Demystifying the Citrix XenApp logon, enumeration and launch steps — new details included

December 19, 2016 by Bas van Kaam / 3 Comments

This continues to be a topic of interest. Not only is it interesting and fun (right?) to know what is going on underneath the hood once you fill in your user credentials, it can also be very helpful when it comes to troubleshooting certain issues. While I have written about the login, enumeration and launch processes before, again I managed to include a couple of subtle changes/details.

External login and enumeration

- A user opens up a web browser and connects to the external URL of the NetScaler Gateway (preferably using SSL over port Nr. 443). Here he or she will fill in his or her username and password. A locally installed Citrix Receiver can also be used to establish a direct connection to the NetScaler Gateway. Citrix Receiver uses so called Beacons to determine if a connection is internal or external and handles it accordingly. Check the (red) link for some more detailed information around Beacons and the discovery process.
- During the login/authentication process an EPA (End Point Analyses) scan might be performed as part of a SmartAccess/SmartControl policy, for example, or NetScaler multi-Factor a.k.a. nFactor

authentication could be configured (optional as of NetScaler 11.0 build 62.x and onwards).

- * Eventually the NetScaler will authenticate the user credentials (session ticket) against Active Directory, preferably using TCP port Nr. 636 (SSL) based upon the configured Authentication Policy. This could also involve two-factor/RADIUS authentication, which is basically considered a must have/minimum these days. Like StoreFront, the NetScaler has its own Authentication Service.
- Once authenticated, the NetScaler will assign a session cookie (note that it does not built/assign the authentication token as part of the initial authentication process), which will be used for any potential subsequent client requests.
- Next the user session and the user authentication credentials get redirected to StoreFront (based upon the configured Session Policy) where it will perform a call-back to the NetScaler (Gateway Virtual Server) that handled authentication to validate the user in the first place. The authentication details will then be send to the StoreFront Authentication Service, which is similar to the Authentication Service of the NetScaler mentioned earlier.
- This is where the earlier mentioned authentication token actually is built/generated — by default the StoreFront Authentication Service will take care of this. However, as of StoreFront version 3.0, Citrix re-introduced XML-based user authentication. By simply running a few PowerShell scripts have a look here user authentication falls back to the XenDesktop/XenApp XML service, which is equal to how Web Interface used to handle things. Particularly useful when StoreFront is not in the same domain as XenDesktop / XenApp and when it is not possible to set up an Active Directory trust, or multiple. Just be aware that this method will be disabled by default. As of StoreFront version 3.5 and upwards PowerShell is no longer needed to enable XML based user authentication, it can be enabled and disabled directly from the StoreFront management console. Here's the accompanying E-Docs page showing you how it's done.
- From here the user credentials will be forwarded, as part of a XML query, to the configured Broker (XML) service on one of the available Delivery Controllers. Both these transactions will use port Nr. 80 by default, which of course can be changed to 443 (SSL).
- In between, StoreFront will check its local data store for any existing recourse subscriptions and stores these in memory.
- The Broker (XML) service will again contact a domain controller (using port Nr. 389 by default, change to 636 for SSL) to validate the user credentials, note that this is different to the user authentication process, as we've established earlier. During this process it will find out to which security groups (SID's) the user belongs.

You basically authenticate/validate against LDAP three times:

1. Through NetScaler (session cookie) -> Active Directory, followed by a redirection of the authentication credentials over to the StoreFront server.
2. Through Storefront, either using the SF Authentication Service or via SF to the XML Service on one of your Delivery Controllers -> Active Directory, this will generate/built the authentication token.
3. Through the XML Service (validation) -> Active Directory, to find out the accompanying security

group SID's used for resource enumeration.

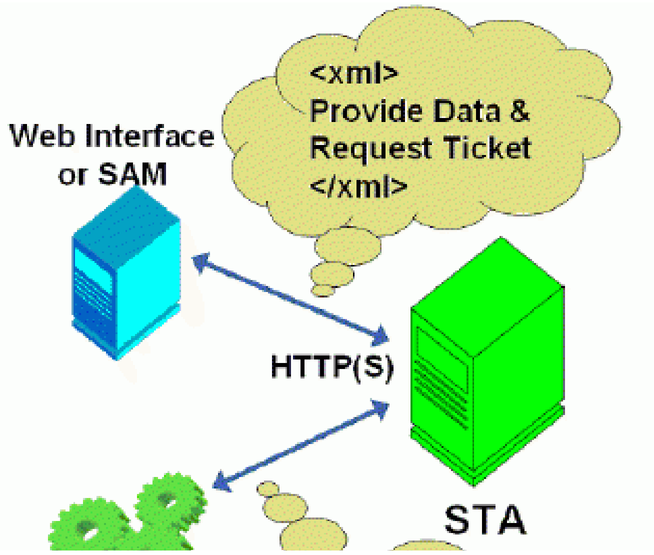
- With this information the Delivery Controller, or Broker (XML) service will contact the Central Site Database to find out which resources have been assigned to the user. It does this over port Nr. 1433 / 1434.
- This data will than be gathered and send back to the StoreFront server in the form of an XML formatted file, through/using the Broker (XML) service.
- Based on this information StoreFront will generate a web page containing all the assigned resources, which will be routed through the NetScaler Gateway and presented to the user. The users home screen will be populated with any pre-subscribed resources (Keywords). Depending on how you connected, your resources will be displayed either directly using a Receiver for web sites or you'll find them within the locally installed Citrix Receiver instead. The user will be able to browse its own personal app store for any assigned resources to which he or she can subscribe and than launch.

* **FMA fact:** If you don't enable authentication on the NetScaler's login page the NetScaler will contact StoreFront and the user will be presented (through the NetScaler) with the StoreFront login page (Receiver for web sites). The user fills in his or her credentials and authentication will be handled by StoreFront.

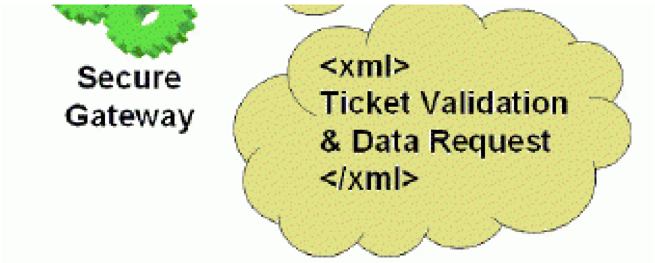
The launch process

Here we basically pick it up where we left off at the end of the resource enumeration process as explained above. Just as with the authentication process, there are some differences in how a recourse is launched with, and without a NetScaler in between. Also, when launching a Hosted Shared Desktop (XenApp) or a published application, as opposed to a VDI virtual machine (XenDesktop) there is an extra load balance step involved as well. Let's see what happens when we launch a published Hosted Shared Desktop trough NetScaler.

But wait, first things first… The Secure Ticket Authority



Before we continue… You might have heard about something called the STA, or the Secure Ticket Authority in full. It was first introduced with one of the earlier Secure Gateway editions over ten years ago. It (the STA) runs as a service and is part of the Broker Service on the Delivery Controller just like the XML service. During the resource launch sequence the StoreFront server as well as the NetScaler will both need to be able to communicate with the STA. As such you need to configure the



NetScaler and the StoreFront server(s) or Web-Interface server(s) to point to the exact same XML/STA service(s)/Deliver Controller(s).

FMA fact: The NetScaler Gateway uses the STA to guarantee that each user is successfully authenticated. If users have valid STA tickets, the gateway assumes that they passed the authentication checks at the web server and should be permitted access. It prevents computers from the 'outside' to have knowledge about the network on the 'inside' of the datacenter and it authorises the NetScaler Gateway ICA Proxy to set up a connection from the 'outside' to the 'inside'. It basically specifies where an outbound connection is allowed to connect to on the 'inside'.

Once a user launches a resource, externally (or internally for that matter) through NetScaler Gateway, at one point a secure ticket will be requested. As we will see shortly the STA ticket will eventually end up in the launch.ica file generated by StoreFront and/or Web-Interface. Once generated, the Delivery Controller hosting the STA service will hold the STA ticket information in memory for a configurable amount of time. As soon as a secure session is established the NetScaler Gateway responsible for handling the session only has to check the STA ticket (as part of the .ica launch file) with the STA service that originally generated the ticket. It (the STA service) does this from memory where the ticket was stored after it was created and send back to the StoreFront server as part of the XML formatted file mentioned earlier.

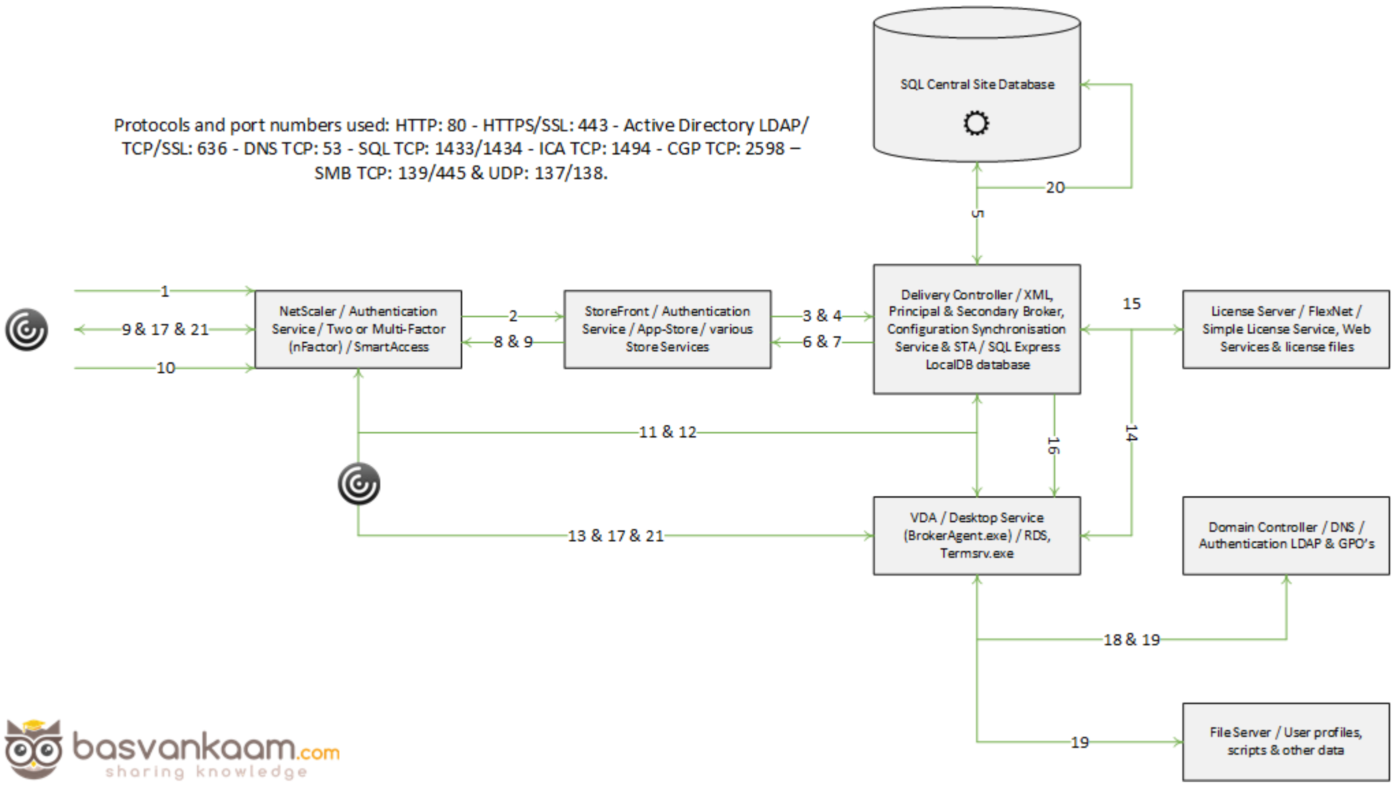
FMA fact: The STA is only used when traffic traverses a NetScaler, so you don't have to worry about the STA service and its tickets when authentication takes place internally through StoreFront, for example.

- Assuming that the login, authentication and enumeration process finished without any issues (see above) the user is now free to subscribe to and launch any applications and/or desktops that might have been assigned to him or her. As an example, let's assume that the user wants to launch a (XenApp) Hosted Shared Desktop session a.k.a. a published desktop.
- After the user clicks the icon the launch request is send to the NetScaler Gateway from where it will be forwarded to the StoreFront server (1 & 2) see image below.
- The StoreFront server will contact the Broker (XML/STA) service, or Delivery Controller, to find out if and where the resource is available and where it can be best started (3). This is where the well-known XenApp load balancing mechanism comes into play. Which as of XenApp 7.x needs to be configured through policies (or use the defaults).
- During this time the StoreFront server will also request an STA ticket from the Broker (XML/STA) service (4). It will include the user, domain and resource name it wants to start. It will also request a 'least loaded' server as part of the load balancing process.
- The Broker (XML/STA) service will query the Central Site Database (ports Nr. 1433 and 1434) to find out which server is able to offer the requested resource (5), which is also referred to as the current

Farm state. The Delivery Controller will than use this information together with its load balance algorithm to decide which server to connect to.

- At this time the Broker (XML/STA) service will create the STA ticket mentioned earlier. This will include information on the server and resource to connect to, amongst other information as discovered in the previous steps mentioned.
- Next, the Broker (XML/STA) service will send this information back to the StoreFront server in the form of an XML formatted file (6 & 7).
- Based on this information the StoreFront server will generate a launch.ica file (it uses the default.ica file as a template) containing the STA ticket and a whole bunch of other connection properties that are, or might, be needed (8). This will also include the FQDN/DNS name of the NetScaler Gateway itself.
- StoreFront passes on this information down through the NetScaler Gateway onto the locally installed Receiver (9) which initiated the connection to begin with.
- The locally installed Receiver will read and auto launch the launch.ica file to set up a connection to the NetScaler Gateway over 443 / SSL (10).
- From here the NetScaler Gateway will first contact the Broker (XML/STA) service (this address is configured on the NetScaler as well) to verify if the earlier generated STA ticket, as part of the launch.ica file is still valid (11).
- The Broker (STA) service will validate the STA ticket from memory. Once verified it will send back the IP address, port Nr. Resource name etc. of the machine and the resource it needs to connect to (12). Once done the STA ticket will be deleted.
- The NetScaler Gateway will set up a new ICA connection using port 1494 (ICA) or 2598 (CGP – Common Gateway Protocol) depending on its configuration (13). Soon to include ‘HDX Enlightened Data Transport’ I’m sure.
- The VDA will verify its license file with the, or a Delivery Controller (14).
- The Delivery Controller checks with the Citrix License server to verify that the end user has a valid ticket (15). This will also be done for any Microsoft (CAL) licenses, with regards to any Hosted Shared Desktops and published applications, that might be involved.
- At this time any applicable Citrix policies will be passed onto the VDA applying them to the session (16).
- The Hosted Shared Desktop session is launched and the NetScaler Gateway acts as a proxy between the user and the XenDesktop resource in the data center (17).
- User (Windows) authentication takes place between the domain controller and the Citrix Worker / Session Host (18).
- The Citrix session will initialize; the Windows welcome screen appears. At this point the user profile is loaded, Group Policies (GPO’s) are applied, scripts will be executed, drive and printer mappings are established and so on (19).
- Somewhere in between the session/connection information will be passed on and registered in the Central Site Database where it will be used for future load balance purposes (20).
- And finally the Hosted Shared Desktop will be fully launched (21).

Click to enlarge.



Protocols and port numbers used: HTTP: 80 - HTTPS/SSL: 443 - Active Directory LDAP/ TCP/SSL: 636 - DNS TCP: 53 - SQL TCP: 1433/1434 - ICA TCP: 1494 - CGP TCP: 2598 – SMB TCP: 139/445 & UDP: 137/138.

SQL Central Site Database
20
5
1
9 & 17 & 21
10
NetScaler / Authentication Service / Two or Multi-Factor (nFactor) / SmartAccess
2
8 & 9
StoreFront / Authentication Service / App-Store / various Store Services
3 & 4
6 & 7
Delivery Controller / XML, Principal & Secondary Broker, Configuration Synchronisation Service & STA / SQL Express LocalDB database
15
License Server / FlexNet / Simple License Service, Web Services & license files
11 & 12
16
14
13 & 17 & 21
VDA / Desktop Service (BrokerAgent.exe) / RDS, Termsrv.exe
Domain Controller / DNS / Authentication LDAP & GPO's
18 & 19
19
File Server / User profiles, scripts & other data
basvankaam.com
sharing knowledge

FMA fact: The STA ticket gets generated and sent back after a user launches an application/desktop, and not during the resource enumeration process. It includes information on the resource to be launched, including the server to launch the resource on (load balance).

The Broker Service is somewhat special

As you have probably noticed, the STA (service) is also part of the Broker service, and has been as of Presentation Server 4.0. Before that it was written as an ISAPI extension for Microsoft Internet Information Services, or IIS. As of XenDesktop 4.x the XML service (ctxxmlss.exe) has been rewritten in .NET and became part of the Broker service as well. So the Broker service is actually built up of three separate services (four, if you include the newly introduced Principal Broker Service), all handling different tasks: it brokers connections, it enumerates resources, takes care of the LHC and it acts as the Secure Ticket Authority, generating and validating STA tickets; however, this only applies to user connections made externally (or internally) through a NetScaler.

Conclusion

This should give you a good understanding of what happens under the hood when users log in and start subscribing to and launching resources. When it comes to Windows there are a lot more sub-process involved not included in this overview. If you would like to find out more about the (Windows) steps involved and how you can use them to your advantage while troubleshooting, for example I would advise you to have a look at the Goliath Logon Guide, you'll find it here.

Takeaways:

- Knowing about (and understanding) what happens after a user fills in his or her user credentials will greatly enhance your ability to troubleshoot login, enumerations and resource launch related issues.
- The Broker Services (Delivery Controller) plays a leading role when it comes the authentication, validation, enumeration, LHC and launch processes.
- The Secure Ticket Authority (STA) only comes into play when recourses are launched through a Citrix NetScaler, either externally or internally.
- The STA as well as the XML service are both part of the Broker Service, and have been as of Presentation Server 4.0/XenDesktop 4.x.
- Aside from a couple of differences on the resource launch process, like load balancing and preparing/booting the VDA for incoming connections, most of this applies to XenDesktop VDI based infrastructures as well.

Bas van Kaam

Pre-sales Director Northern Europe @ Liquidware
Transforming the physical, virtual and cloud based desktop one step at the time. Father, blogger, author of Inside Citrix - The FlexCast Management Architecture, public speaker and an above average runner. One of the 50 Citrix Technology Professionals world-wide, CTA, SME, a myCUGC Leader, NTC, ACE, IGEL Tech Insider, EUC/VDI VIP, lover of all things tech and IoT enthusiast.

Filed Under: Architecture, Authentication, Citrix, Desktop virtualization, XenApp, XenDesktop
Tagged With: 1494, 2598, Active Directory, Authentication, Beacons, CGP, Delivery Controller, Enumeration, EPA, Gateway, HSD, ICA, LDAP, LHC, Licenses, Load Balancing, Login, NetScaler, nFactor, Query, Receiver, Service, STA, StoreFront, VDI, Verification, Windows, XML

3 Comments **www.basvankaam.com** 1 **Login**

♡ **Recommend** **1** **Share** **Sort by Best**

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Sanjo George • 8 months ago

Thanks Bas. As always a great write-up with awesome explanation.
I would suggest following updates for reader's better understanding. Though you've mentioned it correct in later step, readers may misinterpret the whole concept of STA ticket.

"At this time the Broker (XML/STA) service will create the STA ticket mentioned earlier. This will INCLUDE INFORMATION on the server and resource to connect to, amongst other information as discovered in the previous steps mentioned"- STA will only cache the targeted Xenapp server details while issuing a Gateway transversal ticket- Which will be valid only for 100 seconds (by default). Targeted Xenapp server details will not be exposed to end user device while connecting through Netscalar/Access Gateway.

"The locally installed Receiver will read and auto launch the launch.ica file to set up a connection to the NetScaler Gateway over 443 / SSL (10)"- It would be nice if you mention about the SSL handshake here as it will brief the importance of a server/root certificate and a complete certificate chain.

• Reply • Share ›

Ashrafy • 10 months ago

Awesome Explanation ....cheers

• Reply • Share ›

Bas van Kaam **Mod** Ashrafy • 9 months ago

No problem, glad you liked it.

• Reply • Share ›

ALSO ON **WWW.BASVANKAAM.COM**

Book announcement: Inside Citrix – the Flex Management Architecture!

17 comments • 2 years ago

Bas van Kaam — That's great, very happy to hear that. Thank you.

The long awaited… XenApp and XenDesktop 7.12 Local Host Cache

6 comments • a year ago

Stefanos Evangelou — Thank you Bas,Well articulated and highly informative post on long awaited local host cavhe feature by Citrix in

2016 — A personal look in the rearview mirror

3 comments • 9 months ago

Bas van Kaam — Same to you Rasmus, and thanks!

Kindle e-book available now! Inside Citrix – The FlexCast Management Architecture

2 comments • a year ago

Bas van Kaam — Hi there, no, I don't offer a .PDF version. You can download free Kindle viewer software directly from Amazon (all

CPU - MEM - STORAGE - NETWORK
FREE VIRTUAL MONITOR
ESX(I) - HYPER-V - XENSERVER -RED HAT
FREE. UNLIMITED. FOREVER.
turbonomic

Hearing Citrix
is Slow?
Resolve Quickly with the Consultants
who Literally Wrote the ~~Book~~ Books
The Compl Migrating XenApp/X 6.5 to Replacing
The Complet to Understan Citrix Logon for XenApp/Xe
The Citrix Administrato Technical Guid Understanding Troubleshooti Citrix ICA/HD
XenApp and XenDesktop Troubleshooting Assessment
GOLIATH

Search this website …

Return To Top