

# Appgate and Kerberos

Authors: Jamie Bodley-Scott (Appendix by Malcolm Hamilton)

May 11, 2010

## Content

|   |   |
|---|---|
| Appgate & Kerberos .....                                  | 3 |
| Introduction.....   | 3 |
| Implementing Appgate and Kerberos .....                   | 3 |
| Network considerations .....                              | 3 |
| Client machine considerations .....                       | 3 |
| Domain Controller (DC) considerations .....               | 4 |
| Appgate Security Server considerations .....              | 4 |
| Use of Chained Authentication .....                       | 6 |
| Conclusion .....  | 6 |
| Appendix 1 .....  | 7 |
| Kerberos Protocol and Appgate .....                       | 7 |
| Kerberos Basics .....                                     | 7 |
| How Kerberos works with multiple domains and trusts:..... | 8 |
| Appgate and Key Referrals.....                            | 8 |

# Appgate & Kerberos

## Introduction

Kerberos is used in Windows domains and is the default authentication method. It is sometimes very useful to have the Appgate server seen as just another internal resource on the domain so that client machines already logged on to the domain can use it just as they might an email server. Kerberos authentication lets a client machine, which is already logged into the domain log into an Appgate Security Server using their existing Kerberos ticket. Policy on the Appgate server might then allow the client machine to selectively see through the Appgate to some protected resources on a different network.

Kerberos in itself is a quite complex subject matter and for those who are interested there is a more detailed discussion about the inner workings of Appgate and Kerberos included in Appendix 1 of this document.

## Implementing Appgate and Kerberos

The reason why companies implement Appgate with Kerberos is to simplify the user experience when introducing some security access controls to the network. Users don't want to have to go through extra login procedures or remember additional passwords. The whole point of Kerberos is to let users access resources without any additional user interaction. Below are some suggested steps, which if followed, will give users seamless access resources protected by an Appgate Security Server.

### Network considerations

Kerberos authentication is useful when you need to access some resources that are away from the main network. This might be the case for a number of reasons such as to create a separate security zone for compliance reasons or because a joint venture business might have some shared network resources.

The Appgate will allow access to these additional resources on a case-by-case basis. So for two users on the same domain, one might be able to access two of these additional resources through the Appgate, however the other might have no access whatsoever.

To use this authentication method the client machine must already be authenticated to the domain controller so they must reside on the same network. The domain controller is often also the Key distribution centre (KDC) for Kerberos tickets. The client machine must also be able to speak to the KDC so it cannot be located behind the Appgate server.

The Appgate must be sitting between the client machines (users) and the protected resources. This can be done simply by connecting the two different networks to two different interfaces on the Appgate. However if this is not possible then the Appgate understands VLANs, so as long as the client machines and protected resources are on different VLANs then that will work just as well.

### Client machine considerations

There are several things to consider when provisioning access from client machines using Kerberos authentication. Firstly they need to be logged into the domain as stated already. A couple of other areas need to be attended to make the authentication work in a seamless way, namely, software installation and client machine configuration,

Kerberos authentication is useful when you need to access some resources that are away from the main network. This might be the case for a number of reasons such as to create a separate security zone for compliance reasons or because a joint venture business might have some shared network resources

## Software installation

Java is a prerequisite and we recommend the standard Oracle (Sun) Java be installed.

Some Appgate software is required to be installed on all the client machines wishing to use Appgate's Kerberos authentication. As a minimum this will comprise the Appgate client and we recommend the JWS version for this use case. In most situations we also recommend the installation of the Host File Writing Service as well. These together will allow access to almost all types of application and has the advantage of maintaining IP separation between the two networks. If more complete network connectivity is required such as reverse connections, UDP, port ranges, etc. then the Appgate IP Tunneling Driver should also be installed.

These software components could all be installed as part of the standard build, by some sort of network push or by users (as there is no local configuration/settings).

If the client machine is already used for Appgate access then no new software need be installed (and if a new webstart client is required it will download automatically).

## Machine configuration

To enable Kerberos authentication on client machine a registry modification is needed in order to allow the Appgate Client to generate the proper credentials to send to the Appgate Security Server.

The registry modification is that the key `allowtgtsessionkey` (of type `REG_SZ`) in `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters` needs to be set to 1. The key must be created if it does not already exist. The machine must be rebooted after the key has been set. More information can be found in Microsoft kb 308339.

To enable automatic Kerberos authentication the Appgate software will need starting automatically. This can be done easily by putting something in the users auto-start folder such as a BAT file. The Appgate client has been written in such a way that if the server name is specified in the command line then the client attempts to connect to that server without referring to the user. A command such as:

"start javaws -Xnosplash <http://my.appgate.com/webstart2/agclient.jnlp>" will achieve this. The -Xnosplash statement ensures the Java splash screen is suppressed. No user name needs to be entered into the Appgate client because this comes from the users windows login, which is already known.

To enable Kerberos authentication on client machine a registry modification is needed in order to allow the Appgate Client to generate the proper credentials to send to the Appgate Security

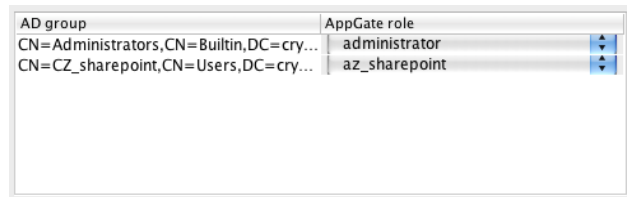
## Domain Controller (DC) considerations

The Appgate will use the DC as the authority for user identity so any users wanting to access resources through the Appgate need to be in the LDAP database. Additionally the Appgate will use group membership and/or user attributes to decide who has access to what. In its simplest form a group would be created for users who need access to Appgate protected resources. The Appgate would use membership of this group to allow those users through to the controlled resources. Users who were not in this group would be denied access.

## Appgate Security Server considerations

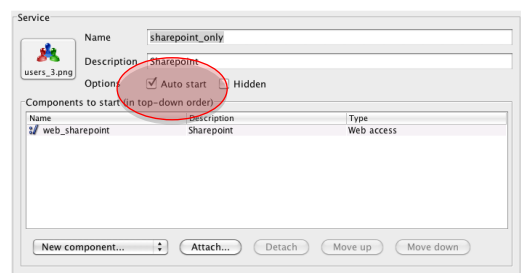
Six things to be considered when provisioning access using Kerberos authentication. The AD group needs to be matched to a role in Appgate. Kerberos authentication needs to be enabled and configured, an access rule might be required for Kerberos, any services should be set to auto-start, if the same Appgate server is to be used by Kerberos and say token users then a separate JWS instance should be created and finally the client configuration files need amending to allow silent log in.

1. There is a dialogue under User Accounts in the Appgate console for matching multiple AD groups to multiple Appgate roles.



2. Kerberos configuration can be somewhat complex and there is already a section included in the Appgate Security Server manual that covers this area. [http://tech.cryptzone.com/download/AppGate-9.2.2/appliance/doc/manual\\_chunked\\_html/ch04s03.html#admin.auth.kerberos](http://tech.cryptzone.com/download/AppGate-9.2.2/appliance/doc/manual_chunked_html/ch04s03.html#admin.auth.kerberos)
3. Access rules are a good idea where the same user might connect to the Appgate in different ways and/or from different places. In this case a user might have two different roles available in Appgate, so in order to ensure seamless login the system must decide which role to use rather than the user deciding. One access rule might just detect "if kerberos" or possibly "if Kerberos and from inside" and this would enable the Kerberos role. The other access rule might just be the opposite "if not Kerberos" or possibly some other authentication option such as "if token" and this would be linked to the other role.

4. Services in the Kerberos role must have auto-start enabled. This ensures connections are opened without the user being required to start the services.



The use of links ensures when the Appgate is upgraded then any changes will apply to this new folder too.

5. A separate webstart folder can be created on the Appgate Security Server (this is optional). The folder /var/opt/appgate/webroot.local/webstart will already exist so something like /var/opt/appgate/webroot.local/webstart2 can be created and it should contain a symbolic links to every file in /webstart with the exception of the agclient.properties file which should be a copy. The use of links ensures when the Appgate is upgraded then any changes will apply to this new folder too.
6. Finally the client configuration file that defines how the client on the users machine should look and behave needs amending. They are set centrally and propagated out to client machines as they connect. The steps taken here again ensure that the logon experience is both automatic and seamless

If a new webstart folder has been created then these adjustments should be made there using the administration console Clients > Client Configuration Files. Any entry made here simply adds to the system generated entries already there. The following lines need to be added:

```
ag_autoconnect=yes
gui_hidesplash=yes
gui_hideafterconnect=yes
gui_hidemainwindow=yes
```

The first instructs the client not to ask the user to OK the login, hidesplash hides the Appgate splash screen and the last two ensure the client is hidden away in the tool tray.

## Use of Chained Authentication

This is a mechanism that Appgate supports for allowing two different authentication methods to be used at once and the results ANDed together. This would make it possible for a network user to have Kerberos authentication specified as one of the links in the chain and say token (via RADIUS) as the other. This makes it possible for users to 'upgrade' their privileges beyond standard network logon as might be the case if a user needed to access some controlled resources such PCI related data.

## Conclusion

By following the guidelines above it is possible to add Kerberos authentication to any existing Appgate Security Server installation. Any usage model already in place such as remote access will not be affected in any way. If a unique webstart instance has been created on the server then this will automatically be replicated onto the clients. The users original webstart application (and desktop shortcut) will not be affected in any way and will still remember their username and preferred login method such as token. The second webstart application will download (or run) to handle the Kerberos authentication method along with its own unique client properties settings.

Exactly the same dual-working model would apply if the user connected to one Appgate when working on the inside using Kerberos but a different Appgate when working on the outside using token authentication.

Dual-working is a key part of the Appgate design and it is there so companies can easily provision access to users through an Appgate without having to worry about how they connect already.

Dual-working is a key part of the Appgate design and it is there so companies can easily provision access to users through an Appgate without having to worry about how they connect already. Very different from IPSec where dual-working is not possible.

# Appendix 1

## Kerberos Protocol and Appgate

This appendix explains how Appgate and the Kerberos protocol interact, as well as explaining how the Appgate system can give access to segmented 3rd party users via Kerberos tickets when trust relationships are in place between Windows domains.

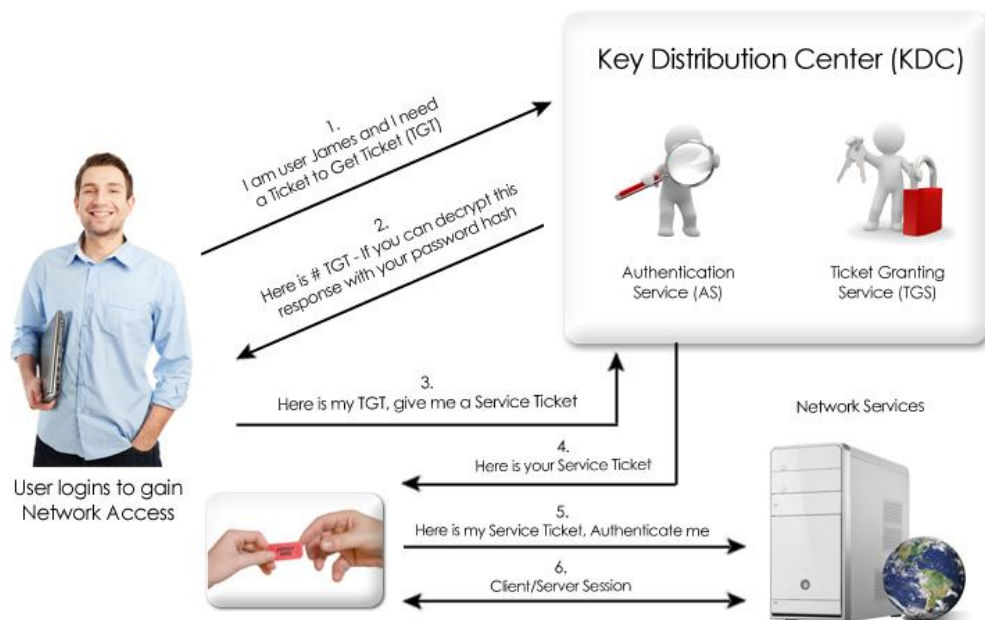
### Kerberos Basics

The KDC (key distribution centre) servers, which in Microsoft world are AD domain controllers, have multiple functions within the one service. AS (Authentication Service) which verifies the users credentials within their domain, TGS (Ticket Granting Service) which if AS is passed, the user is granted a TGT (Ticket Granting Ticket) which is valid for the local domain only. This ticket has a default lifetime of 10 hours and may be renewed multiple times through the users domain log-on session without further authentication. The TGT is cached on the local machine in volatile memory space and used to request sessions with services through out the network.

The TGT is used blindly by the client machine to apply to the TGS part of the KDC for service tickets. When access is desired to a server service the user presents the TGT to the TGS portion of the KDC, TGS authenticates the user's TGT, creates a ticket and session key for both the client and the remote server. This is known as the service ticket and is then cached locally on the client machine. The service ticket is then used to authenticate the client user and establish a server session between the server and client. After the tickets lifetime is exceeded, the service ticket must be renewed using the same process above. Below is a picture to help explain the process.

This ticket has a default lifetime of 10 hours and may be renewed multiple times through the users domain log-on session without further authentication

### Kerberos Ticket Exchange



The Appgate system is configured as a server in the domain and thus has its own long-term key with the KDC. The client machine makes a request to the TGS for a service ticket to use against the Appgate system. Then the connecting client machine blindly passes the server portion of the service ticket received from the TGS to the Appgate server in the client/server request to establish a client/server session. If mutual authentication is enabled the Appgate server returns a time stamp which is encrypted using the service ticket session key.

If the time stamp decrypts correctly, not only has the client authenticated himself to

the Appgate server, but the Appgate server authenticated itself to the client. The Appgate server never has to directly communicate with the KDC to authenticate the users although will need to talk to a user database for role assignment. The process above. Below is a picture to help explain the process.

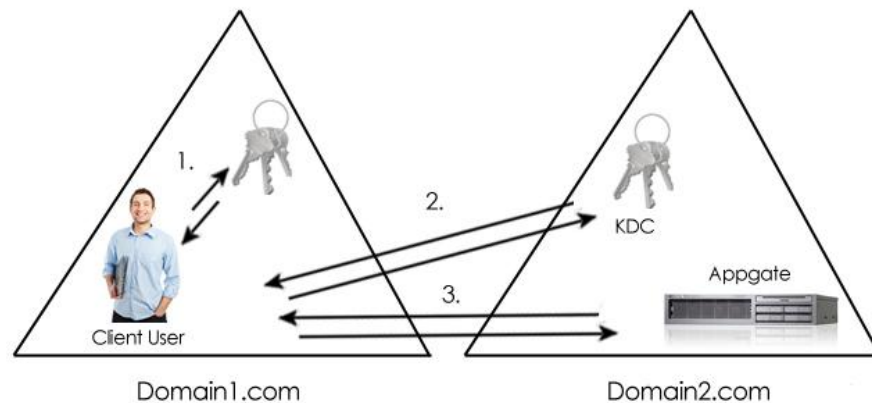
### How Kerberos works with multiple domains and trusts:

As explained above the AS (Authentication Service) and TGS (Ticket Granting Service) are separate within the KDC (Key Distribution Centre). This permits the user to use the TGT obtained from an AS in his domain to obtain service tickets from a TGS in other domains. This is done via referral tickets.

Once a trust has been established between two domains, referral tickets can be granted to clients requesting authorisation for services in other domains.

Once a trust has been established between two domains, referral tickets can be granted to clients requesting authorisation for services in other domains. Where there is a trust established between two domains, an inter-domain key, based on the trust password becomes available for authenticating KDC functions. This can be best explained in Appgate terms of a user/client being a member of domain1 seeking authentication to an Appgate server in domain2 with a Kerberos ticket. This is illustrated below with a user client in domain1.com requests authority for an Appgate server in Domain2.com. He utilises referral tickets. The numbers in picture below correspond to the following numbered explanations:  
 The client contacts its domain KDC TGS using a TGT. The KDC recognizes a request for a session with a foreign domain server and responds by returning a referral ticket for the KDC in the foreign domain. The client contacts the KDC of the foreign domain with the referral ticket. This ticket is encrypted with the inter-domain key. Given that the decryption works, the TGS service for the foreign domain returns a service ticket for the server service in Domain2.com.  
 The client performs the client/server exchange with the server and begins the user session with the service.

Key referral between domains



### Appgate and Key Referrals

In terms of Appgate what does this mean? Well the client machine will somehow need access to their own domain KDC server as well as access to the Appgate's home KDC server. The fact remains that both of the domains are behind an Appgate server, which means that user has no access. Users can login twice through the Appgate system and the first login would be to allow access to the correct domains for the Kerberos process to happen.

#### Step 1

Access needs to be granted to the relevant KDC servers on the relevant ports. Some sort of authentication is needed to the Appgate to be able to assign the correct access rights to the correct domains. This could be an Appgate USB stick with an Appgate client and a certificate or Public key authentication; there are some security concerns about this that need to be considered.

**Step 2**

Once step 1 has been completed an hta script could be displayed to the user, which maps a drive to their domain netlogon share and force's domain authentication, thus enabling the TGT process. This in turn enables the windows clients to get a service ticket from the Appgate's local domain's KDC for authentication against the Appgate server.

One of the features needed from the 9.2 version for this to work is the ability to use IP-tunneling in multiple simultaneous sessions; this will be needed as Kerberos runs over TCP and UDP protocol.

A second in 9.2 is realm resolving which now reads the realm from the agclient.properties file. (If a client machine from the 3<sup>rd</sup> party domain tries to login via Kerberos, the client would otherwise present the wrong realm to the TGS and authentication will fail as a service ticket would not be generated). Full testing with multiple trusted domains with kerberos ticket authentication has not been undertaken.