GSS-API miscellaneous failure matching credentials not found

GSS-API miscellaneous failure matching credentials not found

On this page:

Context question(s)

When trying to log in to SAPgui on my Windows machine, I get an error: GSS-API miscellaneous failure matching credentials not found. How do I resolve this?

I am getting an error: "No credentials cache found" when I try to log in to SAPgui. How do I resolve this?

Overview

This error message means that SAPgui was unable to communicate with Kerberos and/or was unable to see a valid Kerberos ticket on the machine. The desired behavior is for SAPgui, on launch, to check whether there is a valid Kerberos ticket on the machine. If there is no Kerberos ticket, the Kerberos login screen should appear, prompting the user for Kerberos username and password. This will be the same username and password used to check @mit.edu email. After the user successfully acquires a Kerberos ticket, SAPgui should launch.

Solution one - if Kerberos is not installed.

Kerberos may not be installed on the machine. Check **Control Panel** > **Add or Remove Programs** to see if Kerberos is installed.

Solution two - if Kerberos is installed, but tickets are expired.

It may be that there is an expired Kerberos ticket on the machine. SAPgui sees that the Kerberos ticket exists, so it doesn't bring up the Kerberos login screen, but, since the ticket is expired, the credentials are not valid.

1. Follow the menu path **Start** > **All Programs** > **Kerberos for Windows** > **Network Identity Manager**.
2. You may see a message regarding expired credentials. Click to obtain new credentials.
3. If no error message is present, click the yellow icon to obtain new credentials.

Solution three - if there is a problem in the communication between SAPgui and Kerberos.

Troubleshooting steps:

1. Verify that Kerberos for Windows is installed.
2. Try getting a Kerberos ticket directly in Kerberos. To do this:
    a. Follow the menu path: **Start** > **All Programs** > **MIT Kerberos for Windows** > **Leash Ticket Manager**. The menu path may vary slightly, depending on your Kerberos version.
    b. Select **Action** > **Get Ticket**.
    c. Try again to launch SAPgui.
3. If the above steps are successful, we will want to troubleshoot whether SAPgui can successfully launch Kerberos, so that you don't need to do a separate Kerberos launch. To do this:
    a. Restart the machine.
    b. Try again to launch SAPgui.

    c. Let us know whether the Kerberos login screen appears, allows you to acquire a ticket, and SAPgui is launched.
4. If the above steps are not successful, the next steps would be:
    a. Uninstall Kerberos via **Control Panel** > **Add or Remove Programs**.
    b. Uninstall SAPgui via **Control Panel** > **Add or Remove Programs**.
    c. Download and install the latest version of Kerberos for Windows, available from:
5. https://ist.mit.edu/software-hardware?type=All&platform=Windows+XP&users=All&title=kerberos&recommended_only=All
    a. Download and install the latest version of SAPgui for Windows, available from:
6. https://ist.mit.edu/software-hardware?type=All&platform=Windows+XP&users=All&title=sapgui&recommended_only=All
    a. Restart the machine, and try again to launch SAPgui.

Background information

From http://www.faqs.org/faqs/kerberos-faq/general/section-84.html

5.2. What is GSSAPI?

GSSAPI is an acronym; it stands for Generic Security Services Application Programming Interface.

The GSSAPI is a generic API for doing client-server authentication. The motivation behind it is that every security system has it's own API, and the effort involved with adding different security systems to applications is extremely difficult with the variance between security APIs. However, with a common API, application vendors could write to the generic API and it could work with any number of security systems.

How does this relate to Kerberos? Included with most major Kerberos 5 distributions is a GSSAPI implementation. Thus, if a particular application or protocol says that it supports the GSSAPI, then that means that it supports Kerberos, by virtue of Kerberos including a GSSAPI implementation.