonamen angeben. Andernfalls wählt der Verhandlungsprozess immer das NTLM-Protokoll als bevorzugte Authentifizierungsmethode aus.

Browser konfigurieren

Microsoft Internet Explorer

1. Stellen Sie sicher, dass Internet Explorer > Erweitert > Integrierte Windows-Authentifizierung

aktivieren aktiviert ist.

| Internet Options |
|--|
| General Security Privacy Content Connections Programs Advanced |
| Settings |
| Do not submit unknown addresses to your auto-search pro Just display the results in the main window Security Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is involved to check for publisher's certificate revocation Check for server certificate revocation* Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is dc Enable DOM Storage Enable Integrated Windows Authentication* Enable Integrated Windows Authentication* |
| *Takes effect after you restart Internet Explorer |
| Restore advanced settings |
| Reset Internet Explorer settings |
| Resets Internet Explorer's settings to their default Reset |
| You should only use this if your browser is in an unusable state. |
| OK Cancel Apply |

2. AD FS-URL unter Sicherheit >Intranetzonen > Sites hinzufügen.

| Internet Options |
|--|
| General Security Privacy Content Connections Programs Advanced |
| |
| Select a zone to view or change security settings. |
| |
| Internet Local intranet Trusted sites Restricted sites |
| Local intranet |
| This zone is for all websites that are found on your intranet. |
| Local intrapet X |
| |
| Use the settings below to define which websites are included in the local intranet zone. |
| Automatically detect intranet network |
| Include all local (intranet) sites not listed in other zones |
| Include all sites that bypass the proxy server |
| Include all network paths (UNCs) |
| |
| What are intranet settings? Advanced OK Cancel |
| Local intranet 💽 |
| You can add and remove websites from this zone. All websites in |
| this zone will use the zone's security settings. |
| - |
| Add this website to the zone: |
| Add |
| Websites: |
| adts1.clscolive.com |
| |

3. Fügen Sie die CUCM-, IMP- und Unity-Hostnamen zu Sicherheit >Vertrauenswürdige Sites hinzu.

| Internet Options | 8 🕺 | | | | |
|--|---------------|--|--|--|--|
| General Security Privacy Content Connections Prog | rams Advanced | | | | |
| Select a zone to view or change security settings. | | | | | |
| | | | | | |
| Internet Local intranet Trusted sites Restricted sites | | | | | |
| Trusted sites | Sites | | | | |
| Tructed sites | Sites | | | | |
| Trusted sites | | | | | |
| You can add and remove websites from this zone. All websites in this zone will use the zone's security settings. | | | | | |
| | Add | | | | |
| Websites: | | | | | |
| cucm1.ciscolive.com | Remove | | | | |
| imp1.ciscolive.com | | | | | |
| ucxn1.ciscolive.com | | | | | |
| Require server verification (https:) for all sites in this | zone | | | | |
| | Close | | | | |

4. Stellen Sie sicher, dass Internet Explorer > Security > Local Intranet > Security Settings > User Authentication - Logon konfiguriert ist, um die Anmeldeinformationen für Intranet-Sites zu verwenden.

| Internet Options | 82 |
|--|---|
| General Security Privacy Content Connection | s Programs Advanced |
| | Security Settings - Local Intranet Zone |
| Select a zone to view or change security settings. | Settings O Disable |
| Internet Local intranet Trusted sites | Enable Enable XSS filter |
| Local intranet | Disable Enable |
| This zone is for all websites that are found on your intranet. | Scripting of Java applets Disable Enable Prompt |
| Allowed levels for this zone | See Authentication |
| Allowed levels for this zone: All Allowed levels for this zone: Allowed (intranet) Allowed (intrane | Logon Anonymous logon Automatic logon only in Intranet zone Automatic logon with current user name and password Prompt for user name and password III |
| Custom level | *Takes effect after you restart Internet Explorer |
| Reset all zo | Reset custom settings Reset to: Medium-low (default) Reset |
| ОК | OK Cancel |

Mozilla Firefox

1. Öffnen Sie Firefox, und geben Sie **about:config** in die Adressleiste ein.



2. Klicken Sie auf Ich werde vorsichtig sein, verspreche ich!

| (| |
|---|--|
| | Here be dragons! |
| | Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing. |
| | Show this warning next time |
| | I'll be careful, I promise! |
| | |

3. Doppelklicken Sie auf den Präferenznamen **network.negotiate-auth.allow-non-fqdn** auf **true** und **network.negotiate-auth.trust-uris** auf **ciscolive.com,adfs1.ciscolive.com**, um Änderungen vorzunehmen.

| Search: network.n | | | |
|---|----------|---------|---|
| Preference Name | Status | Туре | Value |
| network.negotiate-auth.allow-insecure-ntlm-v1 | default | boolean | false |
| network.negotiate-auth.allow-insecure-ntlm-v1-https | default | boolean | true |
| network.negotiate-auth.allow-non-fqdn | user set | boolean | true |
| network.negotiate-auth.allow-proxies | default | boolean | true |
| network.negotiate-auth.delegation-uris | default | string | |
| network.negotiate-auth.gsslib | default | string | |
| network.negotiate-auth.trusted-uris | user set | string | adfs1.adfs1.ciscolive.com.ciscolive.com |
| network.negotiate-auth.using-native-gsslib | default | boolean | true |
| network.ntlm.send-Im-response | default | boolean | false |
| | | | |

4. Schließen Sie Firefox, und öffnen Sie es erneut.

Überprüfung

Um zu überprüfen, ob die SPNs für den AD FS-Server korrekt erstellt wurden, geben Sie den **setspn-**Befehl ein und zeigen die Ausgabe an.



Überprüfen Sie, ob die Client-Computer Kerberos-Tickets besitzen:

| ex. C:\Wine | idows\system32\cmd.exe | P 💌 |
|-------------|---|----------|
| C:\Users | Nuser1.CISCOLIVE>Klist tickets | ^ |
| Current | LogonId is 0:0xabc6d | |
| Cached T | lickets: <2> | |
| #0> | Client: user1 @ CISCOLIVE.COM Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e0000 -> forwardable renewable initial pre_authent Start Time: 1/17/2015 20:52:47 (local) End Time: 1/18/2015 6:52:47 (local) Renew Time: 1/24/2015 20:52:47 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96 | Е |
| #1> | Client: user1 @ CISCOLIVE.COM Server: host/pc1.ciscolive.com @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a00000 -> forwardable renewable pre_authent Start Time: 1/17/2015 20:52:47 (local) End Time: 1/18/2015 6:52:47 (local) Renew Time: 1/24/2015 20:52:47 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96 | |
| C:\Users | <pre>s\user1.CISCOLIVE></pre> | |

Führen Sie diese Schritte aus, um zu überprüfen, welche Authentifizierung (Kerberos- oder NTLM-Authentifizierung) verwendet wird.

- 1. Laden Sie das Programm Fiddler auf Ihren Client-Computer herunter und installieren Sie es.
- 2. Schließen Sie alle Fenster von Microsoft Internet Explorer.
- 3. Führen Sie das Tool Ordner aus, und überprüfen Sie, ob die Option **Datenverkehr erfassen** im Menü Datei aktiviert ist. Fiddler fungiert als Pass-Through-Proxy zwischen dem Client-Computer und dem Server und überwacht den gesamten Datenverkehr.
- 4. Öffnen Sie Microsoft Internet Explorer, rufen Sie den CUCM auf, und klicken Sie auf einige Links, um Datenverkehr zu generieren.
- 5. Rufen Sie das Hauptfenster von Ordner auf, und wählen Sie eines der Frames aus, in dem das Ergebnis **200** ist (Erfolg), und Kerberos wird als Authentifizierungsmechanismus angezeigt.



6. Wenn der Authentifizierungstyp NTLM ist, sehen Sie **Negotiate - NTLMSSP** am Anfang des Frames, wie hier gezeigt.

| 🚸 Fidd | er Web C | ebugger | | | |
|---------------|-----------|-------------|----------------|-----------------------------|---|
| File Ed | it Rules | Tools Vie | ew Help GET/bo | ok 🔛 GeoEdge | |
| Q fy | Replay 🕻 | <- 🕨 Go | 🔹 Stream 👹 | Decode Keep: All sessions * | 🕀 Any Process 🖄 Find 🔜 Save 🛛 🎼 🕥 🏈 Browse 🔹 🕀 Clear Cache 🎢 TextWizard 🛛 🔂 Tearoff |
| | Result | Protocol | Host | URL | 🖪 🔗 Statistics 🚟 Inspectors 🖉 AutoResponder 📝 Composer 🗖 Filters 🕒 Log 🚍 Timeline |
| Ø 1 | 502 | HTTP | www.bing.com | /favicon.ico | Headers TextView WebForms HexView Auth Cookies Raw JSON XML |
| ≰ ≱2 | 200 | HTTP | cucm.ciscolive | 1 | 5, No Received Authorization Harden in account |
| 23 | 200 | HTTP | cucm.ciscolive | /ciscologo.gif | NO Proxy-Authorization Header is present. |
| = 4 | 200 | HTTP | cucm.ciscolive | /favicon.ico | 1, Authorization Header is present: NTLM |
| N 5 | 302 | HTTP | cucm.ciscolive | /ccmadmin/showHome.do | 58 00 00 00 00 00 00 05 80 00 00 00 00 00 00 00 00 XX. |
| <u>6 (11)</u> | 200 | HTTP | Tunnel to | cucm.ciscolive.com:443 | 58 00 00 00 00 00 00 05 58 00 00 00 00 00 00 00 XX. |
| 07 | 502 | HTTP | www.downloa | /msdownload/update/v3/s | 06 01 81 1D 00 00 00 0F 4E 84 C3 AA 0D D1 81 34 |
| S 8 | 302 | HTTPS | cucm.ciscolive | /comadmin/showHome.do | 78 AA CE A9 41 F3 D1 31 Xº18AÓÑ1 |
| 59 | 302 | HTTPS | cucm.ciscolive | /ssosp/saml/login?relayurl | |
| 10 | 200 | HTTP | Tunnel to | adfs1.ciscolive.com:443 | -[NTLM Type3: Authentication] |
| 5 11 | 302 | HTTPS | adfs1.ciscoliv | /adfs/ls/75AMLRequest=n | Cat Suntaulian Transformer Market Textilian Inscallan Haulian Makidan |
| 12 | 401 | HTTPS | adfs1.ciscoliv | /adfs/ls/auth/integrated/? | 6, Get Syntaxview Transformer [Headers Textview Imageview Hexview Viebview |
| 13 | 401 | HTTPS | adfs1.ciscoliv | /adfs/ls/auth/integrated/? | 7, Auth Caching Cookies Raw JSON XML |
| <>14 | 200 | HTTPS | adfs1.ciscoliv | /adfs/ls/auth/integrated/? | 9, Response Headers [Raw] [Header Definitions |
| 15 | 401 | HTTPS | adfs1.ciscoliv | /favicon.ico | 6, HTTP/1.1 200 OK |
| 16 | 200 | HTTP | Tunnel to | cucm.ciscolive.com:8443 | Cache |
| 17 | 302 | HTTPS | cucm.ciscolive | /ssosp/sami/SSO/alias/CU | Cache-Control: no-cache |
| 18 🏌 | 403 | HTTPS | cucm.ciscolive | /ssosp/relay | 2, Date: Sat, 17 Jan 2015 20:05:06 GMT |
| 2 19 | 200 | HTTPS | cucm.ciscolive | /clscologo.gif | Expires: -1 |
| | | | | | Pragma: no-cache |
| • | _ | | | | Cookies / Login |
| [QuidEx | ec] ALT+C |) > type HE | LP | | |
| Tig Capb | uring | Al Proce | sses | 1 / 19 https://adfs1.ciscol | live.com/adfs/ls/auth/integrated/75AMLRequest=nVLLbtswELznKwjebYryIwphGXBsFDWQNErk9NDbil4BCR55VJp%2B% |

Fehlerbehebung

Wenn alle Konfigurations- und Überprüfungsschritte wie in diesem Dokument beschrieben abgeschlossen wurden und Sie weiterhin Anmeldeprobleme haben, müssen Sie sich an einen Microsoft Windows Active Directory/AD FS-Administrator wenden.