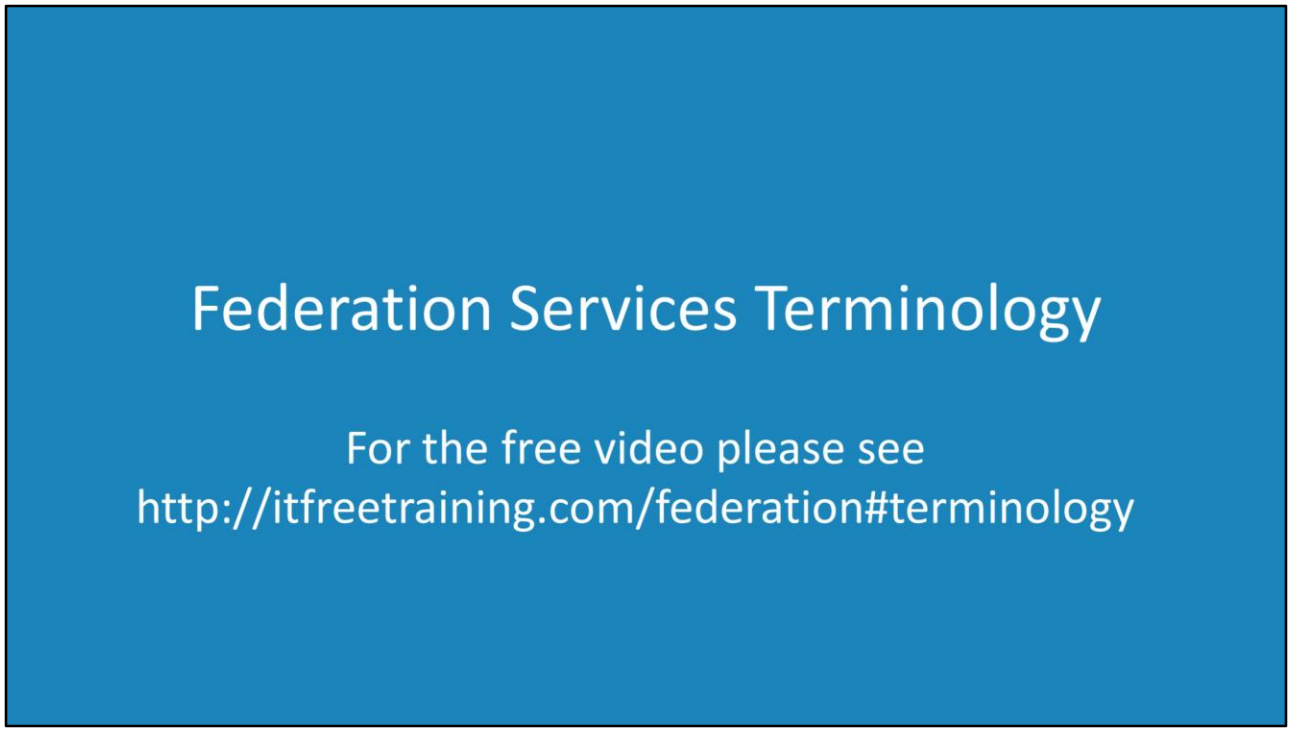
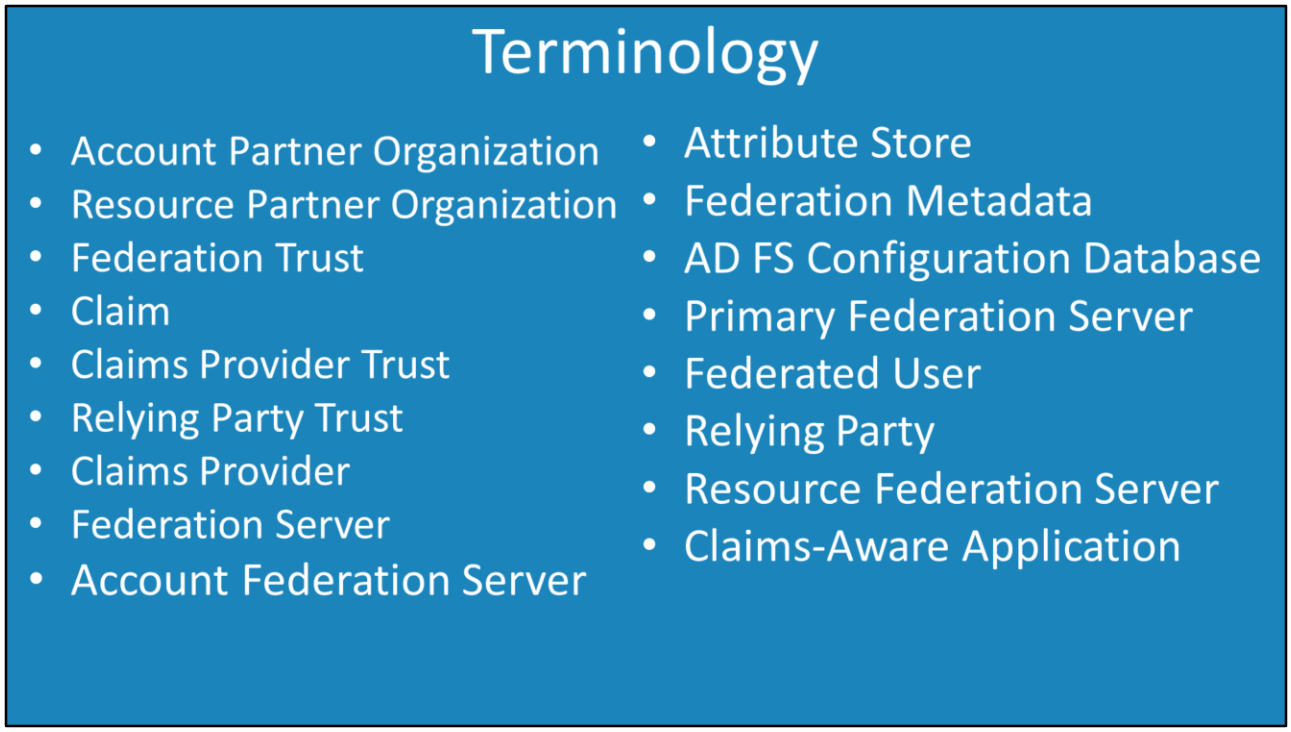


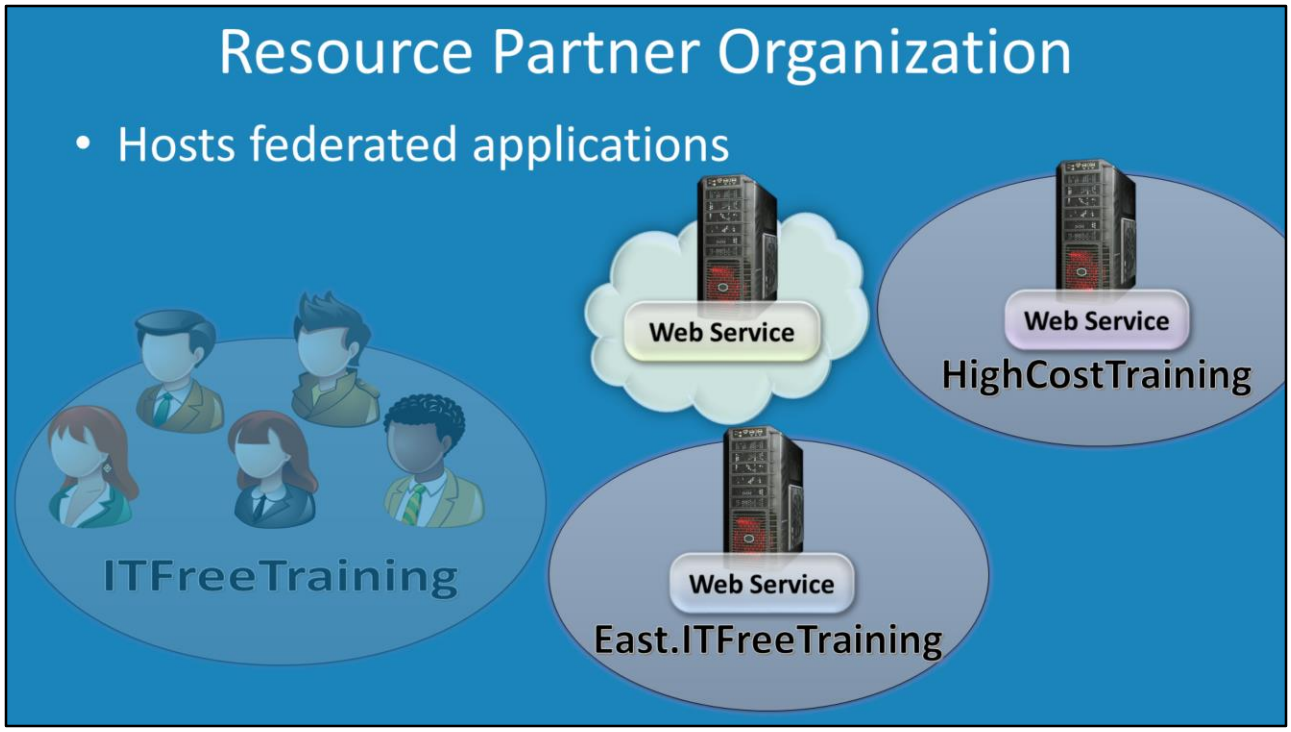
This video will look at the different Terminology that is used with Federation Services. This will give you a good indication of what components make up a Federation Service in Active Directory Federation Services and other Federation services.



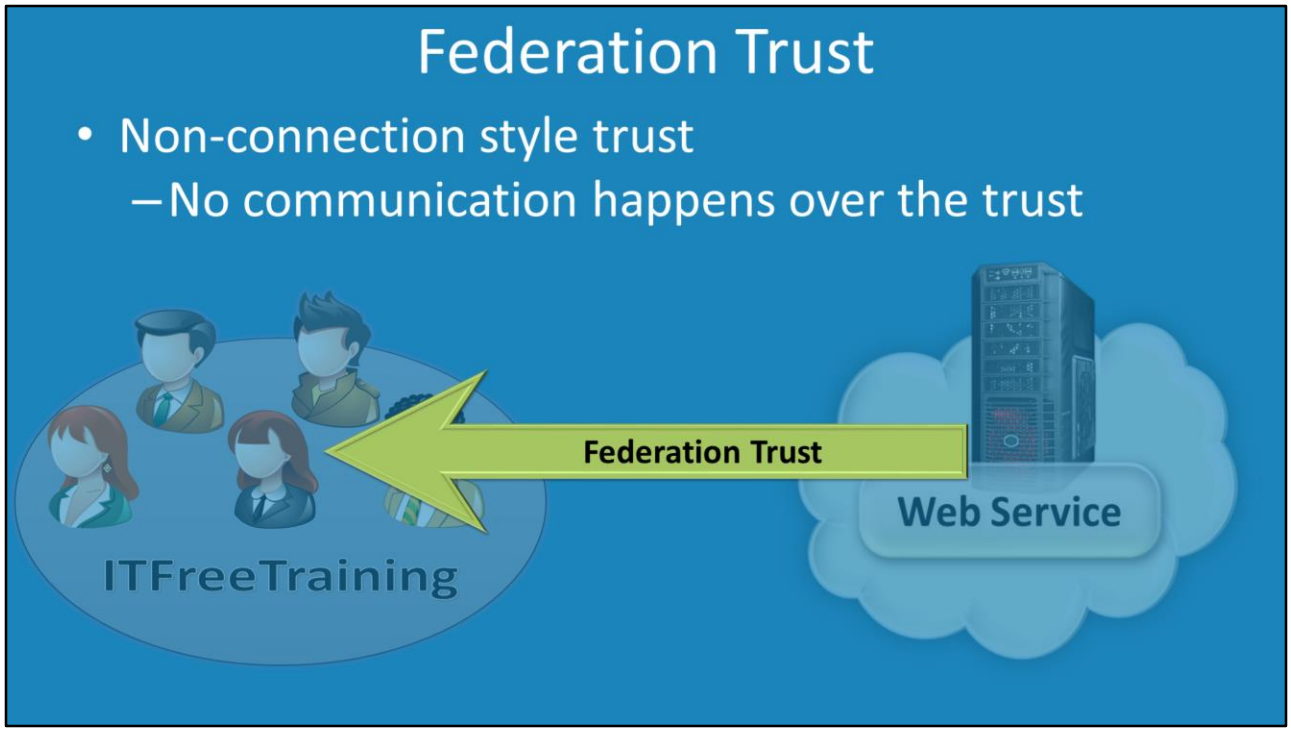
Terminology

This video will look at 17 different Federation Services terms. They have been placed in a logically order to make it easier to understand.

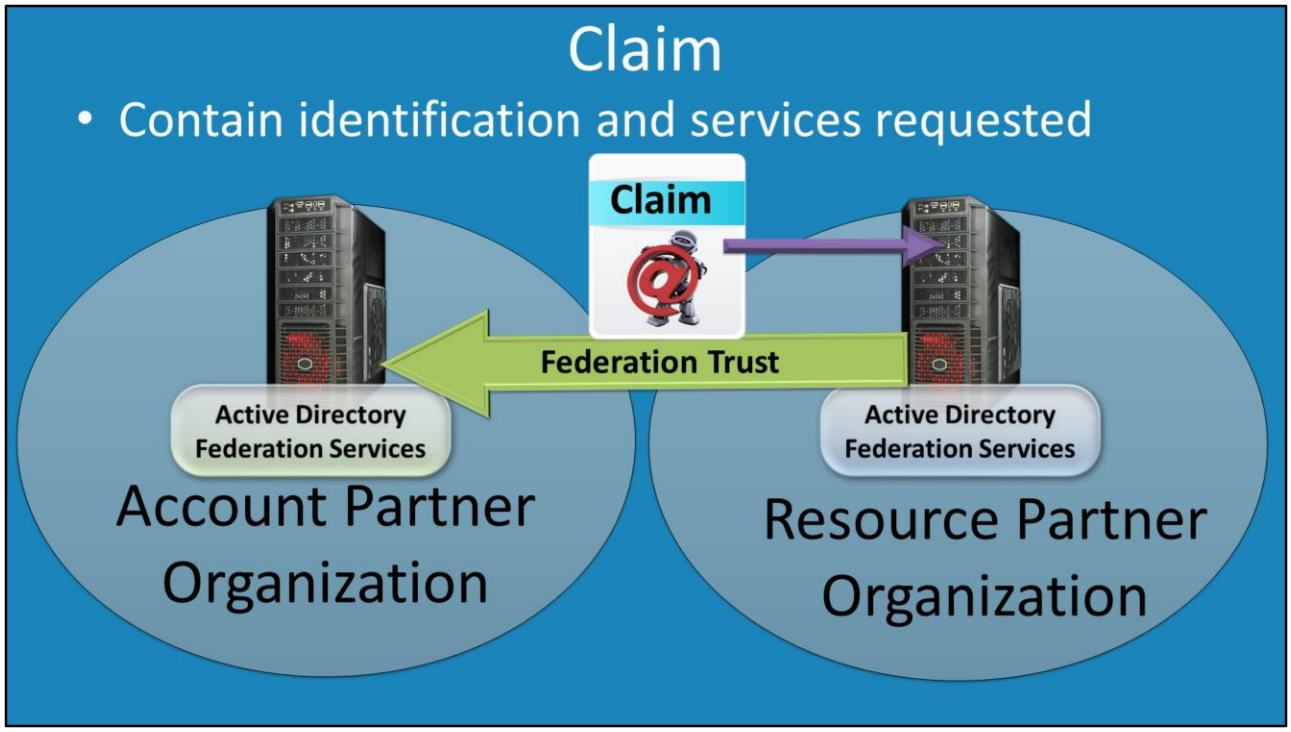
Account Partner Organization
This contains the user accounts that will access the Federation Service. In some cases this may be a domain in other cases it may be a database or simply an e-mail address. The important point to remember is that these are the users that will access Federation Services. This will contain information like their usernames, password and other details about the user.



Resource Partner Organization
A resource partner organization contains the resources that are accessed by the Federation Service Users. Normally this will be external to the company, but in some cases may be on a DMZ of the company. A resource partner could also be in a cloud based application. For example MS Office products located in the cloud.

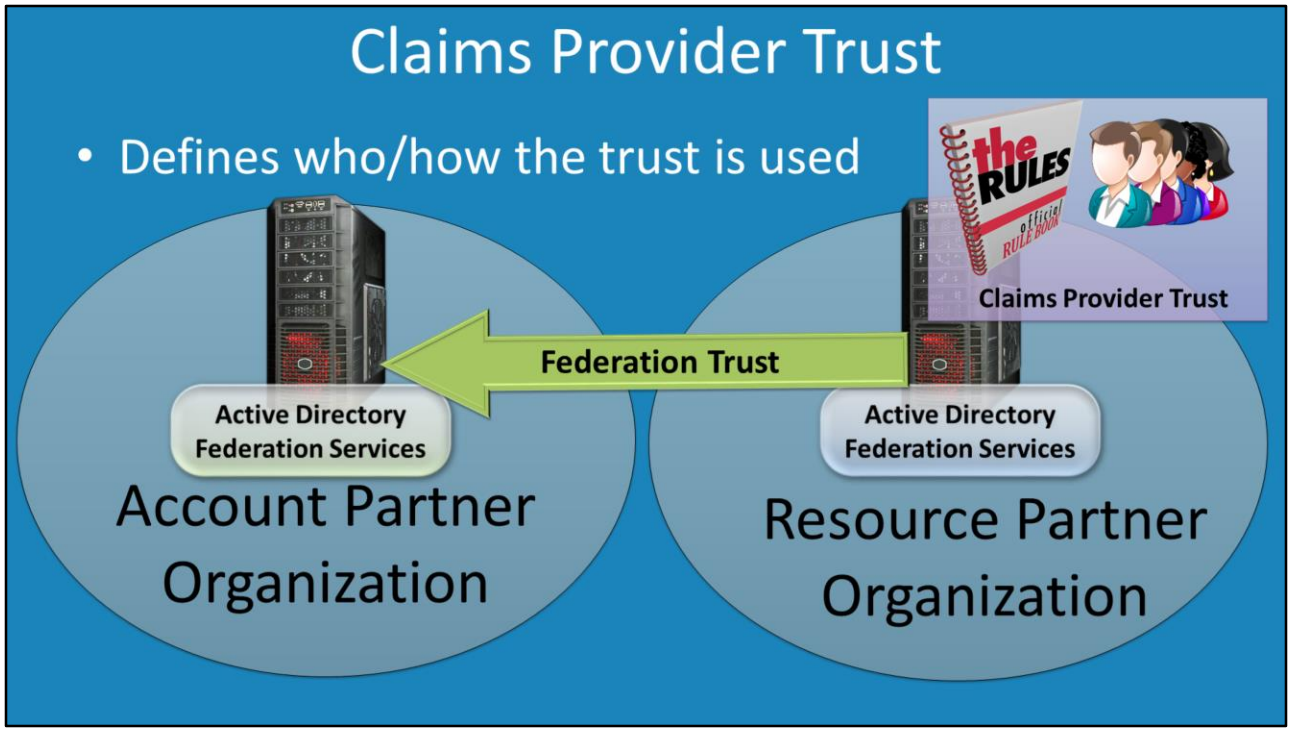


Federation Trust
A Federation Trust is a trust between different parts of Federation Services. An example is the trust between the Account Partner Organization and Resource Partner Organization. The trust is not a connection style trust and thus when created does not require communication to happen over the trust. The trust does not require a direct connection between the two Federation Servers, however it is often simpler to have a connection between the two so that the Federation Server can obtain information that it requires in order to create the trust.



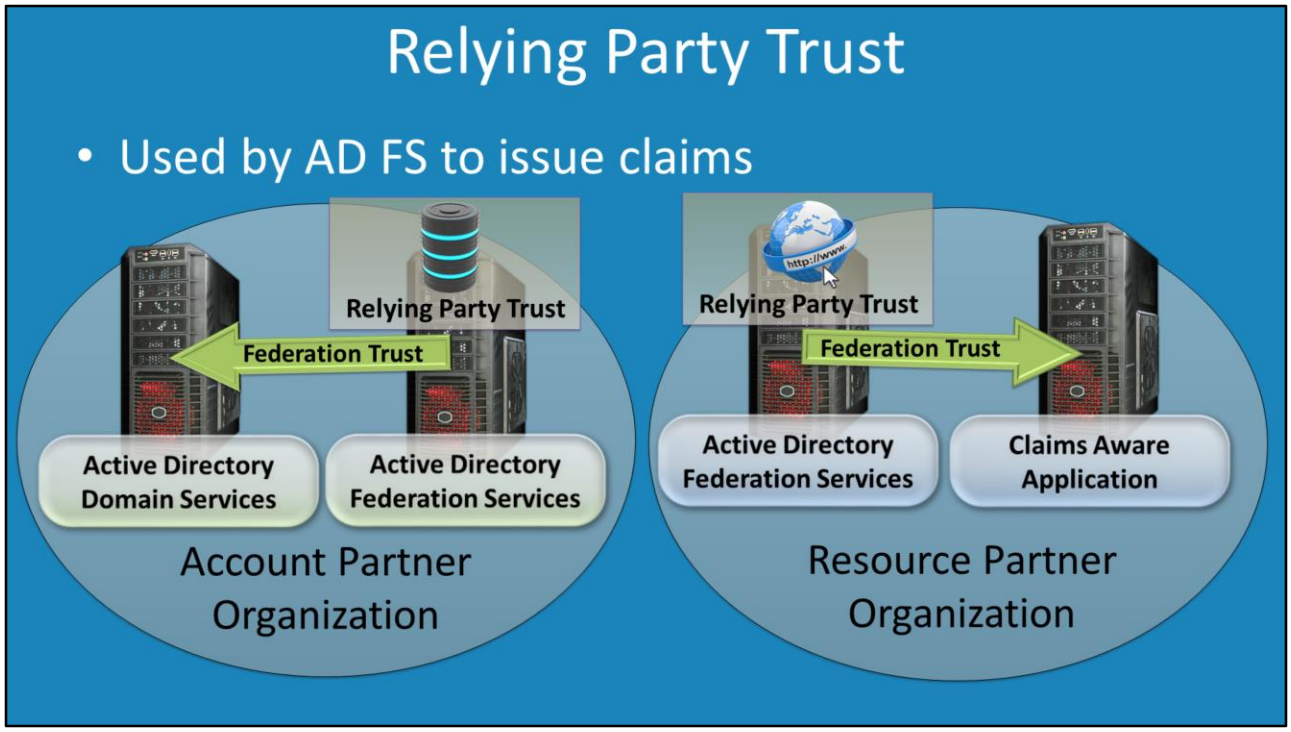
Claim

A claim is essentially a statement about a user. When the claim is created, it will need to be created with information required by the other side. This may include information about what services they require. This may also contain information about groups they are in. The Federation Server creating the claim needs to ensure all this information is put into the claim. The claim is essentially a file that is then transferred to the other party. In a lot of cases, the user may request the claim from their Federation Server and then present this claim to the Federation Server that is providing the service.



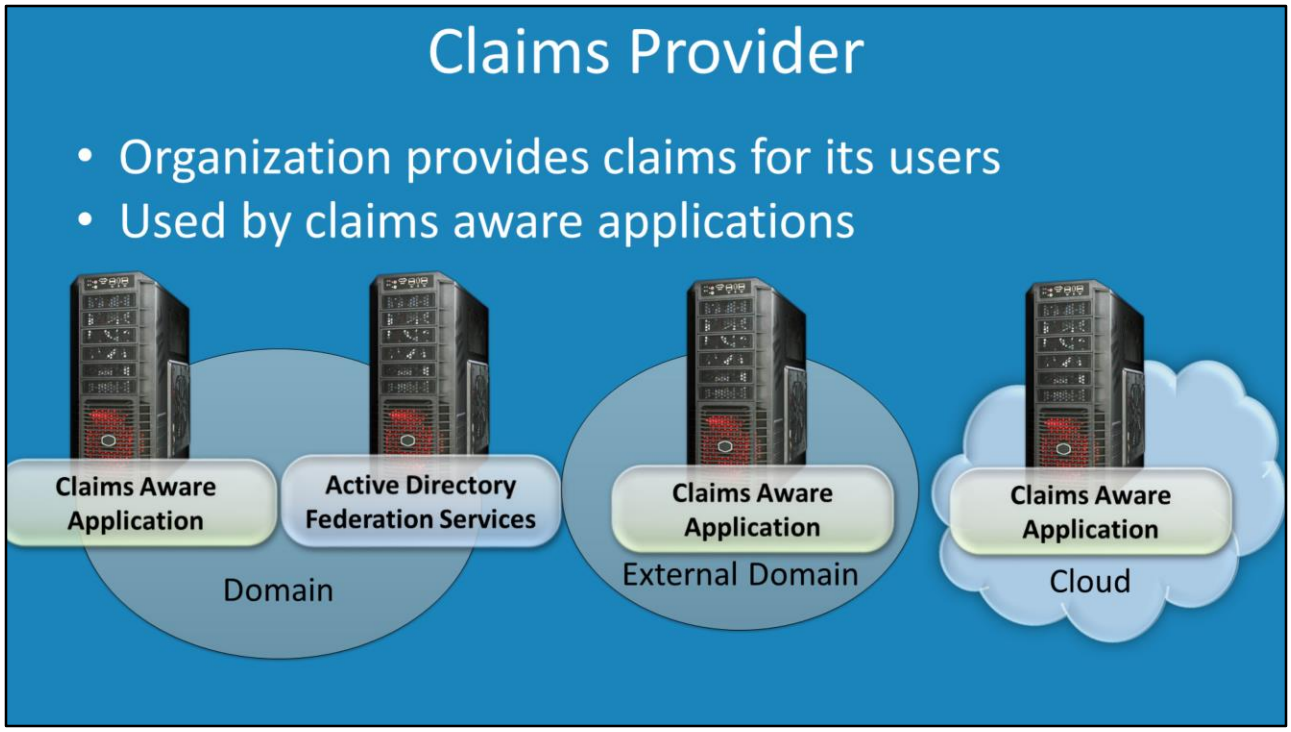
Claims Provider Trust

Active Directory Federation Services has two types of trusts that are used. The first trust is a Claims Provider Trust. A Claims Provider Trust accepts claims. So essentially this trust defines who and how the trust can be used.

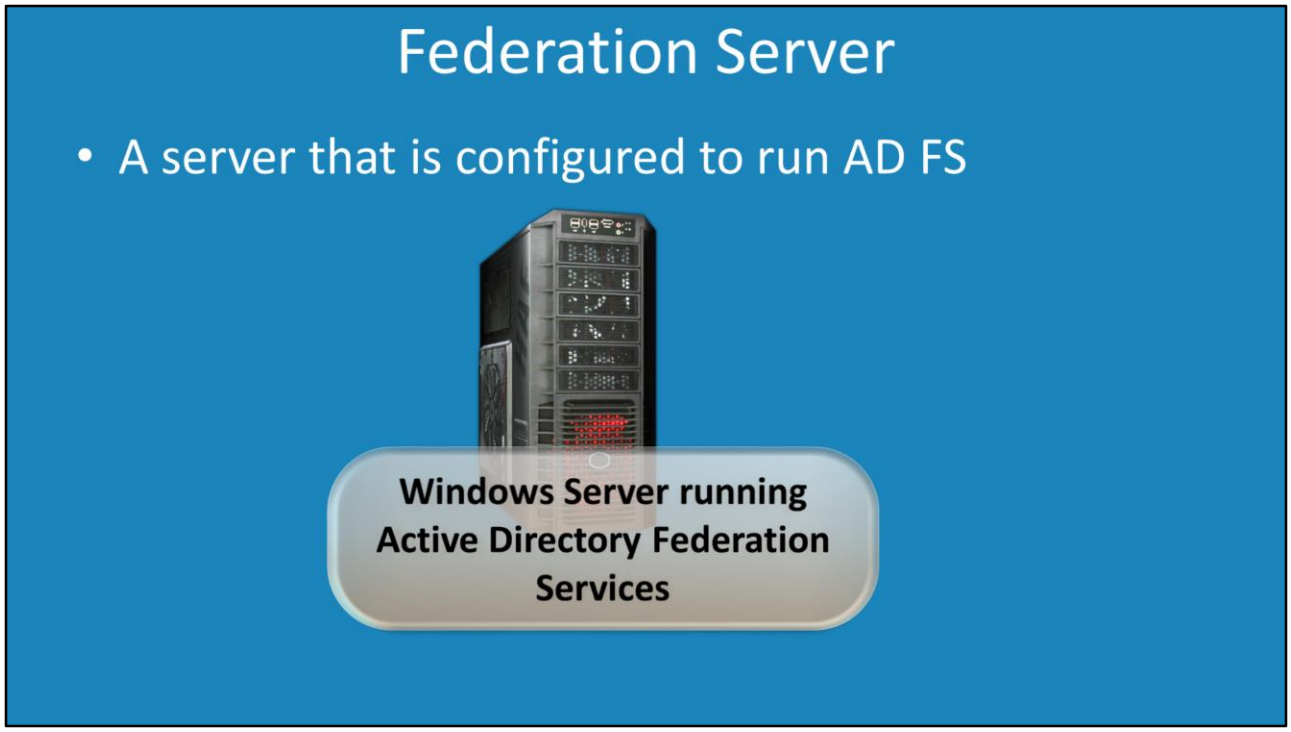


Relying Party Trust

A Relying Party Trust is used to create claims. Once a claim is created it is supplied to a Claims Provider Trust. A Relying Party Trust is required in the account partner organization to create claims that will be used in the Resource Partner Organization. A relying party trust is also used to access resources. For example, if the Active Directory Federation Services needs to access an application or Domain Services.



Claim Provider
A claims provider is an organization that provides claims for users. These claims are normally used by Claims Aware applications that can be in the domain, external domain or in the cloud.



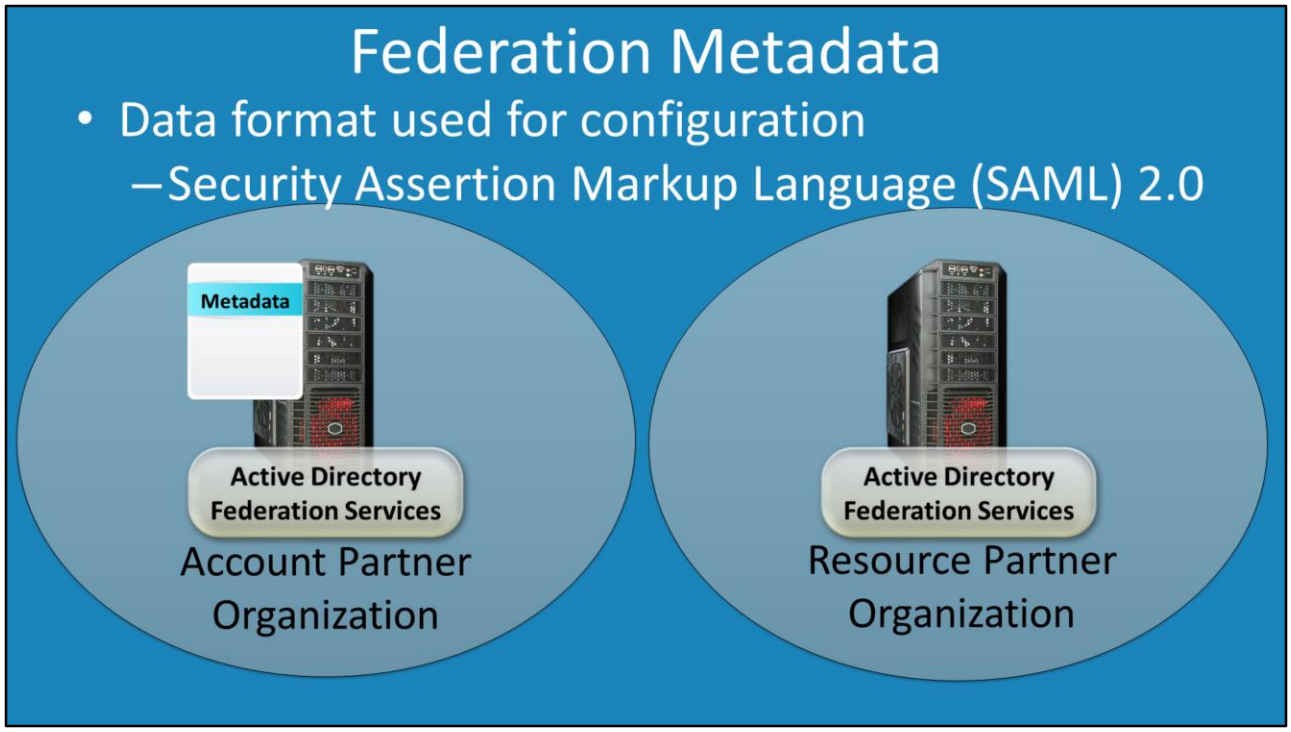
Federation Server
This is a server that is running Federation Services. In the case of Windows this will be Active Directory Federation Services.

Account Federation Server

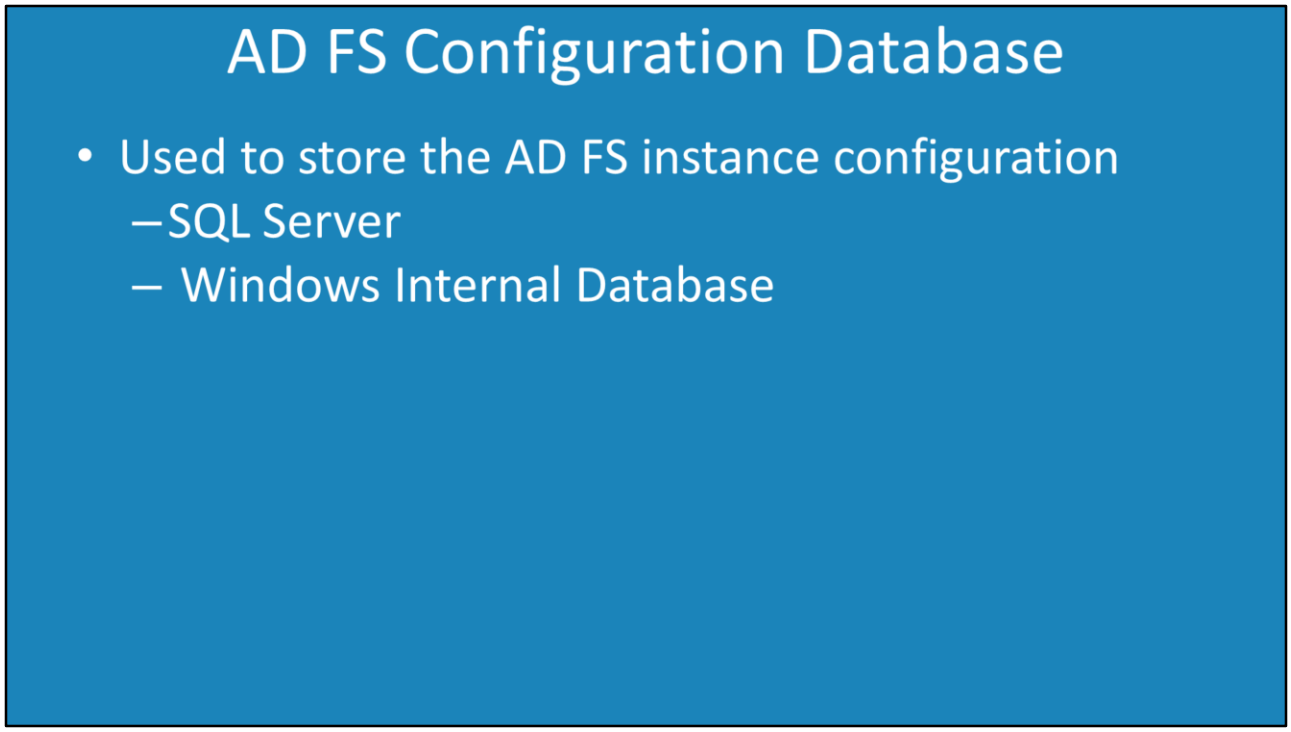
An Account Federation Server provides security tokens that contains claims. These are given to the user. In order to do this the account Federation Server must get this information from somewhere.

Attribute Store

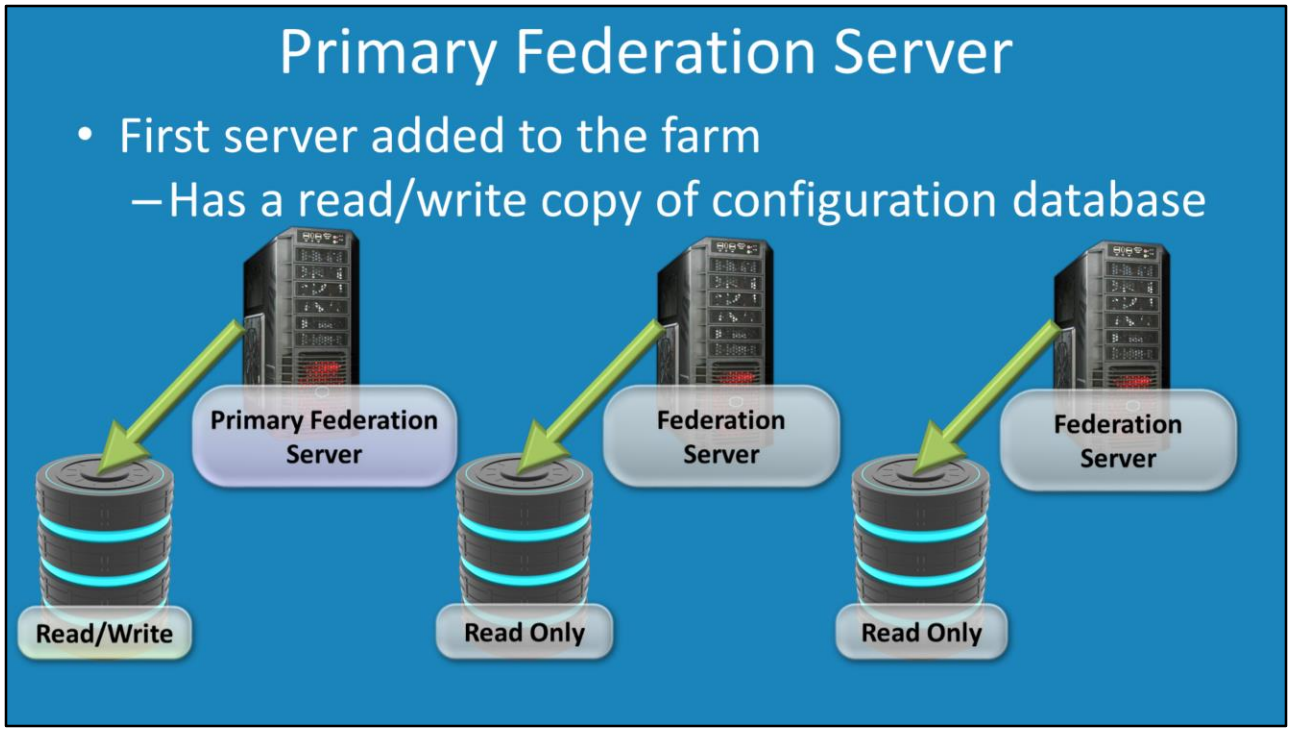
An attribute store contains information about the user. This can be stored in Active Directory Domain Services, SQL Server or Active Directory Light Weight Directory Services. This does not provide authentication. For example a Domain Controller could be used to authenticate the user and then the attribute store could be used to get additional information about the user. For example the attribute store may contain a picture of the user.



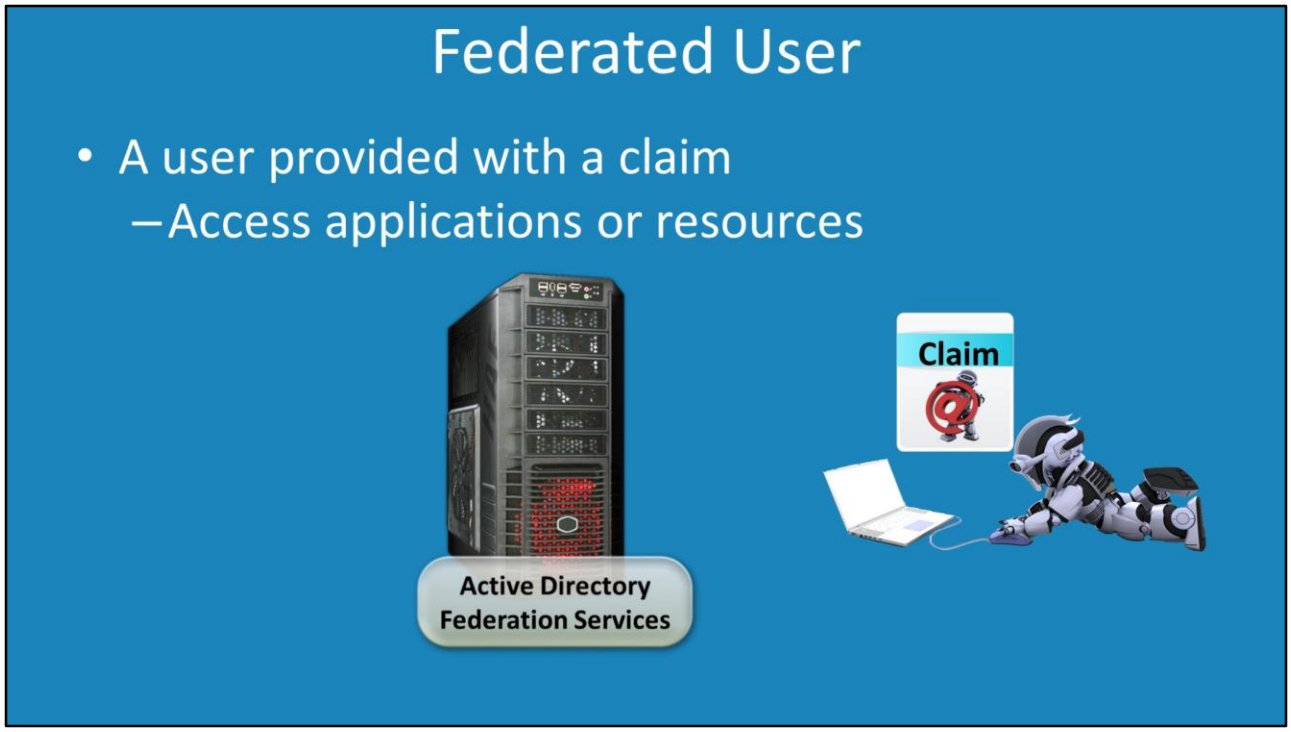
Federation Metadata
This is the configuration information for the Federation Server. When creating a trust, data is required about the other server in order to create the trust. This data can be entered in manually however this is time consuming to do. When creating the trust, you have the option to use the Metadata. This Metadata can be obtained through a direct connection between the two servers. If this is not available, the data can be exported and any method can be used to get the data from one server to the other server.



AD FS Configuration Database
This stores the configuration that is used by Active Directory Federation Services. This can be on SQL server or Windows Internal Database.

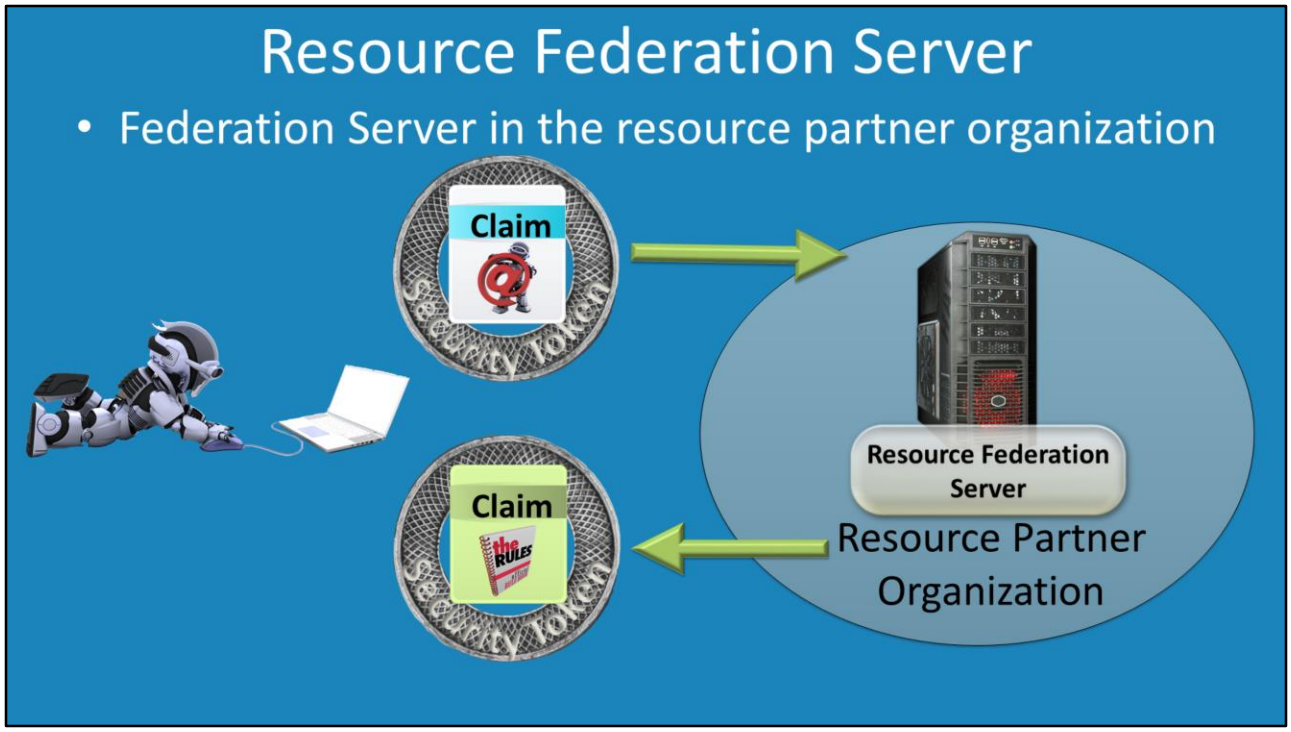


Primary Federation Server
This is the first server that is setup in a farm. It holds a read/write copy of the database. All the other servers in the farm contain a read only copy of the database. These servers needs to replicate changes to the read/write copy of the database.



Federated User
This is a user that has been given a claim. The claim can then be used on another server to gain access to a resource.

Relying Party
A relying party is the organization that receives a claim. In most cases this will be the resource partner organization.



Resource Federation Server
This is a Federation Server in the resource partner organization that accepts claims. When a claim is presented to the server, the server will create a new claim and give this to the user. This claim contains information like what resources they are allowed to access.

Claims-Aware Application
This is any application that can accept claims to provide access to an application. For example MS Office is capable of accepting claims.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 888-896
"Understanding Key Concepts Before You Deploy AD FS 2.0"
http://technet.microsoft.com/en-us/library/ee913566(WS.10).aspx
"Federation trusts" http://technet.microsoft.com/en-us/library/cc738707(v=ws.10).aspx
"Understanding Application Types for AD FS Federation"
http://technet.microsoft.com/en-us/library/cc772483.aspx