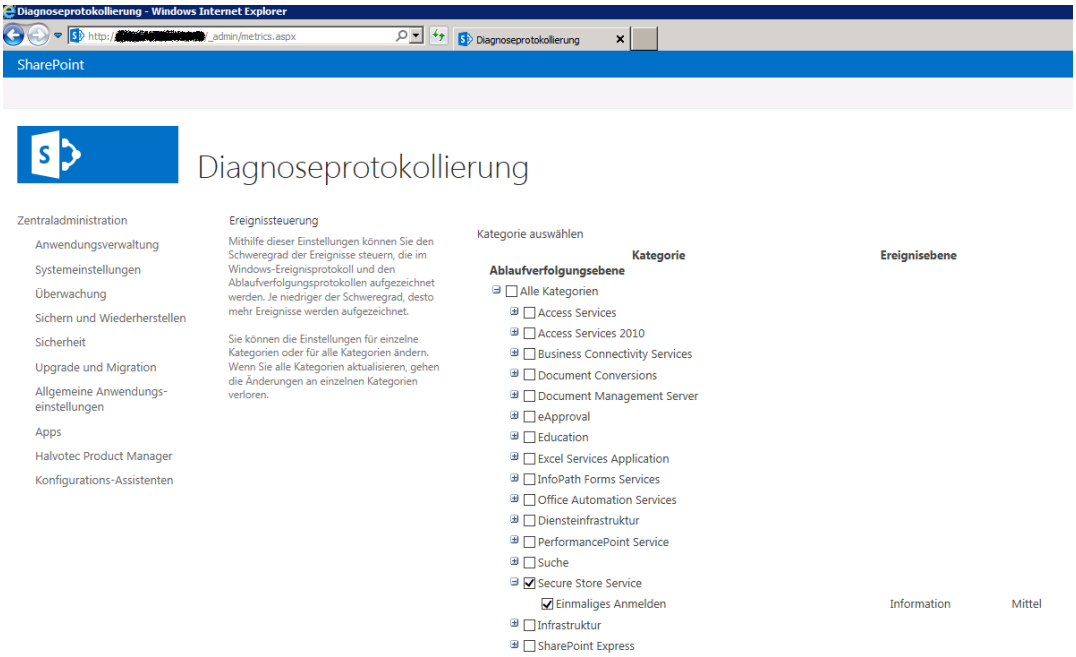
Sharepoint Server 2013 und Anspruchsbasierte Authentifizierung

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

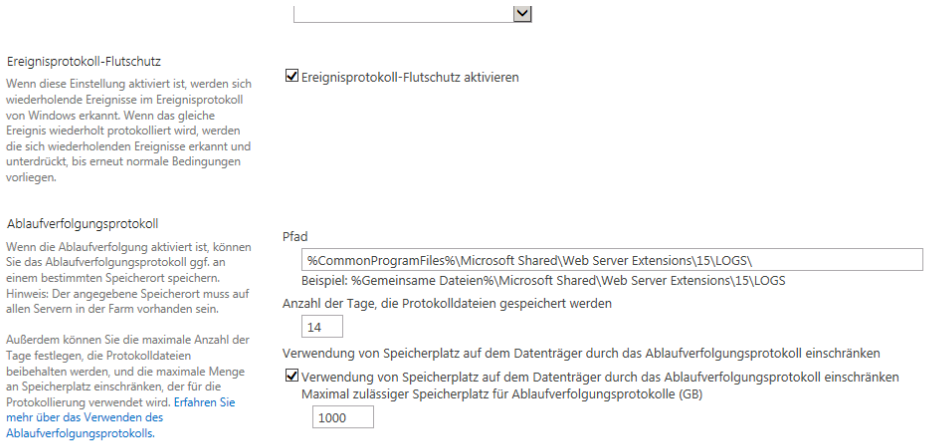
Die Administratoren haben festgestellt, dass man in der Sharepoint Applikation nur Benutzer, aber keine Benutzergruppen berechtigen kann. Wenn statt Benutzer eine Benutzergruppe verwendet wird, erscheint eine Fehlermeldung, dass die entsprechende Anwendung / Funktion nicht aufgerufen werden kann.

Der Sharepoint synchronisiert die Security Principals mit dem Active Directory.

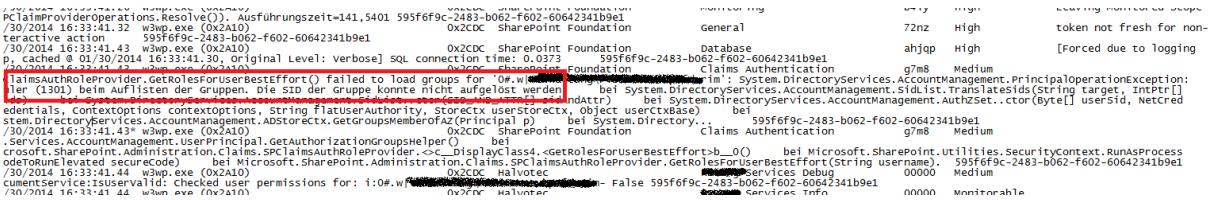
Nachdem wir auf Active Directory Seite alle Sync-Einstellungen / FIM-Sync geprueft hatten und keinen Fehler feststellen konnten, aktivierten wir auf dem Sharepoint Server das Debug Logging.



Das entsprechende Log File verraet dann einiges mehr ….



Log File



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 Domaenencontroller 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.