Kerberos Authentifizierung

Peter Schmelzer, in2success GmbH

Zusammenfassung

Dieser Artikel befasst sich mit der Microsoft Implementierung des Kerberos v5 Protokolls in Verbindung mit Skype for Business- und Exchange-Server.

Das Kerberos-Protokoll ist ein ticketbasierendes Authentifizierungsprotokoll, welches als Implementierung für Unix/Linux und Microsoft zur Verfügung steht. Es wurde ursprünglich 1978 am Massachusetts Institute of Technology (MIT) entwickelt und liegt mittlerweile in der Version 5 vor.

Um eine möglichst sichere Authentifizierung von Benutzern im Netzwerk zu gewährleisten, wurden verschiedene Sicherheitsmchanismen in das Protokoll implementiert. Hierzu gehört u.a. das niemals ein Kennwort über das Netzwerk übertragen wird und das die Kommunikation grundsätzlich verschlüsselt ist. Weiterhin kommen Sitzungsschlüssel und Zeitstempel zum Einsatz, um feststellen zu können, ob aufgezeichnete Netzwerk-Pakete erneut gesendet wurden. Das Kerberos Protokoll ist in der Microsoft Welt in das Actice Directory implementiert.

Das Kern Element des Kerberos Protokolls ist das sogenannte **Ticket**, welches dem jeweiligen Inhaber den authentifizierten Zugriff auf eine Ressource (Webserver, Dateifreigabe etc.) gewährt. Da die Ressource während des Benutzerzugriffs zwecks Authentifizierung nicht mit dem Ticket-ausgebenden-Server kommuniziert, nutzt einem Angreifer auch nicht das Aufzeichnen und Abspielen von Netzwerkverkehr gegen die Ressource. Wenn gleich dies ein großer Vorteil ist, darf aber nicht verschwiegen werden, das es auch Nachteile gibt. So sind alle im Zusammenhang mit der Authentifizierung von Benutzern und Ressourcen gespeicherten Daten im Actice Directory mit einem einzigen Master-Schlüssel verschlüsselt abgespeichert. Wird dieser Schlüssel geknackt besitzt der Angreifer das sogenannte „Goldene Ticket“.

Skype for Business und Exchange Server bieten ebenfalls die Möglichkeit auf die Kerberos Authentifizierung umgestellt zu werden. Dies ermöglicht im internen Netzwerk eine vereinfachte Authentifizierung und eröffnet gleichzeitig neue Möglichkeiten. So können 3rd-Party Produkte in Verbindung mit der Kerberos Constrained Delegation Benutzer und Geräte „im Auftrag“ authentifizieren. Dies wird z.B. eingesetzt, wenn auf mobilen Endgeräten keine Zugangsdaten für das Unternehmensnetzwerk gespeichert werden dürfen.

Das Troubleshooting ist im Vergleich zu anderen Protokollen wie deutlich aufwendiger, da die gesamte Prozesskette während der Authentifizierung verschlüsselt abläuft.

Inhaltsverzeichnis

Versionsgeschichte		
Version 1.2	11.09.2018	PS
Überarbeitung, Korrekturen, verbesserte Formatierung im PDF Output		
Version 1.1	25.08.2018	PS
Erweiterung des Kapitels Troubleshooting, finales Review		
Version 1.0	19.08.2018	PS
Initiale Erstellung		

1. Einführung in Kerberos

Der Name *Kerberos* stammt aus der griechischen Mythologie. Es handelt sich hierbei um den dreiköpfigen Wachhund des Hades[1], einem Gott der Unterwelt. Der Hund bewacht den Eingang zur Unterwelt, damit kein Lebender hinab steigt und kein Toter hinauf steigt. Die drei Köpfe symbolisisieren die drei Komponenten, die beim Kerberos Protokoll für die Authentifizierung benötigt werden:

- Client
- Ressource (Dienst oder Computer)
- Schlüsselverteilungscenter

Das Kerberos-Protokoll wurde für unsichere[2] Netzwerke entwickelt und bietet einen sicheren Authentifizierungsmechanismus, der auf Netzwerkebene fungiert. Es wurde ursprünglich 1978 am Massachusetts Institute of Technology (MIT) entwickelt und liegt mittlerweile in der Version 5 vor. Die genaue Spezifikation ist im RFC 4120[3] beschrieben.

Reduziert man die RFC 4120 Spezifikation auf das wesentliche, kann man sagen das:

- Kerberos ein auf Tickets basierendes Authentifizierungsprotokoll ist,
- Kennwörter nicht lokal gespeichert werden und niemals über das Netzwerk übertragen werden,
- Kerberos mit symmetrischer Verschlüsselung arbeitet,
- Kerberos eine dritte Partei einbindet, das Schlüsselverteilungscenter, *Key Distribution Center (KDC)* genannt.

Es gibt verschiedene Implementierungen des Kerberos-Protokolls für unterschiedliche Plattformen. Die beiden wichtigsten sind:

- **Microsoft Active Directory.** Die Kerberos Anmeldemethode ist im *Active Directory* implementiert und ist seit Windows Server 2003 die bevorzugte und sicherere Anmeldemethode.

- **MIT Kerberos.** Das MIT Kerberos ist eine freie Implementierung des Kerberos Protokolls für Unix und Linux Systeme. Die hierfür benötigten Installationspakete heißen in der Regel krb5* für die aktuelle Kerberos Version.

[1] https://de.wikipedia.org/wiki/Hades
[2] Ein Netzwerk gilt solange als unsicher, bis sichergestellt ist, das nur berechtigte Geräte oder Anwender das Netzwerk benutzen können.
[3] https://tools.ietf.org/html/rfc4120

1.1. Vor- und Nachteile

Grob zusammengefasst hat das Kerberos-Protokoll folgende Vor- und Nachteile:

Vorteile

Netzwerk

- Kerberos sorgt dafür, dass ein sich anmeldender Benutzer sicher authentifiziert wird.

  Bei einer Anmeldung an einem Computer bei Verwendung des NTLM Protokolls wird das Kennwort während des Authentifizierungsprozesses zum Authentifizierungsdienst übertragen. Dies macht die NTLM Anmeldemethode unsicher und anfällig für sogenannte *Replay-Angriffe*, bei dem mitgeschnittene Netzwerkpakete erneut gesendet werden und damit Benutzer ohne eigene Interaktion angemeldet werden können. Bei Verwendung des Kerberos Protokolls bei der Anmeldung wird u.a. nur einen verschlüsselter Hash-Wert des eingegebenen Kennwortes über das Netzwerk übertragen. Daher gilt das Kerberos Protokoll als sehr sicher für die Anmeldung.

- Das Kerberos-Protokoll funktioniert sowohl über das gesicherte TCP- als auch über das ungesicherte UDP-Protokoll. Dies schließt auch die Fähigkeit ein zu erkennen, ob ein verlorengegangenes Datenpaket neu angefordert wurde oder ob ein Replay-Angriff vorliegt.

Authentifizierung

Normalerweise muss der Benutzer sein Kennwort jedes Mal eingeben, wenn auf einen Dienst im Netzwerk zugegreifen möchte. Das Kerberos-Protokoll hingegen bietet eine Authentifizierungsmethode, mit der sich ein Benutzer nur einmal anmeldet und für den Rest der Sitzung dem gesamten Netzwerk vertraut. Dies führt zu einer Entlastung der Domänencontroller, die ansonsten für die Anmeldung zuständig wären.

Nachteile

Active Directory

Die Funktionsweise des Kerberos-Protokolls endet an der Active Directory Domänengrenze. Dies gilt auch für Multi-Domänen Umgebungen, also z.B. an der Firewall oder dem Perimeter-Netzwerk. Dies gilt jedoch nicht für VPN- oder Direct Access Verbindungen.

Troubleshooting

Aufgrund der hohen Komplexität des Protokolls ist eine Fehlersuche deutlich schwieriger als bei anderen Authentifizierungsmechanismen. So reicht bereits eine falsch gehende PC-Uhr dafür, dass eine Anmeldung fehlschlägt.

Ein Weiteres sehr wichtiges Anmeldeprotokoll ist in diesem Zusammenhang OAuth 2.0, welches außerhalb von Domänengrenzen zur Verfügung steht. Dieses wird jedoch in einem anderen Whitepaper beschrieben.

1.2. Schwachstellen

Das Kerberos-Protokoll in der aktuell vorliegenden Version 5 ist gegenüber der Version 4 deutlich sicherer was Schwachstellen angeht. Nichtsdestotrotz gibt es sowohl Schwachstellen im Protokoll als auch in der Implementierung:

- In der im Active Directory vorgenommenen Kerberos Implementierung ist die gesamte Datenbank mit den geheimen Schlüsseln mit einem einzigen Master Key verschlüsselt. Wird dieser kompromittiert sind alle geheimen Schlüssel bekannt und das gesamte System ist unsicher. Der Angreifer kommt damit in den Besitz des sogenannten „Goldenen Tickets[4]“.

  Aus diesem Grund ist dem Schutz des Active Directory große Bedeutung zuzumessen. Hier sei im Bedarfsfall auf Hersteller verwiesen, die die Active Directory Kommunikation überwachen und Angriffsmuster erkennen können.
- Da alle Kerberos-Tickets mit einer Gültigkeitsdauer (von-bis) versehen sind, besteht ein theoretischer Angriffsvektor darin die Server-Uhrzeiten zu manipulieren um so bereits abgelaufene Tickets erneut nutzen zu können.
- Durch Brute-Force-Attacken auf das Kennwort eines Benutzers kann die Kerberos-Authentifizierung insbesondere bei administrativen Konten ausgehebelt werden.

  Es sollte daher sichergestellt sein, dass entsprechende Kennwort-Richtlinien existieren, damit Benutzer sicherere Kennwörter verwenden. Diese sollten mindestens aus drei von vier verschiedenen Gruppen bestehen.
  - Grossschrift
  - Kleinschrift
  - Zahlen
  - Sonderzeichen

  Die Nutzung von Sonderzeichen sollte hierbei eingeschränkt werden, da nicht jede Applikation z.B. mit dem €-Zeichen klarkommt. Weiterhin sollte die Nutzung von Zeichen mit einem ASCII Wert von >127 unterbunden werden, da diese nicht in jedem Zeichensatz vorhanden sind.

1.3. Infrastrukturkomponenten

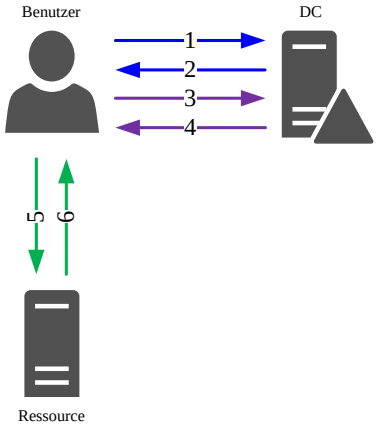
Damit das Kerberos-Protokoll in einer Netzwerkumgebung funktioniert, sind einige grundsätzliche Infrastrukturkomponenten notwendig:

- Zeitserver (*NTP*)
- Authentifizierungsdienst (*AS*)
- Ticket ausstellender Dienst (*TGS*)

[4] https://blog.varonis.com/kerberos-how-to-stop-golden-tickets/

1.4. Ein einfacher Protokollablauf

Ein einfacher Anmeldeprozess läuft beispielsweise wie folgt ab:



1. Ein Client sendet eine Anfrage an den Authentifizierungsservice (AS) um die „Anmeldeinformationen“ für eine bestimmte Ressource zu erhalten.

2. Wenn der AS die Authentizität des Benutzers bestätigen kann, sendet er eine Nachricht zurück an den Client, verschlüsselt mit dem Schlüssel des Clients. Diese Nachricht enthält auch einen Sitzungsschlüssel.

3. Der Client fordert nach der erfolgreichen Authentifizierung ein „Ticket“ für die benötigte Ressource beim Ticket-ausstellenden-Server an. Er verwendet für die Verschlüsselung der Anfrage den zuvor verschlüsselt erhaltenen Sitzungsschlüssel.

4. Der Ticket-ausstellende-Server erstellt ein „Ticket“ für den Client, verschlüsselt mit dem zuvor ausgetauschten Sitzungsschlüssel. Das Ticket enthält weiterhin einen Sitzungsschlüssel, der mit dem Schlüssel der zu verwendenden Ressource verschlüsselt ist.

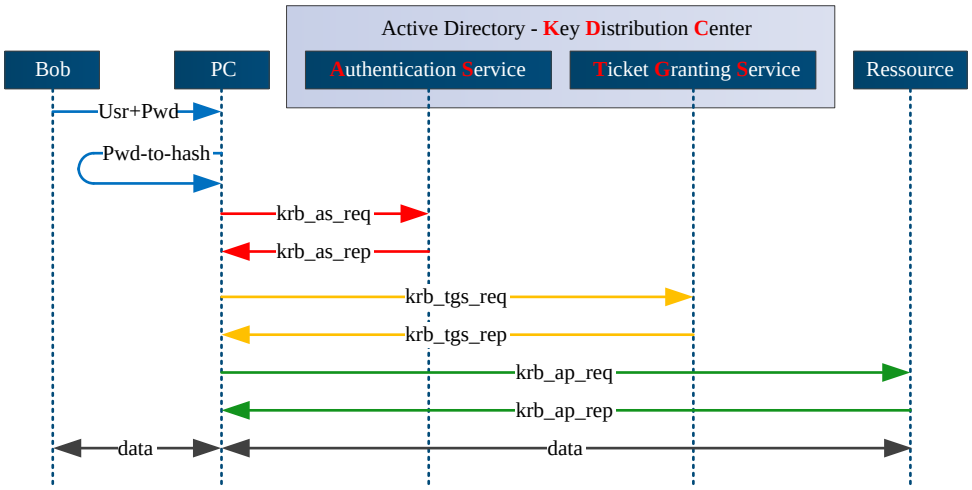
5. Der Client übermittelt jetzt das entschlüsselte „Ticket“ des Ticket-ausstellenden-Servers an die benötigte Ressource. Das Ticket enthält die Identität des Clients und eine Kopie des Sitzungsschlüssels verschlüsselt mit dem Schlüssel der angeforderten Ressource. Der Sitzungsschlüssel (jetzt von Client und Server geteilt) wird zur Authentifizierung des Clients verwendet.

> ***Wichtig***
>
> *Es ist zu beachten, dass viele Anwendungen Kerberos-Funktionen nur beim Start einer streambasierten Netzwerkverbindung verwenden. Auch wenn eine Anwendung eine Verschlüsselung oder einen Integritätsschutz für den Datenstrom durchführt, gilt die Identitätsprüfung nur für die Einleitung der Verbindung. Dies bedeutet jedoch auch, dass nachfolgende Daten in der Verbindung nicht vom selben Absender stammen müssen.*

6. Da der anfragende Client nun erfolgreich authentifiziert wurde, erhält er die angeforderten Daten.

1.5. Komponenten des Kerberos-Protokoll

Um die Arbeitsweise des Kerberos-Protokolls zu verstehen, nehmen wir uns hier nach und nach die einzelnen Protokoll-Elemente vor. Wir orientieren uns hierbei an den englischen Begriffen, die im RFC 4120 verwendet werden.



krb_as_req

Ein Client sendet ein Ticket an den Authentifizierungsdienst (AS), bestehend aus einem unverschlüsselten und einem verschlüsselten Teil. Dieses Ticket beinhaltet u.a. die Uhrzeit im Format YYYYMMDDHHMMSSZ (als *UTC*), den qualifizierten Domänennamen (Realm) in der sich die benötigte Ressource befindet, die Kerberos-Version (v5), den Benutzernamen (`contoso\bob`), den Hash-Wert des eingegebenen Kennwortes sowie eine Zufallszahl zum Schutz vor Replay-Angriffen.

krb_as_rep

Bevor der AS mit dem *krb_as_rep* Ticket die Antwort an den Client sendet, werden verschiedene Prüfungen durchgeführt. Dies sind u.a.:

- Das Vorhandensein des Benutzers
- Das Vorhandensein der angefragten Ressource
- Die Übereinstimmung des empfangenen Hash-Wertes des Kennwortes mit dem Hash-Wert des gespeicherten Kennwortes
- Die Uhrzeit mit einer Abweichung von <5 Minuten

Waren alle Prüfungen erfolgreich, sendet der AS ein mit dem geheimen Schlüssel des Clients verschlüsseltes Antwort-Ticket, dem sogenannten *Authenticator* sowie ein Ticket Granting Ticket (*TGT*), welches mit dem geheimen Schlüssel des KDC verschlüsselt ist und vom Client nicht entschlüsselt werden kann. Dies enthält u.a. folgende Elemente:

- Den Benutzernamen von Bob
- Die Adresse des Ticket Granting Servers (TGS)
- Einen Sitzungsschlüssel
- Die Gültigkeitsdauer des Tickets
- Einen Zeitstempel
- Die Gruppenmitgliedschaften des Benutzers in einem Feld namens PAC (Privilege Attribute Certificate). Diese werden später zum Erstellen des Zugriffstokens für Client verwendet.

krb_tgs_req — Der PC des Clients entschlüsselt den für ihn relevanten Teil des Tickets und wendet sich anschließend mit dem verschlüsselten Teil des TGT an den TGS.

Wenn der TGS den mit dem geheimen Schlüssel des KDC verschlüsselten Teil des TGT entschlüsseln kann, kann er sicher sein, das der die Ressource anfragende Client derjenige ist, für den er sich ausgibt.

krp_tgs_rep — Waren die im *krb_tgs_req* erhaltenen Daten korrekt, erstellt der TGS ein Service-Ticket. Neben dem Service-Ticket, das nur der die Ressource bereitstellende Server mit seinem geheimen Schlüssel entschlüsseln kann, sendet der TGS einen Sitzungsschlüssel für die weitere verschlüsselte Client / Ressource-Kommunikation im sogenannten Authenticator mit. Der Authenticator enthält u.a. die Client-ID von Bob und einen Zeitstempel, verschlüsselt mit dem Client / Ressource-Sitzungsschlüssel.

krb_ap_req — Möchte der Client nun auf die Ressource zugreifen, sendet er das zuvor erhaltene Service-Ticket an den die Ressource bereitstellenden Server, welches nur dieser entschlüsseln kann.

krb_ap_rep — Konnte der die Ressource bereitstellende Server das Service-Ticket entschlüsseln, kann er den ebenfalls mitgesendeten Authenticator des Clients extrahieren und verifizieren. Ist dieser gültig, erstellt der die Ressource bereitstellende Server ein Zugriffstoken für Bob, basierend auf den im PAC enthaltenen Gruppenmitgliedschaften.

Nach dem Erhalt des *krb_ap_rep* Tickets kann Bob die angefragte Ressource mit dem Zugriffstoken verwenden.

Wer es bis hier hin durchgehalten hat und den Ablauf aufmerksam verfolgt hat, dem ist sicherlich eines aufgefallen:

Der die Ressource bereitstellende Server hat überhaupt nicht mit dem KDC kommuniziert um den Client zu verifizieren. Das ist völlig korrekt. Da der KDC alle geheimen Schlüssel kennt, hat er das im *krb_tgs_rep* enthaltene Service-Ticket mit dem Hash-Wert des geheimen Schlüssels des die Ressource bereitstellenden Servers verschlüsselt.

Der beschriebene Protokollablauf lässt sich beliebig fortsetzen wenn ein Client eine Ressource in einem anderen Realm anfragt. Hier übergibt der KDC in einem Session-Ticket den durch die Vertrauensstellung zwischen den Active Directory Domänen bekannten Hash-Wert des geheimen Schlüssel der nächsten Instanz, wo dann der beschriebene Ablauf erneut beginnt.

1.6. Hochverfügbarkeit

Wird eine Ressource durch mehrere Server bereitgestellt, wie es z.B. bei Webservern der Fall ist, muss sichergestellt sein das alle Server das gleiche Kerberos Konto verwenden. Dazu mehr im nächsten Kapitel

2. Kerberos und Skype for Business Server

Die Verwendung von Kerberos als Authentifizierungsprotokoll für Skype for Business vereinfacht die Anmeldeprozesse an Skype for Business Server. Dies gilt insbesondere dann, wenn die Skype for Business Webservices über einen Loadbalancer verteilt werden. Wenn Sie das Kerberos Computerkonto einer Site zuweisen, werden die Service Prinzipal Namen (SPNs) für dieses Konto registriert und an alle Frontend Server der jeweiligen Site verteilt. Alle Skype for Business Frontend Server teilen dann gleiche Kerberos Computerkonto für alle Anfragen.

Der Vorteil der Aktivierung von Kerberos liegt darin begründet, das es egal ist welchen Frontend Server der Client anspricht. Er muss sich nur ein einziges Mal für die nächsten 10 Stunden authentifizieren, sofern der Active Directory Standardwert nicht verändert wurde.

2.1. Aktivierung von Kerberos

Die Einrichtung unter Skype for Business Server gestaltet sich recht einfach.

Anmerkung

*Beachten Sie, das Sie über die benötigten Rechte zur Ausführung des **New-CsKerberosAccount** Powershell Befehls verfügen. Sie müssen Mitglied der folgenden Gruppen sein:*

- *Domänen Administratoren*
- *RtcUniversalServerAdmins*

*Eine Delegierung von Rechten zum Anlegen von Computerkonten ist in der Regel nicht ausreichend, da der **New-CsKerberosAccount** Powershell-Befehl folgende Attribute am Kerberos-Computerkonto vornimmt, die im Regelfall nur Domänen-Administratoren vorbehalten sind:*

```
Get-ADComputer -Identity kerbact -Properties *
[...]
Enabled                                 : True
[...]
LockedOut                               : False
[...]
PasswordNeverExpires                    : True
PasswordNotRequired                     : True
[...]
servicePrincipalName                    : {http/skypewebpool02.contoso.com,
                                           http/skypewebpool01.contoso.com
                                           http/skypepool02.contoso.com,
                                           http/skypepool01.contoso.com}
ServicePrincipalNames                   : {http/skypewebpool02.contoso.com
                                           http/skypewebpool01.contoso.com
                                           http/skypepool02.contoso.com,
                                           http/skypepool01.contoso.com}
[...]
```

1. Anlegen eines Computerkontos für Kerberos.

   Beachten Sie, das der Kontoname **maximal 15 Zeichen** lang sein darf:

   ```
   New-CsKerberosAccount -UserAccount contoso\kerbact `
   -ContainerDN "OU=Special,OU=MyUsers,DC=contoso,DC=com"
   ```

   Dies ist der *NetBIOS* Implementierung zu verdanken, die maximal 16 Zeichen erlaubt.

2. Zuweisen des Kerberos Computerkonto zum Skype for Business Frontend Servers.

   Bei mehreren Sites muss das Kerberos Computerkonto allen Sites zugewiesen werden, damit das Loadbalancing für die Skype for Business Webservices über alle Server hinweg funktioniert.

   ```
   New-CsKerberosAccountAssignment -UserAccount contoso\kerbact -Identity
    "site:Contoso"
   ```

3. Topologie veröffentlichen.

   Bevor das Kennwort für das Kerberos-Computerkonto gesetzt werden kann, muss die Skype for Business Topologie veröffentlicht werden, damit alle Frontend Server Kenntnis von dem neuen Kerberos-Computerkonto erhalten.

   ```
   Enable-CsTopology
   ```

4. Kennwort zuweisen.

   Zum Abschluß der Kerberos Konfiguration wird dem Kerberos Computerkonto ein möglichst komplexes Kennwort zugewiesen.

   ```
   Set-CsKerberosAccountPassword -UserAccount contoso\kerbact
   ```

5. **Enterprise Pool:** Weitere Registrierung von Service Prinzipal Namen

   Bei einer Skype for Business Enterprise Pool Installation muss sichergestellt sein, das der DNS-A-Eintrag für die Skype for Business Webservices (z.B. *skypewebpool01.contoso.com*) auf die Loadbalancer VIP zeigt und das der Name für den/die Skype for Business Web-Pool(s) als zusätzlicher SPN registriert wird.

   ```
   setspn.exe -S http/skypewebpool01.contoso.com contoso\kerbact
   setspn.exe -S http/skypewebpool02.contoso.com contoso\kerbact
   ```

6. **Enterprise Pool:** Topologie veröffentlichen.

   Alle Frontend Server erhalten dadurch Kenntnis von den zusätzlichen Service Prinzipal Namen.

   ```
   Enable-CsTopology
   ```

2.2. Überprüfen der Kerberos Aktivierung

Die durchgeführte Konfiguration kann auf verschiedene Weise überprüft werden. Entweder mit dem `setSPN.exe` Kommandozeilen Tool oder mit der Powershell.

```
C:\Windows\System32\setspn.exe -L contoso\kerbact
Registered ServicePrincipalNames for
CN=kerbact,OU=Special,OU=MyUsers,DC=contoso,DC=com:
        http/skypewebpool02.contoso.com
        http/skypewebpool01.contoso.com
        http/skypepool02.contoso.com
        http/skypepool01.contoso.com
```

Überprüfen Sie, ob der Dienst-SPN in der Liste auftaucht.

Wichtig

*Bitte achten Sie darauf, das die Service Prinzipal Namen nicht mit **https** beginnen. Dies ist falsch und funktioniert nicht, da hier nur der bereitgestellte Dienst gemeint ist und das ist in diesem Fall http.*

Alternativ über die Powershell:

```
Get-ADComputer -Identity kerbact -Properties * | Select-Object servicePrincipalName,
 ServicePrincipalNames
```

Wenn Clients nach der Aktivierung von Kerberos für Skype for Business ein Popup Fenster zur Authentifizierung bei der Anmeldung anzeigen, bedeutet dies das ein Konfigurationsfehler aufgetreten ist. Dies kann relativ einfach per Powershell-Befehl überprüft werden:

```
Test-CsKerberosAccountAssignment -Identity "site:Contoso" -Report "c:\temp\KerbConf.htm"
 -Verbose
```

Am Client-Computer kann die Kerberos-Authentifizierung nach einem Neustart des Skype for Business Clients mittels des `C:\Windows\System32\klist.exe` Befehls geprüft werden, wobei die relevante Zeile jeweils mit `Server:` beginnt:

```
PS C:\Users\schmelpe> klist

Aktuelle Anmelde-ID ist 0:0x68f3a

Zwischengespeicherte Tickets: (5)
[...]
#1> Client: schmelpe @ CONTOSO.COM
 Server: sip/skypepool01.contoso.com @ CONTOSO.COM
 KerbTicket (Verschlsselungstyp): AES-256-CTS-HMAC-SHA1-96
 Ticketkennzeichen 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
 Startzeit: 8/7/2018 14:38:26 (lokal)
 Endzeit:   8/8/2018 0:00:07 (lokal)
 Erneuerungszeit: 8/14/2018 14:00:07 (lokal)
 Sitzungsschlsseltyp: AES-256-CTS-HMAC-SHA1-96
 Cachekennzeichen: 0
 KDC aufgerufen: contoso.com

#2> Client: schmelpe @ CONTOSO.COM
 Server: HTTP/skypewebpool01.contoso.com @ CONTOSO.COM
 KerbTicket (Verschlsselungstyp): AES-256-CTS-HMAC-SHA1-96
 Ticketkennzeichen 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
 Startzeit: 8/7/2018 14:38:25 (lokal)
 Endzeit:   8/8/2018 0:00:07 (lokal)
 Erneuerungszeit: 8/14/2018 14:00:07 (lokal)
 Sitzungsschlsseltyp: AES-256-CTS-HMAC-SHA1-96
 Cachekennzeichen: 0
 KDC aufgerufen: contoso.com
```

3. Kerberos und Exchange Server

Damit die Kerberos Authentifizierung in Verbindung mit den Exchange Servern, auf denen Clientzugriffsdienste ausgeführt werden, verwendet werden kann, müssen die nachfolgend beschriebenen Konfigurationsschritte ausgeführt werden.

Die Konfiguration sollte unabhängig davon durchgeführt werden, ob ein einzelner Exchange Server oder mehrere Exchange Server mit Lastenausgleich der Clientzugriffsdienste ausgeführt werden.

Unter Exchange Server wird für die Kerberos Authentifizierung der sogenannte *Alternative Service Account (ASA)* angelegt und verwendet.

Wichtig

Exchange 2010 und Exchange 2016 können nicht den selben ASA verwenden. Sollten also in ihrer Infrastruktur noch ein Exchange Server 2010 vorhanden sein, muss für Exchange Server 2016 ein neuer ASA angelegt werden.

Weiterhin ist zu beachten, dass der verwendete Namensraum, wie z.B. contoso.com im DNS mit Host A Einträgen und nicht mit CNAME Einträgen hinterlegt ist. Dies wird zwar unterstützt, ist jedoch ausdrücklich nicht empfohlen[5].

3.1. Serverseitige Aktivierung von Kerberos

Alle Exchange Server, auf denen die Clientzugriffsdienste ausgeführt werden und den selben Namensraum und URLs teilen, müssen den gleichen ASA verwenden.

Anmerkung

In dem nachfolgenden Beispiel wird davon ausgegangen das die Exchange Infrastruktur vollständig konfiguriert und bereits in Betrieb ist.

Ist dies nicht der Fall, muss sichergestellt sein, das alle Exchange Webdienste, also

- *Outlook Web Access (OWA)*
- *Outlook Address Book (OAB)*
- *Exchange Control Panel (ECP)*
- *Exchange Webservices (EWS)*
- *Active Sync*
- *Outlook Anywhere*
- *Client Access Service (CAS)*

korrekt konfiguriert wurden.

[5] https://docs.microsoft.com/en-us/exchange/architecture/client-access/kerberos-auth-for-load-balanced-client-access#create-the-alternate-service-account-credential-in-active-directory-domain-services

Alle Konfigurationsarbeiten werden alle in der Exchange Management Shell durchgeführt.

1. Prüfen des *Microsoft Exchange Service Host* Dienst.

   Bevor mit der Konfiguration des Exchange ASA für die Kerberos Authentifizierung begonnen wird, muss geprüft werden, ob der Dienst *Microsoft Exchange Service Host* im Startmodus *Automatisch* steht und läuft. Der Dienst auf dem Server, auf dem die Client-Zugriffsdienste ausgeführt werden, ist für die Verwaltung der ASA-Anmeldeinformationen zuständig. Wenn dieser Dienst nicht ausgeführt wird, ist eine Kerberos-Authentifizierung nicht möglich. Standardmäßig ist der Dienst so konfiguriert, dass er beim Start des Computers automatisch gestartet wird, kann jedoch im Rahmen einer Server Härtung deaktiviert worden sein.

2. Anlegen eines Computerkontos für Kerberos.

   Wie unter Skype for Business auch, wird für den Exchange ASA ein Computerkonto angelegt.

   ```
   New-ADComputer -Name EX2016ASA -AccountPassword
   (Read-Host 'Kennwort' -AsSecureString) -Description 'Exchange Service-Account
   für die Kerberos Authentifizierung' -Enabled $True -SamAccountName EX2016ASA
   -DisplayName "Exchange 2016 ASA"
   ```

   Nach Eingabe eines beliebigen Kennwortes, welches den Kennwortrichtlinien des Unternehmens entspricht, wird das neue Computerobjekt im Active Directory im Zweig „Computers“ angelegt. Das Kennwort wird wird im späteren Verlauf geändert. Bitte daran denken, das neue Exchange ASA Computerkonto anschließend in die gewünschte OU zu verschieben und das Kennwort regelmäßig automatisiert zu ändern.

3. Einrichten des zu verwendenden Kerberos Verschlüsselungsalgorithmus durch den ASA.

   Im Standard ist kein zu verwendender Verschlüsselungsalgorithmus für das Kerberos Computerkonto aktiv. Zur Auswahl stehen folgende Algorithmen:

   - DES-CBC-CRC (Dezimal 1)
   - DES-CBC-MD5 (Dezimal 2)
   - RC4-HMAC (Dezimal 4)
   - AES128-CTS-HMAC-SHA1-96 (Dezimal 8)
   - AES256-CTS-HMAC-SHA1-96 (Dezimal 16)

   Der zu verwendende Verschlüsselungsalgorithmus wird im Active Directory Attribut *msDC-SupportedEncryptionTypes* konfiguriert. Der im AD Attribut zu konfigurierende Wert wird durch einfache Addition ermittelt. Microsoft empfiehlt hier die drei letztgenannten Algorithmen zu verwenden, also 16+8+4=28. Daraus ergibt sich dann folgender Powershell Befehl:

   ```
   Set-ADComputer EX2016ASA -add @{"msDS-SupportedEncryptionTypes"="28"}
   ```

4. Zuweisen der ASA Anmeldeinformationen.

   Zum Zuweisen der neuen ASA-Anmeldeinformationendas muss in das Exchange Scripts Verzeichnis gewechselt werden und das Skript *RollAlternateServiceAccountPassword.ps1* ausgeführt werden:

```
cd C:\"Program Files\Microsoft\Exchange Server"\V15\Scripts

.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServer ex01.contoso.com
-GenerateNewPasswordFor contoso\EX2016ASA$
```

War bis hier hin alles korrekt konfiguriert, ergibt sich folgendes Ergebnis:

```
.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServers
 ex01.contoso.com -GenerateNewPasswordFor contoso\EX2016ASA$
[...]
========== Starting at 08/18/2018 13:36:56 ==========
Destination servers that will be updated:

Name PSComputerName
---- --------------
EX01 ex01.contoso.com
[...]
Credentials that will be pushed to every server in the specified scope (recent
 first):

UserName                                Password
--------                                --------
contoso\EX2016ASA$ System.Security.SecureString
[...]
Prior to pushing new credentials, all existing credentials that are invalid or no
 longer work will be removed from the destination servers.
Pushing credentials to server EX01
Setting a new password on Alternate Serice Account in Active Directory
```

Nach Bestätigung des Kennwortwechsels werden die restlichen Konfigurationen am EX2016ASA$-Konto vorgenommen:

```
Password change
Do you want to change password for contoso\EX2016ASA$ in Active Directory at this
 time?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
Preparing to update Active Directory with a new password for contoso\EX2016ASA$ ...
Resetting a password in the Active Directory for contoso\EX2016ASA$ ...
New password was successfully set to Active Directory.
Retrieving the current Alternate Service Account configuration from servers in
 scope
Alternate Service Account properties:

StructuralObjectClass QualifiedUserName  Last Pwd Update      SPNs
--------------------- -----------------  ---------------      ----
computer              contoso\EX2016ASA$ 8/18/2018 1:37:03 PM
[...]
Per-server Alternate Service Account configuration as of the time of script
 completion:
[...]
   Array: mail.contoso.com

Identity AlternateServiceAccountConfiguration
-------- ------------------------------------
EX01     Latest: 8/18/2018 1:36:59 PM, contoso\EX2016ASA$
         Previous: <Not set>
[...]
========== Finished at 08/18/2018 13:37:04 ==========

        THE SCRIPT HAS SUCCEEDED
```

5. OPTIONAL: Bei **zwei oder mehr** Exchange Servern im gleichen Namensraum muss die ASA Konfiguration auf alle Exchange Server im gleichen Namensraum verteilt werden. Dies

geschieht durch Aufruf des zuletzt verwendeten Skriptes mit leicht veränderter Syntax auf allen weiteren Exchange Servern:

```
cd C:\"Program Files\Microsoft\Exchange Server"\V15\Scripts

.\RollAlternateServiceAccountPassword.ps1 -ToSpecificServer ex02.contoso.com
-CopyFrom ex01.contoso.com
```

Die dem Skript übergebenen Parameter stellen nur ein Subset der Möglichkeiten dar. Weitere Informationen hierzu finden sich in diesem Artikel[6] von Microsoft.

6. Binden des Dienst Prinzipal Namen an Exchange Server.

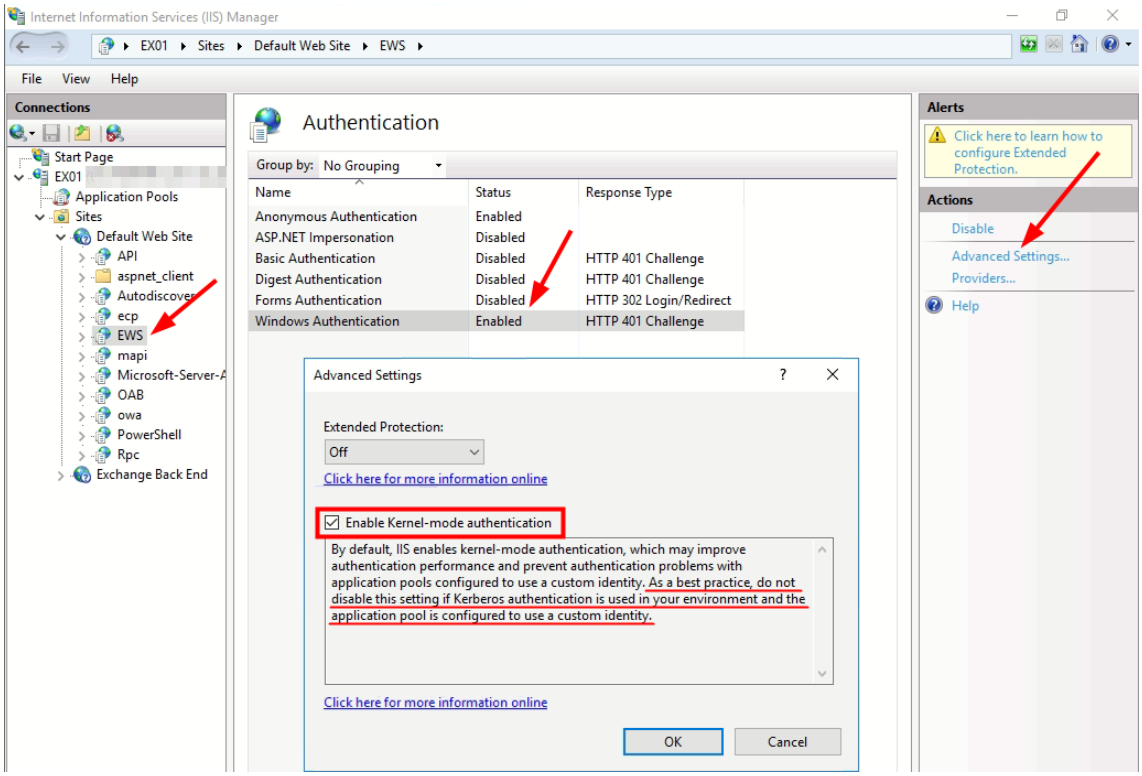
   Um den Exchange Server mit der Kerberos Authentifizierung zu verbinden muss der Dienst Prinzipal Name mit Exchange Server verbunden werden:

```
setspn -S http/mail.contoso contoso\EX2016ASA$
Checking domain DC=contoso,DC=com

Registering ServicePrincipalNames for CN=EX2016ASA,CN=Computers,DC=contoso,DC=com
        http/mail.contoso.com
Updated object
```

7. Anpassen der Exchange Webservices (EWS) im IIS.

   Last but not least muss im IIS noch die Windows Authentifizierung im Kernel Mode aktiviert und der IIS neu gestartet werden:



[6] https://technet.microsoft.com/en-us/library/ff808311%28v=exchg.150%29.aspx

3.2. Clientseitige Aktivierung von Kerberos

Damit die verbundenen Outlook Clients zukünftig auch tatsächlich die Kerberos Authentifizierung verwenden, muss diese noch für Outlook Anywhere aktiviert werden. Outlook Anywhere nutzt das *MAPI over HTTP* Protokoll und ist neben den Exchange Webservices (EWS) und Active Sync das einzige Protokoll, welches für die Clientkommunikation Verwendung findet. Das früher verwendete *RPC over HTTP* Protokoll wurde mit Exchange 2016 abgeschaltet.

```
Get-OutlookAnywhere | Format-List
[...]
ExternalClientAuthenticationMethod : Negotiate
InternalClientAuthenticationMethod : Ntlm
IISAuthenticationMethods           : {Basic, Ntlm, Negotiate}
[...]

Get-MAPIVirtualDirectory | Format-List
[...]
IISAuthenticationMethods        : {Ntlm, OAuth, Negotiate}
[...]
```

Wie im vorangegangenen Printout im Element `InternalClientAuthenticationMethod` zu sehen ist, steht intern im Standard nur NTLM als Anmeldeprotokoll zur Verfügung. Dieses wird mit nachfolgendem Powershell Befehl auf die Kerberos Authentifizierung umgestellt:

```
Get-OutlookAnywhere -Server EX01 | Set-OutlookAnywhere -
InternalClientAuthenticationMethod Negotiate
```

Wichtig

Nach Umstellung auf die Kerberos Authentifizierung können sich keine Exchange Server, die älter als die Version 2013 sind, mehr mit diesem Server verbinden um z.B. Zugriff auf öffentliche Ordner zu erhalten. Dies wird auch als Hinweis beim Abschluss des vorangegangenen Befehls als Hinweis ausgegeben.

```
Get-OutlookAnywhere | Format-List
[...]
ExternalClientAuthenticationMethod : Negotiate
InternalClientAuthenticationMethod : Negotiate
[...]
```

Zum Abschluss der clientseitigen Bereitstellung der Kerberos Authentifizierung wird noch die *OAuth*-Anmeldemethode aus dem virtuellen MAPI Verzeichnis des IIS entfernt.

```
Get-MapiVirtualDirectory -Server EX01 | Set-MapiVirtualDirectory -
IISAuthenticationMethods Ntlm, Negotiate

Get-MapiVirtualDirectory -Server EX01 | Format-List
[...]
IISAuthenticationMethods        : {Ntlm, Negotiate}
[...]
```

3.3. Überprüfung von Kerberos

Die korrekte Anlage und Funktion des Exchange ASA kann einfach per Powershell Befehl geprüft werden:

```
Get-ClientAccessService -IncludeAlternateServiceAccountCredentialStatus| Format-List
 Name, AlternateServiceAccountConfiguration
```

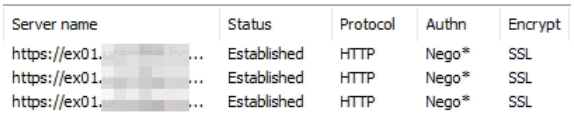
Hier sollte sich folgendes Ergebnis zeigen:

```
Get-ClientAccessService -IncludeAlternateServiceAccountCredentialStatus| Format-List
 Name, AlternateServiceAccountConfiguration
[...]
Name                                : EX01
AlternateServiceAccountConfiguration : Latest: 8/18/2018 1:36:59 PM, contoso\EX2016ASA$
                                       Previous: <Not set>
```

Weiterhin besteht die Möglichkeit, die Kerberos Authentifizierung im Logfile des RpcHTTP-Logs des Exchange Servers zu überprüfen. Das Logfile findet sich unter folgendem Pfad: `%ExchangeInstallPath%\Logging\HttpProxy\RpcHttp\W3SVC2`. Das Schlüsseltwort *Negotiate* signalisiert die erfolgreiche Aktivierung der Kerberos Authentifizierung:

```
2018-08-18T14:42:29.214Z,EX01,RpcHttp,"S:Stage=BeginRequest;
S:OutlookSessionId=""{D6C[…]1A97}Client=ACTIVEMONITORING"";S:AuthType=Negotiate;
S:HttpVerb=RPC_OUT_DATA;S:UriQueryString=?ex01.contoso.com:6001;
S:ServerTarget=87[…]da8@ucandme.local;S:RequestId=26f[…]ab6;
S:AssociationGuid=a98[…]940;S:ClientIp=::1"
```

Zuletzt besteht noch die Möglichkeit die ausgehandelte Verbindung des Outlook-Clients über den *Verbindungsstatus* von Outlook im Windows Systray zu prüfen. Hierzu klicken sie mit der rechten Maustaste, bei gedrückter STRG-Taste, auf das Outlook Icon im Systray und wählen die Option *Verbindungsstatus* aus. Im Verbindungsstatus Fenster können sie dann das ausgehandelte Protokoll überprüfen.



Server name	Status	Protocol	Authn	Encrypt
https://ex01. ...	Established	HTTP	Nego*	SSL
https://ex01. ...	Established	HTTP	Nego*	SSL
https://ex01. ...	Established	HTTP	Nego*	SSL

4. Kerberos Constrained Delegation

Sie haben sich bestimmt schon die ganze Zeit gefragt, warum ich die ausführliche Einrichtung der Kerberos Authentifizierung für Skype for Business Server und Exchange Server beschreibe, ohne einen sinnvollen Anwendungszweck beschrieben zu haben. Die Entlastung von Domänencontrollern unter Verwendung der Kerberos Authentifizierung kann ja sicherlich nicht der einzige Grund sein. Stimmt! Sie haben recht.

Im Unified Communication Umfeld gibt es 3rd-Party Produkte für Skype for Business und Exchange, die die Kerberos Authentifizierung zwingend voraussetzen, um zu funktionieren.

Es gibt Unternehmen, die keine „Full Managed Devices“ wie Mobiltelefone verwenden um den Mitarbeitern den Vorteil der privaten Nutzung zu ermöglichen. In der Regel ist auf den mobilen Geräten daher eine Containerlösung installiert, um die Unternehmensdaten zu schützen. Da die Skype for Business Mobile App jedoch nicht containerfähig ist, müssten für die Nutzung der App die Anmeldedaten des Mitarbeiters für das Unternehmensnetzwerk in der App auf dem Mobiltelefons gespeichert werden. Dies kann je nach Branche des Unternehmens ein Sicherheitsrisiko bedeuten.

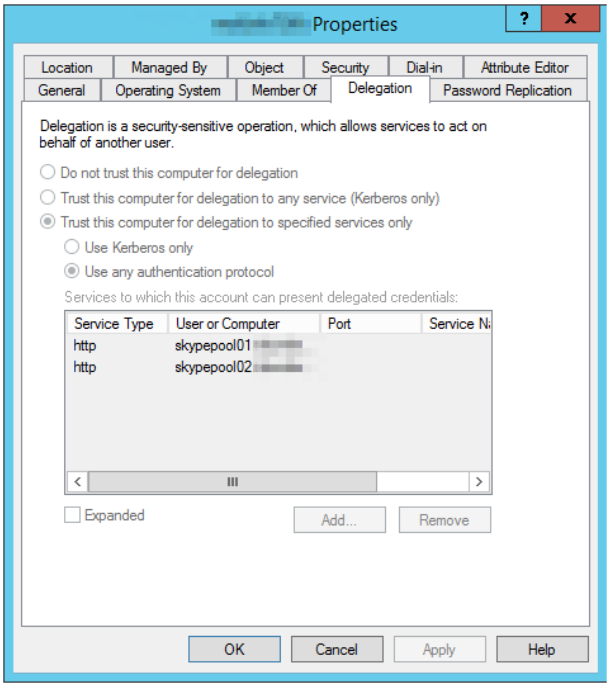
Hier greifen Sicherheitslösungen ein, die zum Ziel haben das der Mitarbeiter keine Anmeldedaten für das Unternehmensnetzwerk mehr auf dem Mobiltelefon speichern muss. Technisch betrachtet definiert der Mitarbeiter persönliche, vom Unternehmensnetzwerk unabhängige Zugangsdaten, bestehend aus Benutzername und Kennwort. Diese werden zusammen mit weiteren Parametern gespeichert. Das 3rd-Party Produkt im Backend sorgt dann in der Kommunikation zwischen Mobiltelefon und Skype for Business Server bzw. Exchange Server dafür, das die selbstdefinierten Zugangsdaten nach erfolgreicher Prüfung mit weiteren Parametern zur Authentifizierung herangezogen werden.

Während des Konfigurationsprozesses dieser Backend Anwendungen wird dem angelegten Kerberos Computerkonto noch die Delegation für bestimmte Dienste erlaubt. Letztendlich bedeutet dies, das das Kerberos Computerkonto „im Auftrag des Benutzers“ agiert. Das ist Kerberos Constrained Delegation (KCD).

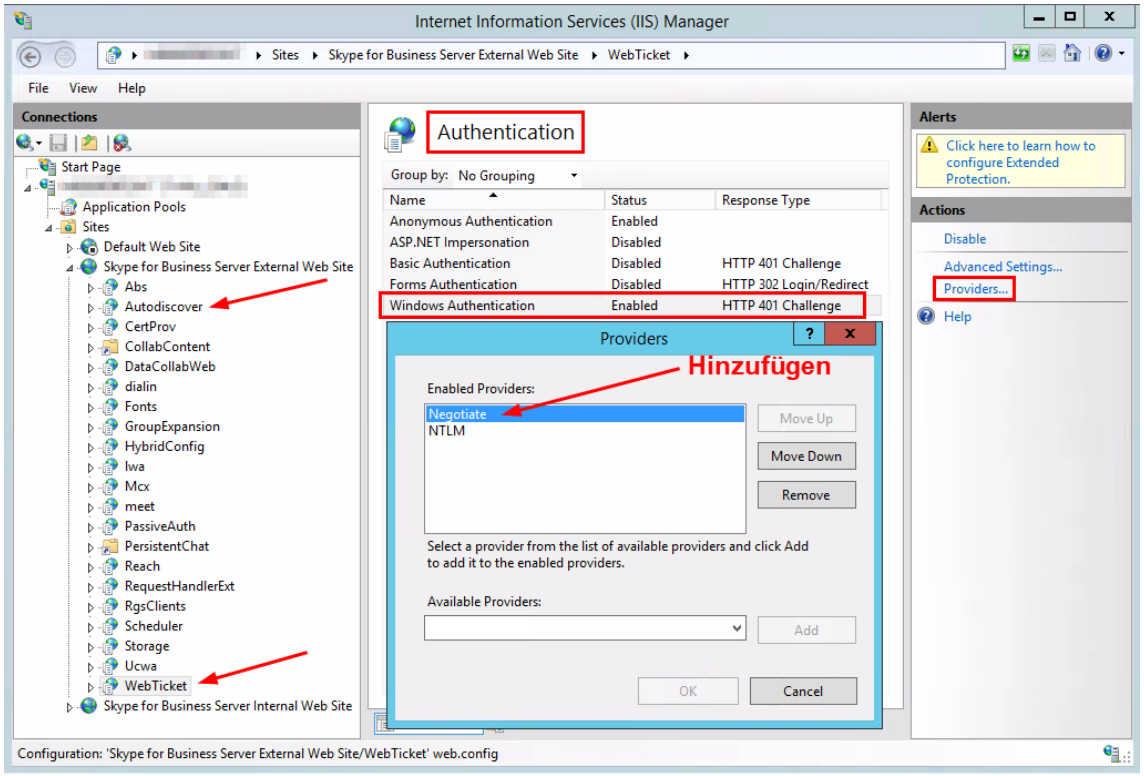
Die Einrichtung von KCD für Skype for Business- und Exchange-Server ist recht einfach zu konfigurieren, da an dem vorhandenen Kerberos Computerkonto nur die Delegation aktiviert werden braucht.

4.1. KCD für Skype for Business Server

Rufen sie die Eigenschaften des Kerberos Computerkontos für Skype for Business Server auf und wechseln auf den Reiter *Delegation*. Aktivieren sie *Trust this Computer for delegation to specified services only* sowie *Use any authentication protocol* und fügen dann ihre(n) Skype for Pool(s) mit dem Service Typ „http“ hinzu.



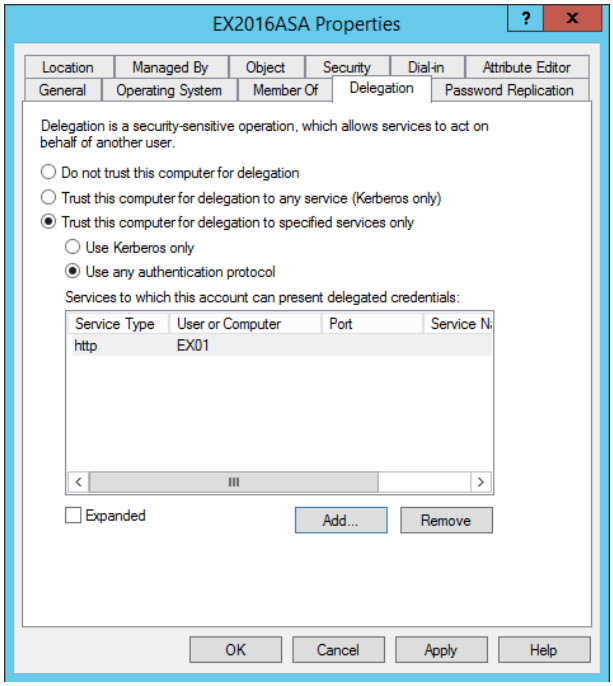
Damit der IIS auf den/dem Frontend Server(n) auch Kerberos Authentifizierung unterstützt, muss nur noch der entsprechende „Provider“ für die Authentifizierung aktiviert werden. Dies muss sowohl für die internen als auch die externen *Autodiscover* und *Webticket* Webseiten vorgenommen werden.



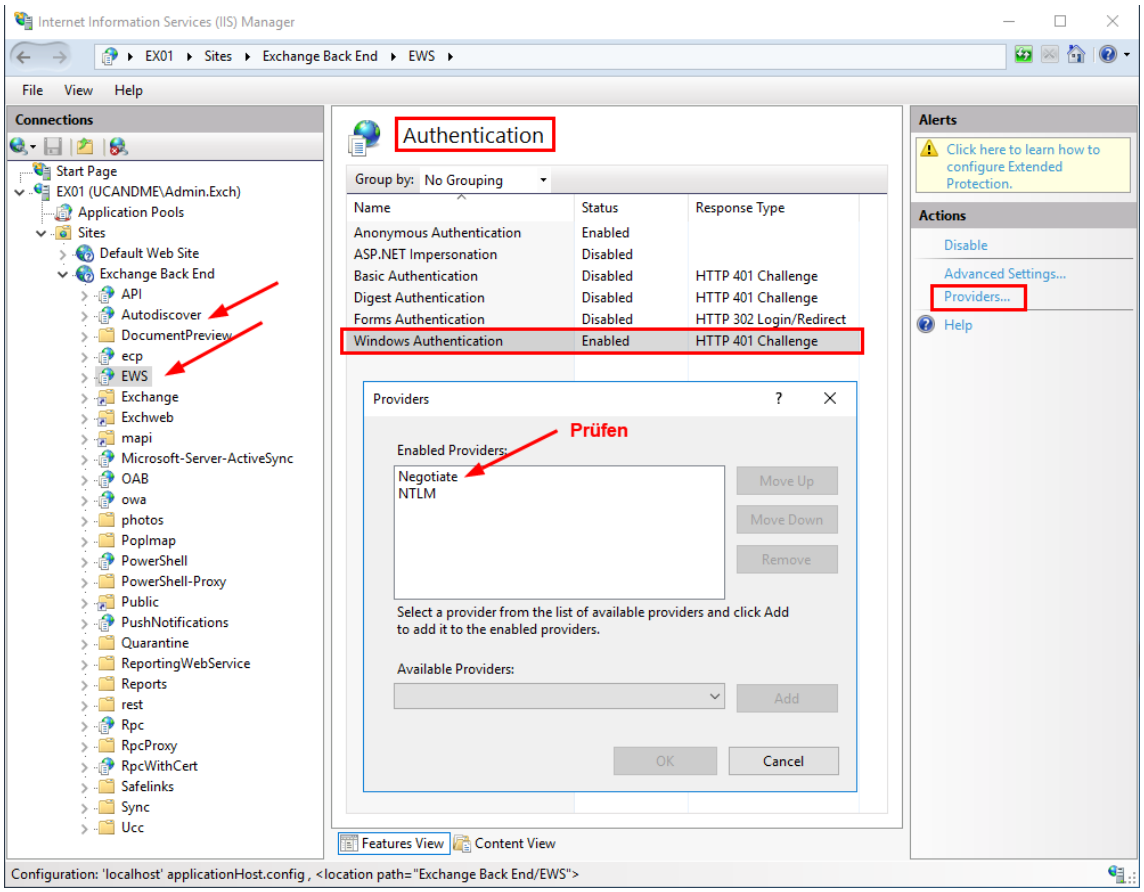
4.2. KCD für Exchange Server

Die Einrichtung con KCD am vorhandenen Exchange ASA Computerkonto verläuft analog zu Skype for Business Server.

Rufen sie die Eigenschaften des Exchange ASA Computerkontos von Exchange Server auf und wechseln auf den Reiter *Delegation*. Aktivieren sie hier *Trust this Computer for delegation to specified services only* sowie *Use any authentication protocol* und fügen dann ihren Exchange Namensraum mit dem Service Typ „http“ hinzu.



Analog zu den Skype for Business Servern müssen auch zwei Exchange Server Webseiten für Kerberos Authentifizierung aktiviert werden. Die Konfiguration wird für die *Autodiscover* und *EWS* Webseiten vorgenommen.


Internet Information Services (IIS) Manager
EX01 ▸ Sites ▸ Exchange Back End ▸ EWS ▸
File View Help
Connections
Start Page
EX01 (UCANDME\Admin.Exch)
Application Pools
Sites
Default Web Site
Exchange Back End
API
Autodiscover
DocumentPreview
ecp
EWS
Exchange
Exchweb
mapi
Microsoft-Server-ActiveSync
OAB
owa
photos
Poplmap
PowerShell
PowerShell-Proxy
Public
PushNotifications
Quarantine
ReportingWebService
Reports
rest
Rpc
RpcProxy
RpcWithCert
Safelinks
Sync
Ucc
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication
Enabled
ASP.NET Impersonation
Disabled
Basic Authentication
Disabled
HTTP 401 Challenge
Digest Authentication
Disabled
HTTP 401 Challenge
Forms Authentication
Disabled
HTTP 302 Login/Redirect
Windows Authentication
Enabled
HTTP 401 Challenge
Providers
Prüfen
Enabled Providers:
Negotiate
NTLM
Move Up
Move Down
Remove
Select a provider from the list of available providers and click Add to add it to the enabled providers.
Available Providers:
Add
OK
Cancel
Features View
Content View
Alerts
Click here to learn how to configure Extended Protection.
Actions
Disable
Advanced Settings...
Providers...
Help
Configuration: 'localhost' applicationHost.config , <location path="Exchange Back End/EWS">
IN2SUCCESS

5. Allgemeine Fehlerbehebung

Bevor Sie sich nun in die Tiefen der Analyse des Kerberos Protokolls begeben um evtl. auftretende Probleme bei der Kerberos Authentifizierung zu lösen, sollten Sie prüfen ob die grundsätzlichen Voraussetzungen zur Funktion von Kerberos überhaupt gegeben sind. Nachfolgend aufgeführte Punkte sind in der Praxis häufig anzutreffen:

- Wurde(n) die/der richtige(n) Service Prinzipal Name(n) registriert und ggf. in einer Applikation, die Kerberos Delegation benötigt, auch richtig konfiguriert?

- Stimmt die Uhrzeit auf allen Rechnern in der Domäne und eventuell in anderen Domänen, die über Vertrauensstellungen angebunden sind?

  Denken Sie daran, dass die gemeinsame Basis die Uhrzeit in UTC ist. Achten sie weiterhin darauf, das ein Zeitserver auf Computern konfiguriert wurde, die kein Domänenmitglied sind, also typischerweise im *Perimeter Netzwerk* stehen.

- Funktioniert die Namensauflösung in ihrer und eventuell weiterer angebundenen Domänen richtig?

  Hier nochmal die wichtigsten DNS Einträge:

```
nslookup -querytype=SRV _kerberos._tcp.contoso.com
nslookup -querytype=SRV _kerberos._udp.contoso.com
```

- Ist der Realm korrekt in Grossbuchtaben konfiguriert?

  Geben Sie hierzu den Befehl `klist.exe` ein und prüfen Sie, ob im Ticket *#0>* der Parameter *`Server:`* wie folgt aussieht:

```
krbtgt/CONTOSO.COM @ CONTOSO.COM
```

- Prüfen Sie mit Wireshark ob Kerberos Pakete, die über UDP transportiert wurden, fragmentiert sind.

  Aufgrund der fehlenden Absicherung von UDP gegen verlorene Pakete, werden fragmentierte UDP Pakete im Kerberos Protokoll nicht unterstützt.

- Gibt es eventuell doppelt registrierte Service Prinzipal Namen innerhalb einer Domäne?

  Prüfen Sie dies mit `setspn.exe -X`.

  Wenn sie doppelt registrierte Service Prinzipal Namen über alle Domänen hinweg suchen möchten, verwenden sie den nachfolgenden Befehl. Beachten sie hierbei bitte das der Befehl u.U. sehr zeit- und ressourcenintensiv ist: `setspn -X -F`.

  Dopelte Service Prinzipal Namen in verschiedenen Domänen sind zulässig. Weiterführende Tipps hierzu finden Sie in diesem Artikel[7].

[7] https://blogs.technet.microsoft.com/389thoughts/2017/02/08/why-you-can-still-have-duplicate-spns-in-ad-2012-r2-and-ad-2016/

5.1. Windows Bordmittel

Mit den Windows Bordmitteln kann man die erhaltenen Kerberos-Tickets und deren Quelle wunderbar inspizieren oder löschen. Das dafür notwendige Kommandozeilenprogramm `klist.exe` befindet sich im Ordner `C:\Windows\System32\` und sollte immer mit dem kompletten Pfad gestartet werden um eventuelle Probleme mit dem gleichnamigen Java[8] Programm auszuschließen.

Mit dem Aufruf von `C:\Windows\System32\klist.exe` werden alle im Cache vorhandenen Kerberos-Tickets angezeigt. Das Kommando kann von jedem Windows-Client oder -Server aus aufgerufen werden und liefert eine vergleichbare Ausgabe zu nachfolgendem Listing. Diese stammt von einem Skype for Business Frontend Server:

```
PS C:\Users\Admin.SfB> klist

Current LogonId is 0:0xbb0f09

Cached Tickets: (6)

#0>     Client: admin.sfb @ CONTOSO.COM
        Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent
 name_canonicalize
        Start Time: 8/7/2018 14:57:24 (local)
        End Time:   8/8/2018 0:33:08 (local)
        Renew Time: 8/14/2018 14:33:08 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: dc01.contoso.com

#1>     Client: admin.sfb @ CONTOSO.COM
        Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent
 name_canonicalize
        Start Time: 8/7/2018 14:33:08 (local)
        End Time:   8/8/2018 0:33:08 (local)
        Renew Time: 8/14/2018 14:33:08 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: dc01.contoso.com
```

5.2. Paketanalyse

Neben dem altbekannten Netzwerksniffer Wireshark[9], der sich hervorragend für eine Ablaufprotokollierung eignet, gibt es z.B. auch das Programm Fiddler[10], welches einen Proxy für Webanfragen darstellt und auch in verschlüsselten Datenverkehr Einblick hat um Authentifizierungsprobleme zu lösen.

[8] https://docs.oracle.com/javase/8/docs/technotes/tools/windows/klist.html
[9] https://www.wireshark.org/#download
[10] https://www.telerik.com/fiddler

Wichtig

*Wenn Sie die Datenpakete mit Wireshark auswerten, beachten sie bitte, das das erste krb_as_req Paket an den AS eine Fehlermeldung[11] mit der Bezeichnung **KDC_ERR_PREAUTH_REQUIRED** enthält.*

Dies ist korrekt, da der Windows Client noch nicht die Verschlüsselungsalgorithmen des AS kennt. Der AS sendet die unterstützten Verschlüsselungsalgorithmen des KDC mit dem Antwort Paket krb_as_rep.

Der im vorangegangenen Absatz enthaltene Link liefert noch zusätzliche Informationen für das Troubleshooting. Daher wird dessen Studium unbedingt empfohlen um falsche von richtigen Meldungen unterscheiden zu können.

5.3. Kerberos Logging

Unter Windows besteht die Möglichkeit das Logging für das Kerberos Protokoll in der Registry zu aktivieren.

Wichtig

Microsoft rät dringend davon ab, die Registry Einstellung vorzunehmen wenn „Last“ auf ihren Domänencontrollern herrscht, da diese durch das aktivierte Logging zusätzlich unter Last geraten und die Performance absinken wird.

Bitte löschen Sie den Registry Eintrag daher unbedingt nach dem Troubleshooting aus der Registry.

Legen Sie zur Aktivierung des Kerberos Protokoll Logging folgenden Registry Schlüssel an:

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

Registry Value: LogLevel
Value Type: REG_DWORD
Value Data: 0x1
```

Obwohl der Registry Eintrag im HKLM Zweig der Registry vorgenommen wird, braucht der Domänencontroller nicht neu gestartet zu werden. Das Logging ist sofort aktiv.

5.4. Kerberos Fehlermeldungen

Tabelle 1. Kerberos Fehlermeldungen[12]

Error	Error Name	Description
0x0	KDC_ERR_NONE	No error
0x1	KDC_ERR_NAME_EXP	Client's entry in KDC database has expired
0x2	KDC_ERR_SERVICE_EXP	Server's entry in KDC database has expired
0x3	KDC_ERR_BAD_PVNO	Requested Kerberos version number not supported
0x4	KDC_ERR_C_OLD_MAST_KVNO	Client's key encrypted in old master key

[11] https://support.microsoft.com/en-ca/help/262177/how-to-enable-kerberos-event-logging
[12] https://technet.microsoft.com/en-us/library/bb463166.aspx

Error	Error Name	Description
0x5	KDC_ERR_S_OLD_MAST_KVNO	Server's key encrypted in old master key
0x6	KDC_ERR_C_PRINCIPAL_UNKNOWN	Client not found in Kerberos database
0x7	KDC_ERR_S_PRINCIPAL_UNKNOWN	Server not found in Kerberos database
0x8	KDC_ERR_PRINCIPAL_NOT_UNIQUE	Multiple principal entries in KDC database
0x9	KDC_ERR_NULL_KEY	The client or server has a null key (master key)
0xA	KDC_ERR_CANNOT_POSTDATE	Ticket (TGT) not eligible for postdating
0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time
0xC	KDC_ERR_POLICY	Requested start time is later than end time
0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested option
0xE	KDC_ERR_ETYPE_NOTSUPP	KDC has no support for encryption type
0xF	KDC_ERR_SUMTYPE_NOSUPP	KDC has no support for checksum type
0x10	KDC_ERR_PADATA_TYPE_NOSUPP	KDC has no support for PADATA type (pre-authentication data)
0x11	KDC_ERR_TRTYPE_NO_SUPP	KDC has no support for transited type
0x12	KDC_ERR_CLIENT_REVOKED	Client’s credentials have been revoked
0x13	KDC_ERR_SERVICE_REVOKED	Credentials for server have been revoked
0x14	KDC_ERR_TGT_REVOKED	TGT has been revoked
0x15	KDC_ERR_CLIENT_NOTYET	Client not yet valid—try again later
0x16	KDC_ERR_SERVICE_NOTYET	Server not yet valid—try again later
0x17	KDC_ERR_KEY_EXPIRED	Password has expired—change password to reset
0x18	KDC_ERR_PREAUTH_FAILED	Pre-authentication information was invalid
0x19	KDC_ERR_PREAUTH_REQUIRED	Additional preauthentication required
0x1A	KDC_ERR_SERVER_NOMATCH	KDC does not know about the requested server
0x1B	KDC_ERR_SVC_UNAVAILABLE	KDC is unavailable
0x1F	KRB_AP_ERR_BAD_INTEGRITY	Integrity check on decrypted field failed
0x20	KRB_AP_ERR_TKT_EXPIRED	The ticket has expired
0x21	KRB_AP_ERR_TKT_NYV	The ticket is not yet valid
0x22	KRB_AP_ERR_REPEAT	The request is a replay
0x23	KRB_AP_ERR_NOT_US	The ticket is not for us
0x24	KRB_AP_ERR_BADMATCH	The ticket and authenticator do not match
0x25	KRB_AP_ERR_SKEW	The clock skew is too great
0x26	KRB_AP_ERR_BADADDR	Network address in network layer header doesn't match address inside ticket
0x27	KRB_AP_ERR_BADVERSION	Protocol version numbers don't match (PVNO)
0x28	KRB_AP_ERR_MSG_TYPE	Message type is unsupported
0x29	KRB_AP_ERR_MODIFIED	Message stream modified and checksum didn't match
0x2A	KRB_AP_ERR_BADORDER	Message out of order (possible tampering)
0x2C	KRB_AP_ERR_BADKEYVER	Specified version of key is not available
0x2D	KRB_AP_ERR_NOKEY	Service key not available
0x2E	KRB_AP_ERR_MUT_FAIL	Mutual authentication failed
0x2F	KRB_AP_ERR_BADDIRECTION	Incorrect message direction
0x30	KRB_AP_ERR_METHOD	Alternative authentication method required
0x31	KRB_AP_ERR_BADSEQ	Incorrect sequence number in message
0x32	KRB_AP_ERR_INAPP_CKSUM	Inappropriate type of checksum in message (checksum may be unsupported)
0x33	KRB_AP_PATH_NOT_ACCEPTED	Desired path is unreachable

Error	Error Name	Description
0x34	KRB_ERR_RESPONSE_TOO_BIG	Too much data
0x3C	KRB_ERR_GENERIC	Generic error; the description is in the e-data field
0x3D	KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation
0x3E	KDC_ERR_CLIENT_NOT_TRUSTED	The client trust failed or is not implemented
0x3F	KDC_ERR_KDC_NOT_TRUSTED	The KDC server trust failed or could not be verified
0x40	KDC_ERR_INVALID_SIG	The signature is invalid
0x41	KDC_ERR_KEY_TOO_WEAK	A higher encryption level is needed
0x42	KRB_AP_ERR_USER_TO_USER_REQUIRED	User-to-user authorization is required
0x43	KRB_AP_ERR_NO_TGT	No TGT was presented or available
0x44	KDC_ERR_WRONG_REALM	Incorrect domain or principal
0x80000001	KDC_ERR_MORE_DATA	More data is available
0x80000002	KDC_ERR_NOT_RUNNING	The Kerberos service is not running

GLOSSAR

A

Active Directory (AD)

Auszug aus Wikipedia zum Active Directory[13].

Active Directory heißt der Verzeichnisdienst von Microsoft Windows Server.

Bei einem solchen Verzeichnis (englisch *directory*) handelt es sich um eine Zuordnungsliste wie zum Beispiel bei einem Telefonbuch, das Telefonnummern den jeweiligen Anschlüssen (Besitzern) zuordnet.

Active Directory ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern. Dazu verwaltet es verschiedene Objekte in einem Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Mit Hilfe von Active Directory kann ein Administrator die Informationen der Objekte organisieren, bereitstellen und überwachen.

Den Benutzern des Netzwerkes können Zugriffsbeschränkungen erteilt werden. So darf zum Beispiel nicht jeder Benutzer jede Datei ansehen oder jeden Drucker verwenden. Die vier Hauptkomponenten des Active Directory sind

- Lightweight Directory Access Protocol (LDAP)
- Kerberos
- Common Internet File System (CIFS)
- Domain Name System (DNS)

Authentication Service (AS)

Der Authentifizierungsdienst stellt sicher, das das eingegebene Kennwort mit dem gespeicherten Kennwort im KDC übereinstimmt. Hierzu hat der AS Zugriff auf die mit einem Master Key verschlüsselten Konto Informationen

Authenticator

In Kombination mit dem Kerberos-Ticket wird ein Authentifikator, im engl. *Authenticator* genannt, verwendet um zu beweisen das derjenige, der ein Ticket vorlegt, wirklich derjenige ist, für den er sich ausgibt. Ein Authentifikator wird unter Verwendung des Sitzungsschlüssels verschlüsselt, der nur dem Client und dem jeweiligen Server bekannt ist.

Ein Authenticator kann nur einmal verwendet werden, im Gegensatz zu einem Ticket. Ein Client kann selbst einen Authentifikator erstellen und enthält folgende Elemente:

[13] https://de.wikipedia.org/wiki/Active_Directory

- Die zuvor erhaltene Zufallszahl (zum Schutz vor Replay Angriffen)
- Den Namen des KDC, in diesem Fall der Name des Domänencontrollers.
- Einen Zeitstempel

C

Common Internet File System (CIFS)

Auszug aus Wikipedia zum Active Directory[14].

Das CIFS-Protokoll ist für die Ablage von Dateien im Netzwerk vorgesehen. Dabei wird DNS zum Auffinden der einzelnen Computersysteme und Dienstinformationen (SRV Resource Record) genutzt. Es stellt außerdem aufgrund des standardisierten Protokolls eine Möglichkeit zur Anbindung an das Internet dar.
Siehe auch Active Directory.

CNAME Resource Record

Auszug aus Wikipedia zum CNAME Resource Record[15].

Ein CNAME Resource Record (CNAME RR) ist im Domain Name System (DNS) dazu vorgesehen, einer Domäne einen weiteren Namen zuzuordnen. Die Abkürzung "CNAME" steht für *canonical name* (canonical = anerkannt, bezeichnet also den primären, quasi echten Namen).
Siehe auch Domain Name System.

D

Domain Name System (DNS)

Auszug aus Wikipedia zum Active Directory[16].

Anders als frühere Windows-Versionen, wie zum Beispiel Windows NT 4.0, welche für die Namensauflösung NetBIOS verwendeten, ist für Active Directory ein eigenes DNS erforderlich. Um voll funktionsfähig zu sein, muss der DNS-Server SRV-Ressourceneinträge unterstützen.

K

Key Distribution Center (KDC)

Ein Key Distribution Center, frei übersetzt mit Schlüssel-Verwaltungs-Zentrale, gibt in einem Netzwerk auf Anforderung einen Schlüssel mit zeitlich begrenzter Gültigkeit aus, welchen der Benutzer/Computer zur Validierung seiner Datenpakete zwecks Authentifizierungs verwendet.

[14] https://de.wikipedia.org/wiki/Active_Directory
[15] https://de.wikipedia.org/wiki/CNAME_Resource_Record
[16] https://de.wikipedia.org/wiki/Active_Directory

L

Lightweight Directory Access Protocol (LDAP)	Auszug aus Wikipedia zum Active Directory[17]. Das LDAP-Verzeichnis stellt beispielsweise Informationen über Benutzer und deren Gruppenzugehörigkeit bereit. Aber auch andere Objekte, wie zum Beispiel die Zertifikate eines Computers, werden in dem Verzeichnis gespeichert. LDAP selbst ist kein Verzeichnis, sondern ein Protokoll, mittels dessen es über eine bestimmte Syntax möglich ist, Informationen eines LDAP-Verzeichnisses abzufragen. Siehe auch Active Directory.

N

NetBIOS	NetBIOS ist eine Programmierschnittstelle zur Kommunikation zwischen zwei Programmen über ein lokales Netzwerk. NetBIOS erlaubt einer Applikation, einen 16 Zeichen langen Namen netzwerkweit zu registrieren. Ursprünglich wurden die Zuordnungen von Namen zu Netzwerkadressen per Broadcast an alle Teilnehmer bekanntgegeben. Jeder NetBIOS-Name ist entweder als eindeutiger Name (exklusiv) oder als Gruppenname (nicht exklusiv) konfiguriert. In Microsoft Netzen werden von den 16 möglichen Zeichen 15 für Namen verwendet. Das 16. Zeichen wird als Suffix benutzt.
NT Lan Manager (NTLM)	NTLM ist ein Authentifizierungsverfahren. Es verwendet die sogenannte Challenge-Response-Authentifizierung. Das Challenge-Response-Verfahren, frei übersetzt etwa Aufforderung-Antwort-Verfahren, ist ein Authentifizierungsverfahren eines Teilnehmers auf Basis von „Wissen“. Hierbei stellt ein Teilnehmer eine Aufgabe (engl. *challenge*), die der andere lösen muss (engl. response), um zu beweisen, dass er eine bestimmte Information (*Shared Secret*) kennt ohne diese über das Netzwerk übertragen zu müssen.
Network Time Protocol (NTP)	Das NTP-Protokoll stellt sicher, das alle Computer in einer Domäne über die gleiche Zeit verfügen. Ein NTP-Server wird benötigt um eine genaue Uhrzeit innerhalb des Netzwerkes bereitzustellen, da z.B. Zeitabweichungen von mehr als 5 Minuten dafür sorgen, das eine Authentifizierung fehlschlägt. Daher ist es wichtig, das sichergestellt ist, das alle Computer im Netzwerk über die gleiche Zeit verfügen. Im Kerberos-Protokoll wird die aktuelle Uhrzeit in UTC übermittelt.

[17] https://de.wikipedia.org/wiki/Active_Directory

	Ein Active Directory Domänen Controller stellt die Uhrzeit im Netzwerk zur Verfügung. Man kann jedoch ach einen anderen Zeit-Server bereitstellen, der dann jedoch allen Komponenten im Netzwerk bekannt gemacht werden muss.

O

Organisationseinheit (OU)	Eine Organisationseinheit (OU, im englischen *Organizational Unit*) genannt, ist ein Containerobjekt, das zum Gruppieren anderer Objekte im Active Directory dient. Eine OU kann neben Objekten auch andere OUs enthalten. Die frei definierbare Hierarchie der OUs vereinfacht die Administration, die Übersichtlichtkeit und die Zuweisung von Richtlinien im Active Directory. Organisationseinheiten sind die unterste Ebene des Active Directory. Siehe auch Active Directory.

P

Perimeter Netzwerk (DMZ)	Bei einem Perimeter Netzwerk, auch Demilitarisierte Zone oder Umkreisnetzwerk genannt, handelt es sich um ein durch Firewalls abgegrenzten Teil des Unternehmensnetzwerks. Typischerweise wird ein Perimeter Netzwerk verwendet, um kontrollierte Zugriffe auf z.B. Webserver zu ermöglichen. Die im Perimeter Netzwerk betrieben Server sind in der Regel kein Mitglied des internen Unternehmensnetzwerkes.

R

Realm	Ein Realm bezeichnet die Gesamtheit aller Einträge in einem Verzeichnis(dienst). Ein Active Directory Domänencontroller ist immer nur für einen Realm wie z.B. `CONTOSO.COM` zuständig. Ein Benutzer oder Computer kann immer nur zu einem Realm gehören. Benötigt ein Client oder Computer Zugriff auf einen anderen Realm, wie z.B. `SALES.CONTOSO.COM`, muss eine Vertrauensstellung zwischen den Active Directory Domänencontrollern bestehen. Ein Realm besteht immer nur aus Grossbuchstaben.

T

Ticket Granting Service (TGS)	Der Ticket Granting Service, frei übersetzt der Berechtigungsschein-gewährender-Dienst, stellt den für die weitere Kommunikation zwischen Client und Ressource benötigten Sitzungsschlüssel (Session Key) bereit, damit dieser sich gegenüber der benötigten Netzwerk Ressource authentifizieren kann.

Ticket Granting Ticket (TGT)	Das Ticket Granting Ticket, frei übersetzt Berechtigungsschein-gewährender Berechtigungsschein, ist ein Datenpaket, welches jemandem wie bei einem Passwort den Zugang zu einer Ressource gewährt.

U

Coordinated Universal Time (UTC)	Die koordinierte Weltzeit, kurz UTC genannt, ist die heute gültige Weltzeit. UTC wird überall dort für Zeitangaben benutzt, wo eine weltweit einheitliche Zeitskala benötigt wird. Das kann z.B. der Flugverkehr sein oder ein weltweit verteiltes Computersystem bei dem die Log-Dateien über eine einheitliche Zeitbasis verfügen müssen. Dies ist z.B. bei Skype for Business der Fall.