

Experience on Single-Sign-On-Test with UNIX Backend and SAS 9.3

AMOS / Bigalke Jan
System architect

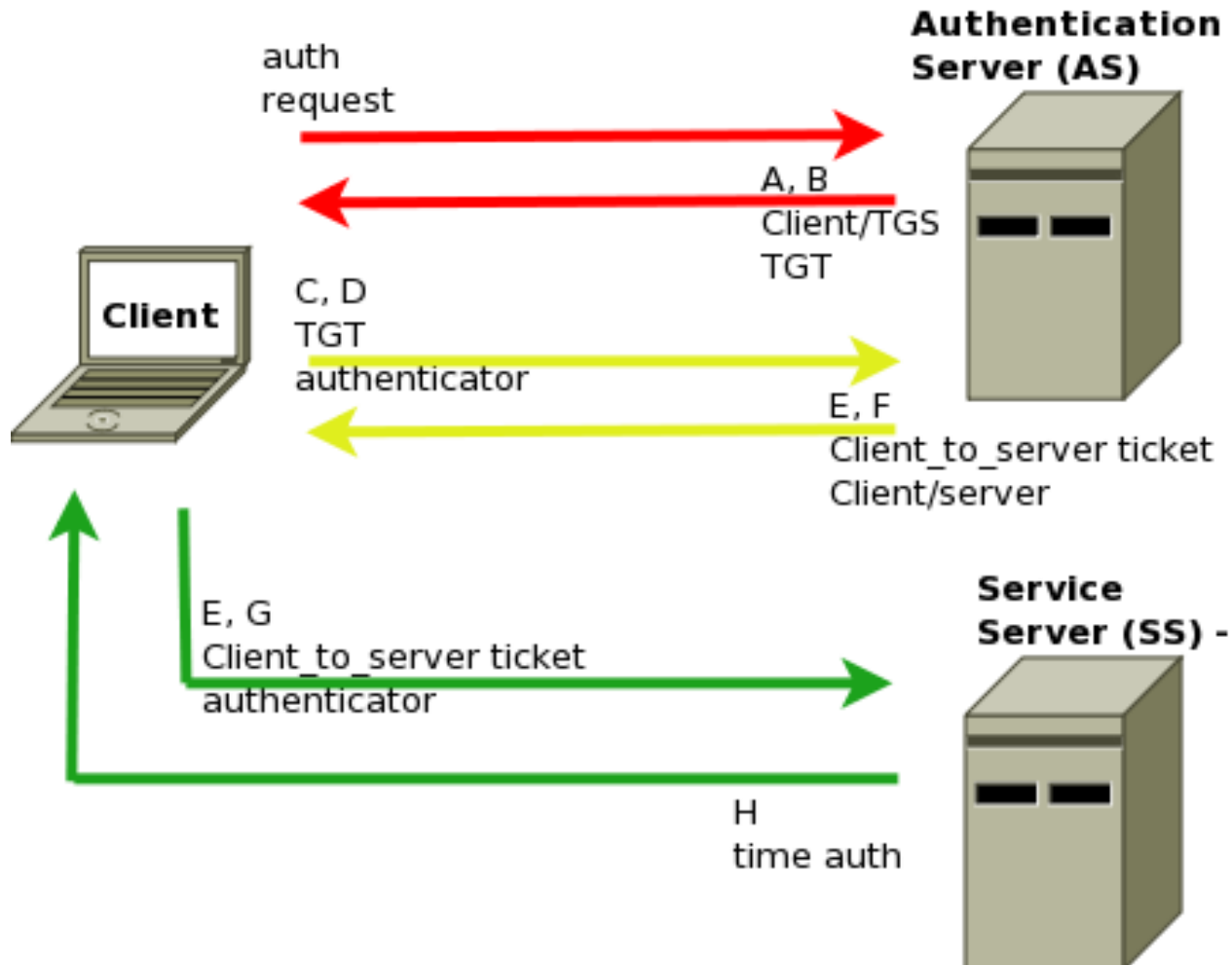
1

- 1 Introduction**
- 2 SAS Components
- 3 SSO Web
- 4 SSO Clients

Introduction SSO

- Single Sign-on
 - One authentication, then access to the services (applications)
- technologies:
 - Kerberos
 - Smart card
 - ...
- SAS: Integrated Windows Authentication
 - SPNEGO, Kerberos,...

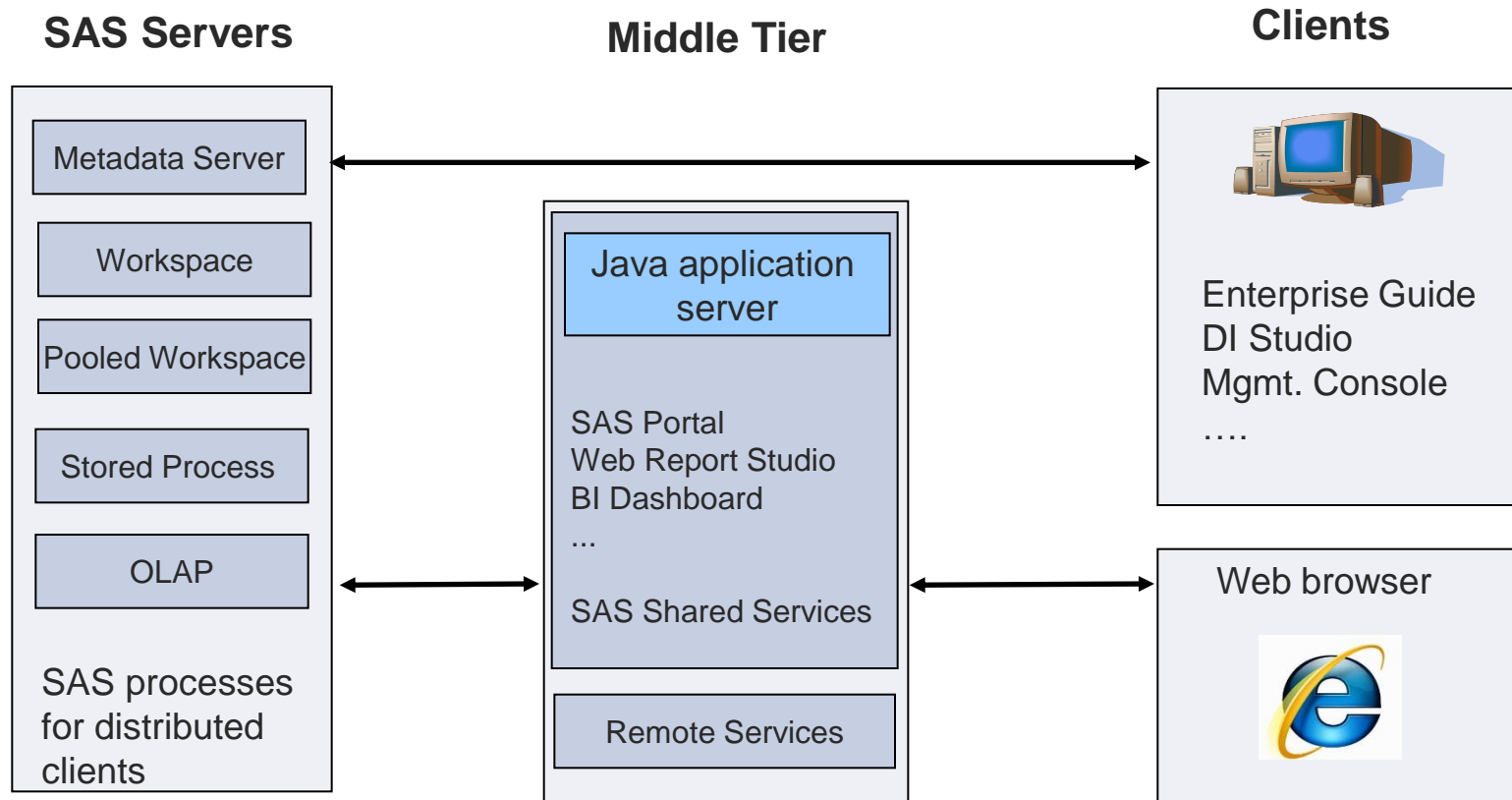
Kerberos (protocol)



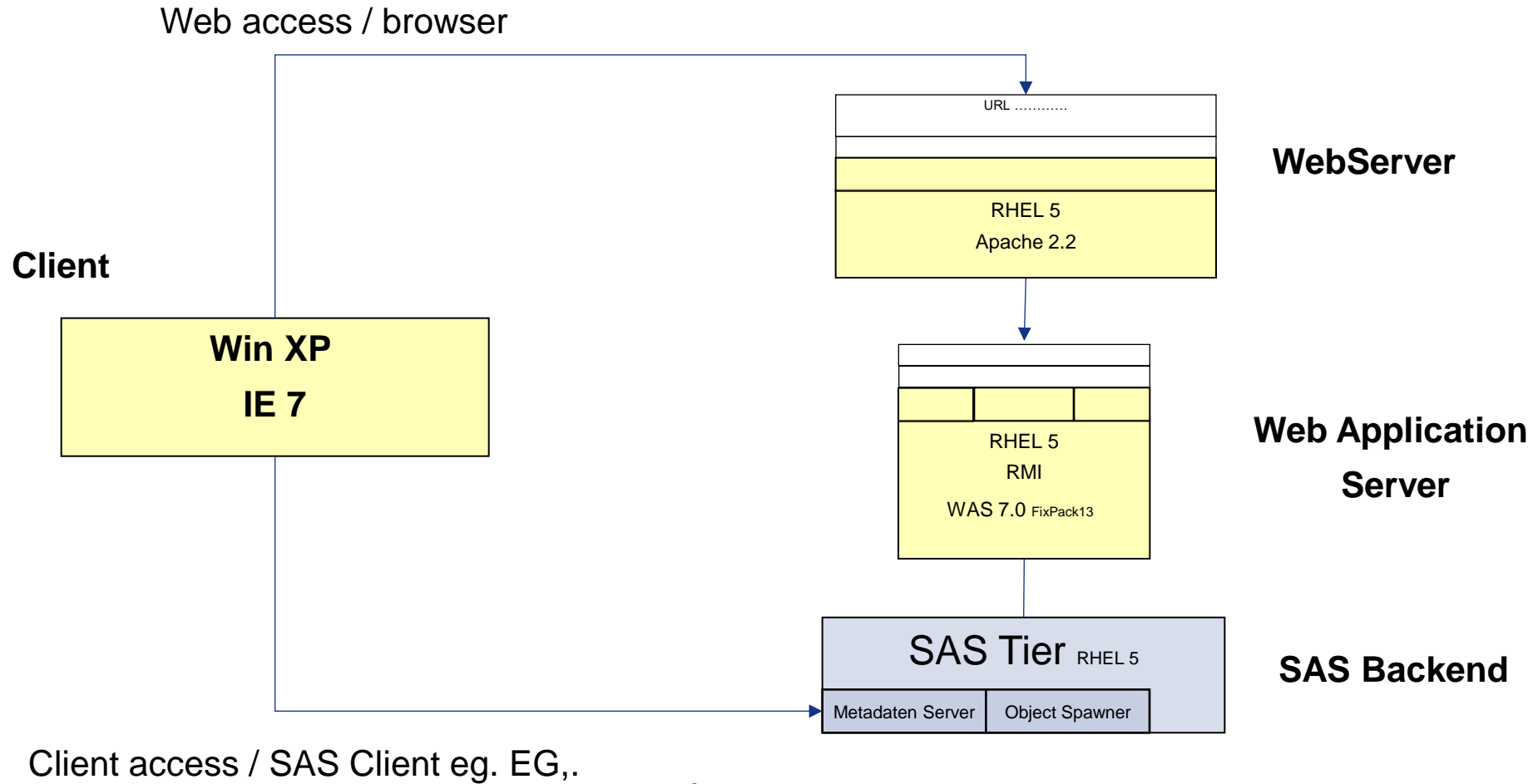
2

- 1 Status
- 2 SAS components**
- 3 SSO Web
- 4 SSO Clients

SAS components



- authentication for client applications
- authentication for web access



3

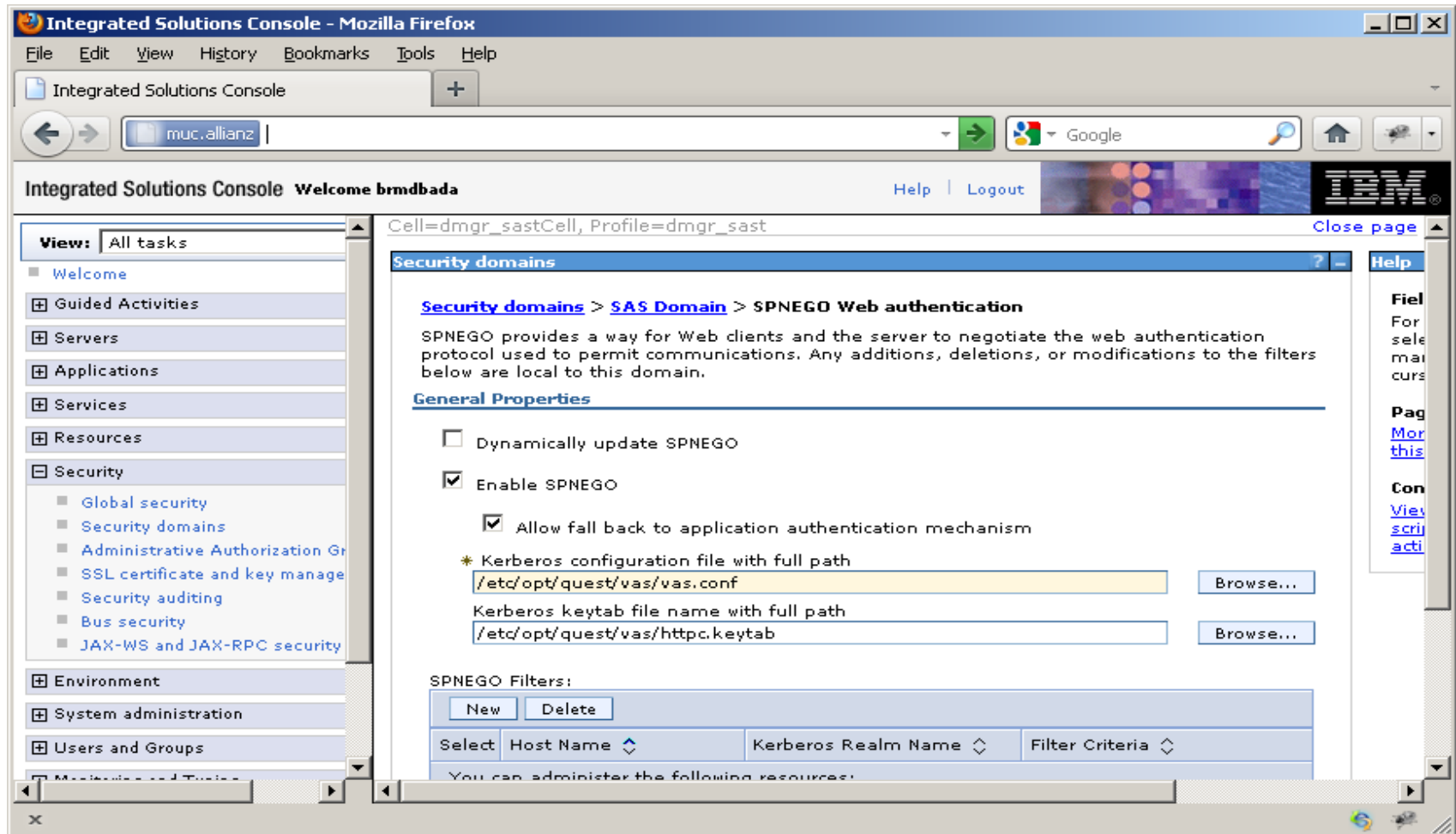
- 1 Status
- 2 SAS components
- 3 SSO Web**
- 4 SSO SAS

Kerberos and Web Access

- base is web authentication
 - Authentication outside from SAS
 - Only authorization is done from SAS, no physical user on the SAS server needed
- Configure Kerberos
 - Create a SPN (Service Principal Name) -> Keytab File
- Configure the application Server
 - SPNEGO Negotiate the authentication protocol
 - Kerberos configuration
- Web browser configuration
 - enable SPNEGO

-> SSO for Web access (also possible with SAS 9,2)

Sample Configuration



Integrated Solutions Console - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Integrated Solutions Console

muc.allianz

Integrated Solutions Console Welcome brmdbada Help Logout

Cell=dmgr_sastCell, Profile=dmgr_sast

Security domains

[Security domains](#) > [SAS Domain](#) > **SPNEGO Web authentication**

SPNEGO provides a way for Web clients and the server to negotiate the web authentication protocol used to permit communications. Any additions, deletions, or modifications to the filters below are local to this domain.

General Properties

☐ Dynamically update SPNEGO

☒ Enable SPNEGO

☒ Allow fall back to application authentication mechanism

* Kerberos configuration file with full path

Kerberos keytab file name with full path

SPNEGO Filters:

Select	Host Name	Kerberos Realm Name	Filter Criteria
You can administer the following resources:			

4

- 1 Introduction
- 2 SAS components
- 3 SSO web
- 4 SSO clients**

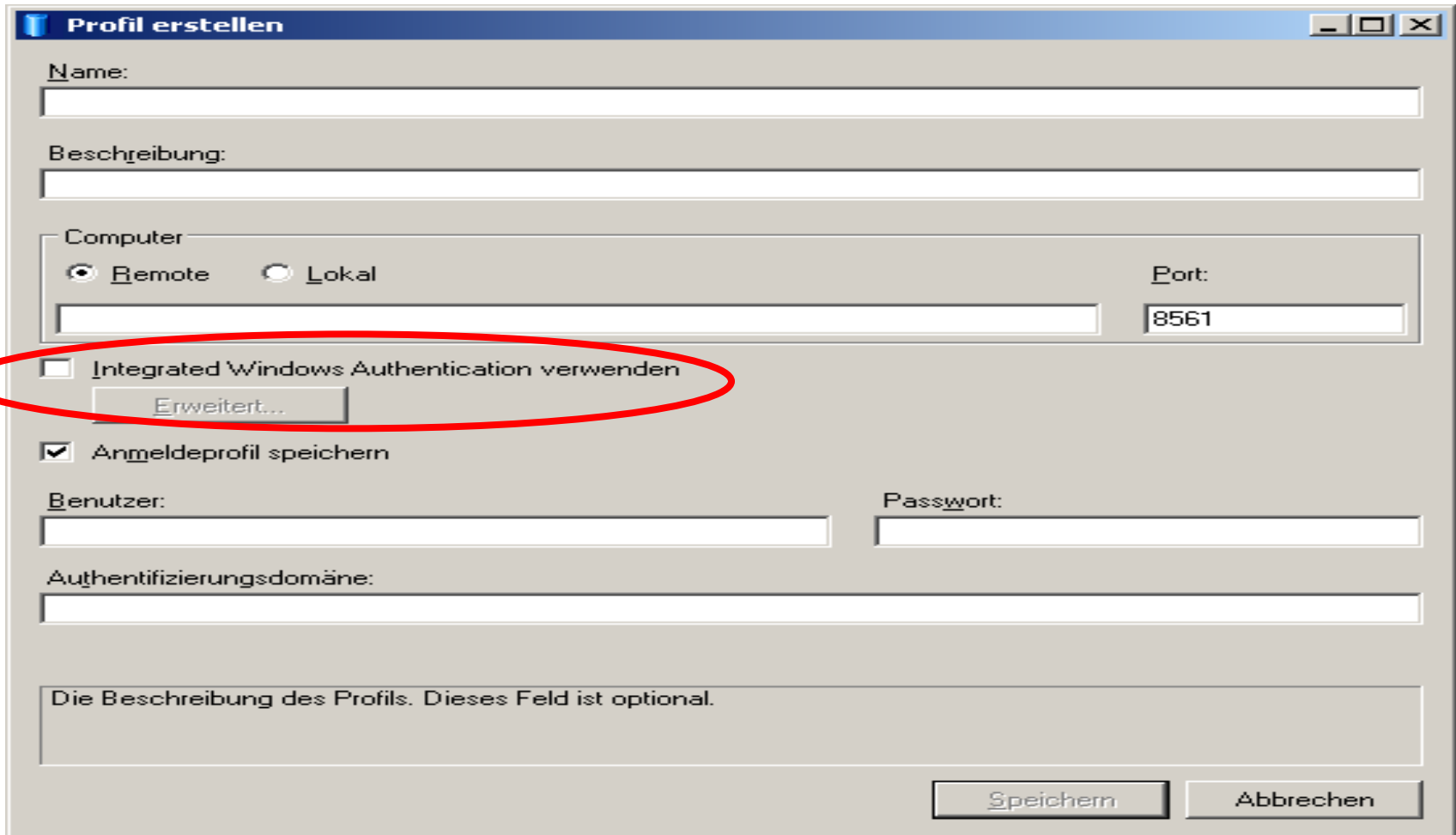
Kerberos SAS using Quest Authentication Services

- SAS use Quest Authentication Services
 - No native support of the operating system Kerberos implementation
 - Version 4 required
 - Active directory configuration necessary
- Quest Authentication Services
 - deep integration of UNIX systems into active directories
 - Supports Linux, Solaris, AIX, HP-UX, OS X ,...
- Install and configure Quest Authentication Services
 - Install Quest authentication Services and configure
 - Quest (join Domain,....)

Kerberos SAS using Quest Authentication Services

- Configure Quest for SAS
 - Create a SPN (Service Principal Name) and keytab for sas
 - Quest Libs into the Path (SAS is using the Quest API)
 - Test the config with Quest test pack
- Configure SAS for Kerberos
 - Create entry /etc/pam.d/sasauth
 - /.../utilities/bin/sasauth.conf set to pam
 - Publish the quest config to sas in /.../Lev1/level_env.sh
 - KRB5_KTNAME=/etc/opt/quest/vas/SAS.keytab
 - export KRB5_KTNAME
 - Restart the SAS servers
- -> Test

Config the Clients eg. Enterprise Guide



Profil erstellen

Name:

Beschreibung:

Computer

☒ Remote ☐ Lokal

Port:

☐ Integrated Windows Authentication verwenden

☒ Anmeldeprofil speichern

Benutzer:

Passwort:

Authentifizierungsdomäne:

Die Beschreibung des Profils. Dieses Feld ist optional.

END