6.15.3 Mapping SAP System Users to Windows Users for Single Sign-On

Use

When you have configured your system, you can enable SAP system users to log on with Single Sign-On by assigning them to Windows users.

Prerequisites

You have completed the following procedures:

- Preparing the Application Server for Single Sign-On [Page 72]
- Preparing SAP GUI and SAP Logon for Single Sign-On [Page 73]

Procedure

1. Log on to the SAP system.
2. Choose *Tools* → *Administration* → *User Maintenance* → *Users*. Alternatively, enter transaction code SU01.

   The *User Maintenance* window appears.
3. Enter the name of the SAP system user and choose *User names* → *Change*.
4. Choose the *SNC* tab. In the field *SNC name*, enter the name of the Windows user that is to be assigned to the SAP system user in **uppercase**:

   p:<DOMAIN_NAME>\<NT_USERNAME>

   `DOMAIN_NAME>` is the Windows domain that the Windows user belongs to and `<NT_USERNAME>` the Logon ID of the Windows user.

   p: is a prefix that all SNC names require

   For the Windows user `Kissnerj`, belonging to the domain `SAP_ALL`, enter **`p:SAP_ALL\ Kissnerj`**
5. Select *Insecure communication permitted.* This permits the user to still access the system without using the Single Sign-On feature, to work in a different domain.
6. Save the entries.

6.16 Configuration of Kerberos Single Sign-On

Use

With Windows 2000, it is possible to implement Single Sign-On using the Kerberos security protocol. Single Sign-On is a method of logging on to the system that simplifies the authentication process for the user. It allows a user that has logged on to Windows 2000 to access other SAP systems without entering an additional user ID or password. The security context for authentication is made available with the Application Programming Interface (API) and Kerberos. The user simply has to select an SAP system in the SAP logon window, or click on its shortcut, to automatically start the authentication process in the background.

The advantage of the Single Sign-On solution based on Kerberos is that the security information which has to be exchanged between the SAP front end and the SAP application server is encrypted. This encryption is not implemented for the solution available for SAP on Windows that is based on the Generic Security Service API (GSS-API) interface

> When using `gsskrb5.dll`, the Microsoft Kerberos Security Service Provider (SSP) is interoperable with Kerberos implementations from other vendors/suppliers. To use SSO with application servers on Unix and Windows 2000 front ends with `gsskrb5.dll`, you might have to purchase a Kerberos implementation for the Unix machine(s).

Prerequisites

Single Sign-On based on Kerberos can only be set up for users that are members of a Windows 2000 domain.

Activities

To prepare users and systems for the use of Single Sign-On, you have to:

1. Prepare the central instance [Page 76]
2. Configure the SAP front ends [Page 77]
3. Configure the SAP logon [Page 78]
4. Map SAP users to Windows 2000 users [Page 78]

The sections that follow describe these steps in detail.

> In the directory paths specified below, `\%win%\` refers to the location of the Windows 2000 directory.

6.16.1 Preparing the Central Instance

Use

To prepare Single Sign-On, you must adapt the central instance profile and ensure that the necessary Dynamic Link Library (DLL) is located in the Windows 2000 directory.

Procedure

Copy the `gsskrb5.dll` file from the `sapserv<x>` to the following directory on the central instance:

`Drive:\%windir%\system32.`

On the `sapserv<x>` the `gsskrb5.dll` file is located in the directory:

`general/misc/security/gssntlm`

In the instance profile of the central instance, set the SAP parameters

```
snc/enable      = 1
snc/gssapi_lib  =<DRIVE>:\%windir%\system32\gsskrb5.dll
snc/identity/as =p:<SAP_Service_User>@<DOMAIN_NAME>
```

`<DOMAIN_NAME>` is the Windows 2000 domain that the user `<SAP_Service_User>` belongs to, for example, `NT5.SAP-AG.DE.`

> Although you can freely choose the Windows account under which the SAP system runs, it is typically SAPService<SAPSID>.

> If you use a local account for SAPService<SAPSID>, most operations are successful. However, any operations or communications where the SAP system is the initiator of an SNC-protected communication to a remote machine do not work with a local account for SAPService<SAPSID>. Therefore, use a domain account.

Stop and restart the SAP system to enable the profile parameters to take effect.

> The `<DOMAIN_NAME>` and the `<SAP_Service_User>` are case-sensitive.
> Make sure you enter upper and lowercase correctly, for example:
> `p:SAPServiceC11@NT5.SAP-AG.DE.`

6.16.2 Configuring the SAP Front End

Use

To enable a logon with Single Sign-On, you have to configure each SAP front end that is in use.

Procedure

When you prepare the SAP front end for Single Sign-On, you can choose between two approaches:

- Configure each front end individually
- Configure all front ends automatically

Configuring SAP Front Ends Individually

Perform the steps on the machine where the SAP front end is running.

1. Log on to the machine where the SAP front end is running.
2. Copy the `SAPSSO.MSI` program from the `sapserv<x>` directory `general/R3Server/binaries/NT/W2K` to a local directory or to a shared directory on the network.
3. Double-click the `SAPSSO.MSI` file.

   The wizard *SAP Single Sign-On Support for Windows 2000* is started and automatically configures the SAP front end.

Configuring SAP Front Ends Automatically

In the following procedure, you define a *Group Policy* for a Windows 2000 domain. This policy causes the Wizard for configuring Single Sign-On to be started automatically in the background the next time any member of the domain logs on to an SAP fontend.

To define the *Group Policy*:

1. Log on to a front-end machine as domain administrator of the Windows 2000 domain.
2. Copy the program `SAPSSO.MSI` from the `sapserv<x>` directory `general/R3Server/binaries/NT/W2K` to a **shared** directory.
3. From the Windows 2000 menu choose *Start* → *Programs* → *Administrative tools* → *Active Directory Users and Computers.*

   The dialog box *Active Directory Users and Computers* appears.
4. Select the domain for which you want to set up Single Sign-On. Right-click and choose *Properties* from the context menu.

   The dialog box *<Domain_Name> Properties* appears.

5. On the *Group Policy* tab, choose *New* to access the dialog box for creating a new policy object.
6. Under *Group Policy Object Links*, enter a name for the new policy object, for example, SAPSSO. Choose *Edit* to define the contents of the policy.
7. In the *Group Policy Editor* choose *User Configuration* → *Software Settings* → *Software Installation.*

   The *Deploy Software* dialog box opens.
8. Right-click and choose *New* → *Package* from the context menu.

   The *Open* dialog box appears.
9. Select the file `SAPMSSO.MSI` from the shared location. Specify the path with the UNC name (`\\<hostname>\<share>`).
10. Select *Assign* and confirm with *OK*.

You have now created a new *Group Policy.* The next time any user logs on to the domain with the SAP front end, the wizard *SAP Single Sign-On Support for Windows 2000* is started and automatically prepares the front end for Single Sign-On.

6.16.3 Activating Single Sign-On for the SAP Logon

Use

The Logon option for Single Sign-On must be activated for each SAP front end.

Procedure

The SAP Logon dialog box includes a list of systems or machines that you can log on to. For each of the systems or machines in the list for which you want to implement Single Sign-On, proceed as follows:

1. Select an entry and choose *Properties* → *Advanced*.
2. Select *Enable Secure Network Communications*.
3. In the *SNC name* field, enter:

   `p:<SAP_Service_User>@<DOMAIN_NAME>`

   where `<DOMAIN_NAME>` is, for example, `NT5.SAP-AG.DE`.

   > Enter the same string that you entered in the central instance profile for `snc/identity/as`
   > If the system *C11* is running on account `SAPServiceC11` of the domain `NT5.SAP-AG.DE`, you would enter:
   > **`P:SAPServiceC11@NT5.SAP-AG.DE`**

   > If the entry you selected in the logon dialog box is a group entry, for example, *C11 (PUBLIC)*, the *SNC name* field is already filled out.
4. Confirm your entries with *OK*.

The SAP Logon window now displays an icon with a key beside the system entry. This indicates that Single Sign-On is active for the system in question.

6.16.4 Mapping SAP Users to Windows 2000 Users

Use

When you have configured your system, you can authorize SAP users to log on with Single Sign-On by assigning them to Windows 2000 users.

Procedure

1. Log on to the SAP system as administrator.
2. Choose *Tools* → *Administration* → *Maintain Users* → *Users*.
   Alternatively, enter transaction code SU01.

   The *User Maintenance* window appears.
3. Enter the name of the SAP user and choose *User names* → *Change.*
4. Choose the *SNC* tab. In the *SNC name* field, enter the name of the Windows 2000 user that is to be assigned to the SAP user in uppercase:

   `p:<WINNT_USERNAME>@<DOMAIN_NAME>`

   Where `<WINNT_USERNAME>` is the Logon ID of the Windows 2000 user and `<DOMAIN_NAME>` the Windows 2000 domain the user is logged on to.

   For the user Kissnerj, belonging to the domain `NT5.SAP-AG.DE` , enter
   `p:kissnerj@NT5.SAP-AG.DE`
5. Select *Insecure communication permitted.* This permits the user to still access the system without using the Single Sign-On feature, to work in a different domain.
6. Save the entries.

You have now completed the process of setting up Single Sign-On.

6.17 Client Copy

Perform the client copy:

The client copy consists of the following procedures:

Maintenance of the client (transaction SCC4).

Copy of the client (local – transaction SCCL).

Copy of the log files (transaction SCC3).

For instructions on how to perform the client copy, see the SAP Library:

Choose *Help* → *SAP Library* in your SAP system.

Choose mySAP Technology Components → SAP Web Application Server → *Change and Transport System* → *Client Copy and Transport*

Alternatively you can access the SAP Library at **`http://help.sap.com`**:

Choose SAP Web Application Server → SAP Web Application Server 6.20.

Select the required language.

Choose mySAP Technology Components → SAP Web Application Server → *Change and Transport System* → *Client Copy and Transport*.