Single Sign On mit ADITO

Kerberos, LDAP und SSPI

AID 032 DE

Autor: FA, MW, KN. Version 5.5. Zuletzt geändert 04.09.2017

Version	Bemerkung
5.5	Anpassung der Formatierungen
5.4	Screenshot getauscht
5.3	Dokumentation ldapauth eingefügt
5.2	Hinweis auf Abfragen von Userlogins über JDito ausführlicher beschrieben
5.1	Letzte Version vor Umstellung auf Versionshistorie im Dokument

Inhaltsverzeichnis

1. Funktionsprinzip

Voraussetzung für die Nutzung des Single Sign On ist

- eine funktionierende **Kerberos**-Infrastruktur und ein LDAP-kompatibler Verzeichnisdienst (z.B. Microsoft ActiveDirectory, Novell NDS)
- oder die Bereitstellung einer **SSPI**-Infrastruktur (vgl. https://msdn.microsoft.com/de-de/library/windows/desktop/aa380493%28v=vs.85%29.aspx) von Microsoft.

Beim Starten des Clients überprüft dieser die Gültigkeit des aktuellen Kerberos-Tickets und stellt dann fest, ob der Benutzername im LDAP-Verzeichnis vorhanden ist. Sind diese Vorbedingungen erfüllt, übergibt der Client die Identität des Benutzers an den Server, der dann die Verbindung akzeptiert.

1.1. Wann Kerberos, wann SSPI?

Empfohlen wird die Verwendung von SSPI ab ADITO 4.4 mit mindestens der JRE 1.8.0_60 (bzw. in der jeweilig freigegebenen Version des ADITO Releases).

1.2. Was ist LDAP-Auth?

Bei LDAP-Auth meldet sich ADITO nicht automatisch mit den Windows-Anmeldedaten an, sondern zeigt wie bei einer Anmeldung mit Benutzername / Passwort den entsprechenden Login-Dialog. Im Fall von LDAP-Auth muss der Benutzer seine LDAP-Anmeldedaten eingeben, der ADITO-Server überprüft die Anmeldung dann beim LDAP-Verzeichnisdienst.

1.3. Voraussetzungen

Damit eine Anmeldung im Single Sign on möglich ist, müssen folgende Kriterien erfüllt sein:

- Windows-Anmeldung mit einem Domänenaccount
- Konfiguration des Servers für Single Sign on (How-to siehe unten)
- Konfiguration des Benutzers (How-to siehe unten)

Ein auf Single Sign on konfiguriertes System erlaubt unter gewissen Umständen am Client auch die Anmeldung mit Eingabe von Benutzername und Passwort. Dazu müssen folgende Voraussetzungen erfüllt sein:

- Windows-Anmeldung mit einem Domänenaccount, ohne Verbindung zum Netzwerk bei der Anmeldung
- Anmeldung bei ADITO durch Angabe von Domäne und Benutzer (user@domain bzw. domain\user)

Es ist nicht möglich, sich mit einem Benutzer anzumelden, der keinen Domänenzugang hat. Es ist bspw. nicht möglich, sich mit dem Benutzer „Admin“ aus dem ADITO online Referenzsystem am Client anzumelden, wenn dieser in keiner Domäne vorhanden ist.

2. Vorgehensweise

2.1. Konfiguration des Servers (ADITO 4)

2.1.1. Für Kerberos

Die serverseitigen Einstellungen konfigurieren Sie im **System-Editor** im Reiter `Preferences` unter `Sicherheit`. Die Kerberos-Einstellungen für das Login von Clients am Server finden Sie unter der Gruppe `Login`, die Einstellungen für die Anmeldung von Designer und Manager unter der Gruppe `Manager login`.

Bei Manager und Designer reicht es, wenn Sie hier den login Type 'kerberos' eintragen. Die genaue Konfiguration sehen Sie weiter unten.

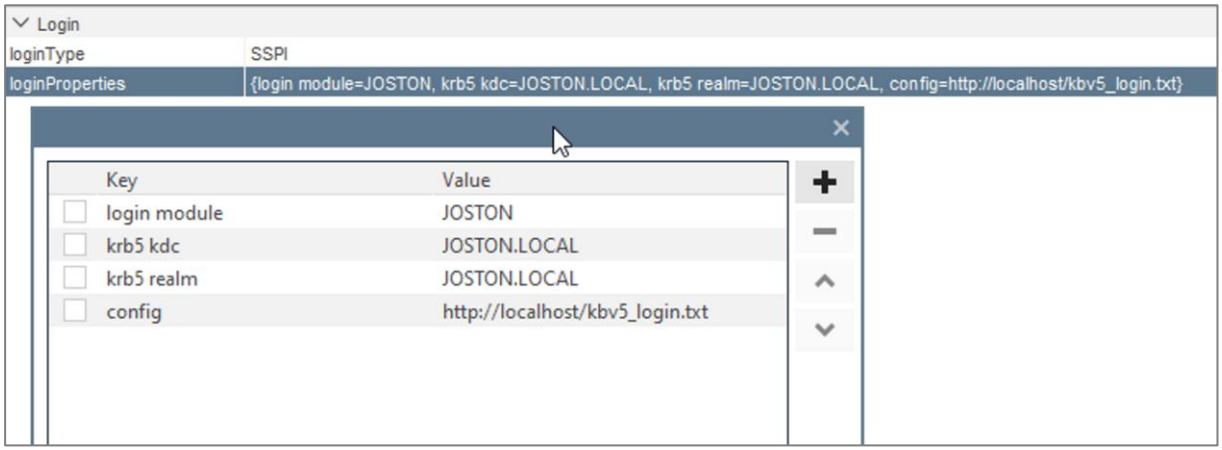
Tragen Sie als `loginType` für das Login beim Client 'kerberos' ein. Geben Sie dann die folgenden `properties` für das Login an. Beim Designer und Manager reicht es, wenn nur der type bei `Manager Login` erfasst wurde. Hier sind keine weiteren `Properties` anzugeben.

`login module`	Name des Login-Moduls. Tragen Sie hier für den Namen des Login-Moduls, bspw. 'ADITO', ein.
`krb5 kdc`	Key Distribution Center (KDC), unter Windows meist der Domänencontroller. Tragen Sie hier den Hostnamen des Kerberos-Servers ein, der die Kerberos-Tickets verteilt.
`krb5 realm`	Name des Kerberos-Realms, unter Windows meist die Domäne mit Suffix (z.B. `company.local`). Tragen Sie hier den Namen Ihres Kerberos5-Realms ein.
`config`	Pfad zur Konfigurationsdatei. Tragen Sie hier den Pfad zur Konfigurationsdatei für den Client ein, z.B. `http://aditoserver/webstart/kbv5_login.conf`. Der Verweis auf die Konfigurationsdatei kann auch auf eine lokale Datei zeigen. Normalerweise liegt diese Datei bei einem System, dessen Clients über Java Webstart verteilt werden, aber auf dem Webserver.

2.1.2. Für SSPI

Bei der Verwendung der SSPI-API zur Anmeldung tragen Sie bei `loginType` den Wert "SSPI" ein. Damit das System auch auf Clients funktioniert, die nicht auf Microsoft Windows-Betriebssystemen laufen, müssen weiterhin die Login-Properties von Kerberos eingetragen werden.

Als Beispiel:



2.2. Konfiguration des Benutzers

Tragen Sie nun für jeden Benutzer (Im System-Editor im Reiter `User`, `Erweiterte Eigenschaften`) beim Key `kerberos principal` / `kerberoslogin` den Kerberos-Principal dieses Benutzers ein.

Der Kerberos-Principal setzt sich zusammen aus Benutzername und Kerberos-Realm, getrennt durch ein '@'-Zeichen, z.B. username@company.local.

Auch diese Eigenschaft des Benutzers können Sie über JDito über

```
user[tools.PARAMS][tools.KERBEROS_LOGIN] = "username@company.local";
```

setzen, wobei "user" ein Benutzer-Objekt ist, wie es `tools.getUser` liefert.

Damit Sie diese Einstellungen nicht bei vielleicht mehreren hundert Benutzern für jeden Benutzer manuell vornehmen müssen, können Sie ein Template angeben, das für alle Benutzer verwendet wird.

Dieses Template geben Sie im Preferences-Editor auf dem Reiter `Security` unter `single sign on template` / `securitySSOUserTemplate` an. In diesem Template können Sie über die Variable `$USERTITLE` auf das Login des Users zugreifen.

Geben Sie beispielsweise folgendes Template an,

```
$USERTITLE@company.local
```

wird für den Benutzer 'adito' der Kerberos-Principal 'adito@company.local' angenommen.

Wird beim Benutzer ein Kerberos-Principal angegeben, überschreibt dieser den Wert, der anhand des Templates ermittelt werden würde.

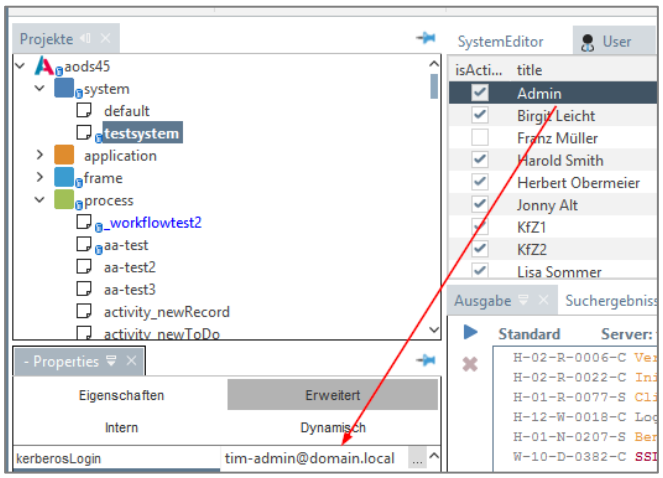
Zusätzlich zu `$USERTITLE@company.local` stehen Ihnen noch die Variablen

- `$USERMAIL` (die E-Mail-Adresse des Benutzers)
- `$USERLOCALPART` (der Teil der E-Mail-Adresse vor dem @)

zur Verfügung.

2.3. ADITO Benutzer, SSO Benutzer und JDito

Ein Single Sign On-Login wird sowohl bei Kerberos als auch SSPI verknüpft. Es ist möglich, dass das ADITO-Login vom Windows-Login unterschiedlich ist, falls kein Abgleich über das User-Template möglich ist:



In diesem Fall ist das Windows-Login `tim-admin@domain.local`, das ADITO-Login allerdings "Admin". Wird in JDito nun auf den Benutzer zugegriffen, so liefert der ADITO-Server immer den **ADITO-Benutzer**, das heißt z.B. die JDito-Systemvariable `$sys.user` liefert "Admin", nicht "tim-admin".

2.4. Konfigurationsdatei

Die Konfigurationsdatei am Client (in diesem Fall kann das auch der ADITO-Server sein, Client bezieht sich hierbei auf den Kerberos-Client) hat folgenden Aufbau:

```
ADITO {
  com.sun.security.auth.module.Krb5LoginModule required debug=true
useTicketCache=true;
};
```

Der Name des Eintrags (hier: 'ADITO') muss mit dem Wert übereinstimmen, den Sie im Designer für das Login unter 'properties' -> 'login module' angegeben haben. Sie können in dieser Datei also mehrere Module angeben, von denen jedes über einen eigenen Namen im Preferences-Editor angesprochen werden kann.

2.5. Sicherheitseinstellungen bei ADITO4

Die Sicherheitskonfiguration für ADITO4 hat sich durch die Verwendung von Java 7 im Vergleich zu den Vorgängerversionen geändert. Java hält sich an eine strengere

Sicherheitskonfiguration, weshalb Single Sign On unter Umständen nur noch mit Anpassung eines Keys in der Registry möglich ist. Starten Sie deshalb den Registrierungs-Editor (`regedit`) und fügen den folgenden Schlüssel ein oder passen Sie ihn an:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters

Wertname: AllowTgtSessionKey

Wert Typ: REG_DWORD

Wert: 0x01  (Hexadezimal 1, Standard ist 0)
```

Details zur erhöhten Sicherheitskonfiguration unter Java 7 finden Sie unter http://info.michael-simons.eu/2012/07/23/java-7-jaas-and-kerberos-single-sign-on-vs-newer-windows-systems/

2.6. Einrichten von Designer und Manager für Single Sign On

Auch mit Designer und Manager können Sie sich an einer Single Sign On-Umgebung anmelden, die Konfiguration ist allerdings anders als die des Clients.

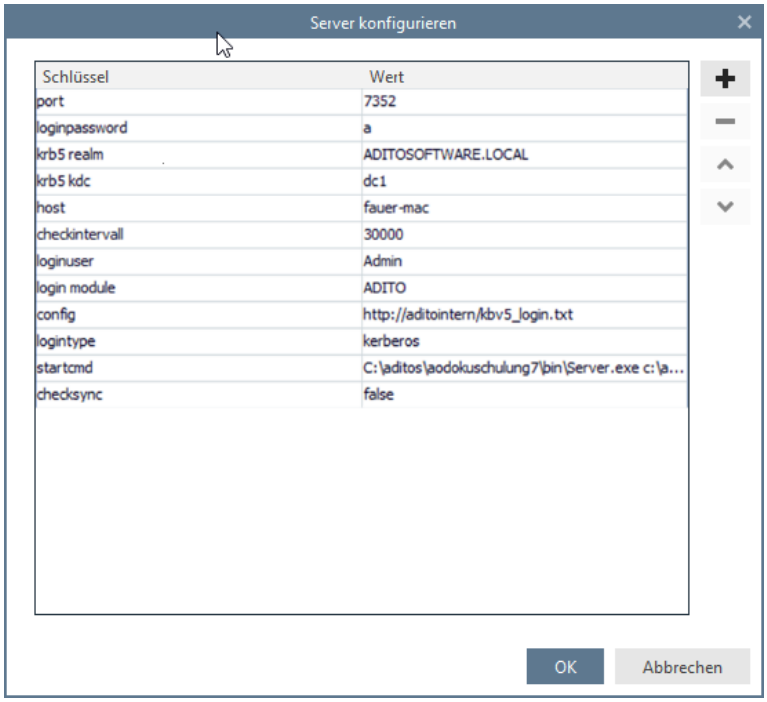
2.6.1. Konfiguration des Designers für Single Sign On

Für ADITO4 stehen mehrere Login-Mechanismen für den ADITO Designer zur Verfügung. Der ADITO Designer meldet sich normalerweise automatisch an der Systemdatenbank an, wenn im `System` eine Serverkonfigurationsdatei angegeben wurde. Wurde diese Datei nicht direkt in den Eigenschaften angegeben, meldet sich der Designer regulär mit Benutzername und Passwort an.

Möchten Sie Single Sign On mit dem Designer verwenden, geben Sie **keine** Konfigurationsdatei im Systemalias an. In den Schlüssel-Wert-Paaren bei den `Login Properties` im Bereich Manager Login geben Sie dann dieselben Informationen an wie im Client.

2.6.2. Konfiguration des Managers für Single Sign On

Damit auch der Manager sich per Single Sign On verknüpfen kann, müssen bei den Serverkonfigurationseinstellungen die Schlüssel-Wert-Paare aus Kapitel 2.1 eingetragen werden.



Die Eigenschaft `loginuser` wird bei der Verwendung von Single Sign On nicht mehr ausgewertet.

3. Anmeldung mit LDAP-Auth

Die folgenden Eigenschaften müssen im System-Editor angegeben werden (Bereich `Preferences`), damit die LDAP-Authentifizierung funktioniert.

loginType ldapauth

loginProperties Hier sind Schlüssel-Wert-Paare einzutragen:

Schlüssel	Beschreibung
ldap provider	Pfad und Port zum Verzeichnisdienst, z.B. `ldaps://myfancyserver.domain:636`
auth method	Anmeldemethode `simple`, `none` oder `strong`. Derzeit wird nur `simple` ausgewertet.
user key	Userschlüssel. Das ist der Wert, den Benutzer beim Login eingeben müssen. Z.B. bei Angabe von `cn` muss der Benutzer im Login seinen "common name" eingeben.
dn base	Basisverzeichnis der Benutzer, z.B. `ou=USER,ou=MASTERORG,o=MASTERCUSTOMER`

4. Troubleshooting

4.1. Message Stream Modified

Falls bei der Anmeldung über SSO dieser Fehler erscheint,

```
[Z-00-N-0011-C] [<!--Exception: KrbApErrException//-->] [<!--
Message: Message stream modified (41)//-->] [<!--Invoked Method:
login.client.adaptor.AbstractFEClientAuth.doAuthentication//-->]
[<!--Line: -1//-->] [<!--Invoker:
login.client.adaptor.FEClientAuthKerberos.doAuthentication//-->]
[<!--Line: -1//-->]

[C][Z-00-N-0011-C] [<!--Exception: LoginException//-->] [<!--
Message: Message stream modified (41)//-->] [<!--Invoked Method:
login.client.adaptor.AbstractFEClientAuth.doAuthentication//-->]
[<!--Line: -1//-->] [<!--Invoker:
login.client.adaptor.FEClientAuthKerberos.doAuthentication//-->]
[<!--Line: -1//-->]

[C][H-35-R-0040-C]

[C][H-35-R-0033-C]
```

sollte der krb5 realm-Name in den Login-Eigenschaften bei den `Preferences` zur Sicherheit in GROßBUCHSTABEN angegeben werden.

4.2. Umlaute im Benutzernamen

Wenn in Benutzernamen Umlaute vorhanden sind, kann es vorkommen, dass sich der Client beim Starten nicht am Active Directory authentifizieren kann. In diesem Fall kann der folgende Startparameter am Client für Abhilfe sorgen:

```
-Dsun.security.krb5.msinterop.kstring=true
```

Wird der ADITO Client über Java Web Start verteilt, so kann der folgende Eintrag in der JNLP-Datei vorgenommen werden:

```
<property name="sun.security.krb5.msinterop.kstring" value="true"/>
```

Dieser Parameter bewirkt, dass für das Encoding UTF-8 und nicht ASCII verwendet wird.

4.3. Single Sign On in Mac OSX

Sollte Single Sign on unter einem Rechner mit Mac OSX nicht funktionieren, muss die Datei

```
/etc/krb5.conf
```

bearbeitet werden. In ihr gibt es den Knoten

```
[libdefaults]
```

Dort ist der Wert `allowweakencryptions` umzustellen auf

```
allowweakencryptions=true
```

4.4. Anmeldefenster bei ADITO4 und Windows 7 (und höher) trotz aktiviertem Single Sign On mit Kerberos

Sollte bei Verwendung von Windows 7 und höher trotz aktiviertem Single Sign On und Anmeldung an der Domäne beim Start der Anwendung eine Nachfrage nach Benutzername und Passwort erfolgen, dann akzeptiert die Domäne den Session Key nicht.

Technische Details hierzu finden Sie unter http://info.michael-simons.eu/2012/07/23/java-7-jaas-and-kerberos-single-sign-on-vs-newer-windows-systems/

Damit die Anmeldung funktioniert, muss ein Registry-Schlüssel ausgeführt werden. Dieses Skript können Sie als sso.reg auf die Festplatte speichern und ausführen:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"allowtgtsessionkey"=dword:00000001
```

Dieser Eintrag sorgt dafür, dass die Benutzerkontrolle das Ticket-Granting Ticket akzeptiert und die Anmeldung erfolgen kann. Bei SSPI tritt dieses Verhalten nicht auf.

4.4.1. Verhalten bei lokalen Administratoren

Ist der Benutzer als lokaler Administrator am System eingerichtet, so erfolgt auch nach Aktivierung des Registry-Eintrags noch eine Nachfrage nach Benutzername und Passwort. Der ADITO4-Client muss in diesem Fall als Administrator ausgeführt werden. Bei SSPI tritt dieses Verhalten nicht auf.