Kerberos Refresher

A *user* in Kerberos is called a **principal,** which is composed of three parts, the primary, instance and realm. The primary is the user component, and is an arbitrary string. It may be the operating system username or the name of a service. The primary is followed by an optional instance, separated from the primary by a slash. The instance, if present, is used to disambiguate multiple principals of a user or service. The third component is the realm, separated from the previous portion(s) by an at-sign (@) which is like a DNS domain, although in DNS a domain is a collection of host names, in Kerberos a realm is a collection of principals. Each realm may have its own settings, such as encryption algorithms, and KDC. Realms are upper case, by convention (and in Kerberos v.5, by implementation). For example, a user principal might be bob@AVALONCONSULT.COM. A service principal might be hdfs/node001@AVALONCONSULT.COM.

Kerberos provides a central, trusted service called the KDC, or Key Distribution Center. The KDC is composed of two services, the Authentication Server (AS) which authenticates a client and provides a ticket granting ticket (TGT) and a Ticket Granting Service (TGS) which, given a valid TGT, can grant a ticket that authenticates a user with a Kerberized service. The KDC contains a database of principals and their keys, similar to */etc/passwd*, and some KDC implementations support storing this database in LDAP or AD.

As an example, consider the user bob that wishes to perform the command "hadoop fs –get /data.txt". When operating in secure mode, the Name Node and Data Node will not permit any operation without a valid Kerberos ticket. Two services must be contacted: the Name Node to retrieve the file metadata and the Data Node to retrieve the file data blocks. To obtain a ticket, the user provides their principal to the AS. The AS returns a TGT encrypted with the principal's password. The client prompts the user for their password and attempts to decrypt the TGT. The decrypted TGT is a valid TGT that may be used to request tickets from the TGS. Note that the password is not passed, but is a shared secret.

To use the Name Node and Data Node services, tickets are necessary. The client encrypts the TGT with a special key, the TGT key, and requests a ticket for a specific service by providing the service principal. The TGS validates the encrypted TGT by decrypting it with the shared TGT key. The TGS sends back to the client a ticket for the service. Within that ticket is a session key that the service can validate with the KDC.

Tickets are issued for a specific time interval, usually 8 or 24 hours. TGT have a lifetime, usually 8 or 24 hours. TGTs are cached and reused, which is why passwords do not need to be re-entered for the lifetime of the TGT. All parties in the same realm must reference a common clock source so that time references are coherent across multiple platforms and services. Clock skew (referring to more than one clock source with a time difference) can cause Kerberos errors.

When user bob receives his two tickets, one for the Name Node and one for the Data Node, he sends the NN ticket to the Name Node. The Name Node service validates the ticket with the KDC and, if verified, provides the file metadata. The client then sends the DN ticket to the Data Node. The Data Node validates the ticket with the KDC, and if validated, provides the file blocks specified in the file metadata.