Kerberos authentication made easy on OpenVMS

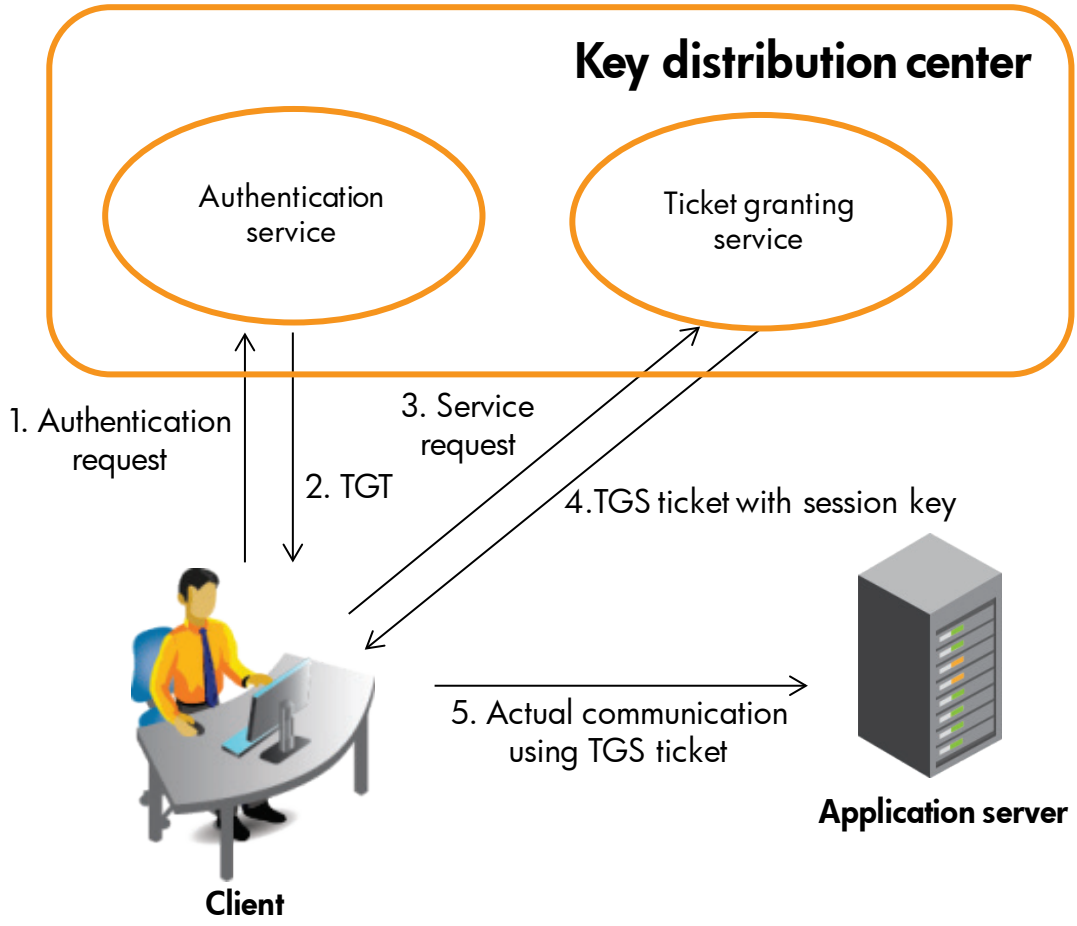
Author: Srinivasa Rao Yarlagadda
yarlagadda-srinivasa.rao@hp.com

Co-Author: Rupesh Shantamurty
rupeshs@hp.com

OpenVMS Technical Journal V18

Table of contents

Figure 1: Kerberos Protocol



Overview

Single sign-on capabilities on OpenVMS are an integral part of integrating OpenVMS into a hybrid computing environment consisting of various other platforms like Windows® Linux or UNIX®. This article provides an introduction to Kerberos protocol and important concepts and features of Kerberos authentication on OpenVMS. The article includes detailed information about Kerberos-based, single sign-on operations and automated authentication process using Kerberized applications like Kerberized telnet on OpenVMS.

Once enabled, this would open up several possibilities for a secure authentication among various platforms in an enterprise environment in a seamless manner.

What is Kerberos?

Kerberos is a network authentication protocol developed by MIT (Massachusetts Institute of Technology). It provides authenticated access for users and services on a computer network.

The name Kerberos comes from Greek mythology. Kerberos is the name of the three-headed dog that guarded the gates of Hades (underworld) in Greek mythology. The three heads involved in the protocol are the client, the server, and a trusted third party that performs secure verification of users and services.

The Kerberos protocol uses strong cryptography, so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity.

Kerberos uses secret-key cryptography, which lets entities communicating over networks prove their identity to each other while preventing "eavesdropping" or replay attacks. It also provides data stream integrity (detection of modification) and secrecy (preventing unauthorized reading) using encryption standards such as Advanced Encryption Standard (AES).

Kerberos is based on the concept of a trusted third party that performs secure verification of users and services. In the Kerberos protocol, this trusted third party is called the key distribution center (KDC). Kerberos is used to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username-and-password authentication mechanism. The ticket can then be embedded in virtually any other network protocol, thereby confirming the identity of the principals involved to the processes implementing that protocol. .

How Kerberos works?

Instead of client sending a password to the application server, Kerberos requests for a ticket from a trusted third party called the KBC. The ticket and the encrypted request are then sent to application server.

The following are commonly used Kerberos terms and their definitions:

Principal name

A principal is a unique identity to which Kerberos can assign tickets. It is analogous to an OpenVMS user. The Kerberos database, which performs a function similar to the SYSUAF.DAT file on OpenVMS, stores information about principals.

By convention, a principal name is divided into three parts:

1. A primary—for a user, a user name. For a system, the word host.
2. The instance—an optional string that qualifies the primary.
3. The realm—generally, the DNS domain name in uppercase letters.

Realm

The administrative domain that encompasses Kerberos clients and servers is called a realm. Each Kerberos realm has at least one Kerberos server, zero or more Kerberos slave servers, and any number of clients. The master Kerberos database for that site or administrative domain is stored on the Kerberos server. Slave servers have read-only copies of the database that are periodically propagated from the master server.

The Kerberos database

The Kerberos database contains all of the realm's Kerberos principals, their passwords, and other administrative information about each principal.

Tickets

Kerberos tickets are known as credentials, and are a set of electronic information used to verify the client's identity.

Kerberos tickets can be stored in a file, or they may exist only in memory. The first ticket you obtain is a generic ticket-granting ticket (TGT), which is granted upon your initial login to the Kerberos realm. The TGT allows you to obtain additional tickets that give you permission for specific services.

Ticket-granting service

Once authenticated, a principal will be granted a TGT and a ticket session key, which give the principal the right to use the ticket. This combination of the ticket and its associated key is known as your credentials. A principal's credentials are stored in a credentials cache, which is often just a file in the principal's local directory tree.

KDC

The ticket-granting service (TGS) and the authentication server are usually collectively known as the Key Distribution Center (KDC).

Each KDC contains its own copy of the Kerberos database. The master KDC contains the primary copy of the database, which it propagates at regular intervals to the slave KDCs. All database changes are made on the master KDC. Slave KDCs provide ticket-granting services only, with no database administration. This allows clients to continue to obtain tickets when the master KDC is unavailable.

Authenticating OpenVMS users with Kerberos

The Kerberos Authentication and Credential Management (ACME) Agent on OpenVMS provides login authentication of OpenVMS users via a Kerberos principal name and password. This agent is provided as part of the Kerberos Version 3.2 release.

After you install and configure Kerberos Version 3.2 on OpenVMS, perform the following steps to configure and start the Kerberos ACME agent.

1. Install ACME Login—See the file SYS$HELP:ACME_DEV_README.TXT for information about installation and setup.
2. Install the Kerberos persona extension by entering the following commands:

   $ MCR SYSMAN

   SYSMAN> SYS_LOADABLE ADD/LOG KERBEROS KRB$ACME_KRB_PERSONA_EXT %SYSMAN-I-IMGADDED, added image KRB$ACME_KRB_PERSONA_EXT for product KERBEROS

   $@SYS$UPDATE:VMS$SYSTEM_IMAGES.COM

3. Reboot the system. This is required one time only, after you have installed the Kerberos persona extension.
4. To start the Kerberos ACME agent automatically, edit the file SYS$MANAGER:ACME$START.COM to uncomment the following line:

   $! @SYS$STARTUP:KRB$STARTUP_KERBEROS_ACME

5. Edit the file SYSTARTUP_VMS.COM to include the following command after all dependent software is started:

   $ SET SERVER ACME/RESTART

6. Create an OpenVMS account with the EXTAUTH flag set.
7. Create a Kerberos principal name that exactly matches (including case) the OpenVMS account name created in step six. Passwords do not need to match. For the Kerberos configuration, you can use either DCL or UNIX-style commands to create the principal.
8. SET HOST or Telnet to the system on which you installed the ACME Agent and the Kerberos persona extension in steps 1 and 2. Enter one of the following commands:

   $ TELNET NODE1

   or

   $ SET HOST NODE1

9. Enter the username and password. For example:

   Welcome to OpenVMS (TM) Alpha Operating System, Version 8.3

   Username: ACMEUSER

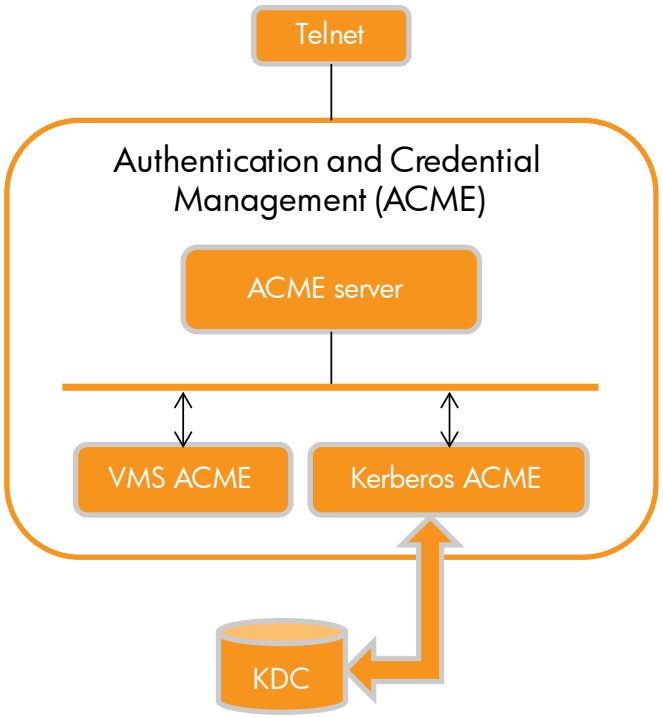
   Password:

   **** Logon Message from ACME_KRB_DOI ACME Agent ***

10. Kerberos login Ticket cache file is stored in the user's default directory.

The Kerberos ACME agent on OpenVMS provides functionality similar to that of the pam_krb5 utility on UNIX systems.

Figure 2: Kerberos authentication on OpenVMS



Kerberos authentication with Active Directory

Kerberos is an integral part of Windows Active Directory domain. The domain controllers (dc) are Kerberos Key Distribution Centers, and the client systems use the Kerberos protocol to authenticate users with the domain controller servers.

Using the Kerberos ACME agent on OpenVMS, users can be authenticated with Active Directory domains. This would enable the integration of OpenVMS into an existing enterprise where Kerberos framework exists.

Kerberized Telnet and SSH

OpenVMS offers Kerberos authentication for telnet and SSH applications. The Kerberos authentication means that once you have a valid Kerberos ticket (obtained manually (kinit) or via a login using Kerberos ACME agent), the applications can use this ticket as an authentication token and once authenticated, successful access will be provided without the need for a password.

Configuration steps for kerberized telnet and SSH applications are explained in the Kerberos documentation.

Secure automatic logins on OpenVMS

Using kerberized telnet and SSH applications, users can login securely without entering the password.

Following are some of the use cases of having this solution on OpenVMS.

1. Network backup administrators can use this for automated backups in a secure manner.
2. Secure authentication to various platforms (HP-UX, Linux, and Windows) from OpenVMS.
3. Integration of OpenVMS into the existing enterprise-wide, single sign-on framework.
4. Administrators can automate remote testing and secure patch/kit installation procedures.

Summary

Adding Kerberos to a network can increase the overall security available to the users and administrators of that network. Integrating OpenVMS into an existing Kerberos framework had previously required a lot of custom-made solutions to be developed. Kerberos ACME agent on OpenVMS provides the basic authentication infrastructure so that it can be integrated/extended to an enterprise-wide, single sign-on framework.

For more information

Kerberos for HP OpenVMS Documentation—http://h71000.www7.hp.com/openvms/products/kerberos/

Smoothly integrate OpenVMS into your Kerberos framework and enhance your single sign-on experience; visit: www.hp.com/go/openvms

4AA4-0526ENW, Created April 2012