Single Sign On for SAP NetWeaver Application Server (ABAP) on Power Systems

How to enable Single Sign On with Secure Network Communication using Kerberos on SAP Application Servers (ABAP) running on Power Linux or AIX with a central Active Directory serving as Kerberos server

Cäcilie Hampel
ODOE Technology & Solutions Development

Oktober 2009

This document can be found on the web, www.ibm.com/support/techdocs

Table of contents

Abstract

The system landscape of companies grows rapidly. At the same time, the number of users increases as in heterogeneous system landscapes one employee often uses several user IDs for different systems. This leads to high maintenance and support effort as well as higher total cost of ownership and security risks.

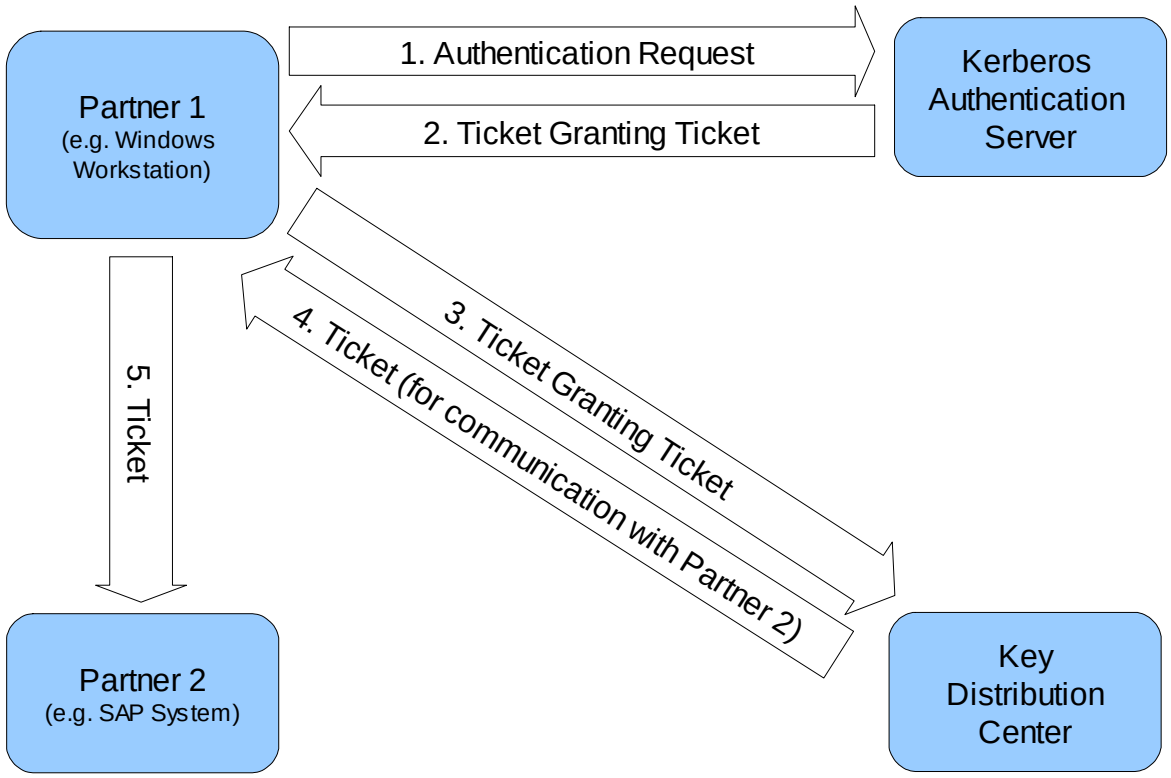
A possible solution to this situation could be Single Sign On (SSO). The name already tells all about SSO: the user has to sign on only once. This means he must remember only one user name and one password.

This paper describes the setup of SSO for SAP® NetWeaver™ Application Server based on the Kerberos™ protocol. It makes use of the common combination of Windows® workstations grouped in a Microsoft® Active Directory™ domain and SAP on Linux® and AIX® running on IBM® Power™ Systems.

Preface

SAP offers Secure Network Communication (SNC) as a component to integrate an external security product into SAP systems. In this paper, the used external security product will be Kerberos.
Kerberos is a network authentication system based on a key distribution model and a central repository. The idea is that every resource authenticates itself against the Kerberos server and receives a key, also called ticket. This ticket is then used during communication with others to identify the resource as a trusted partner and enables single sign on as no passwords will be requested due to the ticket exchange.

The first step for a Kerberos authenticated communication is that a resource authenticates itself against a Kerberos authentication server and requests a ticket. This first ticket is the Ticket Granting Ticket (TGT) that is used for the communication with the Kerberos Key Distribution Center (KDC). Further, during the first communication with the authentication server, a session key is created that can be used for encrypted communication. The Kerberos authentication server and the KDC are two independent servers and could work on different servers but usually, they are part of the same system and are seen as an unit.
When the resource now tries to connect to another party, it needs another ticket. Therefore it sends the TGT and a ticket request to the KDC that creates tickets for the communication with other Kerberos enabled resources. The KDC will respond with a ticket for the communication between the two partners.
The first resource forwards the ticket to the host with which it would like to communicate. If the host accepts the ticket as valid, the resource has been authorized to connect to the system for the duration of the ticket.
The tickets have a limited lifetime and must be renewed after a while, normally after eight to ten hours.
Another security setting is that every ticket is also bound to a unique SPN, Service Principal Name, that clearly identifies a user or resource. The ticket can only be used by the partner to which it was granted.



In the SAP context, the involved parties are the user on his local workstation, the SAP system on a Linux or AIX host, and the central active directory that serves as a Kerberos server, which contains both the authentication server and the KDC.
The user on his workstation that is part of a Microsoft Active directory domain is automatically authenticated against the central Kerberos server during log on. Apart from that only a Generic Security Services Application Programming Interface (GSS-API) library must be installed on the workstation as SNC uses the GSS-API interface to communicate with Kerberos. The same refers to the Linux/AIX host; it needs also the GSS-API lib.
Further, also the host the SAP systems runs on must be registered as domain user. Therefore, a computer account is created in the active directory users section. As there will not be a physical user on the host that will actively authenticate it against the Kerberos server – in fact the SAP system will be started once and then run on its own without direct interaction by an administrator - we will use another mechanism. On the active directory server, a keytab can be created that holds the credentials of the host, as well as its encrypted password of the computer account. This keytab is then copied to the host. It can be called by a local user and all applications running under this user will be enabled for Kerberos authentication. As the SAP system is running under a userid called <sid>adm, this user must be authorized to call the keytab. Not the user itself but the host is then authenticated against the Kerberos server. The user will, however, hold the ticket needed for communication with other parties. So, if there are applications on one host started by different users, there

must be one ticket for each user. The tickets must be renewed in regular intervals. This can be done in an automated job.
After SAP system host and user have authenticated themselves against the Kerberos server, the user is able log in to the SAP application without password input, the authentication is done in the background.
Now, after the technical background has been described, you need to perform the following steps to enable your own SAP system for SSO:

- Kerberos Client Configuration
- Add Linux/AIX Server as host to Active Directory and create keytab
- Enable SAP NetWeaver Application Server (ABAP) for SNC
- Enable SAP User for SNC
- Enable Kerberos and SNC on Windows Client
- Testing SSO

Kerberos Client Configuration

To enable the Linux or AIX Server for Kerberos authentication, it needs a Kerberos client that will talk to the central Active Directory Kerberos server.

Before you start with the configuration of Kerberos client, make sure that you have installed the required packages.
For Linux, the MIT Kerberos5 Implementation-Libraries and the krb5Client as well as the PAM Modules for Kerberos authentication are needed.
For AIX, install the package krb5.client.rte which is located on the expansion CD.

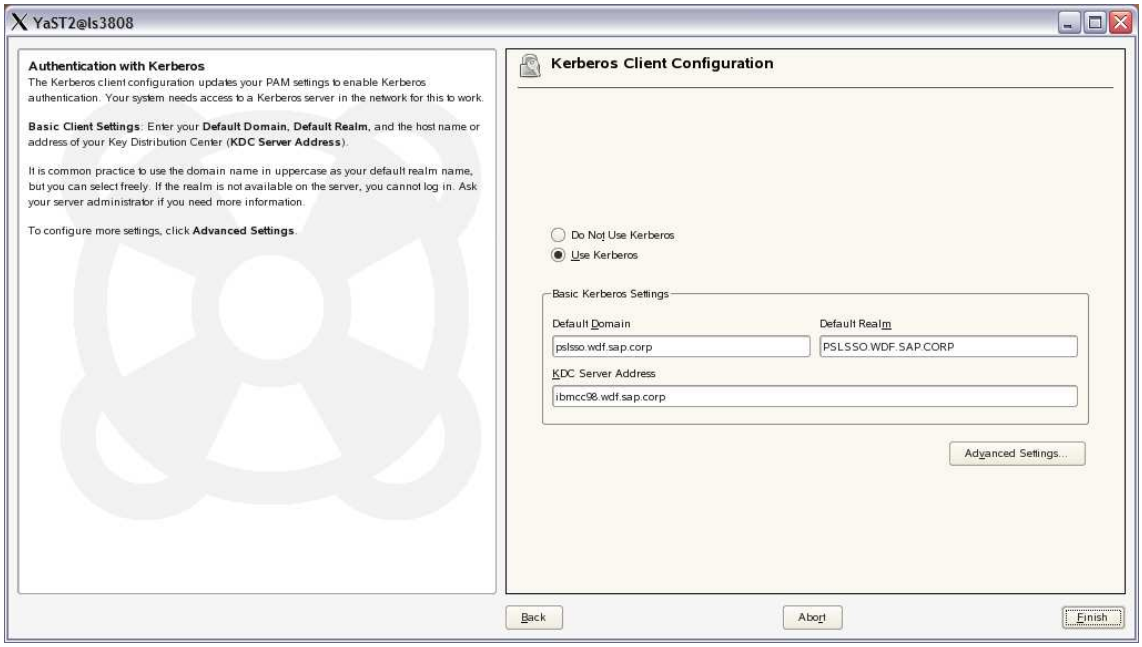
The setup on Linux is a different for Novell® and Red Hat® systems but the same information is needed. While Novell uses yast2 for the Kerberos configuration Red Hat provides the authconfig tool.
This description refers to Novell SUSE® Linux Enterprise Server 10 and Red Hat Enterprise Linux 5 as reference version.

You will need root access to do this configuration on your system.

a.) Novell Linux Kerberos Client Configuration

Open a console on your Linux server and call yast or yast2.
The first step will be to configure the Kerberos client.

1. Navigate to *Network Services → Kerberos client.*



2. Select *Use Kerberos*.

3. Enter the default domain name in the according field. If you are not sure about the domain name have a look at the *Active Directory Domains and Trusts* overviewon your Active Directory (AD) server, it will show you the domains in your AD.

4. The Realm that should be entered into the *Default Realm* field is always the same as the default domain but in capital letters.

5. The last information that is needed is the *KDC Server Address.* This is the name of the Server where the AD runs on. After that press *Finish*.

b.) Red Hat Linux Kerberos Client Configuration

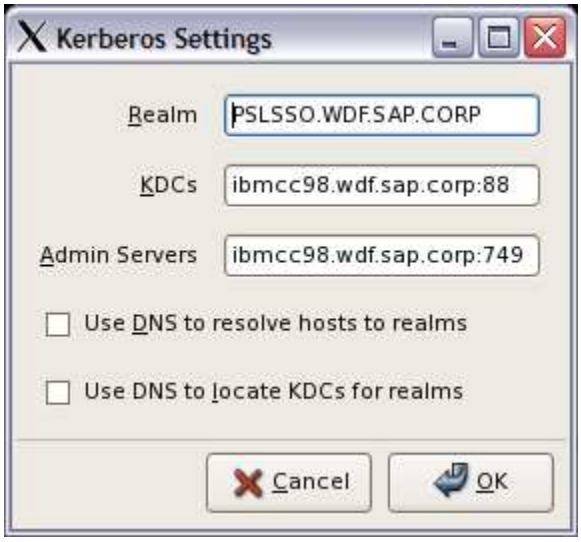
Open a console on your Linux server and call *authconfig-gtk.* A popup *Authentication Configuration* opens. If not you might need to set a Display variable to your local workstation to open an X-window. You will now configure the Kerberos client.

1. Open authconfig-gtk and go to the *Authentication* tab and mark *Enable Kerberos Support*. Now select *Configure Kerberos* and a popup will open.

2. In the *Realm* field, enter the Kerberos Realm which is the same as the Active Directory domain in upper letters. If you are not sure about the domain name have a look at the *Active Directory Domains and Trusts* overview, it will show you the domains in your AD.

3. Put in the fully qualified name of the Active Directory server, which is at the same time the Kerberos Distributions Center (KDC), in the field „KDCs". Add the port that is used by the Kerberos service on the AD server. By default this is port 88. (To look up the port go to *Programs → Administrative Tools → DNS* on your Active Directory server and expand *DNS → <hostname> → Forward Lookup Zones → <your_domain> → _tcp → _kerberos*).
   Your input: <server_name>:<port number>

4. Into the *Admin Server,* enter the name of your Active Directory Server and the port for the admin services (by default 749): <server_name>:<port>



5. Save the settings and close authconfig-gtk by selecting *Ok* twice.

c.) AIX Kerberos Client Configuration

The first step is the kerberos client setup. Therefore run the config.krb5 script which comes with AIX and specify the required parameters.

```
config.krb5 -C -d <domain> -r <realm> -c <kdc_hostname> -s
<kerberos_server>
```

-C just says that you are going to install a Client

-d `<domain>`
The name of the Windows domain (e.g. pslsso.wdf.sap.corp). Note the windows domain and the DNS domain do not have to be the same

-r `<realm>`
The Kerberos realm. This is the domain name in upper letter (e.g. PSLSSO.WDF.SAP.CORP)

- c `<kdc_hostname>`
The key distribution center of the kerberos server. In a windows domain this is the domain controller (e.g. ibmcc98.wdf.sap.corp)

-s `<kerberos_server>`
Name of the kerberos server. In a Windows domain this is the domain controller (e.g. ibmcc98.wdf.sap.corp))

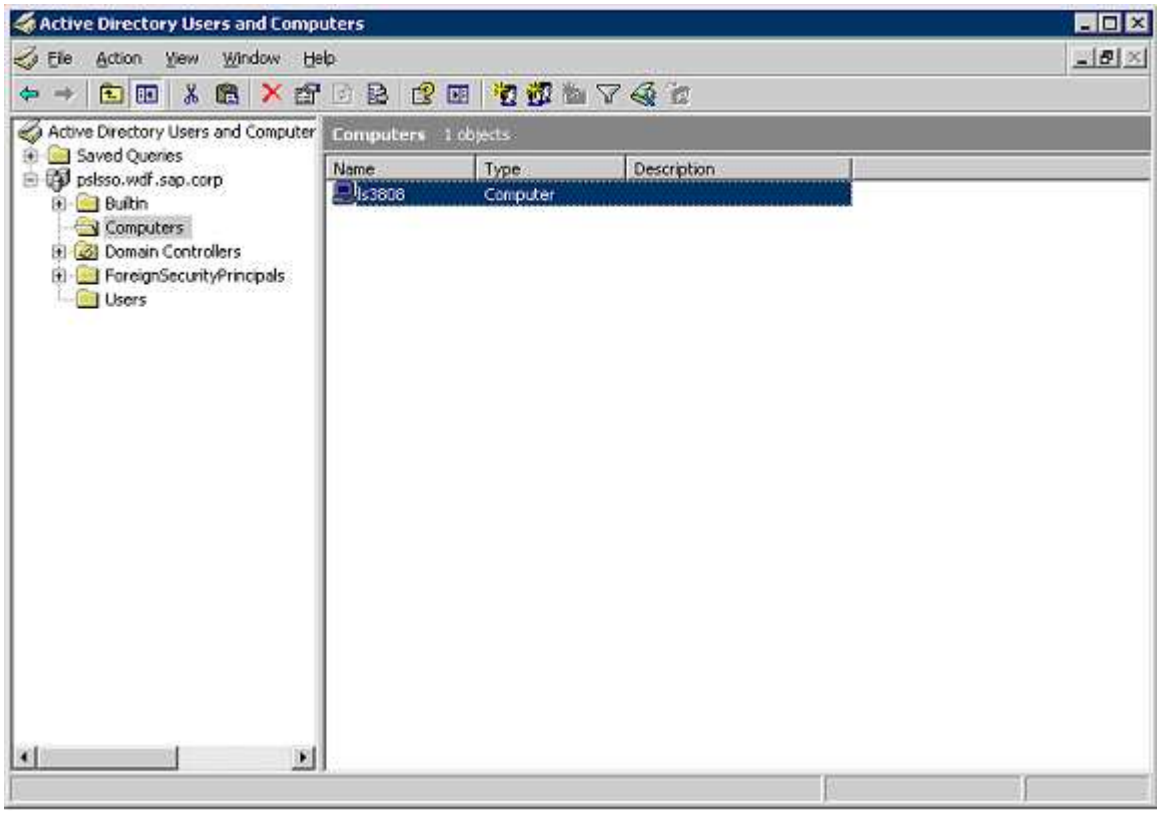
config.krb5 should show the following results:

```
root@is3017$ config.krb5 -C -d pslsso.wdf.sap.corp -r
PSLSSO.WDF.SAP.CORP -c ibmcc98.wdf.sap.corp -s
ibmcc98.wdf.sap.corp
Initializing configuration...
Creating /etc/krb5/krb5_cfg_type...
Creating /etc/krb5/krb5.conf...
The command completed successfully.
```

Add Linux/AIX Server as host to Active Directory and create keytab

The next step is now to create a new computer account for the Linux/AIX server in the Active Directory. Later, the Linux/AIX server will connect to the Kerberos server with this account.
Open *Active Directory Users and Computers* in the administrative Tools and add a new Computer by right-clicking on *Domain → Computers* and select *New → Computer*.

1. Enter the computer name and select *Next → Next → Finish*.



To later enable the Linux/AIX server to connect to the AD kerberos server without being asked for the password ,a keytab is needed. The keytab is generated on the Windows AD server and then copied to the host with the SAP system on it.

1. Open a command line window on the Windows AD server by calling *Start → Run → cmd.*

2. Run the command
```
ktpass -princ <service_principal_name> -mapuser
<windows_domain_name>\<host_name>$ -pass <hosts_password>
-ptype KRB5_NT_SRV_HST -out <host_name>.keytab

ktpass -princ ls3808@PSLSSO.WDF.SAP.CORP -mapuser pslsso\
ls3808$ -pass Sap123Sap -ptype KRB5_NT_SRV_HST -out
ls3808.keytab
```

service principal name	the SPN is the unique name of the participating resource (e.g. the host)
windows_domain_name	name of the windows domain
host_name	name of the host the SAP system is installed on, The name must be the same as defined in *Active Directory Users and Computers*
host_password	the password of the host as defined in the *Active Directory Users and Computers*

a.) Initialize keytab on Linux host

1. On Linux, copy the keytab to /etc on the Linux host and rename it to *krb5.keytab*.

2. Test if the keytab works by running *kinit -k <service_principal_name>* on the host.
   The Service Principal Name (SPN) must be exactly the same as in the keytab. Kinit will compare the given SPN with the one in the keytab and if they are the same no password is needed to request a kerberos ticket because it was already defined in the keytab.

3. When running *kinit -k <service_principal_name>* on Linux, no output is a good sign. There should not be a password request, as this is done by the keytab. To make sure that a new ticket was created run klist. You will get the information “Ticket cache: FILE:/tmp/krb5cc_<user_id>”. The user_id is the id of the user who ran kinit. The ticket is only valid for applications that are run by this user.

4. As the SAP NetWeaver Application Server is running under userid <sid>adm, a ticket must be created using this userid. Log on to the Linux system as

<sid>adm and call *kinit -k <service_principal_name>*. There should now be a ticket in /tmp/krb5cc_<id_of_sidadm> with the id <sid>adm in the name.

5. The ticket is only valid for a defined period of time. You can check this by calling *klist*. Without valid ticket, SSO will not be possible. To ensure that a new ticket is created after some hours, add a cronjob to the crontab that does a *kinit -k <SPN>* in regular time intervals.

b.) Initialize keytab on AIX host

1. Copy the keytab to /etc/krb5 on the AIX host and rename it to *krb5.keytab*.

2. To test if the keytab works run *kinit -k <service_principal_name>* on the host. The SPN must be exactly the same as in the keytab. Kinit will compare the given SPN with the one in the keytab and if they are the same, no password is needed to request a kerberos ticket because it was already defined in the keytab.

3. On AIX, you might get some feedback to tell you that the request finished successfully. (Be careful, if the ticket is not stored in /var/krb5/... please see errors section).

```
root@is3017$ kinit -k is3017@PSLSSO.WDF.SAP.CORP

Done!

New ticket is stored in cache file
/var/krb5/security/creds/krb5cc_<userid>
```

   The ticket refers to a special user id and is only valid for applications run by this user.

4. As the SAP NetWeaver Application Server is run under userid <sidadm, a ticket must be created by this user. Log on to the AIX system as <sid>adm and call *kinit -k <service_principal_name>*. There should now be a ticket in /tmp/krb5cc_<id_of_sidadm> with the id <sid>adm in the name.

5. The ticket is only valid for a defined period of time. You can check this by calling *klist*. Without valid ticket, SSO will not be possible. To ensure that a new ticket is created every several hours, add a cronjob to the crontab that does a *kinit -k <SPN>* in regular time intervals.

Enable SAP NetWeaver Application Server (ABAP) for SNC

The Kerberos client configuration on the host is now completed. Preparing the SAP NetWeaver Application Server for Single Sign On usage is the next step. Therefore,

open a command line window on your Linux/AIX host and log on as <sid>adm. Stop the SAP system with *stopsap* and go to `/sapmnt/<SID>/profile`.

SNC is enabled by adding some parameters into the instance profile of the SAP system (SID_ <workprocesses><instancenr>_<host_name>).
The following four profile parameters must be added to the instance profile with their respective values. For additional SNC instance profile parameters that can be set, see link in the link section.

```
snc/enable                = 1
snc/identity/as           = p:<SPN>@<REALM>
snc/accept_insecure_gui   = 1
```

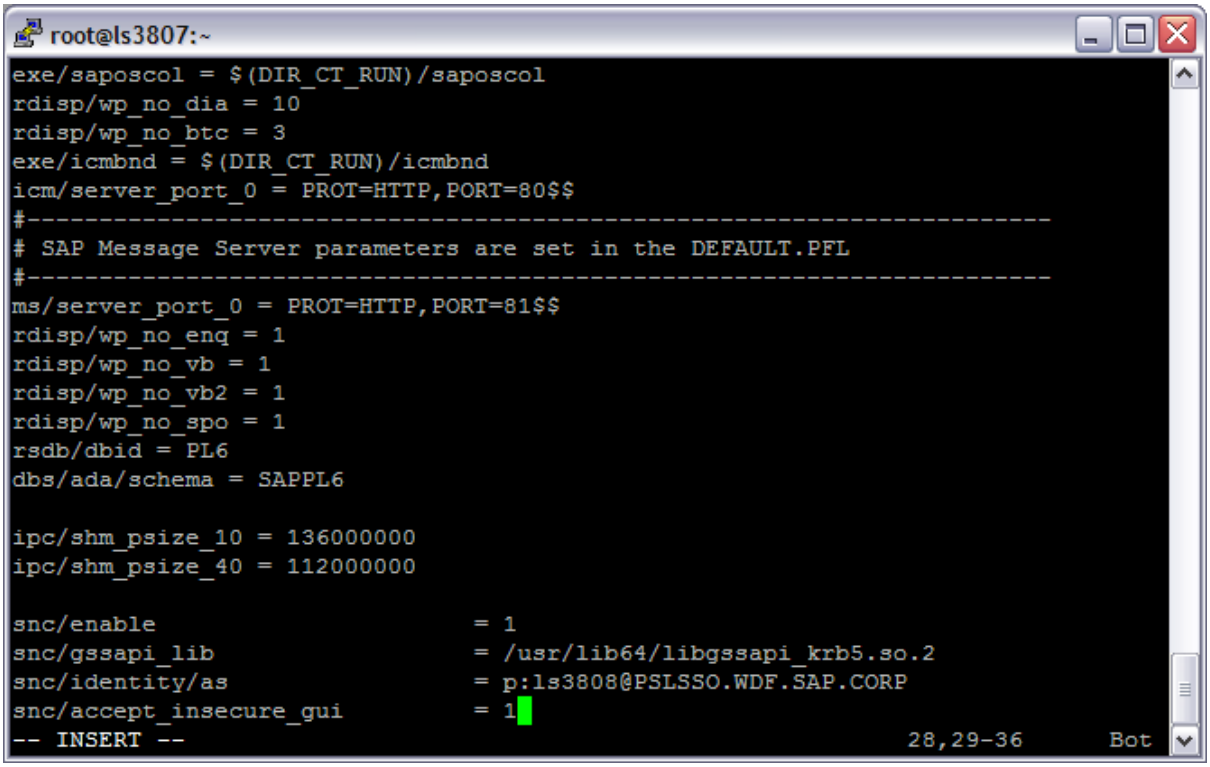
For Linux
```
snc/gssapi_lib            = /<...>/libgssapi_krb5.so
```

For AIX:
```
snc/gssapi_lib            =
/<...>/libgssapi_krb5.a(libgssapi_krb5.a.so)
```

Important for AIX is that the gss library is part of an archive and the shared object must be added in parentheses in the parameter definition of `snc/gssapi_lib.`

snc/enable	„1“ means SNC is activated, “0” disabled
snc/gssapi_lib	Must be set to the path of the gss library, which must be installed as a prerequisite. It is normally found at /usr/lib64/libgssapi_krb5.so.
snc/identity/as	Defines which host identifies itself via which realm. Add the name of the SAP NetWeaver Application Server host and the domain.
snc/accept_insecure_gui	Is login possible only via SSO (“0”) or also per password (“1”) or are only special users like administrators allowed to login with password (“U”)

For the first startup after enabling SNC on the system, use `snc/accept_insecure_gui = 1` because you first need to logon with password and change the user settings to SNC usage. If you start with `snc/accept_insecure_gui = 0,` you will not be able to logon.



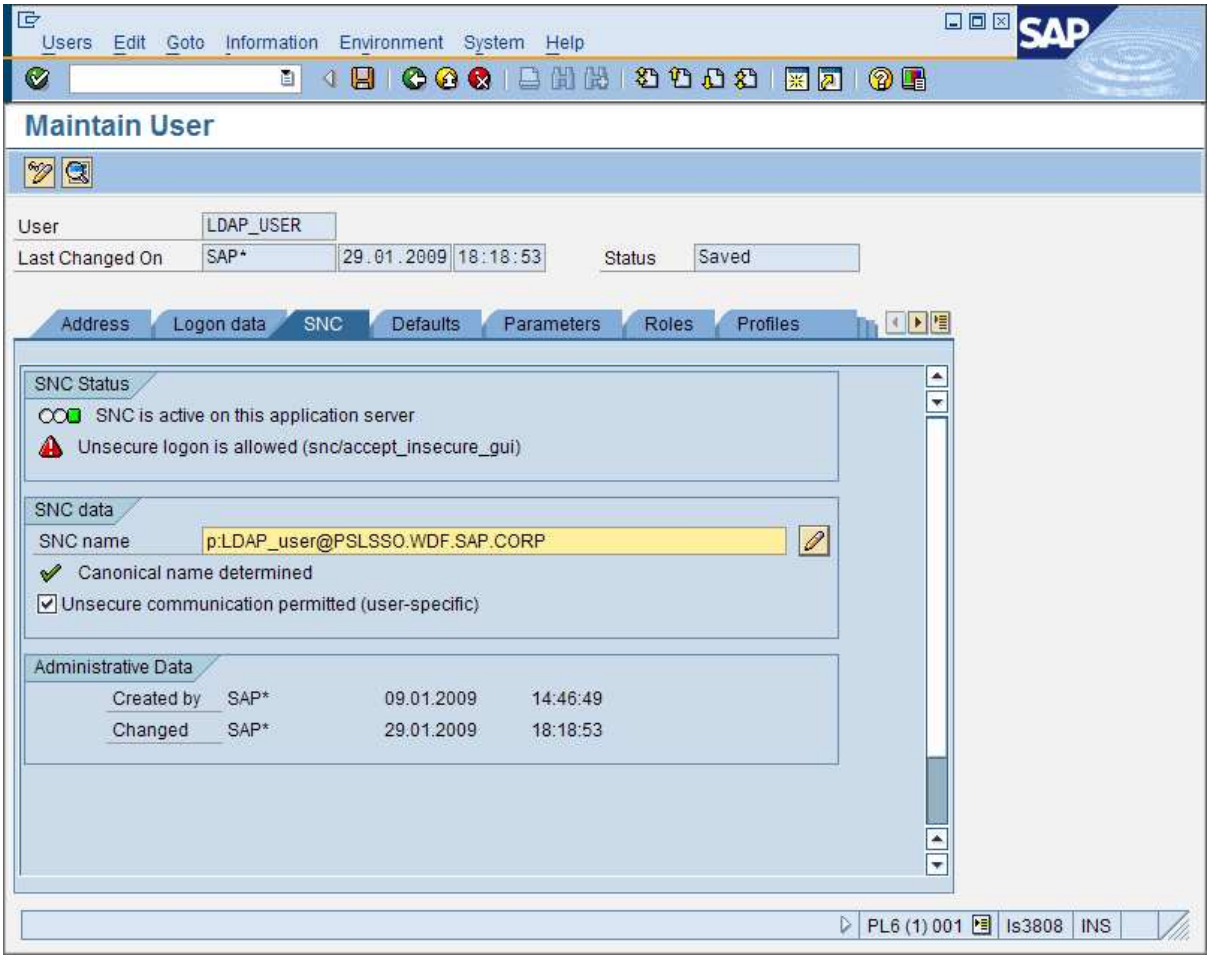
Before the SAP NetWeaver Application Server can be started, the userid <sid>adm needs read access to the kerberos keytab and the configuration file otherwise the system will not start.
Therefore change for Linux the file mode for `/etc/krb5.keytab` and `/etc/krb5.conf` so that <sid>adm can read these files. For AIX the files are `/etc/krb5/krb5.keytab` and `/etc/krb5/krb5.conf`.

Enable SAP user for SNC

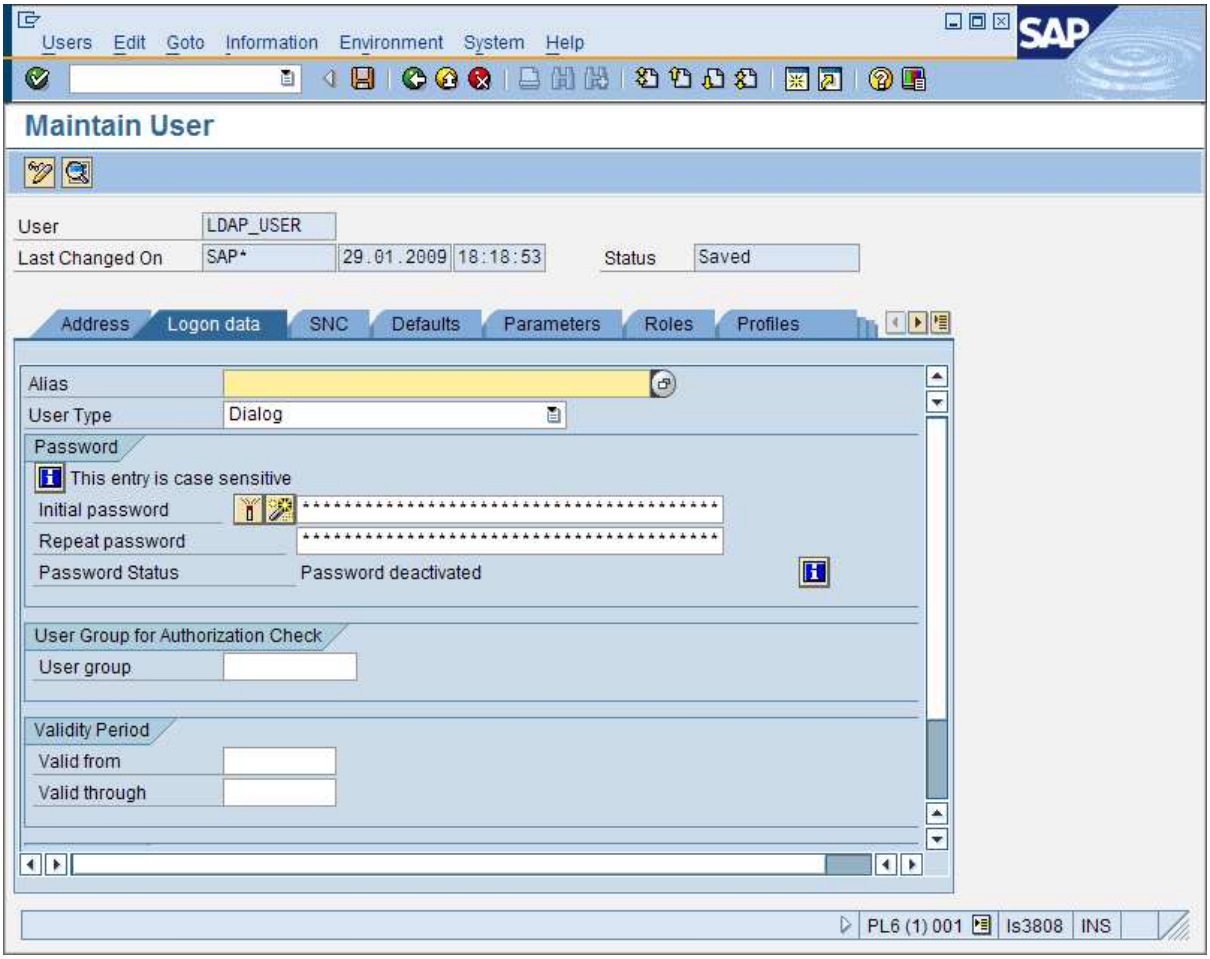
Now it is time to start the SAP instance with *startsap*. The Application Server is already enabled for SSO but the SAP users are not. In order to use SSO, the user properties must be changed to SNC usage.
If the SAP instance does not start, please see the debugging advices in *Error detection/Known problems*.

1. After login to the SAP NetWeaver Application Server as an user with user administration rights, call transaction *su01*.
   Users are client specific so you have to log on to the client to which the user belongs.

2. Change the properties of a user you want to enable for SNC. Go to the *SNC* tab where the necessary SNC settings can be made.



3. Insert "p:<user_name>@<kerberos_realm>" into the field *SNC name*, where <user_name> must be the name of the domain user. After saving the user information you should get the message *Canonical name determined*.



4. Switch to the *Logon data* tab and deactivate the password. The deactivation button is the first one after *Initial Password* in the Password section. After deactivation the Password status will change to *Password deactivated*. The user does not need a password because he will use SSO.

This procedure must be repeated for every user that should use SSO.

Enable Kerberos and SNC on Windows Client

Host and SAP NetWeaver Application Server are already configured to use SNC. What is missing before SSO can be tested is the configuration of the local Windows workstation.

To enable the Windows workstation for Kerberos, a Windows dynamic-link library (DLL) that implements the GSS API and Kerberos is needed. SAP provides a wizard, that is attached to SAP note 595341 *Installation issues with Single Sign-On and SNC*.

1. Log on to the Windows workstation as a user with local administration rights.

2. Download SAPSSO.zip from SAP note 595341 from SAP Service Marketplace and extract SAPSSO.msi.

3. Double click the SAPSSO.msi file and the installation wizard for the DLL will start. Chose *Next* → *Finish*. It takes only some seconds to complete the installation.

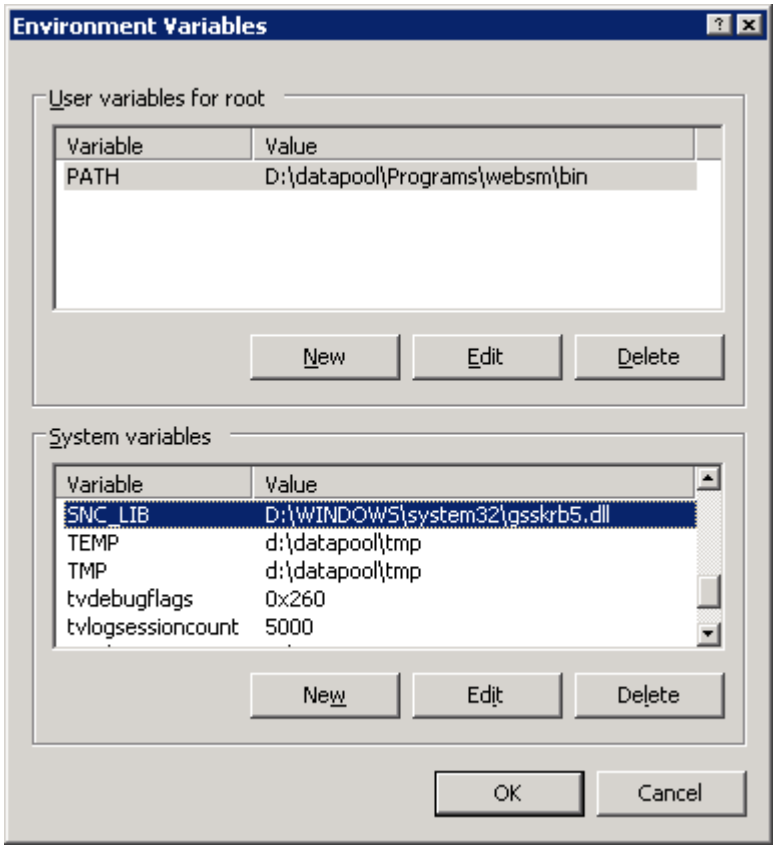
The installation wizard placed the library gsskrb5.dll in the *\WINDOWS\system32* directory, but SAP GUI expects the lib to be named *sncgss32.dll* in the same directory. Therefore the environment variable *SNC_LIB* must be set.

1. On the Windows Workstation, right click *My Computer* and select *Properties* → *Advanced* → *Environment Variables*

2. Under *System Variables,* select *New* and create a new variable with the name *SNC_LIB* and as value the path to the gsskrb5.dll library (e.g. C:\WINDOWS\system32\gsskrb5.dll").

3. Confirm with *OK.*

4. Log off to activate the changes.



The final step is to adjust the system entry of the SAP instance in SAP logon on your local PC. You might need to repeat this for every windows user on this workstation unless you have a centralized configuration for all users.

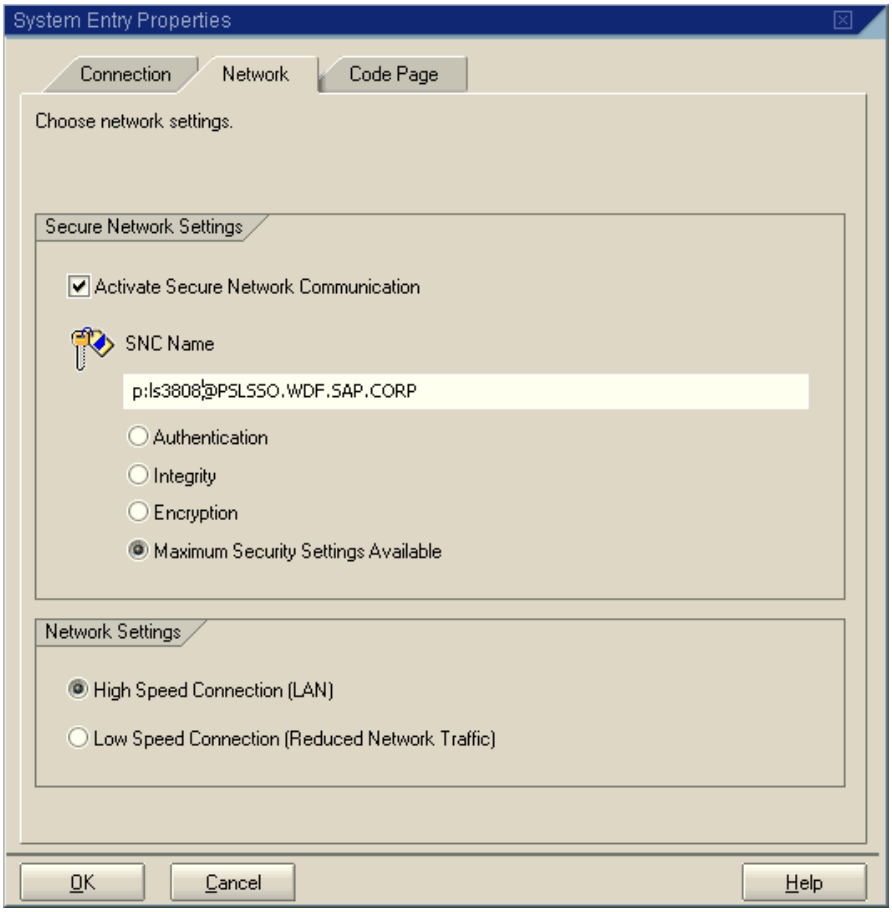
1. Log on again. This time administration rights might not be needed if you do not have a centralized SAP logon configuration for all windows users.

2. Open SAP logon and select the entry of the SAP instance that has now been configured for SSO and select *Change entry*. If the system is not yet defined, a new entry has to be created with *User defined* and the required values must be filled.

3. In the popup window, select *Others.*

4. In the next Window under *Security-Network-Properties* select *Switch on SNC* and put in “p:<SPN>@<REALM>” with maximum security. The service principal name is the name of the host the SAP instance is installed on. The Realm is the Domain name – the same values as given in the keytab.

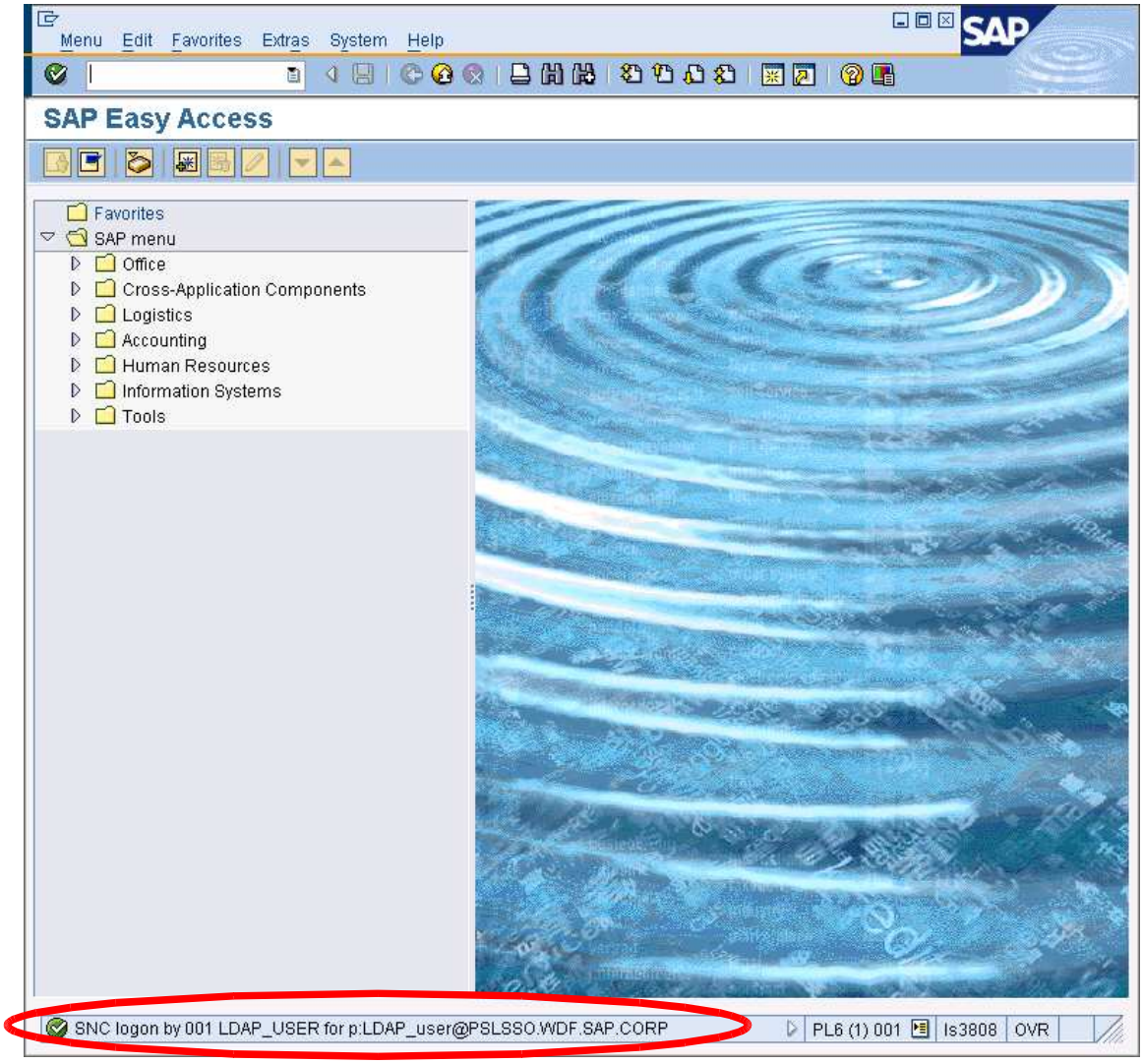
5. Select *Ok* and *Save*.



The installation of the DLL and the adjustment of the system entry must be performed on all workstations where SSO for SAP should be used. SAP logon will automatically use the domain user the user logged on with to authenticate at the SAP NetWeaver Application Server. If the workstation is not part of the domain or the user is a local user without domain membership, the user will still get a password request as long as the SAP instance profile parameter “snc/accept_insecure_gui” is not set to “0”.

Testing SSO

Finally the setup is complete and ready to be tested. If it works as required, you should be able to log on to the SAP NetWeaver Application Server without password submission.
Log on to a Windows workstation as a domain user, open SAP Logon and double click the entry of the SSO enabled SAP system. Instead of being asked for a password, you should now see the *SAP Easy Access* screen.



Note the "SNC logon" entry in the status bar.

Error detection/Known problems

- If you experience problems with gss, there is a small test program by SAP: gsstest, download link is given in SAP note 150380

- After generating a new keytab on the Active Directory server, copy it directly to the Linux/AIX host. Ktpass resets the password and you might experience problems when using the old keytab since the password has been changed because of a newly generated keytab.

- With AIX, it has been the case that kinit places the kerberos tickets in the wrong directory and filename. Instead of /var/krb5/security/creds/krb5cc_<userid>, they are in /home/sidadm/krb5cc_<sidadm>

If you face this problem use kinit -k <SPN> -c FILE:/var/krb5/security/creds/krb5cc_<user_id> instead. The ticket will then be routed to the file you specified for the -c parameter.

- What to do if kinit does not work after copying the keytab to the Linux/AIX host:
  Check if the values in the kerberos client configuration were given correctly.

- What to do if the SAP Systems does not come up after configuring SNC:
  Does the SPN given in the keytab fit to the SNC parameter value in the instance profile?
  Does the sidadm have authorization to read krb5.keytab and krb5.conf?
  Is there a valid ticket, check with *klist*?
  Check the dev traces in `/usr/sap/<SID>/>instance>/work`.

- If *kinit -k* does not work on Windows 2003 with an "incorrect password" error, but *kinit* does, check that your ktpass.exe version is higher than 5.2.3790.4 and visit the following sites:
  http://support.microsoft.com/?scid=kb%3Ben-us%3B939980&x=10&y=12
  http://support.microsoft.com/kb/926027/EN-US/

Links and Resources

- How to configure Kerberos on AIX with config.krb5 (IBM White paper)
  http://www-03.ibm.com/systems/resources/systems_p_os_aix_whitepapers_aix_kerberos2.pdf
- Expanding Single Sign-on for SAP Landscapes on i5/OS® (IBM White paper)
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/5cb5ed706d254a8186256c71006d2e0a/e80c98604a2b52268625738b005e0913/$FILE/sapSsoOnSystemi.pdf
- SAP Notes
  #150380 - Is MIT Kerberos 5 supported for use with SNC?
  #352295 - Microsoft Windows Single Sign-On options
  #595341 - Installation issues with Single Sign-On and SNC
- SNC Instance Profile Parameters

http://help.sap.com/saphelp_nw04/helpdata/EN/19/164442c1a1c353e10000000a1550b0/content.htm

Products used in this paper

Kerberos 5
AIX 5.3
Red Hat Enterprise Linux 5
Novell SuSE Linux Enterprise Server 10
Windows Server 2003 R2

About the author

Cäcilie Hampel is a Software Engineer in the IBM Systems and Technology Group leading the porting team for Linux running on IBM Power Servers at SAP AG, Walldorf. Email: caecilie.hampel@de.ibm.com

Acknowledgements

Thank you to the following reviewers:
Olaf Rutz, Elmar Billen, James Nugen, Walter Orb

Trademarks and special notices

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

IBM, the IBM logo, System p, System i, POWER6, AIX and i5/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both.

SAP, SAP NetWeaver and all other SAP related trademarks are trademarks of SAP AG, in Germany, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

SUSE and SUSE LINUX Enterprise Server are registered trademarks of SUSE LINUX AG, a Novell company.

Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Red Hat and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc.

Kerberos is a trademark of the. Massachusetts Institute of Technology (MIT).

Other company, product, or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.