Paper SAS3443-2016

Kerberos Delegation with SAS® 9.4

Stuart J Rogers, SAS Institute Inc., Cary, NC

ABSTRACT

Do you want to see and experience how to configure SAS® Enterprise Miner™ single sign-on? Are you looking to explore setting up Integrated Windows Authentication with SAS® Visual Analytics? This hands-on workshop demonstrates how you can configure Kerberos delegation with SAS® 9.4. You see how to validate the prerequisites, make the configuration changes, and use the applications. By the end of this paper, which is also being presented as a workshop, you will be empowered to start your own configuration.

INTRODUCTION

Integrated Windows Authentication for SAS® 9.4 gives the end user access to SAS client applications without entering a user name and password. This means that no user name and password are transmitted across the network from the client machine to the SAS servers.

SAS 9.4 has a three-tier architecture. There is the client tier where a mixture of Java clients, .Net clients, and browser clients run. This client tier either directly connects to the SAS server tier or connects to the SAS middle-tier and submits code that is then run on the server tier. We want the configuration to enable the delegation of the end-user credentials from the client machine all the way through to the back-end SAS processing and possibly onto the data source, as shown in Figure 1. We want code running on the server tier to run as the end user and not as a service account.

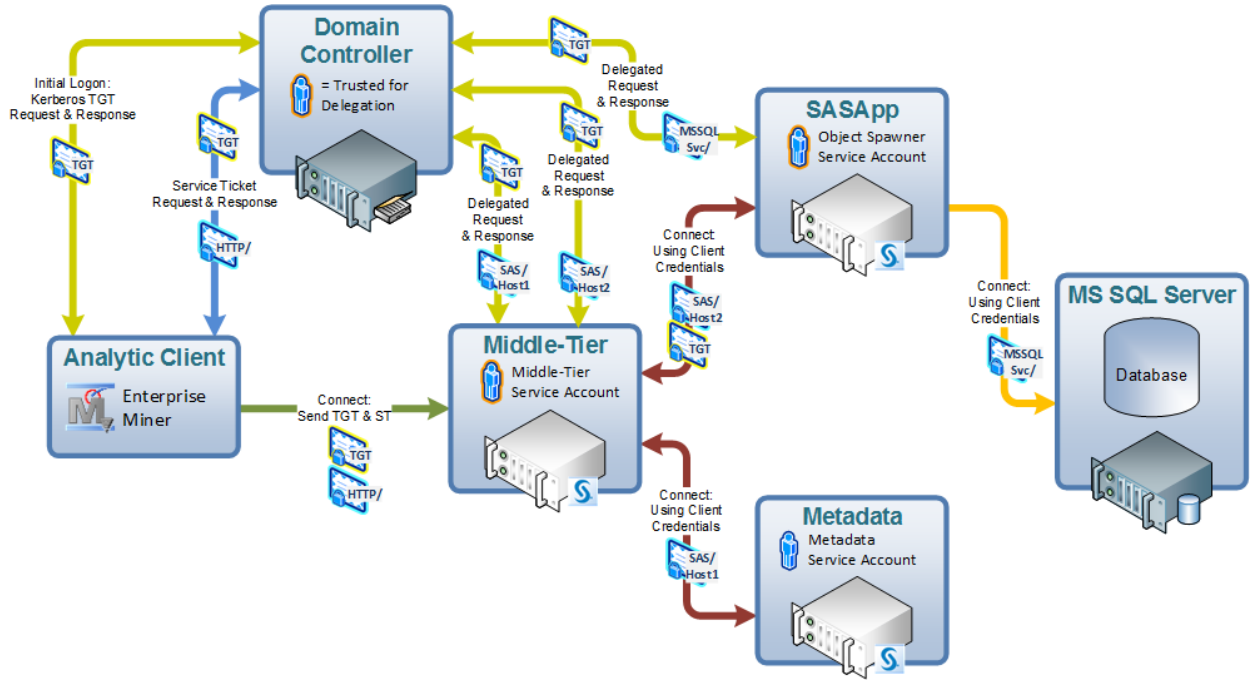

Figure 1. Example of Kerberos Delegation

Enabling Integrated Windows authentication means using Kerberos authentication for the SAS client application. Kerberos authentication is based on the use of Kerberos tickets that represent the password of the end user. See the paper "Kerberos and SAS 9.4: A Three-Headed Solution for Authentication" (Rogers, 2013) for a more through explanation of how Kerberos works. For the configuration of the SAS

environment we need to consider each of the tiers within the architecture. The configuration requires that both the middle-tier and server tier are able to process these Kerberos tickets. The configuration of the server tier and middle-tier are different. The configuration of the server tier is dependent on the operating system, while the configuration of the middle-tier is independent of the operating system.

The aim of the configuration of Kerberos delegation is to allow you to launch a process on the server tier under the end user's identity--without having to either store passwords in the SAS metadata or transmit passwords across the network.

PREREQUISITES

Configuration of Integrated Windows Authentication involves tightly integrating the SAS environment into an Active Directory Domain. Such integration requires a number of prerequisites that must be complete before the configuration will work. The prerequisites for each tier within the architecture are similar, but there are some key differences. The dependence of the server tier on the operating system means there are different prerequisites for Windows, Linux, or UNIX server tiers. In this paper we will focus on Windows and Linux; for details about UNIX servers, see *Configuration Guide for SAS 9.4 Foundation for UNIX Environments*.

SAS IOM SERVERS ON WINDOWS

SAS Integrated Object Model (IOM) Servers include the SAS® Metadata Server, SAS® Object Spawner, SAS® Workspace Server, SAS® Pooled Workspace Server, and SAS® Stored Process Server. The configuration of Kerberos authentication for Windows servers is quite straightforward. In many circumstances the configuration can be completed automatically, and as such there are very few prerequisites. However, some topologies will require more manual configuration and hence more prerequisites.

Windows Simple Topologies

SAS 9.4 topologies with a single SAS Metadata Server and a single SAS Workspace Server are simple topologies. The SAS Metadata Server could be running on the same host as the SAS Workspace Server or on a separate host. In this case the SAS servers will automatically register themselves, against the computer object, with Active Directory for Kerberos authentication. As such, there are no additional prerequisites for the configuration of Kerberos authentication.

Windows Advanced Topologies

SAS 9.4 supports clustering for the SAS Metadata Server. Clustering the SAS Metadata Server is an advanced topology. The clustered SAS Metadata Server must be run as a service account, and as such cannot automatically register the cluster members with Active Directory. For the service account running the SAS Metadata Server cluster members, the service principals for each cluster member must be manually registered against the service account; examples of how you can do this are given in the next section of the paper. A separate service account can be used for each cluster member, but this is not required.

SAS IOM SERVERS ON LINUX

The configuration of Integrated Windows Authentication relies upon tightly integrating the SAS servers and clients with Active Directory and the client desktop. With the second maintenance release of SAS 9.4, more options for integrating SAS IOM Servers on Linux with Active Directory are available.

With SAS IOM Servers on Linux either the third-party tool Quest Authentication Services can be used, or other third-party tools, such as Centrify Server Suite, or Operating System provided shared libraries can be used to integrate with Active Directory. Specifically, for releases after the second maintenance release for SAS 9.4 on Linux platforms, you must ensure that a shared library that implements the GSSAPI with Kerberos 5 extensions is installed and configured to allow authentication against the Active Directory domain or Kerberos realm.

This paper will focus on using the operating system-provided shared libraries to enable Integrated Windows Authentication for the third maintenance release of SAS 9.4.

OS Shared Libraries

A shared library is a library that is loaded by a program when that program starts. In the context of providing Kerberos authentication we need a library that implements the Generic Security Services Application Program Interface (GSSAPI). With Red Hat Enterprise Linux (RHEL), this would be from the krb5-libs package, while on SUSE this would be from the krb5 package. To run any of the Kerberos client applications such as kinit for testing, either the krb5-workstation package on RHEL or the krb5-client package on SUSE is required. Putting this together a system administrator on RHEL would install the packages with the following command:

```
yum install krb5-libs krb5-workstation
```

By contrast, a system administrator on SUSE would install the packages with the following command:

```
zypper install krb5 krb5-client
```

Both Red Hat Enterprise Linux (RHEL) and SUSE use MIT Kerberos based shared libraries. There is a known issue with certain versions of these libraries. The bug was introduced in version 1.10, resolved in version 1.12.2, and then the resolution was back-ported to the 1.10.3 branch. For RHEL, version 6.5 of the operating system contains the bug, while version 6.6 of the operating system contains the fix. Specifically, version 1.10.3-33 available with RHEL 6.6 is known to work correctly. Any version greater than 1.10.3-23 will have the fix incorporated. A system administrator can use the following command to verify the version of the shared libraries installed on the system:

```
rpm -q krb5-libs
```

RHEL 6.6 Issue

Red Hat 6.6 does not complete all the steps necessary to make the shared library available to the Linux system. The SAS server processes expect to find the shared library in /usr/lib. However, the Red Hat YUM tool does not create the required symbolic link. The system administrator can create the required symbolic link by running first the following command:

```
ln -s /lib64/libgssapi_krb5.so.2 /usr/lib/libgssapi_krb5.so
```

And then by running this command:

```
ldconfig
```

POSIX User Attributes

The SAS Workspace Server will run as the user authenticated by Kerberos. As such, to run a process on the Linux server the user must have valid POSIX user attributes. The POSIX user attributes are UID, GID, home directory, and shell. There are multiple mechanisms to provide the POSIX user attributes; they can be stored in Active Directory or an LDAP server and retrieved using Winbind or System Security Services Daemon (SSSD). Or the POSIX user attributes can be dynamically mapped using SSSD on Linux. The provision of POSIX user attributes relies on the configuration of Pluggable Authentication Modules, which will be covered in more detail below.

Red Hat has published materials on Integrating Red Hat Enterprise Linux with Active Directory. The first deals with RHEL 6 (Red Hat, 2014), while a presentation from the Red Hat summit provides details about RHEL 7 and future direction (Heslin & Pal. 2014).

The System Security Services Daemon (SSSD) presents one of the most straightforward mechanisms for providing POSIX user attributes. SSSD can either return the values from one or more different directory servers or use mapping algorithms to generate UID and GID values based on Active Directory Security

Identifies (SID) values. Configuring SSSD with the AD provider will enable Kerberos authentication as well as the provision of POSIX user attributes.

The POSIX user attributes for a given domain user can be validated using the getent command. The following command will return the user name, UID, GID, name, home directory, and shell for the given user account.

```
getent passwd domainUser
```

The getent command above is shown with the following parameters:

- passwd: directs getent to show the type of information usually found in a UNIX /etc/passwd file.
- domainUser: substitute this with the specific user account you want the attributes for. If no user account is given, then getent will show attributes for all users.

This will produce output similar to the following:

```
domainUser:*:2129800419:3440:domain User:/home/domainUser:/bin/bash
```

PAM Configuration

PAM stands for Pluggable Authentication Module and is a common UNIX authentication API. A PAM module provides a PAM implementation. PAM modules can be stacked together to allow a single UNIX host to authenticate using several back-end authentication providers. There are multiple PAM modules available to integrate a Linux system with Active Directory.

As stated above, a preferred mechanism for configuring the integration of a Linux system with Active Directory is using the System Security Services Daemon (SSSD). Correctly implementing SSSD will update the PAM configuration settings in the /etc/pam.d directory. For SAS IOM Servers a /etc/pam.d/sasauth file must exist defining the PAM modules used by SAS. As a best practice this /etc/pam.d/sasauth file can be a symbolic link to the /etc/pam.d/password-auth-ac file.

Active Directory Accounts

A number of Active Directory accounts are required for the configuration of Integrated Windows Authentication with SAS IOM Servers on Linux. There are two types of accounts that may be created within Active Directory: computer accounts represent the actual Linux servers and user accounts represent the SAS IOM Server processes.

Computer Accounts

A Computer Account represents the host in Active Directory. The Computer Account is created as part of "joining" a host to Active Directory. The use of the Computer Account, while not required for IWA with SAS, will enable features beyond SAS, such as SSH using GSSAPI and Kerberos as well as PAM integration enabling user name and password logon.

User Accounts

Service Accounts are similar to standard user accounts but are typically reserved to run services or daemons. The Service Accounts represent the SAS IOM services in Active Directory. Ideally these Service Accounts will be excluded from regular password change policies. Changing the password will require regeneration of any Kerberos Keytabs used by the SAS IOM Services.

There is a choice as to either using one user account per service or link multiple services to one account. While having multiple services linked to one account can simplify the management of the environment, it will mean that any security breach of this account impacts all the services. As such, many organizations will require a separate user account per service.

The User Principal Name (UPN) is used to uniquely identify a user in Active Directory. The UPN will be used when connecting back to Active Directory. Depending on the mechanism used to register Service

Principal Names, the UPN might not be the standard user name of the Service Account. If you are logged in to Windows with a Service Account, you can use the following command to find out the UPN:

```
whoami /UPN
```

Alternatively, from within Active Directory Users and Computers, select View ⇨ Advanced Features, and open properties for Service Account. Then use the Attribute Editor tab and view the value of the UserPrincipalName attribute.

Table 1 provides examples of how the SAS Service Accounts can be configured:

SAS IOM Server	User Name	User Logon Name	User Logon Name (pre-Windows 2000)	User Principal Name
SAS Metadata Server	hostname1-SAS	SAS/hostname1	Domain/ hostname1-SAS	SAS/hostname1@REALM
SAS Object Spawner	hostname2-SAS	SAS/hostname2	Domain/ hostname2-SAS	SAS/hostname2@REALM

Table 1. SAS Server on Linux Suggested Service Accounts – Active Directory Attributes

Service Principal Names

Service Principal Names (SPN) must be registered in Active Directory against some entity for each service class. Each instance of an SPN must be unique. Multiple SPNs can be registered against a single account object. The default form of an SPN is <ServiceClass>/<hostname>, where the service class is simply a standardized label and the host name should reflect the host names used by clients to connect to the service. If DNS Aliases are used, then the DNS Aliases should be used in the SPN.

The default Service Class agreed upon for SAS IOM Servers is “SAS”. Therefore, the SPNs registered for SAS will be SAS/<hostname> and will be registered against the service account. The Service Class for Secure Socket Shell (SSH) is “host”. The SPNs registered for SSH will be host/<hostname> and will be registered against the computer object. Table 2 summarizes the SPNs that you must register.

AD Object	Name	SPN 1	SPN 2
Computer Account	hostname1	host/hostname1.domain.com	host/hostname1
Computer Account	hostname2	host/hostname2.domain.com	host/hostname2
Service Account	hostname1-SAS	SAS/hostname1.domain.com	SAS/hostname1
Service Account	hostname2-SAS	SAS/hostname2.domain.com	SAS/hostname2

Table 2. SAS Servers on Linux Service Principal Names

There are multiple methods that can be used to register SPNs:

- Interactively using the “Active Directory Users and Computers” GUI
- Manually using the “setspn” Windows command-line tool
- Manually using the “ldapmodify” Linux command-line tool

For all methods, the user making the change must have sufficient permissions in Active Directory to write changes to the user or computer object. This often requires domain administrator privileges, which are typically granted only to a few individuals within an organization.

Register SPN with GUI

Registering a Service Principal Name with Windows GUI requires access to the Attribute Editor tab. To enable the Attribute Editor tab, select "Advanced Features" under the View menu of the Active Directory Users and Computers tool. On the Service Account or Computer Account, select the Attribute Editor tab, scroll through attributes to servicePrincipalName and select Edit. Multiple entries can be added, edited, or deleted from within the GUI.

Register SPN with Windows Command-Line

Registering a Service Principal Name with Windows Command-Line means using the setspn command. The setspn command reads, modifies, and deletes the Service Principal Names (SPN) directory property for an Active Directory account (https://technet.microsoft.com/en-us/library/cc731241.aspx). To add an SPN use this command:

```
setspn -s service/hostname account
```

For example, to register both the fully qualified host name and short name use this command:

```
setspn -s SAS/hostname1.domain.com hostname1-SAS
setspn -s SAS/hostname1 hostname1-SAS
```

Older versions of the setspn command used "–a" to add an SPN to an account. Microsoft now recommends using "-s" since this now adds the SPN only after verifying that no duplicates exist.

Register SPN with Linux Command-Line

Registering a Service Principal Name with Linux Command-Line means using the ldapmodify command. The ldapmodify command is part of the Open LDAP Client Tools. On RHEL as root you need to run the following command to install these tools

```
yum install openldap-clients.x86_64
```

While on SUSE as root you need to run the following command to install these tools:

```
zypper install openldap2-client
```

The ldapmodify command will take input in LDIF format and apply the changes. More details about the ldapmodify command can be found here: http://www.zytrax.com/books/ldap/ch14/#ldapadd. Here is an example command to run the ldapmodify tool authenticating using Kerberos to Active Directory:

```
ldapmodify -v -Y GSSAPI -H ldap://ldap.server.com -f /tmp/UserMod.ldif
```

The example LDIF file might contain the following:

```
dn: CN=hostname1-SAS,OU=ServiceAccts,DC=domain,DC=com
changetype: modify
replace: servicePrincipalName
servicePrincipalName: SAS/hostname1.domain.com
servicePrincipalName: SAS/hostname1
```

Kerberos Keytabs

The Kerberos Keytab contains the credentials for the Active Directory object for which it is created. The keytab is used by Server processes to connect back to Active Directory. As such the keytab must be secured so that only the expected process is able to read the file. The Kerberos Keytab for the SAS Service Account should contain the following:

- The User Principal Name
- The Service Principal Names

- All available encryption types

There are multiple ways of creating the Kerberos Keytab; for example, it is possible to do so manually using the “ktpass” Windows command-line tool or manually using the “ktutil” Linux command-line tool. The recommended best practice is using the ktutil command-line tool.

Creating Keytabs with Windows Command-Line Tool

Using the ktpass command requires that the user running the command has sufficient permissions in Active Directory to write changes to the user or computer object. The ktpass command takes several command-line parameters:

- /out – Specifies the name of the Kerberos Keytab file to generate
- /princ – Specifies the principal name
- /mapuser – Maps the name of the Kerberos principal to the specified domain account
- /pass – Specifies a password for the Kerberos principal
- /crypto – Specifies All to use all supported cryptographic types
- /ptype – Specifies KRB5_NT_PRINCIPAL

For more information about the KTPASS command, see https://technet.microsoft.com/en-us/library/cc753771.aspx. Here is an example KTPASS command line:

```
ktpass /out C:\temp\sas.keytab /princ SAS/hostname1.domain.com
/mapuser hostname1-SAS /pass * /crypto all /ptype KRB5_NT_PRINCIPAL
```

This will prompt for the password for the Service Account.

Creating Keytabs with Linux Command-Line Tool

Using the ktutil command does not require any permissions within Active Directory; in fact, the command does not even connect to Active Directory. However, to use ktutil to add an entry you will need to know the password for the Service Account. The ktutil command invokes a command interface from which an administrator can read, write, or edit entries in a keytab:

- add_entry {-key|-password} -p principal -k kvno -e enctype
- Add principal to keylist using key or password
- write_kt keytab
- Write the current keylist into the Kerberos V5 keytab file keytab

For more information about the ktutil command, see http://web.mit.edu/kerberos/krb5-1.12/doc/admin/admin_commands/ktutil.html. Here is an example of using the KTUTIL command:

```
$ ktutil
ktutil: addent -password -p SAS/hostname1.domain.com -k 2 -e RC4-HMAC
Password for SAS/hostname1.domain.com@DOMAIN.COM:
ktutil: addent -password -p SAS/hostname1.domain.com -k 2 -e aes256-cts-
hmac-sha1-96
Password for SAS/hostname1.domain.com@DOMAIN.COM:
ktutil: addent -password -p SAS/hostname1 -k 2 -e RC4-HMAC
Password for SAS/hostname1@DOMAIN.COM:
ktutil: addent -password -p SAS/hostname1 -k 2 -e aes256-cts-hmac-sha1-96
Password for SAS/hostname1@DOMAIN.COM:
ktutil:  wkt /tmp/sas.keytab
ktutil:  quit
```

As can be seen from the example, using the ktutil command it is very easy to add multiple principals to a single Kerberos Keytab file. Also, ktutil can be used to combine existing separate Kerberos Keytab files

into a single file by reading in the separate files and writing out a single combined file. To combine files you do not need to know the passwords of the associated Service Accounts.

Kerberos Configuration Files

The Kerberos Configuration file contains Kerberos configuration information for the Kerberos client. This includes the locations of Key Distribution Centers and admin servers for the Kerberos realms of interest. It also includes defaults for the current realm and mappings of host names onto Kerberos realms. For more information about the Kerberos configuration file, see http://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html#krb5-conf-5.

The krb5.conf file may contain the sections listed in Table 3:

Section	Description
[libdefaults]	Settings used by the Kerberos V5 library
[realms]	Realm-specific contact information and settings
[domain_realm]	Maps server host names to Kerberos realms
[capaths]	Authentication paths for non-hierarchical cross-realm
[appdefaults]	Settings used by some Kerberos V5 applications
[plugins]	Controls plug-in module registration

Table 3. Kerberos Configuration File Sections

An example Kerberos configuration file (/etc/krb5.conf) might contain the following:

```
[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 udp_preference_limit = 1

[realms]
 EXAMPLE.COM = {
  kdc = kerberos.example.com
  admin_server = kerberos.example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Kerberos can look up information about the Kerberos Realm from DNS records. This enables the Kerberos configuration file to be very simple. Setting the following two options removes the requirements for site-specific information in the [realms] and [domain_realm] sections:

- dns_lookup_realm = true
- dns_lookup_kdc = true

.

SAS MIDDLE-TIER

Before Integrated Windows Authentication can be configured for the SAS Middle-Tier, a number of prerequisite tasks must be completed. These are very similar to the tasks completed for the SAS IOM Servers.

Active Directory Users and Groups

A Service Account is required to represent SAS Web Application Server within Active Directory. This is required for the Simple Protected Negotiation (SPNEGO) or Kerberos configuration. Only a single Service Account is required even if there are multiple instances of SAS Web Application Server running on multiple hosts. It is important that the user name is different from the server name.

Service Principal Names and Keytabs

A Service Principal Name (SPN) must be registered against the Service Account for the SAS® Web Application Server. The SPN for the middle-tier is in the format HTTP/<hostname>, where the hostname is the name used to access the SAS Middle-Tier. Normally, this host name will be the name of the host running the SAS Web Server. Also, a Kerberos Keytab file is required for our SAS Web Application Server Service Account. The Kerberos Keytab file contains the credentials for the SAS Web Application Server Service Account and is used to decrypt the Service Tickets presented by the clients.

The Active Directory administrator can define the Service Principal Name and create the Keytab file using a single command:

```
ktpass -princ HTTP/<SAS WEB SERVER>@<REALM> -pass * -mapuser domain\user -
out <some_path>\<SAS NODE>.keytab -ptype KRB5_NT_PRINCIPAL
```

In some situations running the ktpass command can corrupt the password for the user account. As such, it is good to verify that the password is still correct before proceeding. Alternatively, the steps outlined in the preceding section on SAS IOM Servers on Linux can be used.

The Kerberos Keytab file created above is to be securely copied to the SAS Server. For example, it may be placed in location such as this:

```
<SAS_CONFIG_DIR>/Web/WebAppServer/SASServer1_1/conf/
```

Encryption Strength

The Kerberos tickets, used to authenticate users, are often encrypted using AES-256bit encryption. However, by default Java is unable to process this strength of encryption, which means the SAS Middle-Tier will be unable to process such Kerberos tickets.

To enable Java to process AES-256 Kerberos tickets requires the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. These can be downloaded from Oracle here: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html. For AIX system from IBM, these can be downloaded from here: https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=jcesdk&lang=en_US

The files must then be copied into the SAS Private Java Runtime Environment on each host running instances of the SAS Web Application Server.

KERBEROS DELEGATION

Delegation or “double-hop” authentication allows the user who is authenticated to one service to access a second service from the first. For SAS IOM Servers this applies mainly to the SAS Object Spawner. In such a case an authenticated user starts a SAS Workspace Server, and then code within the SAS Workspace Server uses Kerberos to access a data source (for example, a Secured Hadoop cluster). Delegation can also apply to the middle-tier, where the user authenticated to the middle-tier starts a SAS Workspace Server.

For Integrated Windows Authentication to work for a number of SAS client applications, the initial connection to the middle-tier must be able to pass on the connection to the server tier. These client applications must launch a SAS Workspace Server as part of the client initialization, SAS Enterprise Miner, SAS® Forecast Studio, and SAS® Studio are all examples of these types of client applications. Additional browser-based applications can use the same authentication infrastructure to provide a secure mechanism to launch individual SAS Workspace Server sessions; examples of such client applications are SAS® Visual Analytics Administrator and SAS® Visual Data Builder.

Delegation is set against the object where the Service Principal Name is registered. The delegation tab, shown in **Error! Reference source not found.**, within the Active Directory Users and Computers tool is available only after a Service Principal Name has been registered. Microsoft has extended Delegation to include “Constrained Delegation”, which is supported for the SAS Object Spawner, but not supported for SAS Middle-Tier.

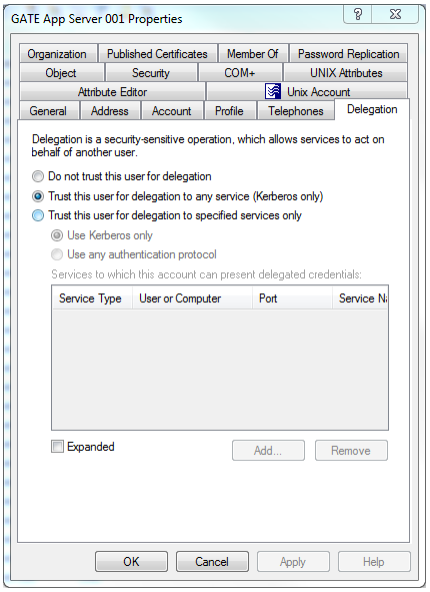

Figure 2. Example Delegation Tab from Active Directory Users and Computers

Constrained Delegation

To use constrained delegation, all services that will be connected to must be defined against the account being configured for constrained delegation. If there are multiple hosts and multiple services, each one must be defined. For example, with a Microsoft SQL Server cluster each host must be defined in the constrained delegation section of the Active Directory Users and Computers tool. It is a recommended practice to test without constrained delegation and then work through adding the required services and testing each one in turn as they are defined.

CLIENTS

As the third tier of the SAS 9.4 environment there are also some requirements on the client PC that must be completed for the configuration to work correctly.

Encryption Strength

As with the SAS Middle-Tier, the SAS Java clients are unable, by default, to processes Kerberos tickets using AES-256bit encryption. To enable Java to process AES-256 Kerberos tickets requires the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. These can be downloaded from Oracle here: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

The files must then be copied into the Java Runtime Environment on the client PC being used by the SAS client. This could either be the SAS Private Java Runtime Environment for some desktop client applications or another JRE if the Java Web Start version of SAS client application is used.

JCE with SAS Java Desktop Clients

SAS Java desktop clients uses the SAS Private Java Runtime Environment. Therefore, the JCE Policy Files must be added to the SAS Private JRE. Extract the two Policy Files to <SASHOME>\SASPrivateJavaRuntimeEnvironment\9.4\jre\lib\security.

JCE with SAS Java Web Start Clients

SAS Java Web Start clients run on a client PC where no SAS deployment tools have been run. As such, the SAS Private Java Runtime Environment is not installed. To use the Java Web Start client, a version of Java must still be installed on the client PC. The JCE Policy files must therefore be added to this other version of Java installed on the client PC.

Making the TGT Available

By default, Microsoft Windows does not allow access to the session key of the Ticket Granting Ticket to processes that are outside Windows. For Java to access the session key and hence use the TGT to request a Service Ticket requires a Windows Registry entry, as shown in Figure 3.

```
Entry: AllowTgtSessionKey
Type: REG_DWORD
Default Value: 0
Required Value: 1
```

This registry key must be added to the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
```

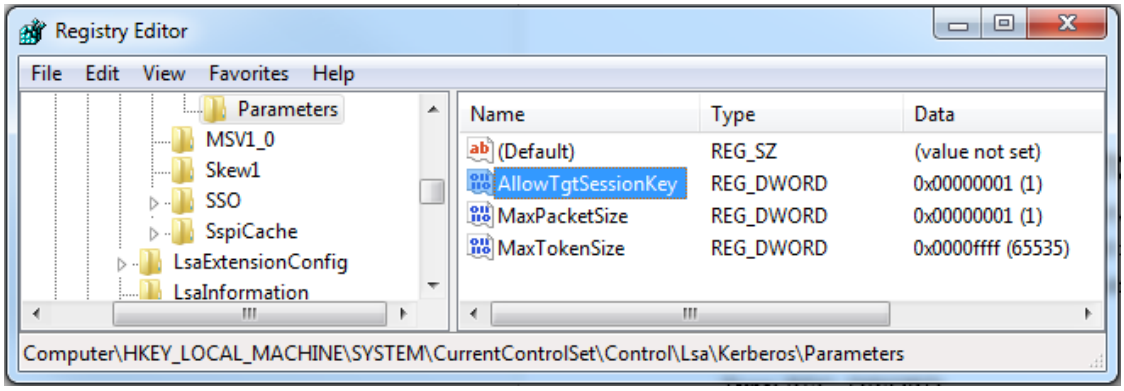

Figure 3. Example Windows Registry Key

More details are available from http://support.microsoft.com/kb/837361. This registry key will be required for SAS Enterprise Miner and SAS Forecast Studio.

ENVIRONMENT CONFIGURATION

The following sections provide you with the detailed steps to complete the configuration of Kerberos Authentication with SAS 9.4.

SAS IOM SERVERS ON WINDOWS CONFIGURATION

As detailed in the prerequisites section with a simple topology, the configuration of the SAS IOM Servers on Windows can be performed automatically. The option to provide IWA can be selected while the SAS Deployment Wizard runs or can be configured after the deployment is complete. If the option is selected while the SAS Deployment Wizard is running, no further configuration afterward is necessary.

Manual Configuration of IWA

To manually enable IWA for the SAS Workspace Server after SAS installation:

1. Launch SAS® Management Console and log in using an unrestricted user, such as sasadm@saspw.
2. Expand Server Manager ⇨ SASApp.
3. Right-click SASApp – Logical Workspace Server and select Properties.
4. Select the Options tab.
5. Select Negotiate from the Security package drop-down menu.
6. Select OK.

After you complete these steps, the SAS Object Spawner will need to reread its metadata configuration. This can be accomplished by either restarting the Object Spawner or, in SAS Management Console, directing it to refresh its metadata.

Metadata Server Clusters

When you are configuring the first member of the SAS Metadata Server cluster, the SAS® Deployment Wizard prompts for the valid domain user account that will be used to run the SAS Metadata Server process. This domain user account must have the Service Principal Names (SPN) registered against it in Active Directory. The SPNs should have been registered as part of the prerequisites when the account was created. A separate user account can be used for each cluster member, but this is not required.

The SAS Deployment Wizard will provide the user account with the "logon as a service" security permission automatically and this does not have to be set as a prerequisite. No further configuration is required for a cluster of SAS Metadata Servers.

If one of the SAS Metadata Server cluster members also has the SAS Object Spawner and SAS Workspace Server deployed, further steps are required. In this case, the SAS Object Spawner must be configured to run as the same domain user account as the SAS Metadata Server. This prevents issues arising with the SAS Object Spawner registering duplicate Service Principal Names.

SAS IOM SERVERS ON LINUX CONFIGURATION

As detailed in the prerequisites section, the SAS IOM Server on Linux requires a shared library implementing the GSSAPI with Kerberos 5 extensions. The shared library must be installed and configured before starting the SAS IOM Server configuration detailed here.

Setting SAS Authentication Method

The SAS IOM Servers on Linux will be configured to use PAM as part of the configuration of IWA. This can be performed as part of the deployment when running the SAS Deployment Wizard or after the deployment. If the setting is changed after the deployment, all SAS IOM Servers should be stopped and the following file updated:

```
<SASHOME>/SASFoundation/9.4/utilities/bin/sasauth.conf
```

You must change the value of methods from "pw" to "pam". Then restart the SAS IOM Servers.

Note: This requires that the /etc/pam.d/sasauth file already exists.

If the SAS Metadata Server is on a different host to the SAS Object Spawner, then this step must be completed on both hosts. If a SAS Metadata Server cluster is deployed, the same steps must be completed on all cluster members.

Setting IWA for SAS Workspace Server

The SAS Workspace Server must be configured for Integrate Windows Authentication. This can be done during the initial deployment when running the SAS Deployment Wizard; it is done by selecting the IWA

check-box. Alternatively, after the deployment, the changes can be made using SAS Management Console. To make the changes after configuration:

1. Launch SAS Management Console and log in using an unrestricted user, such as sasadm@saspw.
2. Expand Server Manager ⇨ SASApp.
3. Right-click SASApp – Logical Workspace Server and select Properties.
4. Select the Options tab.
5. Select Negotiate from the Security package drop-down menu.
6. Select OK.

After you complete these steps, the SAS Object Spawner will need to reread its metadata configuration. This can be accomplished by either restarting the Object Spawner or it can be done in SAS Management Console, directing it to refresh its metadata.

Identifying the SAS Keytab File

SAS IOM Servers on Linux must be able to access the keytab file for the SAS service account in Active Directory. The keytab file was created as part of the prerequisites. An environment variable is set to point to the location of the keytab file.

The environment variable is set in the following file:

```
<SAS_CONFIG_DIR>/Lev1/level_env_usermods.sh
```

The following command adds the environment variable to the file:

```
echo export KRB5_KTNAME=/full/path/to/SAS.keytab >>
<SAS_CONFIG_DIR>/Lev1/level_env_usermods.sh
```

If the SAS Metadata Server is on a different host from the SAS Object Spawner, then this step must be completed on both hosts. If a SAS Metadata Server cluster is deployed, the same steps must be completed on all cluster members.

Identifying the Shared Library

The SAS Metadata Server on Linux must be able to locate the Shared Library implementing the GSSAPI with Kerberos 5 extensions. An environment variable is set to point to the location of the shared library.

The environment variable is set in the following file:

```
<SAS_CONFIG_DIR>/Lev1/level_env_usermods.sh
```

The following command adds the environment variable to the file:

```
echo export TKSECURE_GSSAPI_LIBRARY=/usr/lib/libgssapi_krb5.so >>
<SAS_CONFIG_DIR>/Lev1/level_env_usermods.sh
```

If a SAS Metadata Server cluster is deployed, the same steps must be completed on all cluster members.

SAS MIDDLE-TIER CONFIGURATION

The middle-tier configuration can be split into two parts; the first part covers steps that are common to any web authentication configuration. The second part covers the steps specific to configuring SPNEGO to provide Integrated Windows Authentication.

Within this document the SAS provided Fall-Back authentication mechanism will be configured. This will enable Kerberos authentication with browsers configured for Integrated Windows Authentication (IWA) and the standard form-based authentication for browsers that are not configured for IWA.

Generic Web Authentication Steps

These generic web authentication steps will need to be completed irrespective of the authentication method. These steps configure the SAS Middle-Tier to trust the authentication carried out by a third party. In this case the third party will be the SAS Web Application Server authenticating the Kerberos tickets.

Edit web.xml.orig

Edit the following file:

```
<SASHOME>/SASWebInfrastructurePlatform/9.4/Configurable/wars/sas.svcs.logon
/WEB-INF/web.xml.orig
```

You must uncomment the <error-page> section toward the bottom of the file.

Integrated Windows Authentication Steps

The following steps will configure the SAS Web Application Server to authenticate Kerberos tokens using the SPNEGO valve. In addition, we configure the SAS Fall-Back module to enable alternative authentication using the standard SAS Logon Manager form.

Update the SAS Logon Manager Context XML File

Edit the following file:

```
<SASHOME>/SASWebInfrastructurePlatform/9.4/Static/wars/sas.svcs.logon/META-
INF/context.xml
```

Before the closing </Context> tag add the following lines:

```
<Valve
className="com.sas.vfabrictcsvr.authenticator.SasFallbackAuthenticatorValve
" authMethod="SPNEGO" />
<Realm className="com.sas.vfabrictcsvr.realm.GSSContextEstablishedRealm"
commonRole="ROLE_USER"
/>
```

Create Kerberos Configuration File

Edit the following file:

```
<SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/conf/krb5.ini
```

Add the following lines:

```
[libdefaults]
default_realm = <REALM>
default_keytab_name =
forwardable=true
udp_preference_limit=1

[realms]
<REALM> = {
   kdc = <DNS NAME OF DOMAIN CONTROLLER>
}

[domain_realm]
<domain.com> = <REALM>
.<domain.com> = <REALM>
```

The following values should be used to complete the krb5.ini:

- <REALM> is the uppercase Kerberos Realm. Most often this is the same as the domain name.
- <domain.com> is the lowercase domain name.
- <DNS NAME OF DOMAIN CONTROLLER> should be the name of a valid domain controller for the middle-tier server. This could be a DNS alias that provides load-balancing across domain controllers.

Update the jaas.config File

Edit the following file:

```
<SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/conf/jaas.config
```

Add the following definition to the end of the file:

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    doNotPrompt=true
    principal="HTTP/<######>.<domain.com>@<REALM>"
    useKeyTab=true
    isInitiator=false
keyTab="<SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/conf/appsrv.key
tab"
    storeKey=true;
};
```

Be careful to set the principal name “HTTP/<hostname>.<domain.com>@<REALM>” to your server host name. This principal value is not the Service Principal Name but is actually the User Principal Name of the service account used to represent the SAS Web Application Server.

In addition, add the following two parameters to the existing Platform Foundation Services (PFS) entry in the jass.config:

```
        "idpropagation"="sspi"
        "sspisecuritypackagelist"="KERBEROS"
```

Horizontal Middle-Tier Clusters

For environments with a horizontal cluster of SAS Web Application Server instances, copy the following files, which have just been updated on the primary middle-tier host to all middle-tier node hosts:

1. <SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/conf/krb5.ini
2. <SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/conf/jaas.config
3. <SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/conf/appsrv.keytab

Rebuild and Redeploy

To rebuild and redeploy the web applications, we use SAS Deployment Manager. When SAS Deployment Manager appears, complete the following steps:

1. At the language prompt select **English** and select OK.
2. Select **Rebuild Web Applications** and select Next.
3. Select Next.
4. Enter the sasadm@saspw password and select Next.
5. Select **Web Infrastructure Platform 9.4** from the list of applications and select Next.
6. Select Start.
7. Once the rebuild process is completed, select Finish and SAS Deployment Manager will close.

Launch SAS Deployment Manager again; when SAS Deployment Manager appears, complete the following steps:

1. At the language prompt select **English** and select OK.
2. Select **Deploy Web Applications** and select Next.
3. Select Next.
4. Enter the sasadm@saspw password and select Next.
5. Select **Allow the application server to stop** and select Next.
6. Select **Web Infrastructure Platform 9.4** from the list of applications and select Next.
7. Select Start.
8. Once the deploy process is completed, select Finish and SAS Deployment Manager will close.

Horizontal Middle-Tier Clusters

Once the applications have been deployed on the main middle-tier host, they need to be deployed to the middle-tier node hosts. Copy the updated contents of the <SAS_CONFIG_DIR>/Lev1/Web/Staging directory from the main middle-tier host to the middle-tier node host. The SAS Configuration Scripting tool can be used to undeploy and deploy the applications on the middle-tier node. More details of the SAS Configuration Scripting tool can be found here: http://support.sas.com/documentation/cdl/en/bimtag/66823/HTML/default/viewer.htm#n0sf5pji2pcfu3n1aa50t5o2yp85.htm.

Check the contents of <SAS_CONFIG_DIR>/Lev1/Web/WebAppServer/SASServer1_1/sas_webapps to ensure that the updated applications have been deployed.

USER DEFINITIONS IN METADATA

Finally, we consider how the end users will need to be defined in metadata. Each metadata identity will require logins defined for the correct form of the user ID being presented. If the wrong form of the user ID is used in metadata, it will not match the value from the authentication provider and the end user will be considered as PUBLIC.

SAS IOM Servers on Windows

With a Windows IOM Server, the format of the user ID returned by Integrated Windows Authentication is username@REALM, while the format of the user ID that is returned by the Middle-Tier is username. Therefore, we require two logins for each end user:

- DefaultAuth = username@REALM
- WebAuth = username

Note: No passwords are stored in metadata.

SAS IOM Servers on UNIX

With a SAS IOM Server on UNIX, the format of the user ID returned by Integrated Windows Authentication is username. While the format of the user ID returned by the Middle-Tier is also username. Therefore, we only require one login for each end user:

- DefaultAuth = username

Note: No passwords are stored in metadata.

CLIENT CONFIGURATION

Before the Integrated Windows Authentication environment can be used by SAS client applications, some further configuration steps must be completed on the client PC, as listed in the prerequisites section earlier.

BROWSER CONFIGURATION FOR IWA

Before end users can access the web applications with their browsers, the browser must be configured to enable Integrated Windows Authentication. If you include the configuration of the SAS Fall-Back module, the standard SAS Logon Manager form will be displayed even if the browser is not configured for IWA.

Internet Explorer

1. Open Internet Options, either from a browser window from Tools ⇨Internet Options or from the Control Panel.
2. Select Security.
3. Select Local intranet.
4. Select Sites.
5. Select Advanced.
6. Add the SAS Web Server address: http://sasserver.mycompany.com.
7. This completes the setup required for Internet Explorer.

Mozilla Firefox

1. Navigate to about:config.
2. Accept the security warning “Here be dragons!”
3. Enter “network.negotiate” in the filter.
4. Double click “network.negotiate-auth.trusted-uris”.
5. Add the SAS Web Server address: http://sasserver.mycompany.com, note this is a comma separated string.
6. Double click “network.negotiate-auth.delegation-uris”.
7. Add the SAS Web Server address: http://sasserver.mycompany.com, note this is a comma separated string.
8. This completes the setup required for Firefox.

Google Chrome

Google Chrome by default disables the delegation of Kerberos credentials. A Windows Registry key must be added to enable Kerberos delegation.

1. Open a registry editor.
2. Add the following REG_SZ key: Software\Policies\Google\Chrome\AuthNegotiateDelegateWhitelist.
3. Set the value to the SAS Web Server host name: sasserver.mycompany.com.
4. This completes the setup required for Chrome.

For more details see: http://dev.chromium.org/administrators/policy-list-3#AuthNegotiateDelegateWhitelist.

CONCLUSION

Kerberos delegation enables the secure reuse of the end user’s credentials to run processes or access data stored on system remote from where the end user has logged in. Using Kerberos delegation with your SAS 9.4 environment involves configuring all tiers in your environment to process Kerberos authentication. While the configuration from the SAS perspective is straightforward, getting the prerequisites completed can be challenging. Most issues with Kerberos delegation involve problems with the prerequisites. Either Service Accounts are not configured correctly or there are issues with the

Service Principal Names. Also sometimes we see issues around the encryption used in both the Kerberos keytabs and tickets.

Planning out the prerequisites and ensuring all the correct teams in your organization are involved is key to success. Once complete, this configuration provides your end users with a seamless and secure access to the power of SAS® Analytics.

REFERENCES

Red Hat. 2014. "Integrating Red Hat Enterprise Linux 6 with Active Directory". Available at http://www.redhat.com/en/resources/integrating-red-hat-enterprise-linux-6-active-directory.

Heslin, Mark & Pal Dmitri. 2014. "Interoperability Update: Red Hat Enterprise Linux 7 beta and Microsoft Windows". Red Hat Summit 2014. Available at http://docplayer.net/7645094-Interoperability-update-red-hat-enterprise-linux-7-beta-and-microsoft-windows.html.

Li, Zhiyong & Mike Roda. 2014. "An Advanced Fallback Authentication Framework for SAS 9.4 and SAS Visual Analytics". *Proceedings of the SAS Global Forum 2014 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings14/SAS102-2014.pdf.

Rogers, Stuart. 2013. "Kerberos and SAS 9.4: A Three-Headed Solution for Authentication". *Proceedings of the SAS Global Forum 2013 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings13/476-2013.pdf.

Massachusetts Institute of Technology. "Kerberos: The Network Authentication Protocol." Available at http://web.mit.edu/kerberos/.

Massachusetts Institute of Technology. "ktutil" in MIT Kerberos Documentation. Available at http://web.mit.edu/kerberos/krb5-1.12/doc/admin/admin_commands/ktutil.html.

Microsoft. "Microsoft Kerberos (Windows)." Available at http://msdn.microsoft.com/enus/library/windows/desktop/aa378747(v=vs.85).aspx.

Microsoft. "Kerberos Authentication Overview." Available at http://technet.microsoft.com/enus/library/hh831553.aspx.

Microsoft. "TechNet Command-Line Reference: Setspn". Available at https://technet.microsoft.com/en-us/library/cc731241.aspx.

Microsoft. "Ktpass Command-Line Reference". Available at https://technet.microsoft.com/en-us/library/cc753771.aspx.

ACKNOWLEDGMENTS

I would like to thank the following people for taking the time to review and contribute to this paper:

- Rob Collum
- Mike Roda
- Philip Hopkins

RECOMMENDED READING

- *Configuration Guide for SAS 9.4 Foundation for UNIX Environments*
- *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide*
- *SAS 9.4 Intelligence Platform: Installation and Configuration Guide*
- *SAS 9.4 Intelligence Platform: Security Administration Guide*

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Stuart J Rogers
SAS Institute Inc.
stuart.rogers@sas.com
http://www.sas.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.