February 2007

Integration of Windows File Servers into the SAP KM platform using SSO and the WebDAV repository manager

Summary

Integrating external repositories into the SAP KM platform allows for a unified access to existing repositories in an enterprise. Integrating Windows File Servers can be done using the File system repository manager while Web Servers can be integrated using the Web repository manager or the WebDAV repository manager.

Integrating Documents from a Windows System into KM using the file system repository manager is not supported if the portal runs on UNIX and if the Active Directory runs in native mode. In such a case it is possible to use the following workaround:

IIS supports the publishing of Windows File Servers using WebDAV. As a result windows file systems that are published using IIS can be integrated into SAP KM using the Web DAV repository manager rather than the file system repository manager.

The limitations for this workaround are it does not support all features that are supported by the file system repository manager and that search performance might be limited under certain circumstances. However there is one advantage this workaround can make use of SSO based on SAP Logon Tickets thus eliminating the need of user mapping.

Applies to

- SAP NetWeaver Portal 6.0 SP9 or higher
- Microsoft Active Directory 2003 (forest functional level set to Windows Server 2003)
- IIS 6.0 and Windows Server 2003

Contact

For feedback or questions you can contact the Collaboration Technology Support Center via the .NET Technologies forum in the .NET interoperability area of SDN. Please check the .NET interoperability area in SDN for any updates or further information.

Author Bio

André Fischer works at **SAP AG** in the Strategic Alliance Microsoft Team. He is also a member of the Collaboration Technology Support Center – Microsoft (CTSC – MS) that addresses various kinds of interoperability topics regarding SAP and Microsoft solutions. Before joining SAP three years ago, André has lent his talents as an SAP technology consultant for more than eight years, and has gained significant experience in both the SAP and the Microsoft solution stack. In the last two years, André has also specialized in single sign-on, SAP active directory integration, SAP Exchange Infrastructure BizTalk integration and knowledge management Microsoft Windows integration.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Contents

Introduction

CM repository manager framework

In addition to the internal repositories, you can integrate external repositories into CM, like the following:

- Web Repository
- WebDAV Repository
- File System Repository

You can establish a connection to these repositories by configuring appropriate repository managers (also called connectors).

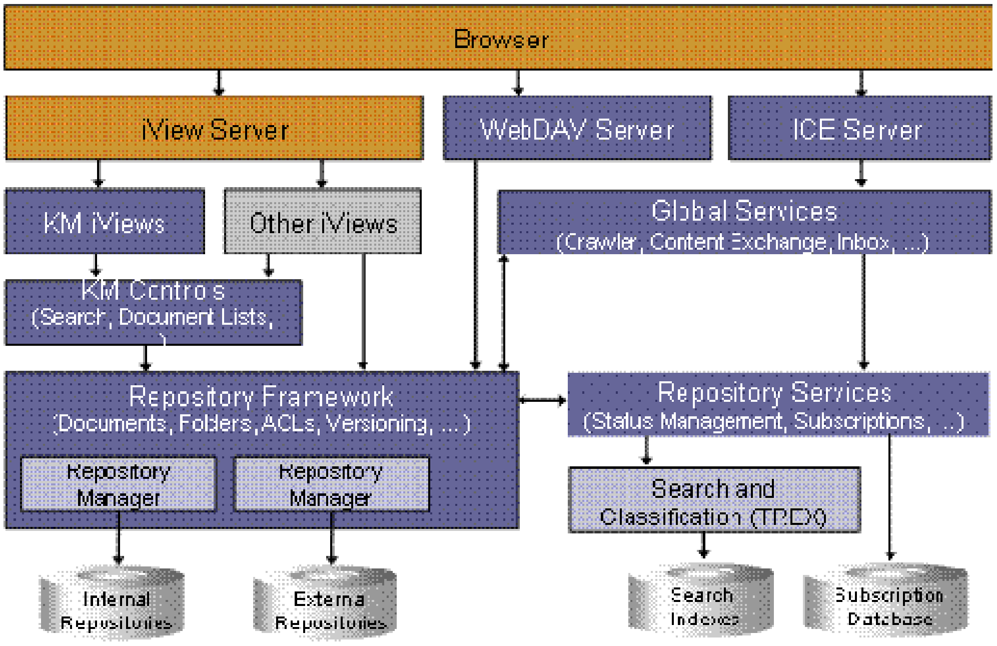


Figure 1 repository manager framework

The corresponding repository manager has to provide the credentials for logging on to the remote server for all users that access the remote repository. This information is read from the mapping data of the user who is trying to access the repository. These credentials have to be maintained for each user and each system. If Single Sign-on can be used to access external repositories by the SAP KM platform this reduces a large amount of user maintenance tasks.

A number of global services and repository services need to perform operations on resources in various repositories. For example, the index management service must read all resources it is meant to index. When an index is created, the service user *index_service* is used. Therefore, this user has to have at least read access to all repositories that are to be indexed. Other users that are used by the SAP KM platform are the service users *notificator_service* and *cmadmin_service*. When a search is taking place, it is the user that is currently logged on to the portal.

Problems when integrating Windows File Systems

Integrating Documents from a Windows System into KM using the file system repository manager is not supported if the portal runs on UNIX and if the Active Directory runs in native mode. This issue is described in the SAP Online Help in section Integrating Documents from a Windows System into KM. In such a case it is possible to use the workaround described in the following.

Using IIS as a workaround

IIS supports the publishing of Windows File Servers using WebDAV. As a result windows file systems that are published using IIS can be integrated into SAP KM using the Web DAV repository manager rather than the file system repository manager.

The limitations for this workaround are the following: The WebDAV implementation provided by the IIS does neither support all WebDAV methods nor does it support all features that are supported by the file system repository manager. It has also been observed that the search performance might be poor under certain circumstances as described in section *Possible Performance Problems*. Before using this scenario productively you should therefore analyze whether these issue does apply for you.

However there is one advantage when using this workaround since it can make use of SSO based on SAP Logon Tickets thus eliminating the need of user mapping if the Microsoft Active Directory is running in Windows Server 2003 native mode.

How is it possible to use Single Sign-on?

Single Sign-on in SAP environment is established using SAP Logon Tickets while in Microsoft environments Single Sign-on is achieved using Windows Integrated authentication that is based on the Kerberos protocol. A seamless integration between the two security environments can be established using a ticket bridging mechanism that has been developed by SAP. The SSO22KerbMap Module allows SAP Logon Tickets to be used for Windows Integrated authentication leveraging an enhancement of the Kerberos protocol provided by Microsoft with the Kerberos implementation in Windows Server 2003. The same mechanism can also be used for a seamless integration of any web based Microsoft application running on IIS that uses Windows Integrated authentication into SAP Enterprise Portal (e.g. Outlook WebAccess).

The HTTP system of a WebDAV repository manager can be configured in a way, that the SAP Logon Ticket of the user logged on to the SAP EP will be forwarded to the remote WebDAV server. This way a WebDAV repository that accepts SAP Logon Tickets for authentication can be accessed using SSO.

The IIS can be configured such that it can be used to publish Windows File Systems via WebDAV. When the IIS is configured to use Windows Integrated authentication the access to files and folders is regulated by Windows security.

The Ticket bridging mechanism can thus be leveraged for the integration of Windows based file systems using the WebDAV repository manager.

When a search is taking place, a security manager of a repository manager makes sure, that the user can see only documents in the result list, where he has read access.

However a security manager for the WebDAV repository manager is only available for SAP based WebDAV repositories.

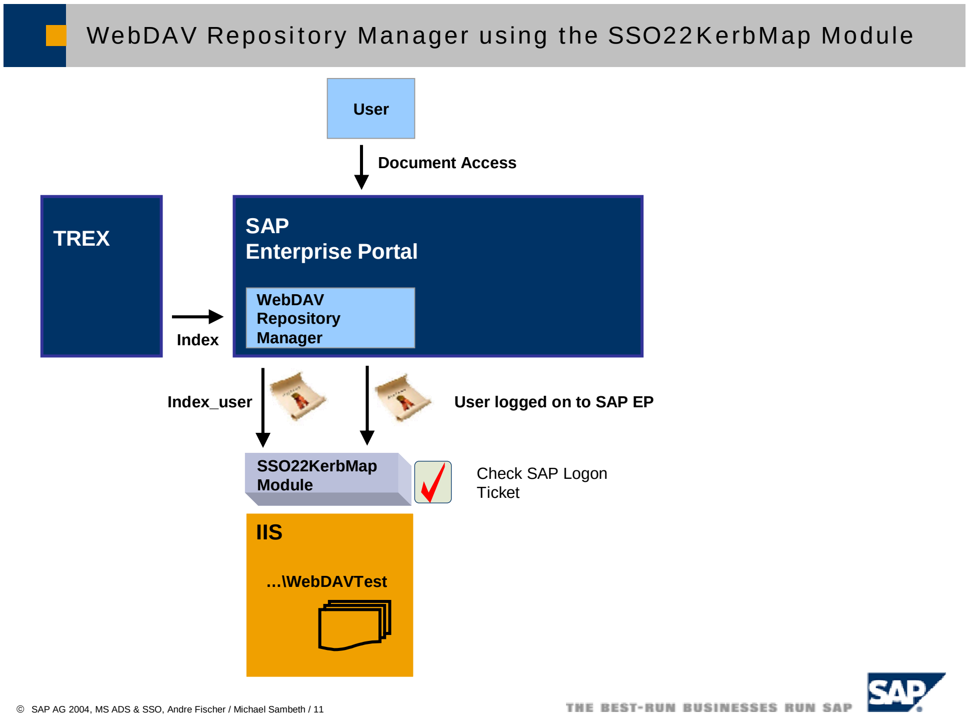
When using the SSO22KerbMap Module no security manager is necessary since the access to the WebDAV repository is performed using Windows Integrated authentication. The access to the folders that are published via WebDAV using IIS is controlled by the existing Windows access control lists.

The SSO22KerbMap Module

A detailed description of the SSO22KerbMap Module can be found in the collaboration brief *"Using SAP Logon Tickets for SSO to Microsoft-based Web Applications"*.

The ticket bridging mechanism leverages an enhancement of the implementation of the Kerberos protocol that has been introduced by Microsoft with Active Directory 2003.

Using *constrained delegation* a service may request a (constrained) Kerberos ticket on behalf of a user for specified services only. Using *protocol transition* it is possible that the client may be authenticated using other methods than Kerberos. Based on this technology SAP has developed an ISAPI Filter called *SSO22KerbMap Module*.



WebDAV Repository Manager using the SSO22KerbMap Module

© SAP AG 2004, MS ADS & SSO, Andre Fischer / Michael Sambeth / 11

Figure 2 WebDAV Repository Manager using the SSO22KerbMap Module

The SSO22KerbMap Module that allows for the authentication using SAP Logon Tickets (protocol transition) works as follows:

1. The ISAPI Filter checks the SAP Logon Ticket in the incoming http request.
2. If the ticket is valid the filter extracts the SAP username from the SAP Logon ticket.
3. After the SAP user name has been determined the filter performs a search in Active Directory for the corresponding Active Directory user. The user in Active Directory is

identified by the user attribute that contains the (unique) portal logon ID. If the Active Directory is used as the user persistence store it is the attribute that is used as the portal logon id (j_user).

4. Based on this authentication the filter can acquire a Kerberos Ticket on behalf of the user that is authenticated by the SAP Logon Ticket (constrained delegation).

The ISAPI Filter must be installed on the IIS that publishes the directories using WebDAV.

SSO for internal service users

Setting up Single Sign-On for the internal CM service users used by the SAP KM platform has to be outlined in more detail. The reason is that the internal users are only defined in the portal database. The process of impersonation will fail since no corresponding user is found in Active Directory.

Therefore user accounts have to be created in Active Directory for the CM service users. These users must fulfill the following requirement. The user attribute in Active Directory that is mapped to the portal user id (j_user) must be filled with the appropriate value, for example *index_service*.

However one has to make sure that the users that have been created in Active Directory for the internal services users are not taken into account by the User Management Engine (UME). This behavior can be established by specifying the *ume.ldap.negative_user_filter* property for the LDAP data sources in the data source configuration file. Using this property one can define that all users and accounts that match the defined conditions are filtered out by the UME API. A detailed documentation can be found in the SAP Online Help:

In the following example of a data source configuration file for Microsoft Active Directory Server the attribute *userPrincipalName* is used as Logon ID of a portal (j_user).

Here the user accounts that have one of the following Logon ID's (index_service, *notificator_service* and *cmadmin_service*) are filtered out.

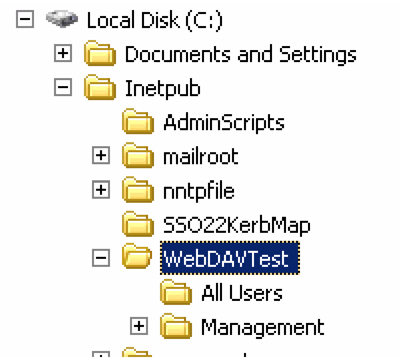
```
<dataSources>
    ...
    </dataSource>
    <dataSource id="CORP_LDAP">
        ...
        <privateSection>
            ...
            <ume.ldap.negative_user_filter>
 userPrincipalName=[index_service,notificator_service,cmadmin_service]
            </ume.ldap.negative_user_filter>
        </privateSection>
    </dataSource>
</dataSources>
```

Caution:

If no measures are taken into account like defining a negative filter this might cause confusion and malfunction when using UME. Internal and external users will be displayed in the user interface in UME with the same user name.

Integration scenario

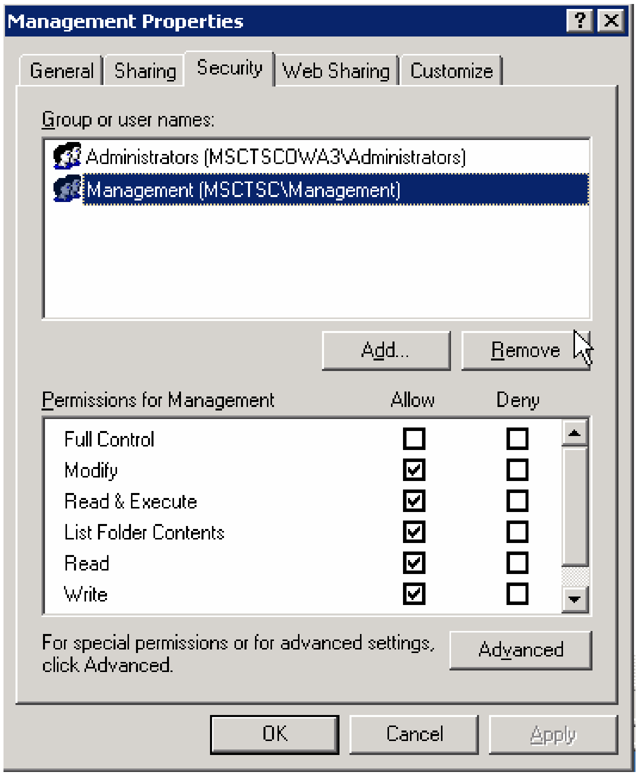
In the following an example scenario is described, where the access control lists on file system level are taken into account if the WebDAV repository manager together with the SSO22KerbMap Module is used.



```
⊟ Local Disk (C:)
    ⊞ Documents and Settings
    ⊟ Inetpub
        AdminScripts
        ⊞ mailroot
        ⊞ nntpfile
        SSO22KerbMap
        ⊟ WebDAVTest
            All Users
            ⊞ Management
```

Figure 3 Published Windows Filesystem

The physical directory *C:\inetpub\WebDAVTest* is published by the IIS using the virtual directory *WebDAVTest.* As a result it can be accessed using the URL: http://msctscowa3.msctsc.sap.corp/WebDAVTest



Management Properties

Group or user names:

Administrators (MSCTSCOWA3\Administrators)

Management (MSCTSC\Management)

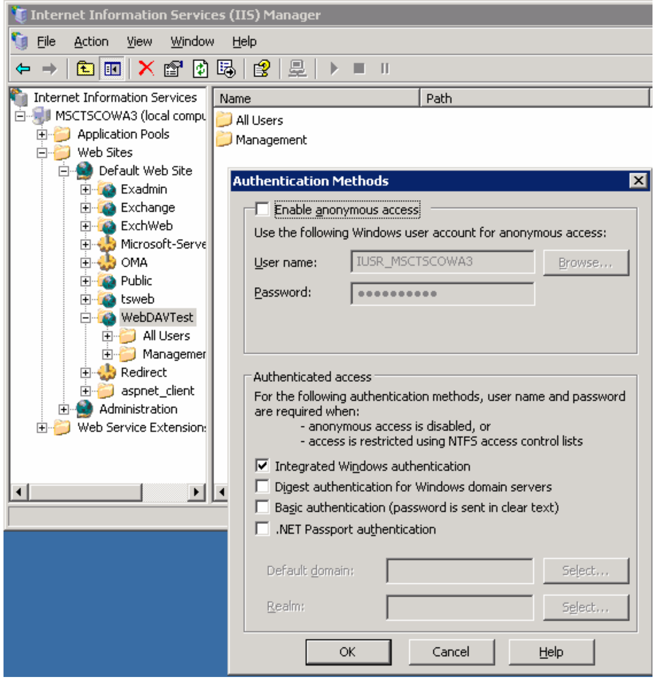
Permissions for Management	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

Figure 4 Security settings on the Windows file system

The directory *WevDAVTest* contains two subdirectories *All Users* and *Management*. The security settings are such that only members of the group Management have access to the folder Management while the folder All Users can be accessed by everyone.

Windows integrated authentication is configured for the virtual directory WebDAVTest http://msctscowa3.msctsc.sap.corp/WebDAVTest .



☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_MSCTSCOWA3

Password: ••••••••••

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

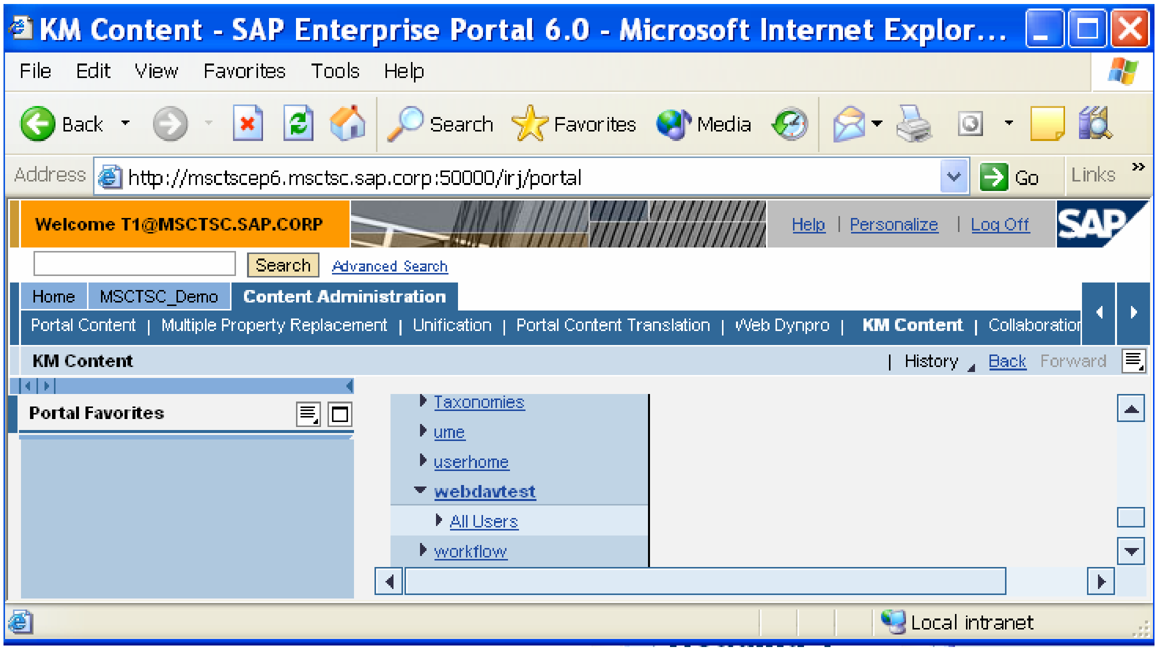
Default domain:

Realm:

Figure 5 IIS: Security settings of virtual server

As part of the setup two users have been created. User T1@CTSC.SAP.CORP is a normal domain user whereas user T2@MSCTSC.SAP.CORP is a member of the group *Management* and thus having access to folder Management.

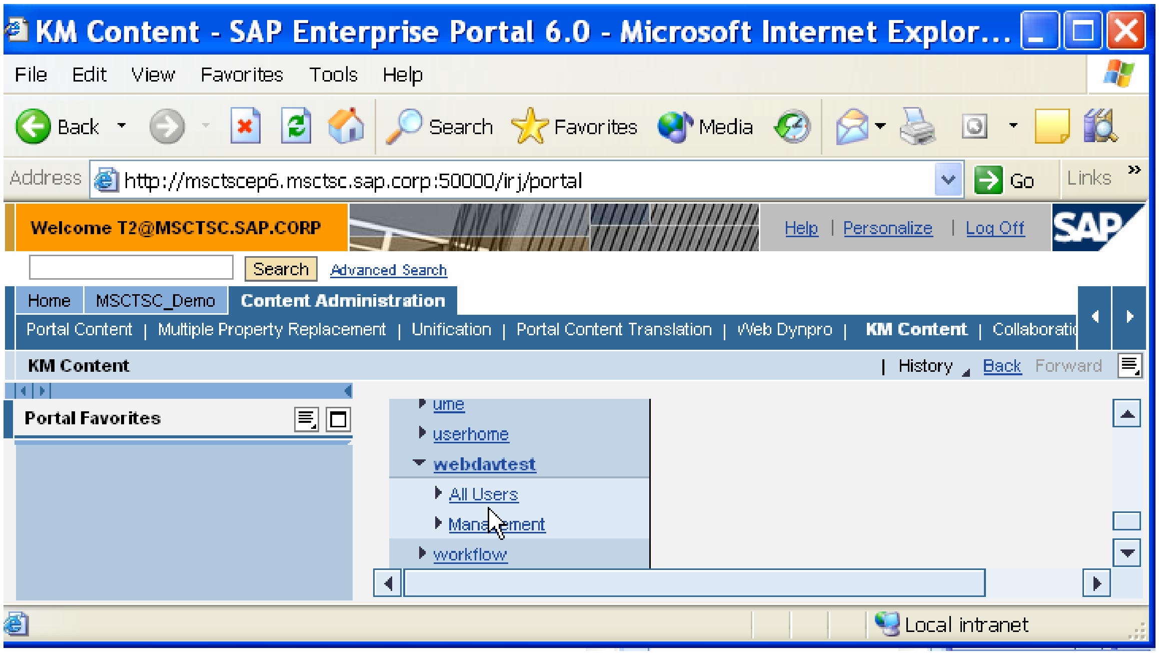
The result is shown in the following screenshots. While the user T2 can browse to both subfolders the normal user T1 is only allowed to see the subfolder *All Users*.


KM Content - SAP Enterprise Portal 6.0 - Microsoft Internet Explor...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Help | Personalize | Log Off
Search Advanced Search
Home MSCTSC_Demo Content Administration
Portal Content | Multiple Property Replacement | Unification | Portal Content Translation | Web Dynpro | KM Content | Collaboratior
KM Content
| History Back Forward
Portal Favorites
Taxonomies
ume
userhome
webdavtest
All Users
workflow
Local intranet

Address: http://msctscep6.msctsc.sap.corp:50000/irj/portal

Welcome T1@MSCTSC.SAP.CORP

Figure 6 KM Content viewed by normal user

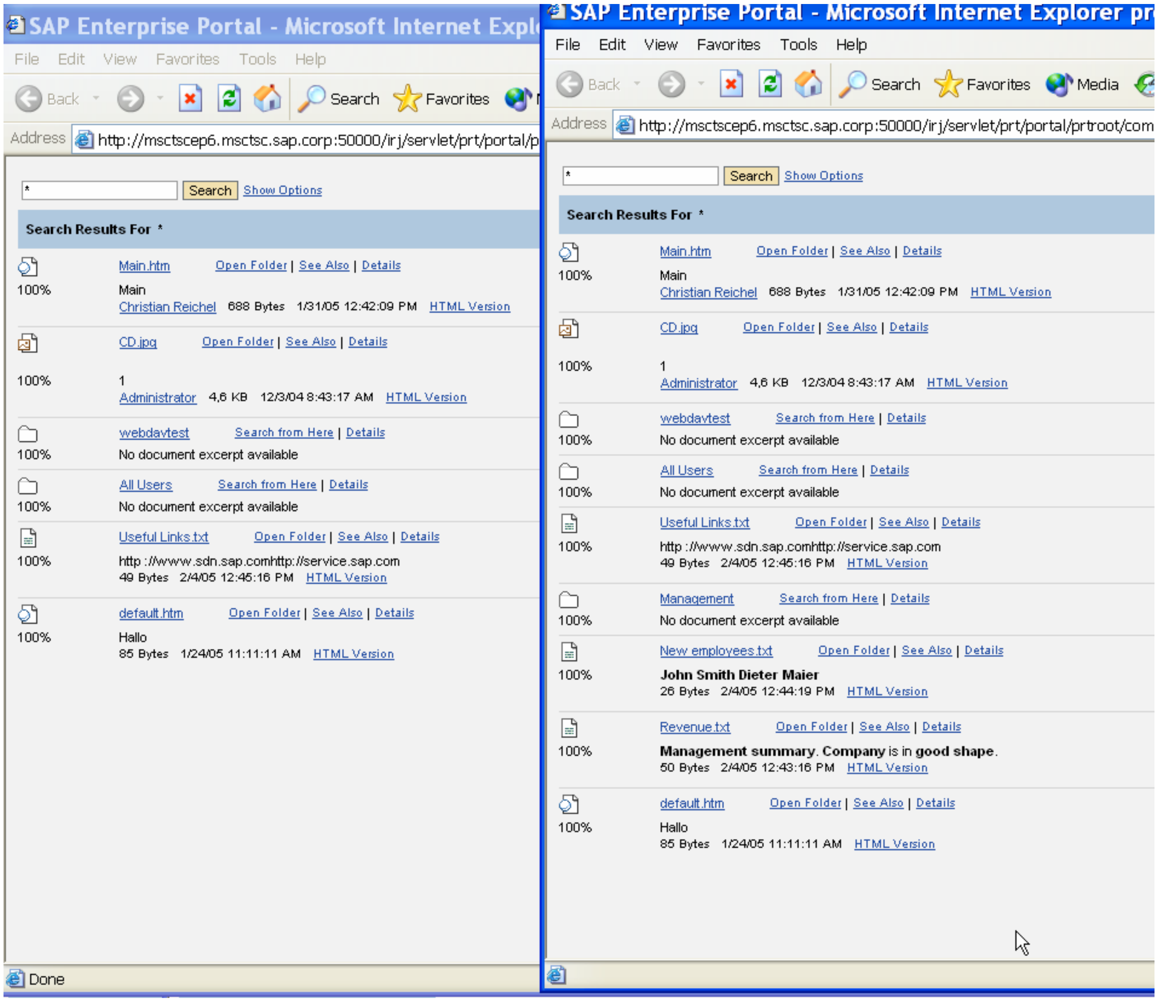

KM Content - SAP Enterprise Portal 6.0 - Microsoft Internet Explor...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Help | Personalize | Log Off
Search Advanced Search
Home MSCTSC_Demo Content Administration
Portal Content | Multiple Property Replacement | Unification | Portal Content Translation | Web Dynpro | KM Content | Collaborati
KM Content
| History Back Forward
Portal Favorites
ume
userhome
webdavtest
All Users
Management
workflow
Local intranet

Address: http://msctscep6.msctsc.sap.corp:50000/irj/portal

Welcome T2@MSCTSC.SAP.CORP

Figure 7 KM Content viewed by member of the group Management

Besides browsing the Windows access control lists are also taken into account if both users perform a search in the SAP KM platform. In the following example the two users are starting the same search. As a result for their search they get only a list of those documents / folders that they are allowed to access according their windows authorizations.


SAP Enterprise Portal - Microsoft Internet Expl
File Edit View Favorites Tools Help
Back Search Favorites
Address

http://msctscep6.msctsc.sap.corp:50000/irj/servlet/prt/portal/p

* Search Show Options

Search Results For *

Main.htm Open Folder | See Also | Details
100% Main
Christian Reichel 688 Bytes 1/31/05 12:42:09 PM HTML Version

CD.jpg Open Folder | See Also | Details
100% 1
Administrator 4,6 KB 12/3/04 8:43:17 AM HTML Version

webdavtest Search from Here | Details
100% No document excerpt available

All Users Search from Here | Details
100% No document excerpt available

Useful Links.txt Open Folder | See Also | Details
100% http ://www.sdn.sap.comhttp://service.sap.com
49 Bytes 2/4/05 12:45:16 PM HTML Version

default.htm Open Folder | See Also | Details
100% Hallo
85 Bytes 1/24/05 11:11:11 AM HTML Version

Done

SAP Enterprise Portal - Microsoft Internet Explorer pr
File Edit View Favorites Tools Help
Back Search Favorites Media
Address

http://msctscep6.msctsc.sap.corp:50000/irj/servlet/prt/portal/prtroot/com

* Search Show Options

Search Results For *

Main.htm Open Folder | See Also | Details
100% Main
Christian Reichel 688 Bytes 1/31/05 12:42:09 PM HTML Version

CD.jpg Open Folder | See Also | Details
100% 1
Administrator 4,6 KB 12/3/04 8:43:17 AM HTML Version

webdavtest Search from Here | Details
100% No document excerpt available

All Users Search from Here | Details
100% No document excerpt available

Useful Links.txt Open Folder | See Also | Details
100% http ://www.sdn.sap.comhttp://service.sap.com
49 Bytes 2/4/05 12:45:16 PM HTML Version

Management Search from Here | Details
100% No document excerpt available

New employees.txt Open Folder | See Also | Details
100% John Smith Dieter Maier
26 Bytes 2/4/05 12:44:19 PM HTML Version

Revenue.txt Open Folder | See Also | Details
100% Management summary. Company is in good shape.
50 Bytes 2/4/05 12:43:16 PM HTML Version

default.htm Open Folder | See Also | Details
100% Hallo
85 Bytes 1/24/05 11:11:11 AM HTML Version

Figure 8 Comparison of search results

How can this behaviour be explained though no security manager is used?

Since no security manager is used the WebDAV repository manager tries to access all URL’s that are provided by TREX as the result of the search. However only those documents and folders are displayed as the result of the search that can be accessed using the credentials of the current logged on user. For this a HTTP Get request is performed using the credentials of the currently logged on user for each document or folder that has been found by TREX. If the HTTP request fails the document is not listed in the list of search results.

Possible Performance Problems

This “trial and error” behaviour can have an impact on the search performance of such a scenario. If the worst comes to the worst a user might perform a search with a very large result set though his Windows ACL’s allow him to see only a small subset of these documents. If for example a search would deliver a result set of 10.000 documents but the user is only allowed to access 10 of these documents in the worst case 9990 unsuccessful HTTP Get requests have to be performed before any search results can be displayed to the user. When implementing the scenario you therefore have to have in mind that additional document attributes can be used to narrow down the result set.

How to Guide section

The following How-To Guide section describes the steps necessary to integrate a windows file system into the SAP KM platform using the WebDAV repository manager and the SSO22KerbMap Module.

Setting up the IIS

WebDAV is an optional component of IIS 6.0 and is not installed by default. WebDAV can be added to the IIS installation using Control Panel. For a detailed documentation on how to create a WebDAV publishing directory see:

http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/pub_dav_aboutwebdav.mspx

Installing and enabling WebDAV

1. From the *Start* menu, click *Control Panel*.
2. Double-click *Add or Remove Programs*.
3. Click *Add/Remove Windows Components*.
4. In the *Components* list box, click *Application Server*.
5. Click *Details*.
6. Click *Internet Information Services Manager*.
7. Click *Details* to view the list of IIS optional components.
8. Click *World Wide Web Service*
9. Click *Details* to view the list of World Wide Web Service optional components.
10. Select *WebDAV Publishing*
11. Click OK until you are returned to the Windows Component Wizard.
12. Click Next and complete the Windows Component Wizard.

After WebDAV is installed, it has to be enabled through the Web Service Extensions node in IIS Manager.

1. From the *Start* menu, click *Control Panel*.
2. Click *Administrative Tools*
3. Click *Internet Information Services (IIS) Manager*
4. In IIS Manager, expand the *local computer*, and then click *Web Service Extensions*.
5. In the details pane, click the Web Service Extension (here WebDAV) that you want to enable or disable.
6. To enable the WebDAV Web service extension, click Allow.

Setting up a publishing directory

Setting up a WebDAV publishing directory on your server is as straightforward as setting up a virtual directory through IIS Manager. In the following find a brief description how to set up a WebDAV publishing directory on IIS.

1. Be sure the WebDAV extension is enabled in IIS Manager.
2. Before setting up your WebDAV publishing directory, ensure that your publishing directory resides in an NTFS partition. Create or choose an existing directory on your Web server and set the desired NTFS permissions. This directory can be created anywhere on your Web server.
3. In IIS Manager, create a virtual directory and
    a. set the desired virtual directory permissions
    b. Choose an alias for this virtual directory,
    c. and link it to the physical directory you created in Step 1.

WebDAV publishing and file management requires the following permissions on the NTFS directory:

- Read: Enables users to read the contents of a file.
- Read and Execute: Enables user to read a file and run scripts or Common Gateway Interfaces (CGIs).
- List: Enables users to view the contents of the directory.
- Write: Enables users to access and change the source of a script and to publish files.
- Modify: Enables users to rename or delete a directory or file.

WebDAV publishing and file management requires the following permissions on the IIS virtual directory:

- Read: Enables users to read the contents of a file.
- Directory Browsing: Enables users to view the contents of the directory.
- Write: Enables users to access and change the source of a script and to publish files.

Configuration of the SSO22KerbMap Module

The SSO22KerbMap Module has to be installed as described in the documentation. In the configuration file the attribute that is used as j_user must be specified

```
########################################################################
#######
# This is the property file for the SSO2 to Kerberors mapping filter
# example:
#
# PseFile = c:\sec\verify.pse
# ServicePrincipalName = HOST/pcintel102.nt51.sap-ag.de
# FilterPriority = High
# LogLevel = 1
# SSO2AccountAttribute = userPrincipalName
#
########################################################################
#######
```

```
# Specify the full path of the verify.pse file, which contains the
# digital certificate of the Portal Server.
PseFile = C:\Inetpub\SSO22KerbMap\verify.pse

# These are the log levels.
# 0 - only global information written to the file
# 1 - Only errors are written to the file
# 2 - All information is written to the file
LogLevel = 1

# Specify the SPN shown by setspn.exe
ServicePrincipalName = HOST/msctscowa3.MSCTSC.SAP.CORP

# Specify the priority for the filter (Low, Medium or High)
FilterPriority = High

# Specify the ADSI Attribute of the account provided by
# the SAP Logon Ticket
# this can be any attribute like sAMAccountName, userPrincipalName,...
# SSO2AccountAttribute = userPrincipalName
SSO2AccountAttribute = userPrincipalName
#
```

Make sure that the virtual directory is associated with an application pool that runs under the account *local system*. By default application pools operate under the *NetworkService* account, which has the least user rights that are required to run Web applications. However the local system account is required for the SSO22KerbMap Module to function properly. You can check which application pool is used as described in the following:

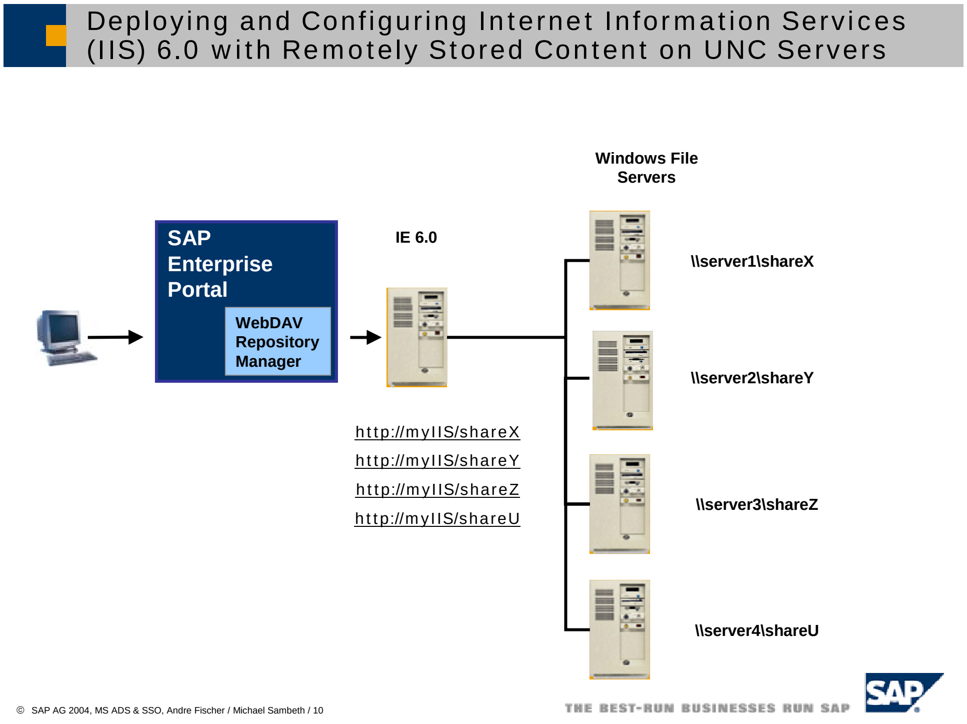
1. In IIS Manager, expand the local computer, right-click your WebDAV Web site (the site that contains the virtual directory mapped to your WebDAV publishing directory) and click Properties.
2. Click the *Virtual Directory* tab.
3. From the list box chose an appropriate application pool.
4. Click Apply.
5. Click OK.

Checking the IIS installation

After the IIS has been configured the installation can be tested if one tries to include the WebDAV repository as a Web folder in Windows® Explorer.

Using Remotely Stored Content on UNC Servers - Shares

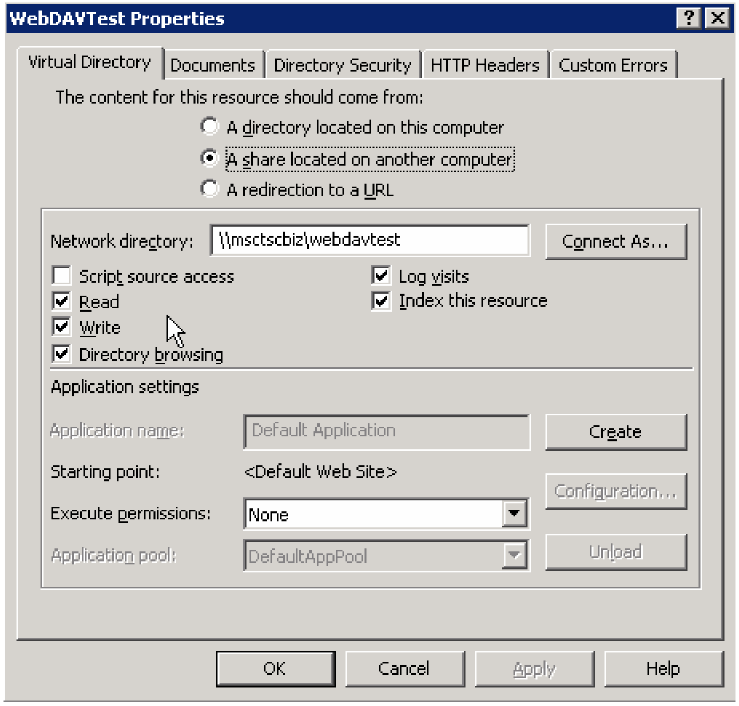
IIS is not only able to publish local file systems but also file systems that IIS can connect to via a share. This way it is possible to install the IIS on a different machine than the file server. Moreover it is possible to use a single IIS to connect and publish different shares simultaneously thus working as a WebDAV gateway.



Deploying and Configuring Internet Information Services (IIS) 6.0 with Remotely Stored Content on UNC Servers

Please review the article "Deploying and Configuring Internet Information Services (IIS) 6.0 with Remotely Stored Content on UNC Servers and NAS Devices" in the Microsoft TechNet.

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/webapp/iis/remstorg.mspx


WebDAVTest Properties

Virtual Directory | Documents | Directory Security | HTTP Headers | Custom Errors

The content for this resource should come from:

○ A directory located on this computer
● A share located on another computer
○ A redirection to a URL

Network directory: \\msctscbiz\webdavtest

☐ Script source access
☑ Read
☑ Write
☑ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

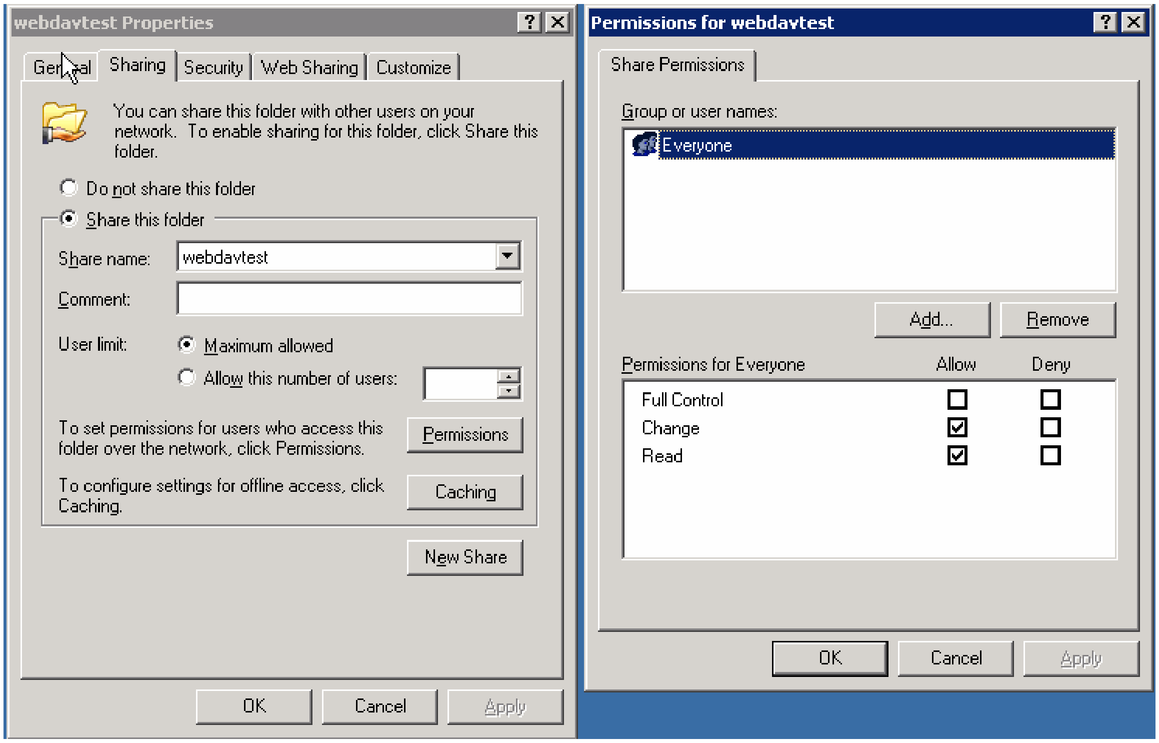
Application name: Default Application

Starting point: <Default Web Site>

Execute permissions: None

Application pool: DefaultAppPool

The share on the remote server has to offer read and write access over the network if it should be possible to change documents.


webdavtest Properties

General | Sharing | Security | Web Sharing | Customize

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder
● Share this folder

Share name: webdavtest

Comment:

User limit: ● Maximum allowed
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

Permissions for webdavtest

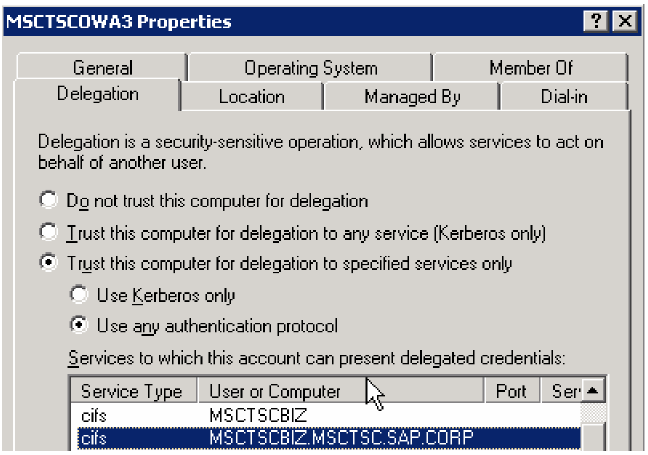
Share Permissions

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	☐	☐
Change	☑	☐
Read	☑	☐

Since the file system resides on another computer delegation for the server where the IIS is running has to be configured. In addition to the Service type *HOST* one has to allow the server account that it also presents delegated credentials to the *cifs* Service. This delegation configuration is shown in the following screen shot.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

○ Use Kerberos only

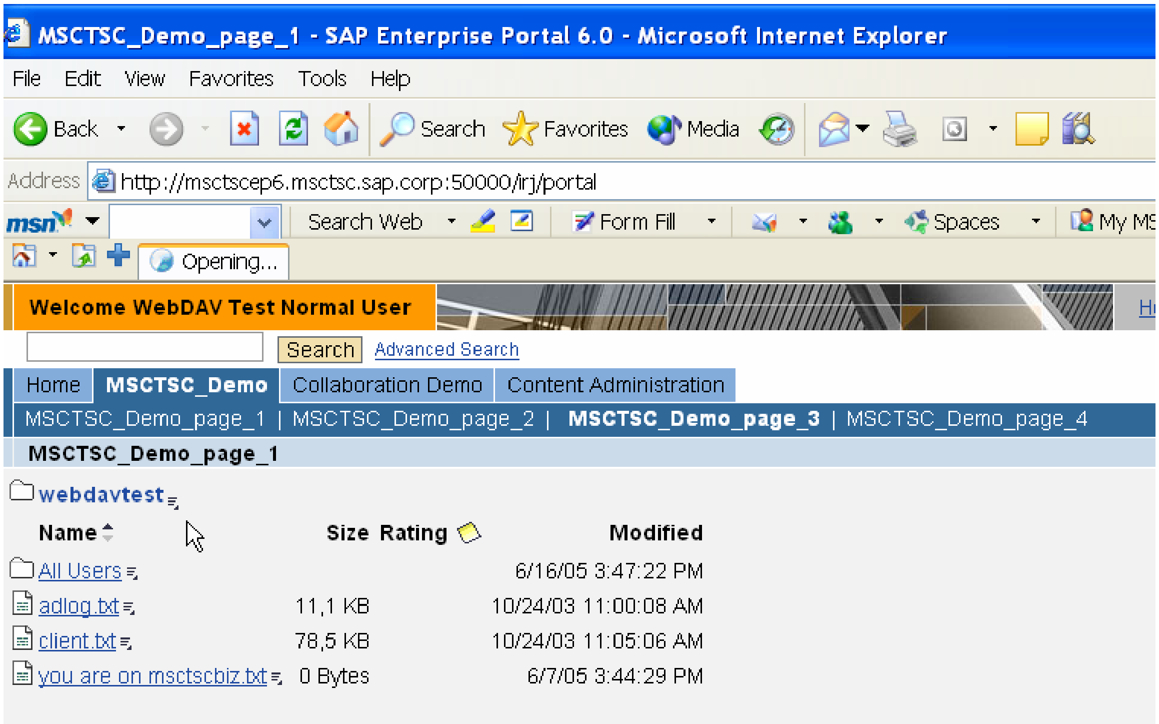
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Ser
cifs	MSCTSCBIZ		
cifs	MSCTSCBIZ.MSCTSC.SAP.CORP		

As with local file systems the remote connected file system can also be integrated into SAP Enterprise Portal using the WebDAV repository manager.

As with file systems that are connected locally windows ACL's configured the test users mentioned above only see those files and directories that they are allowed to see according to their ACL's.



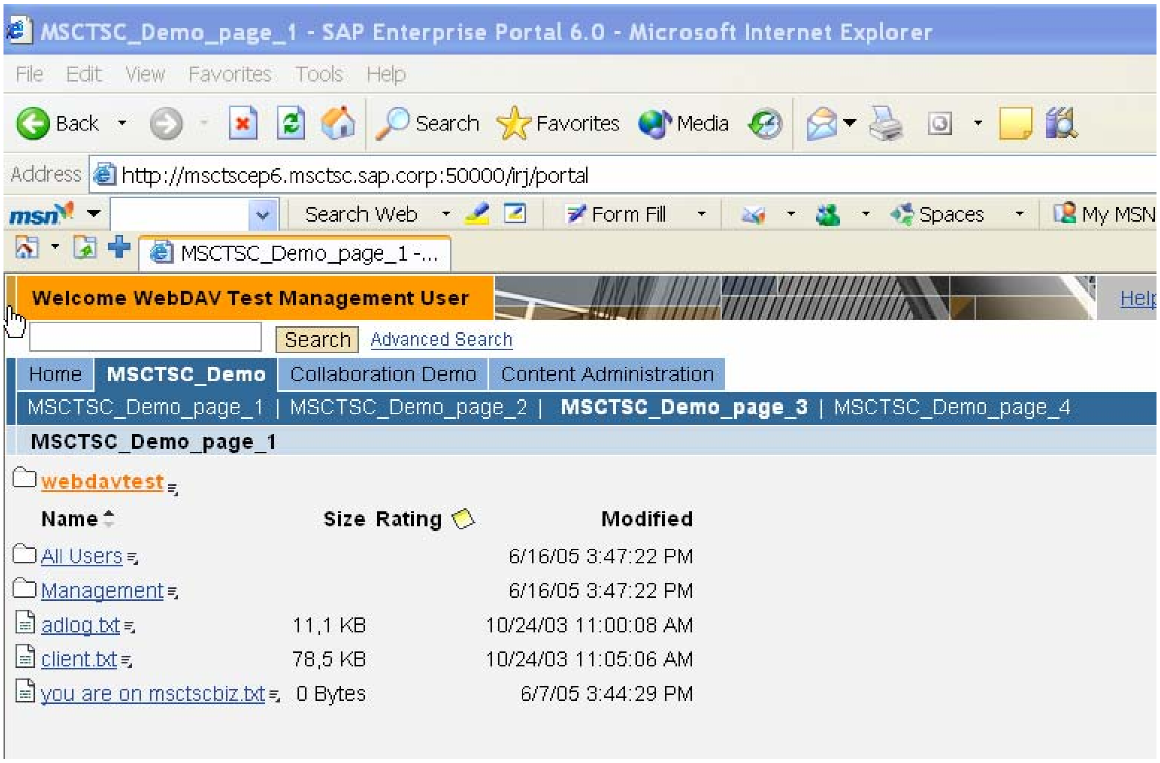
Address http://msctscep6.msctsc.sap.corp:50000/irj/portal

Welcome WebDAV Test Normal User

MSCTSC_Demo_page_1

webdavtest

Name	Size	Rating	Modified
All Users			6/16/05 3:47:22 PM
adlog.txt	11,1 KB		10/24/03 11:00:08 AM
client.txt	78,5 KB		10/24/03 11:05:06 AM
you are on msctscbiz.txt	0 Bytes		6/7/05 3:44:29 PM


MSCTSC_Demo_page_1 - SAP Enterprise Portal 6.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
msn
Search Web
Form Fill
Spaces
My MSN
MSCTSC_Demo_page_1 -...
Welcome WebDAV Test Management User
Help
Search
Advanced Search
Home
MSCTSC_Demo
Collaboration Demo
Content Administration
MSCTSC_Demo_page_1 | MSCTSC_Demo_page_2 | MSCTSC_Demo_page_3 | MSCTSC_Demo_page_4

Address: http://msctscep6.msctsc.sap.corp:50000/irj/portal

MSCTSC_Demo_page_1

webdavtest

Name	Size	Rating	Modified
All Users			6/16/05 3:47:22 PM
Management			6/16/05 3:47:22 PM
adlog.txt	11,1 KB		10/24/03 11:00:08 AM
client.txt	78,5 KB		10/24/03 11:05:06 AM
you are on msctscbiz.txt	0 Bytes		6/7/05 3:44:29 PM

Setting up SAP KM

The following steps have to be carried out in the portal and on the KM platform before you are able to access documents provided by the IIS using the WebDAV repository manager.

- Define an HTTP system in the CM system landscape.
- Configure the repository manager parameters for the WebDAV Repository Manager.
- Since user mapping is used for the service users you have to create a WebDAV system in the portal system landscape
- Carry out user mapping for the WebDAV system for internal CM service users. (The configuration of user mapping can be left out since the SSO22KerbMap Module is used.) or create corresponding users in Active Directory for the CM service users.

A detailed description on how to perform a configuration of the WebDAV Repository Manager can be found in the SAP Online Help *Integration and Configuration of the WebDAV Repository Manager.*

Define a HTTP-System in the CM-system landscape

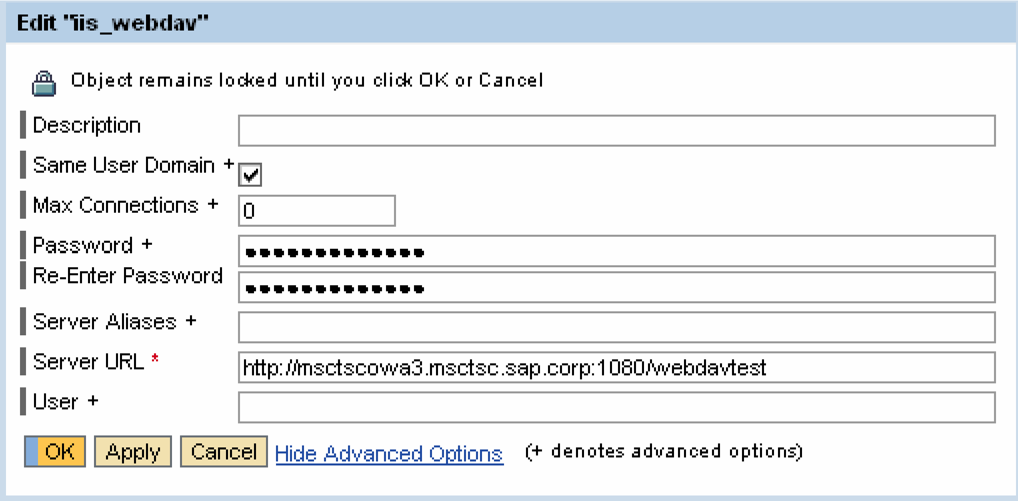
A detailed description on how to create a HTTP system can be found in the SAP Online Help *Integration and Configuration of the WebDAV Repository Manager*.
The configuration necessary to define an HTTP system can be found under *System Administration* in the top-level navigation bar of SAP Enterprise Portal. In the SAP Enterprise Portal choose *System Administration* -> *System Configuration*.

In *Detailed Navigation* choose *Content Management* → *Global Services* → *System Landscape Definitions* → *Systems* → *HTTP System*.

On this page you can create the HTTP system. Click *New* and then *Advanced Options* and add the appropriate parameters:

System ID *	iis_webdav
Server URL *	http://msctscowa3.msctsc.sap.corp:1080/webdavtest/
Same User Domain:	x

Activating the option *Same User Domain* causes the WebDAV Repository manager to send a SAP Logon Ticket.



Edit "iis_webdav"

Object remains locked until you click OK or Cancel

Description	
Same User Domain +	☑
Max Connections +	0
Password +	••••••••••••••
Re-Enter Password	••••••••••••••
Server Aliases +	
Server URL *	http://msctscowa3.msctsc.sap.corp:1080/webdavtest
User +	

Figure 9 KM configuration: HTTP system

Please be sure to remove the values for the user mapping. If a username and password is provided in the definition of the HTTP system this setting overrides all user mapping settings that are maintained by the users in their personal settings and will also override the setting for sending SAP Logon Tickets.

Hint:

Entering User mapping data might be useful for troubleshooting. This way one can distinguish whether the problem is a general one or if the configuration of the SSO22KerbMap Module has to be checked.

Create a WebDAV system template

Please log on to the portal using the role System-Administrator. In the SAP Enterprise Portal choose *System Administration -> System Configuration*. In *Detailed Navigation* choose *System Landscape.*In the Portal Content catalog choose *Templates -> System Landscape Templates*. Clicking the right mouse button having *System Landscape*

Templates selected the context menu opens. Choose *New From PAR → System*. In the *system wizard* choos the portal archive *com.sap.km.cm.repository.manager* and click *Next*. Choose the Portal Component *KMWebDAV_System* and click *Next* and enter the required data:

Systemname = KMWebDAV_System

System-ID = KMWebDAV_System

Choose *Save as system template* and click *Next* and then *Finish*. For the KMWebDAV-System the property editor opens. Scroll down and mark the parameter *User Mapping Type*.

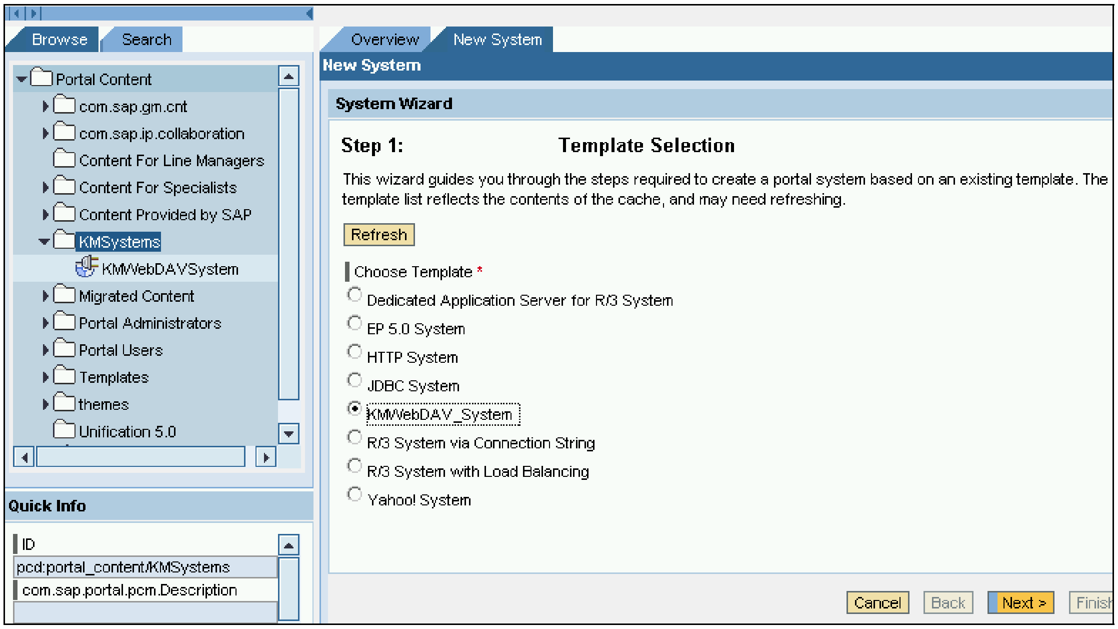
Using this parameter you can specify whether only administrators, only users or both groups are allowed to maintain user mapping data for a user.

As a default you should choose *admin, user*. Click *Save* to leave the property editor. Check whether a folder *KMSystems* does exist in Portal Content. If not, click on portal Content using the right mouse button and choose *New folder*. In the dialog enter the name *KMSystems*. This folder will be used to create WebDAV-Systems in KM.

Create a WebDAV system in the portal system landscape

In the SAP Enterprise Portal choose *System Administration* -> *System Configuration*. In *Detailed Navigation* choose *System Landscape.* In the Portal Content catalog choose the folder *KMSystems.* Clicking the right mouse button having *KMSystems* selected choose *New* -> *System* from the context menu. Choose the *KMWebDAV_System* and click *Next*.

> Hint:
>
> If the *KMWebDAV_System* that has been created in the previous step is not available try to restart the portal.



Step 1: Template Selection

This wizard guides you through the steps required to create a portal system based on an existing template. The template list reflects the contents of the cache, and may need refreshing.

Choose Template *

○ Dedicated Application Server for R/3 System
○ EP 5.0 System
○ HTTP System
○ JDBC System
● KMWebDAV_System
○ R/3 System via Connection String
○ R/3 System with Load Balancing
○ Yahoo! System

Please enter a system name (*KMWebDAV_System*) and a *System-id* and press Next. In the following screen press *Finish* to save your settings.

In our example the following parameters have been used:

KMWebDAV_System:	KMWebDAVSystem
ID:	KMWebDAVSystem
UserMappingType:	admin,user

Open the object for editing and choose the *System Alias Editor* choosing *System Aliases* from the drop down box *Display*. Enter an Alias for the WebDAV System. Please note that the alias must be the same than the System-ID that has been chosen the CM system landscape definition. In our example the following parameters have been used:

Alias:	iis_webdav

Maintain user mapping data for the WebDAV-System

1.) *Personalize -> User mapping*

2.) From the drop down box select the system *webdavtest*

Repository-Manager configuration

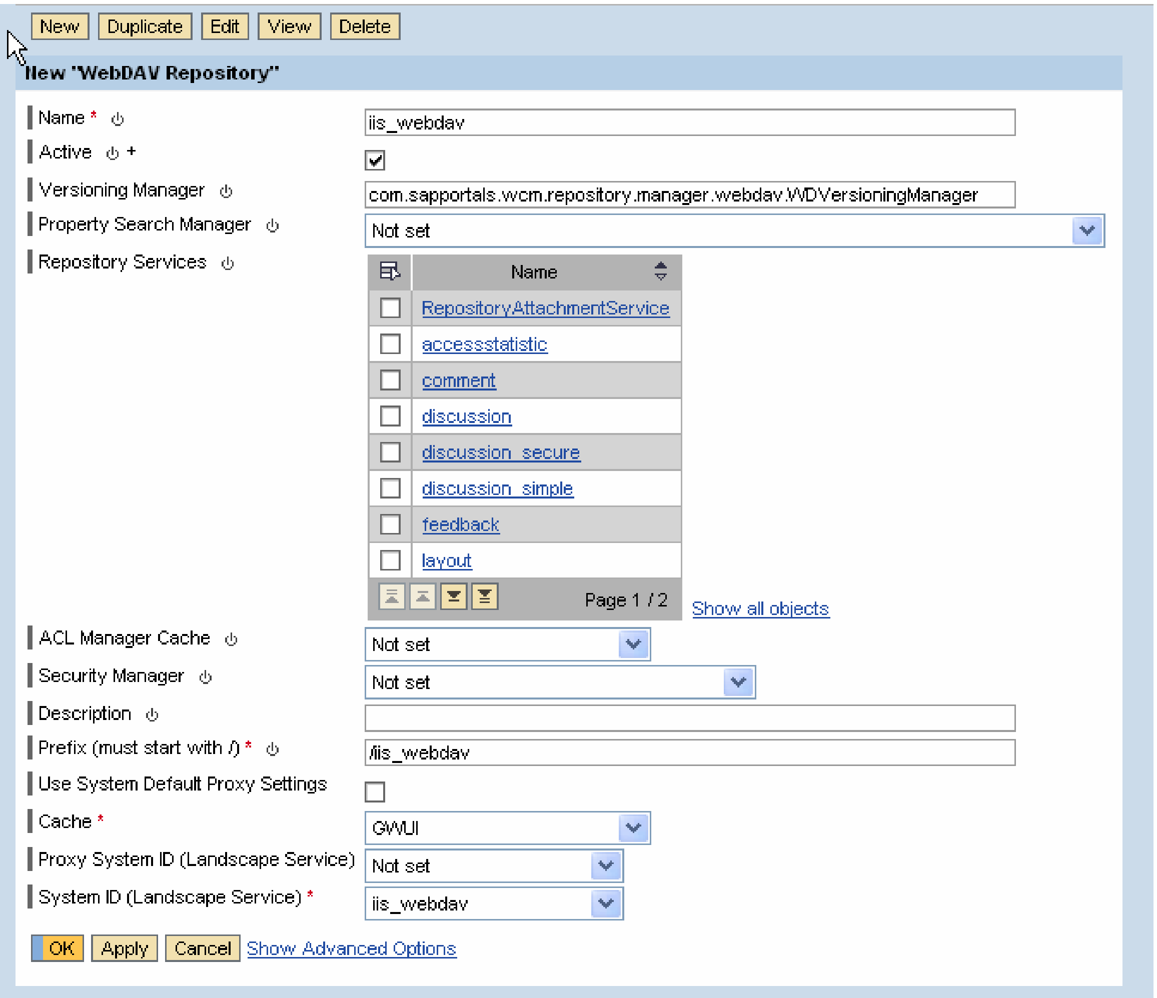
The configuration necessary to define a repository manager can be found under *System Administration* in the top-level navigation bar of SAP Enterprise Portal. In the SAP Enterprise Portal choose *System Administration -> System Configuration*.

In *Detailed Navigation* click *Knowledge Management -> Repository Managers -> WebDAV Repository*

On this page you can create the WebDAV repository manager. Click *New* and add the appropriate parameters:

Name:	iis_webdav
Prefix:	/iis_webdav
System ID (Landscape Service) *	iis_webdav

(this is the name of the HTTP system that has been created in the previous step)



New "WebDAV Repository"

Name *	iis_webdav
Active +	☑
Versioning Manager	com.sapportals.wcm.repository.manager.webdav.WDVersioningManager
Property Search Manager	Not set
Repository Services	

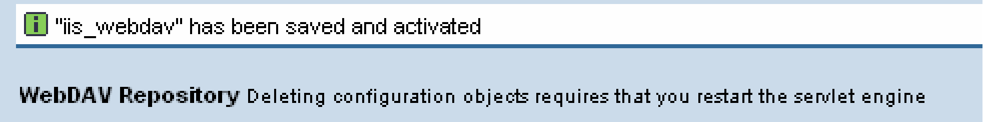
	Name
□	RepositoryAttachmentService
□	accessstatistic
□	comment
□	discussion
□	discussion_secure
□	discussion_simple
□	feedback
□	layout

Page 1 / 2

ACL Manager Cache	Not set
Security Manager	Not set
Description	
Prefix (must start with /) *	/iis_webdav
Use System Default Proxy Settings	□
Cache *	GWUI
Proxy System ID (Landscape Service)	Not set
System ID (Landscape Service) *	iis_webdav

Figure 10 KM configuration: WebDAV repository manger I

Click OK to activate your changes. A warning message informs you that deleting configuration objects requires you to restart the servlet engine.



"iis_webdav" has been saved and activated

WebDAV Repository Deleting configuration objects requires that you restart the servlet engine

Figure 11 KM configuration: WebDAV repository manger II

Hint:

If the WebDAV repository is not displayed after the configuration steps described before a solution might be to restart the servlet engine to activate the changes.

Checking the installation

From the top-level navigation bar of SAP Enterprise Portal choose *Content Administration.* Klick on *KM Content* and wait for the system to initialize all KM repositories.

Troubleshooting

The search for errors in the scenario described above is not easy since several components and authentication processes are involved.

1. After the configuration of WebDAV in the IIS it should be possible to connect to this ressource using web folders and the windows explorer.
2. If the WebDAV repository is not shown in the KM content one can use to store hardcoded user credentials in the definition of the http system or user mapping for troubleshooting if the second approach is taken into account.
   Using user mapping it is possible to compare the connection to the WebDAV repository published by the IIS using the SSO22KerbMap Module and using basic authentication. This way configuration problems with the SSO22KerbMap Module can identified.
3. Check the logfile of the SSO22KerbMap Module. If necessary increase the log level to log level 3.

Limitations

The most important limitation is that search performance might be poor under certain circumstances as described in section *Possible Performance Problems*. Before using this scenario productively you should analyze whether these issue does apply for you.

The WebDAV implementation provided by the IIS does neither support all WebDAV methods and it does also not support all features that are supported by the file system repository manager.

Conclusion

Though the usage of the WebDAV repository manager together with the IIS shows some limitations it is option that can be used as a work around if Windows file systems cannot be integrated using the file system repository manager. An advantage of the solution described is that no user mapping has to be maintained.

References

- SAP Library – Knowledge Management
  “Including a Knowledge Management Folder as a Web Folder”
  http://help.sap.com/saphelp_nw04/helpdata/en/30/75b62c659d724fb908c74ade23af51/frameset.htm
- Step-by-Step Guide: SSO22KerbMap ISAPI Module
- Collaboration Brief “*Using SAP Logon Tickets for Single Sign on to Microsoft based web applications*”
- Managing WebDAV Security
  Internet Information Services 6.0 Product Documentation
  http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/pub_dav_webdav.mspx
- Installing IIS – IIS 6.0 Operations Guide
  http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/gs_installingiis.mspx
- How to define a HTTP system
  http://help.sap.com/saphelp_nw04/helpdata/en/e1/977231e5f2394587955e8a6526739c/content.htm
- Integration and Configuration of the WebDAV Repository Manager.
  http://help.sap.com/saphelp_erp2004/helpdata/en/4a/217fb6c33c6748a1715a161ac942cd/content.htm
- Deploying and Configuring Internet Information Services (IIS) 6.0 with Remotely Stored Content on UNC Servers and NAS Devices
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/webapp/iis/remstorg.mspx