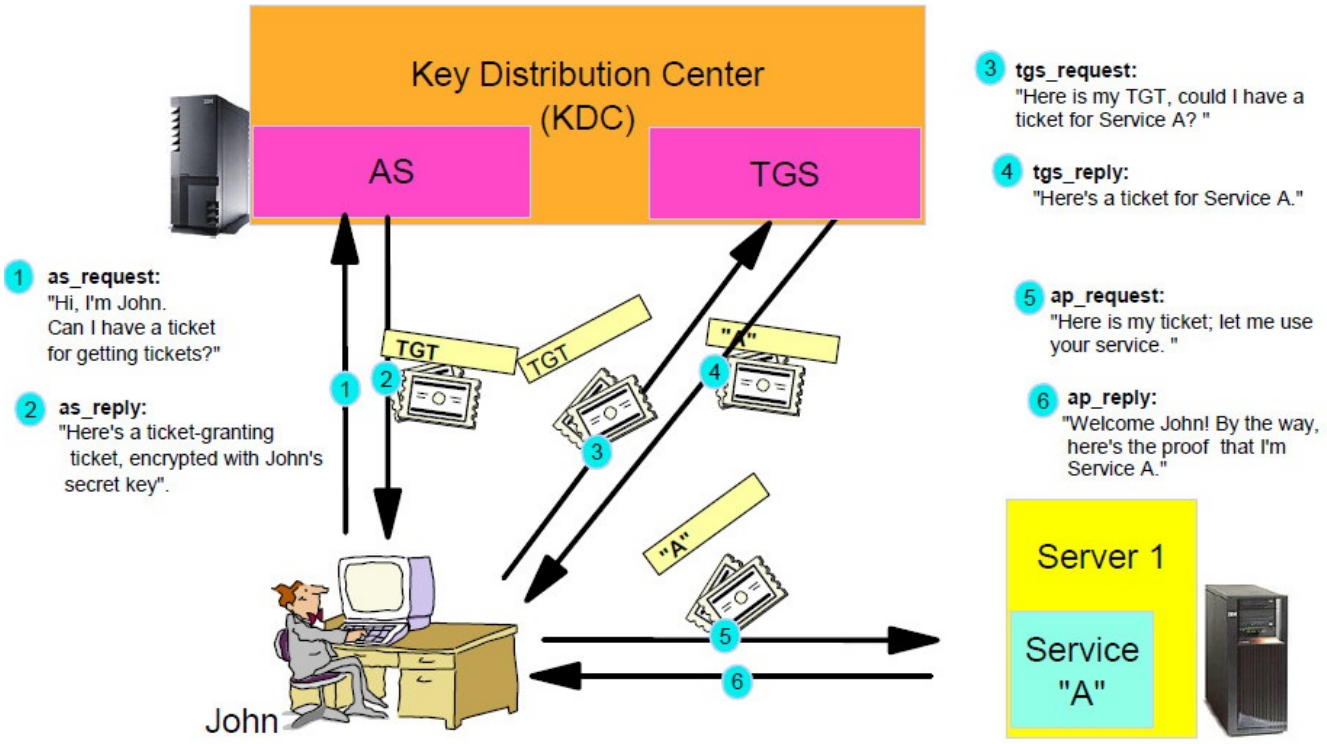
Kerberos Components

Kerberos is integrated with many operating systems including linux distributions such as Red Hat Enterprise Linux. Kerberos is also an integral part of Microsoft Active Directory and is supported by Red Hat Directory Server and Red Hat IDM.



Tickets

A `Ticket` is a form of a security token that Kerberos uses for issuing and making authentication and authorization decisions about principals.

Authentication Service

The **`Authentication Service`**, or **AS**, challenges principals to log in when they first log into the network. The authentication service is responsible for issuing a `Ticket Granting Ticket` or TGT, which is needed for authenticating against the `Ticket Granting Service` and subsequent access to secured services and resources.

Ticket Granting Service

The **`Ticket Granting Service`**, or **TGS**, is responsible for issuing `Service Tickets` and specific session information to principals and the target server they are attempting to access. This is based on the TGT and destination information provided by the principal. This service ticket and session information is then used to establish a connection to the destination and access the desired secured service or resource.

Key Distribution Center

The **Key Distribution Center**, or **KDC**, is the component that houses both the TGS and AS. The KDC, along with the client, or principal, and server, or secured service, are the three pieces required to perform Kerberos authentication.

Ticket Granting Ticket

A **Ticket Granting Ticket**, or **TGT**, is a type of ticket issued to a principal by the AS. The TGT is granted once a principal successfully authenticates against the AS using their username and password. The TGT is cached locally by the client, but is encrypted such that only the KDC can read it and is unreadable by the client. This allows the AS to securely store authorization data and other information in the TGT for use by the TGS and enabling the TGS to make authorization decisions using this data.

Service Ticket

A **Service Ticket**, or **ST**, is a type of ticket issued to a principal by the TGS based on their TGT and the intended destination. The principal provides the TGS with their TGT and the intended destination, and the TGS verifies the principal has access to the destination based on the authorization data in the TGT. If successful, the TGS issues an ST to the client for both the client as well as the destination server which is the server containing secured service/resource. This grants the client access to the destination server. The ST, which is cached by the client and readable by both the client and server, also contains session information that allows the client and server to communicate securely.

There is a tight relationship between Kerberos and the DNS settings of the network. For instance, certain assumptions are made when clients access the KDC based on the name of the host it is running on. As a result, it is important that all DNS settings in addition to the Kerberos settings are properly configured to ensure that clients can connect.

Authentication and Authorization with Kerberos in Desktop-Based SSO

To provide authentication and authorization, Kerberos relies on a third party, the KDC, to provide authentication and authorization decisions for clients accessing servers. These decisions happen in three steps:

1. Authentication exchange. When a principal first accesses the network or attempts to access a secured service without a Ticket Granting Ticket, they are challenged to authenticate against the Authentication Service with their credentials. The AS validates the user’s provided credentials against the configured identity store, and upon successful authentication, the principal is issued a TGT which is cached by the client. The TGT also contains some session information so future communication between the client and KDC is secured.
2. Ticket granting, or authorization, exchange. Once the principal has been issued a

TGT, they may attempt to access secured services/resources. The principal sends a request to the Ticket Granting Service, passing the TGT it was issued by the KDC and requesting a Service Ticket for a specific destination. The TGS checks the TGT provided by the principal and verifies they have proper permissions to access the requested resource. If successful, the TGS issues an ST for the principal to access that specific destination. The TGS also creates session information for both the client as well as the destination server to allow for secure communication between the two. This session information is encrypted separately such that the client and server can only decrypt its own session information using long-term keys separately provided by the KDC to each, from previous transactions. The TGS then responds to the client with the ST which includes the session information for both the client and server.

3. `Accessing the server.` Now that the principal has an ST for the secured service as well as a mechanism for secure communication to that server, client may now establish a connection and attempt to access the secured resource. Client starts by passing to the destination server the ST, which also contains the server component of the session information, it received from the TGS for that destination. The server attempts to decrypt the session information passed to it by the client using it’s long-term key from the KDC. If it succeeds, the client has been successfully authenticated to the server and the server is also considered authenticated to the client. At this point, trust has been established and secured communication between the client and server may proceed.

Last update: **2017/09/08 12:16**