

Best Practice Berechtigungen



Inhalt: Vorschlag Berechtigungskonzept

Autor: Daniel Schnyder

Version Nr.: 02.02.01

Last Revision Date: 30.11.2011

Dokument Status: FINAL

Inhaltsverzeichnis

1.	Einleitung.....	3
2.	Ausgangslage	3
3.	Ziele.....	3
4.	Berechtigungen.....	4
4.1	Prinzip	4
4.2	Berechtigungsstufen	4
4.2.1	Vorgesehene Berechtigungsstufen	5
4.3	Websitesammlungsadministratoren	6
4.4	Administratoren	6
4.5	Namenskonvention.....	6
4.5.1	Beispiel.....	7
4.6	Ablage im Active Directory	8

1. Einleitung

Das folgende Dokument dient als Grundlage zur Implementierung von Berechtigungen in einer Windows SharePoint Services und Microsoft Office SharePoint Server 2007 Umgebung. Der Bereich Audience (Zielgruppen) wird nur vom Microsoft Office SharePoint Server (SHAREPOINT SERVER) unterstützt.

Im Konzept wird grundsätzlich davon ausgegangen, dass ein Active Directory (AD) vorhanden ist. Sollte dies nicht der Fall sein (Selfcreation Mode), kann das Konzept analog mit SharePoint-Gruppen aufgebaut werden.

2. Ausgangslage

In der Praxis zeigt es sich dass die von Microsoft vorgesehenen Konzepte zur Selbstverwaltung der Berechtigungen nur beschränkt durchführbar sind. Oft führt dies zu einem chaotischen Zustand bei den Berechtigungen. Innerhalb kurzer Zeit ist nicht mehr klar, wer auf welche Ressourcen Zugriff hat.

Ein weiteres Problem ist die Mischung von Active Directory Gruppen und SharePoint Gruppen zur Vergabe von Rechten, was zu einem noch undurchsichtigeren Gebilde führt.

Da in SharePoint nur ein sehr beschränktes Auswerten der Zugriffsrechte möglich ist, ist hier ein weiterer Schwachpunkt auszumachen. Dieser kann zwar durch den Einsatz von Dritttools behoben werden, was aber zu nicht unerheblichen Lizenzkosten führt.

3. Ziele

Mit der Einführung dieses Berechtigungskonzeptes werden die folgenden Ziele verfolgt:

- Klarheit bei der Vergabe von Rechten, so dass die Fehlerquote bei der Vergabe von Rechten gesenkt werden kann.
- Verringerung des administrativen Aufwandes
- Möglichkeit auszuwerten Wer auf welche Ressourcen Zugriff hat.
- Berechtigungen können an einem zentralen Ort administriert werden.
- Bei einem Neueintritt oder Abteilungswechsel sollen die Berechtigungen im AD vergeben werden können.

4. Berechtigungen

SharePoint ist unter anderem eine Kollaborations- bzw. Zusammenarbeitsplattform, daher sollen möglichst viele Informationen einem breiten Publikum zur Verfügung stehen. Die Berechtigungskonzepte der bestehenden Datenstruktur auf eine SharePoint Plattform zu portieren führt daher oft zu Problemen. Ein eigentlicher Paradigmenwechsel zu einer offenen Kommunikationskultur ist erforderlich. Die bestehenden Berechtigungskonzepte der Dateistruktur 1:1 in SharePoint abzubilden scheitern oft.

Das Berechtigungskonzept verfolgt daher die folgenden Grundsätze

- So offen wie möglich, so eingeschränkt wie nötig
- Wenn immer möglich sollen die Berechtigungen geerbt werden
- Berechtigungen für einzelne Personen sollen vermieden werden und wenn immer möglich über Gruppen abgebildet werden
- Berechtigungen auf einzelne Bibliotheken/Listen oder gar Elemente sollen vermieden werden. Auch hier werden neue Gruppen erstellt ->Es gilt stets Abzuwägen ob wirklich Berechtigungen auf einzelne Objekte notwendig sind.

4.1 Prinzip

Alle Berechtigungen werden via Active Directory Gruppen administriert. Dies bietet den Vorteil, dass die Vergabe der Rechte zentral durch die IT-Abteilung administriert werden kann. Insbesondere bei einem Neueintritt oder Abteilungswechsel können die Rechte an einem Punkt vergeben werden. Objekte die Berechtigungen erben, erhalten keine eigenen AD-Gruppen.

4.2 Berechtigungsstufen

SharePoint sieht vor, dass pro Objekt unterschiedliche Berechtigungsstufen vergeben werden können. Bei SHAREPOINT SERVER sehen diese Stufen wie folgt aus: (bei FOUNDATION sind weniger Stufen vorhanden)

Berechtigungen:

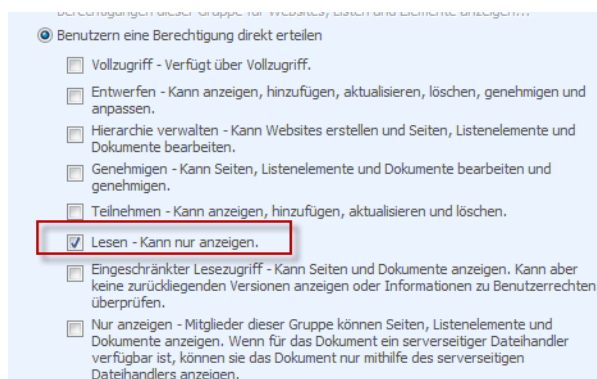
- Vollzugriff - Verfügt über Vollzugriff.
- Entwerfen - Kann anzeigen, hinzufügen, aktualisieren, löschen, genehmigen und anpassen.
- Hierarchie verwalten - Kann Websites erstellen und Seiten, Listenelemente und Dokumente bearbeiten.
- Genehmigen - Kann Seiten, Listenelemente und Dokumente bearbeiten und genehmigen.
- Teilnehmen - Kann anzeigen, hinzufügen, aktualisieren und löschen.
- Lesen - Kann nur anzeigen.
- Eingeschränkter Lesezugriff - Kann Seiten und Dokumente anzeigen. Kann aber keine zurückliegenden Versionen anzeigen oder Informationen zu Benutzerrechten überprüfen.
- Beschränkter Zugriff - Kann bestimmte Listen, Dokumentbibliotheken, Listenelemente, Ordner oder Dokumente anzeigen, wenn die Berechtigungen erteilt werden.
- Nur anzeigen - Mitglieder dieser Gruppe können Seiten, Listenelemente und Dokumente anzeigen. Wenn für das Dokument ein serverseitiger Dateihandler verfügbar ist, können sie das Dokument nur mithilfe des serverseitigen Dateihandlers anzeigen.

Diese können bei SHAREPOINT SERVER nach Bedarf ergänzt werden.

4.2.1 Vorgesehene Berechtigungsstufen

In der Praxis haben sich die folgenden Berechtigungsstufen als relevant herauskristallisiert. Diese werden daher auch im Konzept berücksichtigt:

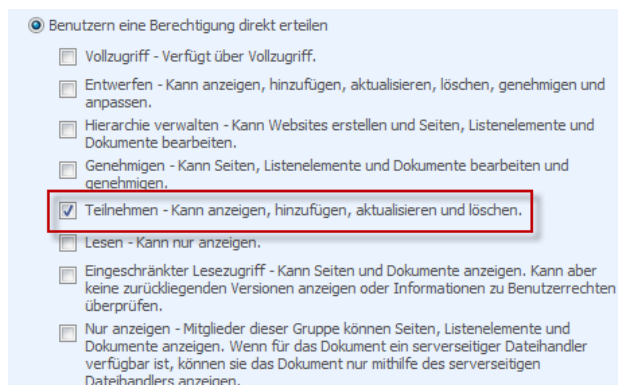
READ: Benutzer können Objekte nur lesen



Benutzern eine Berechtigung direkt erteilen

- Vollzugriff - Verfügt über Vollzugriff.
- Entwerfen - Kann anzeigen, hinzufügen, aktualisieren, löschen, genehmigen und anpassen.
- Hierarchie verwalten - Kann Websites erstellen und Seiten, Listenelemente und Dokumente bearbeiten.
- Genehmigen - Kann Seiten, Listenelemente und Dokumente bearbeiten und genehmigen.
- Teilnehmen - Kann anzeigen, hinzufügen, aktualisieren und löschen.
- Lesen - Kann nur anzeigen.
- Eingeschränkter Lesezugriff - Kann Seiten und Dokumente anzeigen. Kann aber keine zurückliegenden Versionen anzeigen oder Informationen zu Benutzerrechten überprüfen.
- Nur anzeigen - Mitglieder dieser Gruppe können Seiten, Listenelemente und Dokumente anzeigen. Wenn für das Dokument ein serverseitiger Dateihandler verfügbar ist, können sie das Dokument nur mithilfe des serverseitigen Dateihandlers anzeigen.

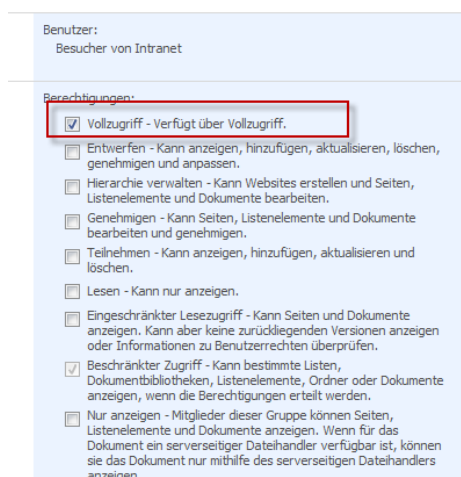
Write: Benutzer können Dokumente bearbeiten, Artikel verfassen, jedoch nichts am Design ändern und keine Bibliotheken erstellen.



Benutzern eine Berechtigung direkt erteilen

- Vollzugriff - Verfügt über Vollzugriff.
- Entwerfen - Kann anzeigen, hinzufügen, aktualisieren, löschen, genehmigen und anpassen.
- Hierarchie verwalten - Kann Websites erstellen und Seiten, Listenelemente und Dokumente bearbeiten.
- Genehmigen - Kann Seiten, Listenelemente und Dokumente bearbeiten und genehmigen.
- Teilnehmen - Kann anzeigen, hinzufügen, aktualisieren und löschen.
- Lesen - Kann nur anzeigen.
- Eingeschränkter Lesezugriff - Kann Seiten und Dokumente anzeigen. Kann aber keine zurückliegenden Versionen anzeigen oder Informationen zu Benutzerrechten überprüfen.
- Nur anzeigen - Mitglieder dieser Gruppe können Seiten, Listenelemente und Dokumente anzeigen. Wenn für das Dokument ein serverseitiger Dateihandler verfügbar ist, können sie das Dokument nur mithilfe des serverseitigen Dateihandlers anzeigen.

ADMIN: Vollzugriff



Benutzer:
Besucher von Intranet

Berechtigungen:

- Vollzugriff - Verfügt über Vollzugriff.
- Entwerfen - Kann anzeigen, hinzufügen, aktualisieren, löschen, genehmigen und anpassen.
- Hierarchie verwalten - Kann Websites erstellen und Seiten, Listenelemente und Dokumente bearbeiten.
- Genehmigen - Kann Seiten, Listenelemente und Dokumente bearbeiten und genehmigen.
- Teilnehmen - Kann anzeigen, hinzufügen, aktualisieren und löschen.
- Lesen - Kann nur anzeigen.
- Eingeschränkter Lesezugriff - Kann Seiten und Dokumente anzeigen. Kann aber keine zurückliegenden Versionen anzeigen oder Informationen zu Benutzerrechten überprüfen.
- Beschränkter Zugriff - Kann bestimmte Listen, Dokumentbibliotheken, Listenelemente, Ordner oder Dokumente anzeigen, wenn die Berechtigungen erteilt werden.
- Nur anzeigen - Mitglieder dieser Gruppe können Seiten, Listenelemente und Dokumente anzeigen. Wenn für das Dokument ein serverseitiger Dateihandler verfügbar ist, können sie das Dokument nur mithilfe des serverseitigen Dateihandlers anzeigen.

Sollten weitere Berechtigungsstufen erforderlich sein, können diese nach demselben Schema erstellt werden

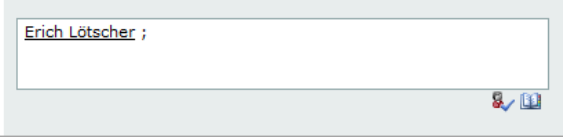
4.3 Websitesammlungsadministratoren

Websitesammlungsadministratoren haben vollen Zugriff auf sämtliche Einstellungen der Sitecollection. Diese Berechtigungen sind unabhängig von der Administratorengruppe SP_SiteAdmin.

Leider ist es nicht möglich die Websitesammlungsadministratoren via eine AD Gruppe zu vergeben. Daher ist es notwendig diese Rechte direkt zu vergeben.

Websitesammlungsadministratoren

Websitesammlungsadministratoren erhalten Vollzugriff auf alle Websites der Websitesammlung. Sie empfangen ggf. auch Bestätigungs-E-Mails über die Websiteverwendung. Geben Sie die Benutzer getrennt durch Semikolon ein.



4.4 Administratoren

Die AD Gruppe **SP_SiteAdmin** beinhaltet alle Benutzer welche Rechte zum Design und zur Vergabe von Rechten brauchen, jedoch nicht den vollen Funktionsumfang der Websitesammlungsadministratoren (z.B. Websitefeatures aktivieren) haben sollen. Entsprechen die Websitesammlungsadministratoren allen Benutzern die Admin-Rechte auf den Subwebs haben sollen, kann auf die Erstellung dieser Gruppe **verzichtet** werden

4.5 Namenskonvention

Für die Bezeichnung der AD Gruppen schlagen wir die folgende Namenskonvention vor.

SP__Path_Objektnamen_READ

SP: Signalisiert, dass es sich um eine Active-Directory Gruppe für Sharepoint handelt.

Path: Path zum Objekt, massgebend ist die Inhalts- und Strukturansicht von SharePoint (URL)

Objektnamen: Name des Subwebs oder der Liste

READ Berechtigungsstufe

Die Kursiv geschriebenen Teile entsprechen den Eigenschaften des betroffenen Objektes. Durch den Path ist die eindeutige Identifizierung des Objektes jederzeit möglich.

4.5.1 Beispiel

Am folgenden einfachen Beispiel soll die Anwendung verdeutlicht werden. Es sollen die Berechtigungen für die folgende Webseitenstruktur abgebildet werden.

Homepage

 Produktion

 Management

 Führung

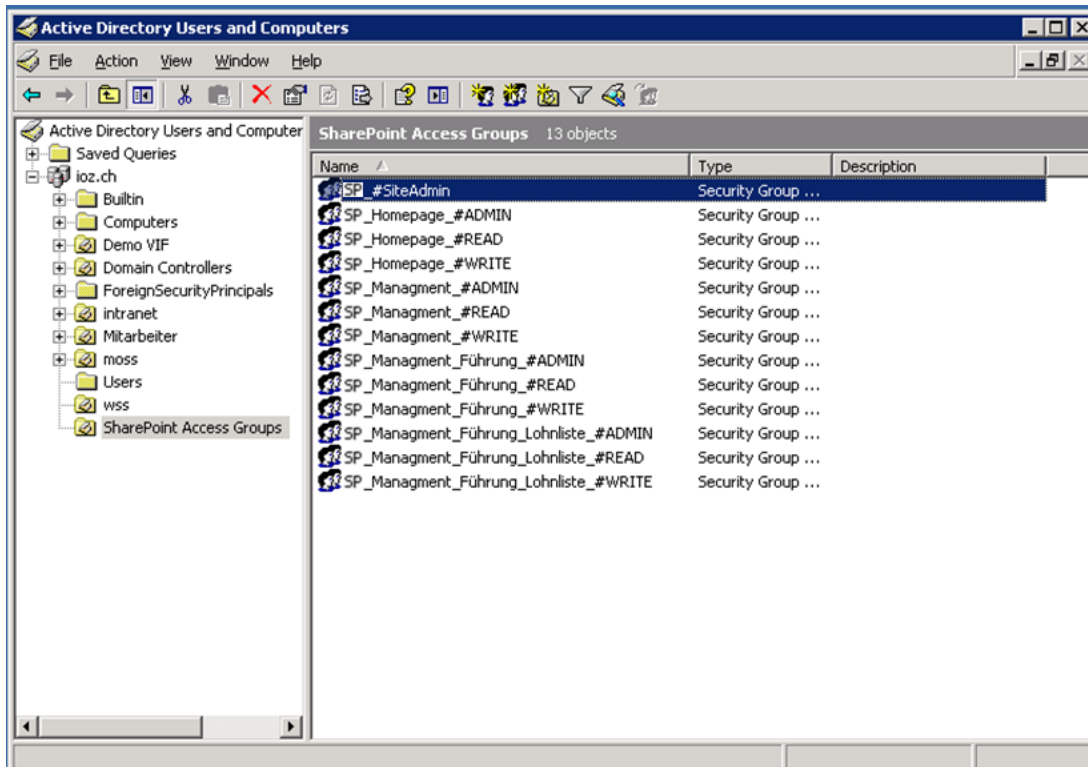
 Personal

 Lohnliste

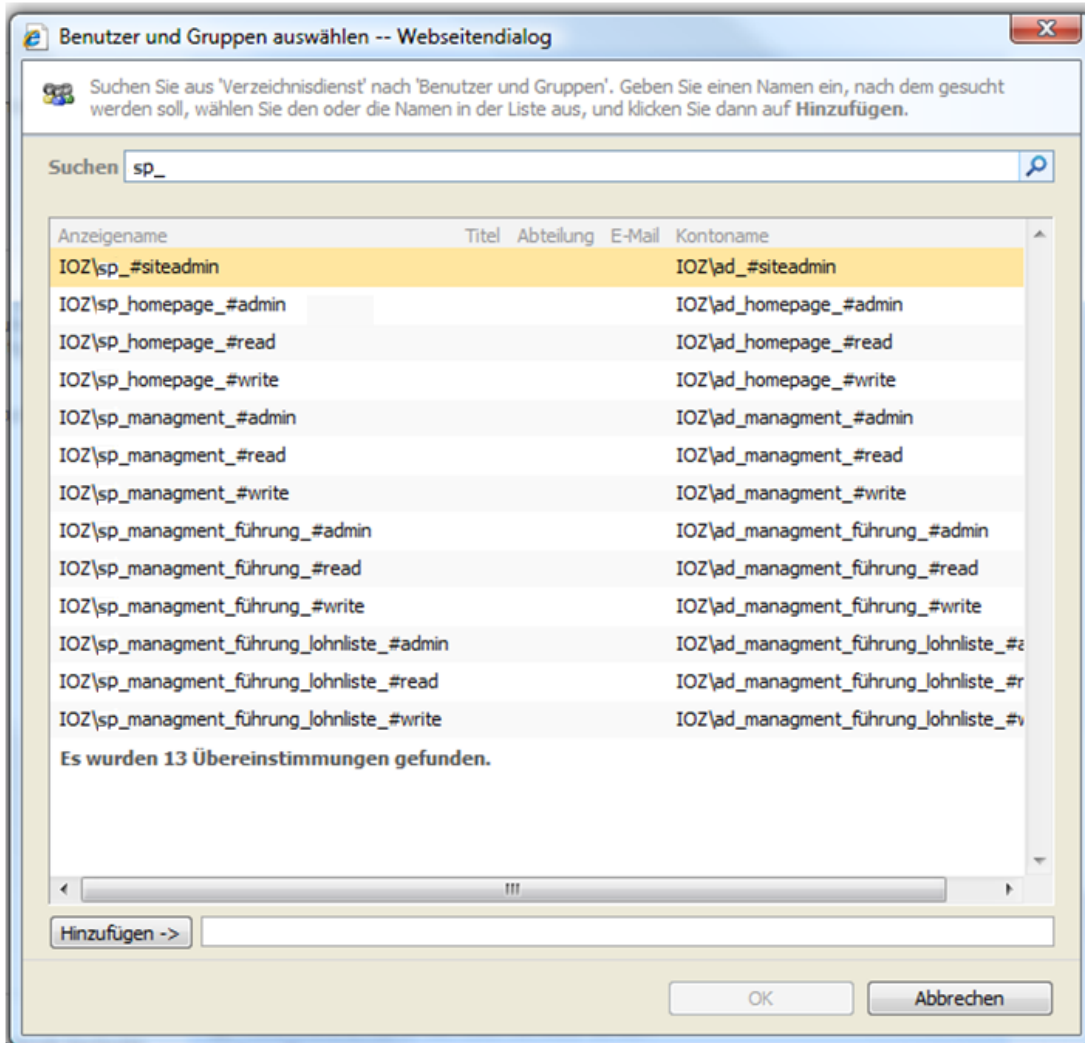
Path	Vererbt	Gruppen
Homepage	Nein	SP_SiteAdmin SP_Homepage_READ SP_Homepage_WRITE SP_Homepage_ADMIN
Produktion	Ja	Keine, da geerbt
Management	Nein	SP_SiteAdmin SP_Management_READ SP_Management_WRITE SP_Management_ADMIN
Führung	Nein	SP_SiteAdmin SP_Management_Führung_READ SP_Management_Führung_WRITE SP_Management_Führung_ADMIN
Personal	Ja	Keine, da geerbt
.....Lohnliste	Nein	SP_SiteAdmin SP_Management_Führung_Lohnliste_READ SP_Management_Führung_Lohnliste_WRITE SP_Management_Führung_Lohnliste_ADMIN

4.6 Ablage im Active Directory

Es wird empfohlen die AD-Gruppen zentral in einer OE „SharePoint Access Groups“ im AD abzulegen. So sind diese zentral auffindbar und administrierbar.



Entsprechende Ansicht in SharePoint:



5. Berechtigungen Stadt Sursee

5.1.1 Beispiel

Am folgenden einfachen Beispiel soll die Anwendung verdeutlicht werden. Es sollen die Berechtigungen für die folgende Webseitenstruktur abgebildet werden.

Homepage

Ressourcenplattform

Martigny-Platz

Viehmarktplatz / Zitrusplatz

Allmend / Trainingsplatz

Path	Vererbt	Gruppen
Homepage	Nein	Vorerst - Keine Berechtigung
Ressourcenplattform	Nein	rgH-sp-Ressourcenplattform-admin rgH-sp-Ressourcenplattform-write rgH-sp-Ressourcenplattform-read
.....Öffentlicher Grund	Nein	
.....Parkplätze	Nein	
....Sportplätze	Nein	
.....Martigny-Platz	Nein	rgH-sp-Ressourcenplattform-admin rgH-sp-Martigny-Platz-admin rgH-sp-Martigny-Platz-write rgH-sp-Martigny-Platz-read
.....Viehmarktplatz / Zir- kusplatz	Nein	rgH-sp-Ressourcenplattform-admin rgH-sp-Viehmarktplatz--Zirkusplatz-admin rgH-sp-Viehmarktplatz--Zirkusplatz-write rgH-sp-Viehmarktplatz--Zirkusplatz-read
.....Allmend / Trainingsplatz	Nein	rgH-sp-Ressourcenplattform-admin rgH-sp-Allmend--Trainingsplatz-write rgH-sp-Allmend--Trainingsplatz-admin rgH-sp-Allmend--Trainingsplatz-read