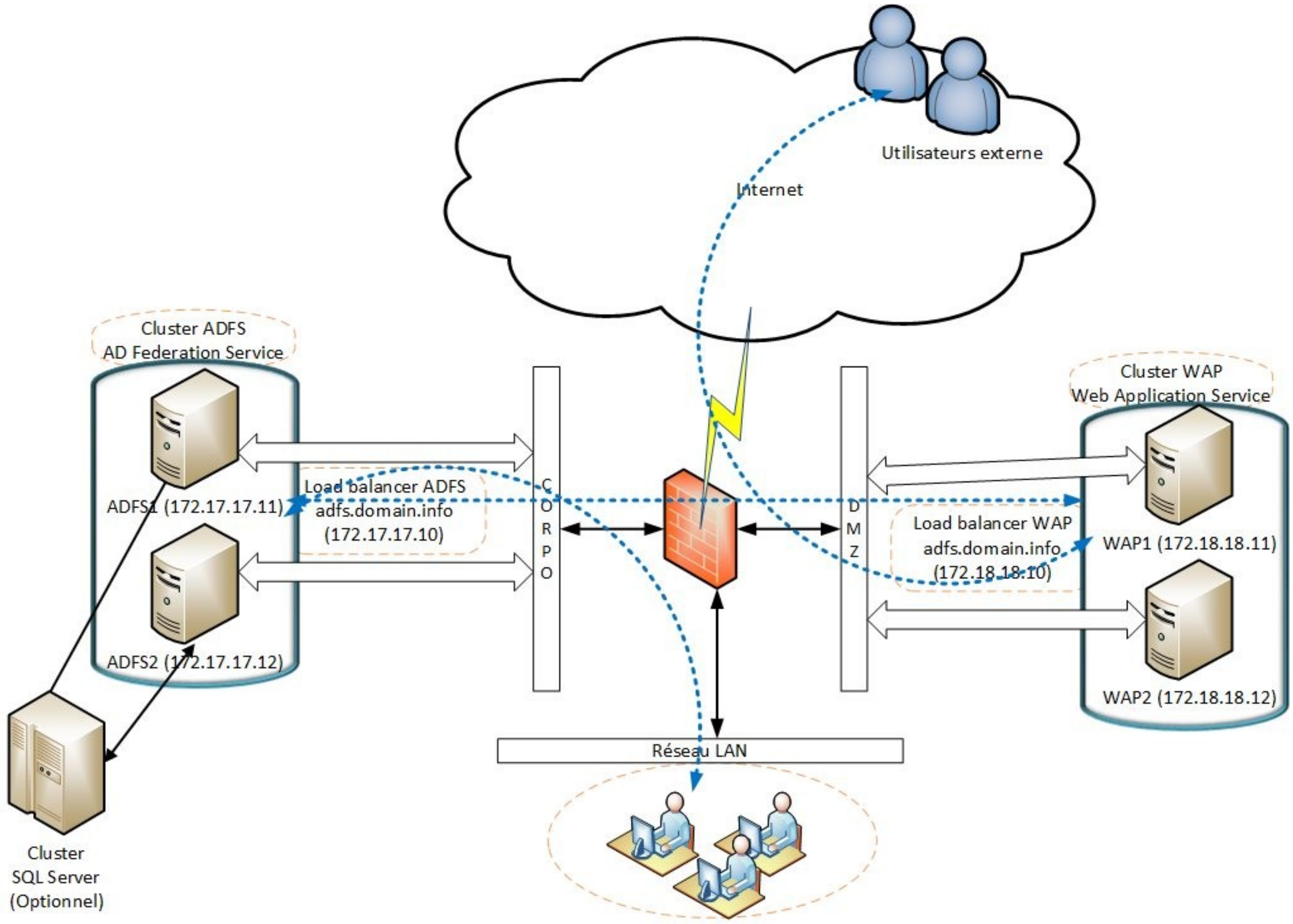
ADFS

Explication de ADFS en quelques schémas.
ADFS = Active Directory Federation Services



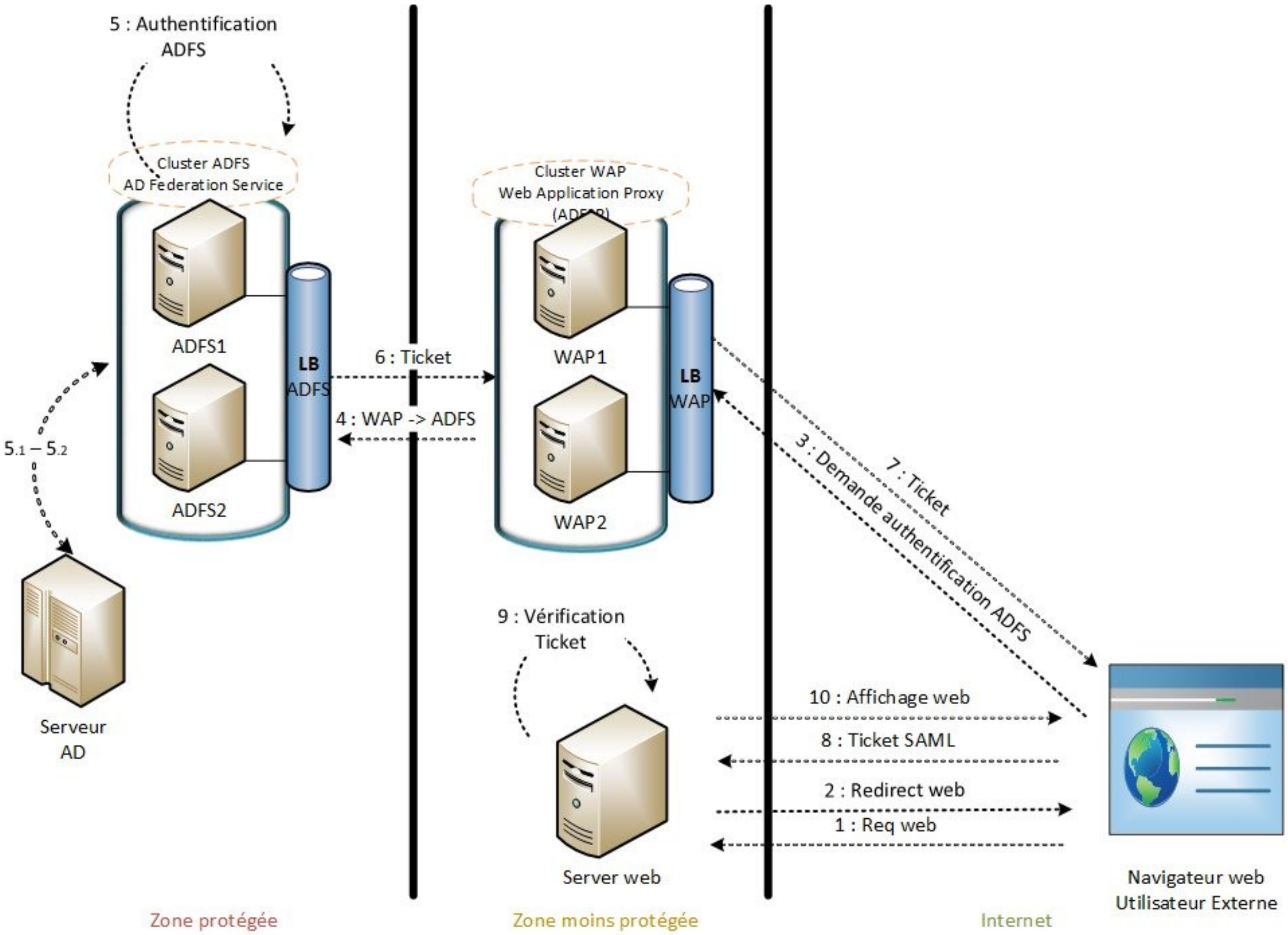
Dans ce schéma, nous avons un cluster ADFS (interne) composé de 2 serveurs ADFS et d'un cluster de SQL Server. Les SQL Servers sont optionnels et ne sont utiles que dans des cas extrêmement rare d'une architecture ADFS.

« ACBrown & Walter – Since you guys both bring up the topic of SQL vs.
WID, I figured I would answer this at once. For all the ADFS deployments that I've done,
rarely have I found a great reason to deploy SQL. Like ACBrown said, "the added infrastructure, software licensing, and support usually can't be justified". Microsoft recommends SQL for three reasons: 1.)
Token Reply Detection – This is only relevant to customers where their ADFS will be receiving tokens.

If you have ADFS for the sole purpose of providing your users access to federated applications,

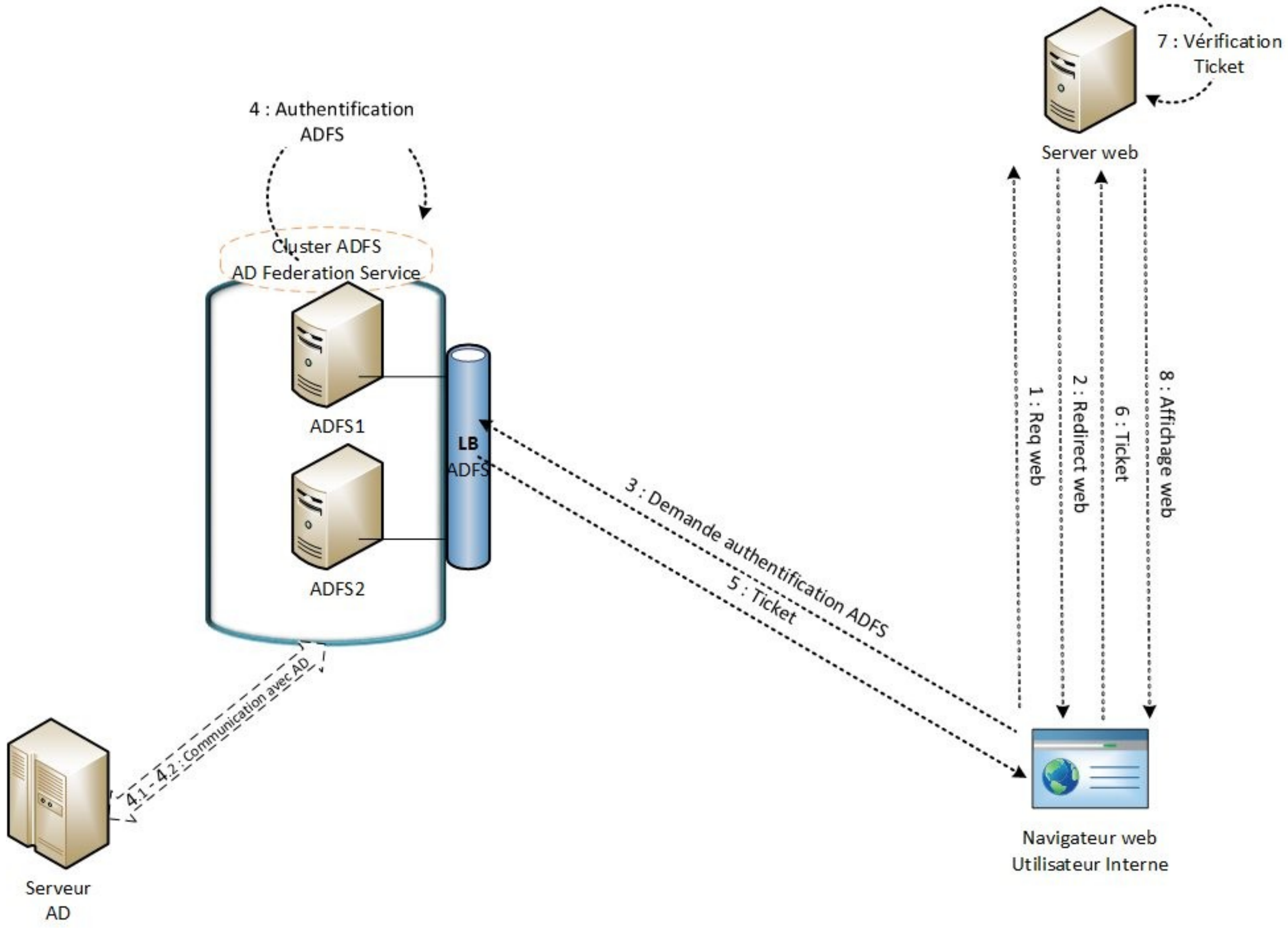
this feature doesn’t matter to you because you’re sending tokens, not receiving them.
If you host applications that users from other partners and/or organizations will need access to
then TRD is relevant to you because you’re receiving inbound tokens.
In theory, WID can perform TRD but WID replication isn’t fast nor robust enough
to safeguard against TRD across all members in the farm.
2.) Artifact Resolution – In all my ADFS deployments of the past many years, I’ve never seen this deployed.
Once again, in theory, WID could perform this but replication isn’t fast nor robust enough
to ensure all DB’s are in-sync ensuring a consistent experience across all servers in the farm.
3.) So, all we’re left with is scalability.
Microsoft recommends SQL if you have 1,000 relying party trusts or more than 50,000 active users on ADFS.
Since most customers probably have less than 20 RP’s and rarely do RP’s change,
the only reason to move to SQL is if you have so many users that WID just can’t keep up
but then you have to consider the reliance on a SQL server that is managed by somebody else across a network that is managed by another team.
Consequently, from my experience, WID is completely suitable for the majority of ADFS deployments. »

Le cluster ADFS cause avec des serveurs AD comme on le verra dans notre prochain schéma.
Grâce à un load balancer, ces 2 ADFS internes se partagent une VIP, et sont contactés directement par les clients internes.
Les clients Internet vont d'abord contacter les serveurs WAP, qui jouent le rôle de ADFS-P (Proxy ADFS), qui vont transférer la requête au cluster ADFS interne.



Ce schéma décrit le fonctionnement de ADFS avec SAML.
Nous avons un client externe (navigateur web), qui veut s'authentifier auprès de son serveur web.

1- Le client tente d'accéder à une page web.
2- Le serveur web se rend compte que le client n'est pas authentifié et le redirige vers une page d’authentification (Il lui demande d'aller voir le serveur ADFS).
3- Le client contacte le WAP pour s'authentifier
4- Le WAP transfère la requête d'authentification à l'ADFS
5- L'ADFS fait appel à AD pour valider les credentials fournis
6- L'ADFS revient vers le client avec un ticket SAML
7- Le WAP transmet le ticket au client
8- Le client présente le ticket au serveur web
9- Le serveur web vérifie le ticket
10- Le serveur web affiche la page demandée.



Pour ce schéma (plus simple), notre client est interne.

Sources :

https://blogs.technet.microsoft.com/askds/2012/06/26/an-adfs-claims-rules-adventure/
https://blogs.technet.microsoft.com/askds/2012/01/05/understanding-the-ad-fs-2-0-proxy/
https://technet.microsoft.com/en-us/library/dn584113.aspx
http://technet.microsoft.com/en-us/library/hh831502.aspx
https://technet.microsoft.com/en-us/library/dn554242.aspx
http://blogs.technet.com/b/platformspfe/archive/2014/08/28/part-1-windows-server-2012-r2-ad-fs-federated-web-sso.aspx
http://blog.rhysgoodwin.com/cloud/salesforce-sso-with-adfs-2-0-everything-you-need-to-know/
http://www.vemployee.com/blog/adfs-configuration-and-saml-20-drupal/