

# Sharepoint Server 2013 und Anspruchs-basierte Authentifizierung

Bei einem Kunden wurden Sharepoint Server 2013 implementiert und spezielle Applikationen eingerichtet, welche die anspruchs-basierte (Claims based Authentication) verwenden.

Die Administratoren haben festgestellt, dass man in der Sharepoint Applikation nur Benutzer, aber keine Benutzergruppen berechtigen kann. Wenn statt Benutzer eine Benutzergruppe verwendet wird, erscheint eine Fehlermeldung, dass die entsprechende Anwendung / Funktion nicht aufgerufen werden kann.

Der Sharepoint synchronisiert die Security Principals mit dem Active Directory.

## Synchronisierungsverbindung bearbeiten

Konfigurieren Sie auf dieser Seite eine Verbindung mit einem Verzeichnisdienstserver zum Synchronisieren von Benutzern.

\* Bezeichnet ein Pflichtfeld.

**Verbindungsname**

**Typ**

**Verbindungseinstellungen**

Geben Sie für den Active Directory-Verzeichnisdienstserver Werte für **Gesamtstrukturname** und **Domänencontrollername** ein.

Damit Active Directory-Verbindungen funktionieren, muss dieses Konto über Berechtigungen zum Synchronisieren von Verzeichnissen verfügen.

Active Directory

Gesamtstrukturname:

Domänencontroller automatisch ermitteln

Geben Sie einen Domänencontroller an:

Domänencontrollername:

Authentifizierungsanbietertyp:

Windows-Authentifizierung

Authentifizierungsanbieterinstanz:

Kontoname: \*

Beispiel: DOMÄNE\benutzername

Kennwort: \*

Kennwort bestätigen: \*

Anschluss:

SSL-gesicherte Verbindung verwenden

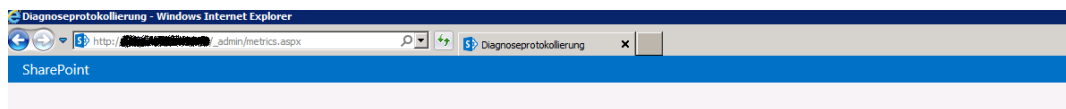
Container mit Daten auffüllen

**Container.**

Wählen Sie aus, welche Container synchronisiert werden sollen.

Geben Sie zum Anzeigen der ausgewählten Container das Kennwort ein, und klicken Sie auf die Schaltfläche "Container mit Daten auffüllen".

Nachdem wir auf Active Directory Seite alle Sync-Einstellungen / FIM-Sync geprüeft hatten und keinen Fehler feststellen konnten, aktivierten wir auf dem Sharepoint Server das Debug Logging.



## Diagnoseprotokollierung

Zentraladministration

Anwendungsverwaltung

Systemeinstellungen

Überwachung

Sichern und Wiederherstellen

Sicherheit

Upgrade und Migration

Allgemeine Anwendungseinstellungen

Apps

Halvotec Product Manager

Konfigurations-Assistenten

Ereignissteuerung

Mithilfe dieser Einstellungen können Sie den Schweregrad der Ereignisse steuern, die im Windows-Ereignisprotokoll und den Ablaufverfolgungsprotokollen aufgezeichnet werden. Je niedriger der Schweregrad, desto mehr Ereignisse werden aufgezeichnet.

Sie können die Einstellungen für einzelne Kategorien oder für alle Kategorien ändern. Wenn Sie alle Kategorien aktualisieren, gehen die Änderungen an einzelnen Kategorien verloren.

Kategorie auswählen

**Ablaufverfolgungsebene**

- Alle Kategorien
- Access Services
- Access Services 2010
- Business Connectivity Services
- Document Conversions
- Document Management Server
- eApproval
- Education
- Excel Services Application
- InfoPath Forms Services
- Office Automation Services
- Dienstinfrastruktur
- PerformancePoint Service
- Suche
- Secure Store Service
- Einmaliges Anmelden
- Infrastruktur
- SharePoint Express

**Ereignisebene**

Information Mittel

## Das entsprechende Log File verrät dann einiges mehr ....

### Ereignisprotokoll-Flutschutz

Wenn diese Einstellung aktiviert ist, werden sich wiederholende Ereignisse im Ereignisprotokoll von Windows erkannt. Wenn das gleiche Ereignis wiederholt protokolliert wird, werden die sich wiederholenden Ereignisse erkannt und unterdrückt, bis erneut normale Bedingungen vorliegen.

Ereignisprotokoll-Flutschutz aktivieren

### Ablaufverfolgungsprotokoll

Wenn die Ablaufverfolgung aktiviert ist, können Sie das Ablaufverfolgungsprotokoll ggf. an einem bestimmten Speicherort speichern. Hinweis: Der angegebene Speicherort muss auf allen Servern in der Farm vorhanden sein.

### Pfad

%CommonProgramFiles%\Microsoft Shared\Web Server Extensions\15\LOGS\

Beispiel: %Gemeinsame Dateien%\Microsoft Shared\Web Server Extensions\15\LOGS

Anzahl der Tage, die Protokolldateien gespeichert werden

14

Verwendung von Speicherplatz auf dem Datenträger durch das Ablaufverfolgungsprotokoll einschränken

Verwendung von Speicherplatz auf dem Datenträger durch das Ablaufverfolgungsprotokoll einschränken

Maximal zulässiger Speicherplatz für Ablaufverfolgungsprotokolle (GB)

1000

## Log File

```

/30/2014 16:33:41.32 w3wp.exe (0x2A10) 595F6F9C-2483-B062-F602-60642341B9E1 general High token not fresh for non-
Active action 595F6F9C-2483-B062-F602-60642341B9E1 0x2C0C SharePoint Foundation database ahjap High [Forced due to logging
/30/2014 16:33:41.43 w3wp.exe (0x2A10) 595F6F9C-2483-B062-F602-60642341B9E1 0x2C0C SharePoint Foundation Claims Authentication g7m8 Medium
ClaimsAuthProvider.GetRolesForUserBestEffort() failed to load groups for 'of w...'. The error message is: System.DirectoryServices.AccountManagement.PrincipalOperationException:
ler (1301) beim Auflisten der Gruppen. Die SID der Gruppe konnte nicht aufgelöst werden. bei System.DirectoryServices.AccountManagement.SidList.TranslateSids(String target, IntPtr[]
System.DirectoryServices.AccountManagement.ADStorExtX.GetGroupsMemberOfAZ(Principal p) bei System.Directory... 595F6F9C-2483-B062-F602-60642341B9E1
System.DirectoryServices.AccountManagement.UserPrincipal.GetAuthorizationGroupsHelper() bei System.DirectoryServices.AccountManagement.SidList.TranslateSids(String target, IntPtr[]
Services.AccountManagement.UserPrincipal.GetAuthorizationGroupsHelper() bei Microsoft.Sharepoint.Utilities.SecurityContext.RunAsProcess
crossf.Sharepoint.Administration.Claims.SPClaimsAuthProvider.<<C_DisplayClass4.<GetRolesForUserBestEffort>b__0() bei Microsoft.Sharepoint.Utilities.SecurityContext.RunAsProcess
/30/2014 16:33:41.44 w3wp.exe (0x2A10) 595F6F9C-2483-B062-F602-60642341B9E1 0x2C0C SharePoint Foundation Claims Authentication g7m8 Medium
currentService:IsUserValid: Checked user permissions for: i:0#.w\... False 595F6F9C-2483-B062-F602-60642341B9E1
/30/2014 16:33:41.44 w3wp.exe (0x2A10) 595F6F9C-2483-B062-F602-60642341B9E1 0x2C0C SharePoint Foundation Claims Authentication g7m8 Medium

```

Fehlermeldung: Die SID der Gruppe konnte nicht aufgelöst werden.

System.DirectoryServices.AccountManagement.SidList.TranslateSids(String target, IntPtr[]

Fehlermeldung: UserPrincipals.GetAuthorizationGroups An error (1301) occurred while enumerating the groups. The group's SID could not be resolved

### Ursache:

Die Domänencontroller des Kunden wurden vor geraumer Zeit auf Windows Server 2012 und letztes Jahr auf Windows Server 2012 R2 hochgestuft.

Mit Windows Server 2012 hat Microsoft zwei neue SID in die Anmeldetoken fuer die NTLM und Kerberos Authentifizierung gepackt, was bei manchen Applikationen Probleme bereiten kann (Quelle: <http://blogs.technet.com/b/deds/archive/2013/08/12/probleme-mit-dem-umwandeln-von-sids-in-namen.aspx>)

- 1-18-1 kommt ins Access Token, wenn die Anmeldung auf einer Prüfung von Credentials basiert, also zum Beispiel einem Kennwort, Zertifikat oder einer biometrischen Eigenschaft.
- S-1-18-2 packt der Domain Controller ins Token, wenn die Anmeldung auf einer Kerberos S4U Proxy Anfrage basiert, also zum Beispiel eine Protocol Transition durchgeführt wurde

Die Fehlermeldung welche erscheinen kann entspricht in etwa der Meldung im Sharepoint Debug Logging:

"An error (1301) occurred while enumerating the groups. The group's SID could not be resolved." when performing a UserPrincipal.GetAuthorizationGroups()

**Loesung:**

Microsoft stellt fuer betroffene Systeme einen Hotfix zur Verfuegung, welcher in diesem Fall auf den Sharepoint Servern eingespielt wurde:

<http://support.microsoft.com/kb/2830145>

Nach einem Reboot des Systems konnte die Sharepoint Applikation mit Benutzern, welche Mitglied in Benutzergruppen sind problemlos aufgerufen werden.