Inside Citrix chapter twenty three – The one with all the troubleshooting

When it comes to troubleshooting our XenDesktop and/or XenApp environments there are a lot of (free) tools that can be of assistance. Some are aimed at solving a specific issues, while other tools are more generic and can be helpful in multiple ways. However, while this is all great, I do think that a lot of IT administrators forget about the basics: you need to know and understand the products that you are working with before anything else, here's my list of things to think about when it comes troubleshooting, and note that these bullets apply to all sorts of technologies / products, not just Citrix:

- You need to understand the architecture you are dealing with, the FMA in our case. Its main components and services, communication paths, and so on.
- Expected behaviour and interaction: how does it all work under 'normal' circumstances?
- Traffic flow throughout the infrastructure and its components: this helps to identify potential bottlenecks.
- Assemble a personal tool kit. As mentioned, we have a lot of tools at our disposal: sometimes it can be hard to find out what the exact purpose of a tool is or how it should be operated. By doing some research beforehand this will potentially save you valuable time when things do go wrong. And we all know this is going to happen sooner or later, right?
- Only when you apply the first three steps you will be able to know where and when to apply which tool.
- Know where to find information. This may sound a bit silly, but it doesn't hurt to go over some of the options you have when it comes to finding useful information. Which forums do you visit? Think about (ex-)colleagues or community folks you can contact. Perhaps make yourself a top 10 of blog authors and so on. Give this some thought. And don't forget about social media.

Efficiency and general tips

When troubleshooting, it is all about efficiency: fixing an issue should take as little time as possible. This calls for a structured approach or methodology: Investigate, Analyse and Implement.

First of all it needs to be acknowledged that there actually is a problem. Who is your source? The helpdesk, the company's CEO, a user who always has something to complain about? I think you know where I am going with this, right?

Secondly, you need to know, or find out what is going on, what the actual issue is. How many users or departments etc. are affected? How do they describe what is going on? Talk to your users and the Helpdesk.

What is the overall impact to the business and beyond? Are there any business critical systems and/or processes involved? If you are dealing with a potential major outage, try to estimate the amount of time and resources needed to come up with a potential fix, even if it is just temporary. Can the problem be reproduced? Whom do we need to talk to?

As mentioned, try to isolate the issue: which components and/or services are actually affected? Plan accordingly.

What do the event logs tell us? A Doctor Watson log perhaps. Is there any monitoring software in use? What does it tell us? Were there any changes made to the environment during the last couple of days or hours even? Maybe Studio and/or Director can help, see previous chapters on this as well. A simple PING or Tracert might tell us something more.

My point is: start small and take the relatively 'easy' steps first, try to make some progress. Are there any quick fixes you can try or implement? Is there a workaround available?

All this is exactly why those first few bullets are so important.

By preparing yourself in times of 'peace' you can and will save yourself valuable time when things start to go wrong. Once you have familiarised yourself with the basics as mentioned previously, you are good to go. Here are some more general troubleshooting tips I picked up along the way:

- Never try to guess the solution: always base your actions on facts.
- Don't assume anything, no matter how obvious it may seem. You know what they say about assumptions, right?
- Try to isolate the issue, make it smaller and take it step by step.
- Make sure to inventorise all information found.
- Categorise and prioritise information. Once you have an idea of what some of your next steps might be, and a lot of the time you will have multiple options, think about what to do first, second etc. For example, you might want to try the option with the least impact first. List your options and prioritise them; always have a plan B, though.
- Come up with a morning ritual. We have all been there: an issue that seemed obvious to solve, which two weeks later is still giving you grey hairs. In most cases a lot of the same people will be involved on a daily basis. By getting together at the start of the day, only if it is for five to ten minutes, everybody knows what the (attack) plan for the day is and what he or she needs to be doing. Any progress and/or setbacks can also be discussed, including any actions that need to be taken etc.
- Make sure to assign a specific issue or problem to a person. This way you have a single point of reference, which also helps during the earlier-mentioned morning ritual.
- Keep track of what you have been doing individually, and as a team when applicable. You don't want to run the same tests over and over, or install a certain hotfix for the third time without even knowing about it, do you? I think this particular point is often underestimated. It can save you a serious amount of time and effort.
- Think out loud and share information. I don't think I have to explain what I mean with this one.

- Do not forget about social media. The potential 'reach' you have on Twitter, to name one, is amazing. Even if you do not have hundreds or thousands of followers, a single retweet might do the trick.
- And finally, another BIG one: Ask for help! Don't think you know it all, because you don't. When in doubt, ask! You do not want to be the one responsible for making a big problem even worse, just because you were not 100% sure of what to do.

Troubleshooting in action

Throughout this next section I will list several issues, solutions, troubleshooting steps, tips and tricks, troubleshooting tools, articles and other potential, hopefully helpful material.

XDDBDiag

The XenDesktop Database Diagnostic tool. It was first designed with XenDesktop version 5 but can be used with all new 7.x editions as well. This command-line support tool performs a consistency data check on the data and connectivity verification in a XenDesktop database. A great tool to do some proactive administrating as well. Diagnostic output can be saved in the form of a comma-separated value (.CSV) file located in a compressed file (.zip) named:

Computername_XDDBDiag_Output.zip to the same directory in which the programme is located. It provides the following information:

- Site information
- Virtual Desktop Agent information
- Current connections / Connection log
- Hypervisor connections
- Policy information
- Desktop group
- Controller information
- SQL information, and more.

It will automatically search for new updates when launched, but this is something that can easily be turned off as well. Check out the following CTX article for some more details on how to use it: CTX128075.

XDPing

Another command-line tool originating back to XenDesktop version 5 and commonly used to trace and track down connectivity issues. As of version 2.2 the XDPing tool also supports all current XenDesktop 7.x editions. It automates the process of checking for the causes of common configuration issues in a XenDesktop environment. The tool can be used to verify configuration settings on both the XenDesktop Broker and VDA machines, both from the console and remotely. Read through this CTX article to see which command-line options you have when executing the tool; it also includes a short video on how to use it: CTX123278. It can also monitor and check certain XenDesktop services information and query the local event log to check for known events that are related to XenDesktop. All in all a great tool to handle some of those more common proactive admin tasks as well.

Services and logs overview

With both XenDesktop & XenApp, it is important to understand what is taking place under the covers, which processes and services are involved when enumerating applications, connecting and disconnecting users, provisioning new machines etc. Having said that, with XenDesktop we can enable something called service logging.

Service logging can be enabled either from the command-line or through Citrix Scout (installed by default on XenDesktop and XenApp Delivery Controllers) using a Graphical User Interface. Just keep in mind that Scout still lacks the ability to log data for certain services like the Broker Agent: this is part of the VDA as of version 7.x (an important one). When you enable service logging using the command-line, all services will be available. Other services that can be monitored using Scout include, the ADIdentity, Broker, Configuration, Host, Machine Identity and Machine Creation services. This is what a manual command-line may look like:

```
Citrix.MachineCreation.SdkWcfEndpoint.exe-LogFile C:\XDLogs\Name.log
```

Next to the Delivery Controller (Broker Service log) and the VDA (VDA Broker Agent log) the PortICA service a.k.a. the ICA Service is probably one of the most important ones to keep an eye on (and log information on) when troubleshooting connectivity issues. It handles just about everything from an ICA / HDX perspective except for direct communication with the Delivery Controller.

Read this CTX article for more information on VDA Broker Agent logging: CTX117452.

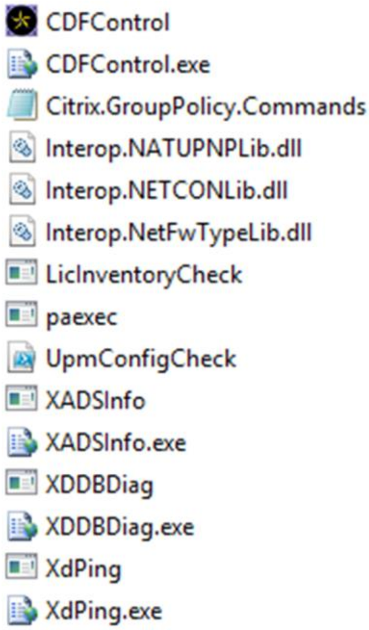
PortICA logging, in addition to enabling the VDA Broker Agent log, can also be (very) useful when troubleshooting issues regarding the Desktop Virtual Desktop Agent (VDA). PortICA logging is not enabled by default on the VDA. Check out: CTX118837. More on this as we progress.

HDX Monitor

This tool will provide you with detailed diagnostics information on all HDX technologies known today. HDX Monitor version 3.x has been upgraded to also support version XenDesktop version 7.x, as well as XenApp 6.5. This CTX article will tell you all you need to know: CTX135817. Note that HDX Monitor is built into Director as well.

Scout

As of XenDesktop and XenApp 7.5, Citrix Scout is installed on your Delivery Controllers by default. It is a powerful tool that combines, or aggregates, a bunch of the individual tools discussed throughout this chapter. In fact, if you have a quick peek in the Scout installation directory, the Utilities folder to be exact, you'll see that there are several applications listed, CDF control being one of them.



CDFControl
CDFControl.exe
Citrix.GroupPolicy.Commands
Interop.NATUPNPLib.dll
Interop.NETCONLib.dll
Interop.NetFwTypeLib.dll
LicInventoryCheck
paexec
UpmConfigCheck
XADSInfo
XADSInfo.exe
XDDBDiag
XDDBDiag.exe
XdPing
XdPing.exe

Scout utilities folder

These applications can be started just as if they were downloaded separately and will include all features and functionality that you might be used to: no exceptions. CDF control is an important one; it is used by Scout to perform the actual CDF tracing locally or on the remote machine.

After clicking the 'Start CDF Trace' button, one of the first things you'll do is select the machines to run the actual CDF trace on. The Delivery Controller from where Scout is started will be selected by default.

Prerequisites

You won't be able to actually perform a CDF trace, or much else for that matter, until you have made sure that certain prerequisites are met. This is what needs to be in place:

- Local administrative privileges on the Delivery Controller
- Local administrative privileges on the remote machines
- WinRM needs to be enabled / configured on the remote machine
- Remote Registry needs to be enabled on the remote machines
- File and print sharing needs to be enabled on the remote machines
- All machines need to share the same domain

- .NET Framework 3.5 with SP1 or .NET 4.0
- Microsoft PowerShell 2.0.

If the selection will include any remote machines, Scout will immediately check if it is able to communicate with these machines: this is where some of the earlier mentioned prerequisites come into play. If it runs into any issues while trying to connect it will tell you what is wrong. File and print sharing, WinRM or perhaps Remote Registry, needs to be enabled on the remote machine.

Collecting data

The second big feature of Scout. It enables you to collect data (referred to as Data points) related to the systems BIOS, the OS installed, memory information and drivers; it also reads certain registry keys, system and application event logs, Site and Farm information, WinRM settings, and a lot more!

Data needs to be collected before it can be automatically uploaded to Citrix. First you need to select a certain number of machines from where data will be collected, reviewed and eventually uploaded (this is also where Citrix Insight Services comes into play). You can select up to 10 machines in total. Once collected the data will first be analysed, and if any possible corrective actions are found they will be shown on-screen, giving you the option to execute them. Next you will be asked to choose a location where you would like to store the data in a .zip format.

Once the data is saved you will be presented with a dialogue explaining the upload & analysis process. Click Continue on this to proceed. Then the Upload to Insight Services dialogue appears: enter your My Citrix Username, password etc. and click Upload. The status report is sent directly to Citrix Technical Support. An MD5 checksum test is performed to ensure your upload was successful. Also see Insight Services on page 402.

PortICA / picaSvc2.exe logging

When performing a CDF trace, by default, all main FMA services will be included (although you are able to manually exclude services: more on this in a bit) during a CDF trace: all except for one, the PortICA service. Before I continue, it's important to understand that the PortICA service, renamed as picaSvc2.exe as of XenDesktop 7.x and also known or referred to as the ICA Service, is one of the most important services when it comes to your virtual desktop infrastructure (VDI).

It 'lives' on your desktop OS-based VMs (VDAs) and as mentioned earlier, it takes care of almost everything that is going on the machine except for direct communication with the Delivery Controller (Desktop service). If you have a closer look at the involvement of the PicaSvc2 service during the initial user connection phase, I think it goes without saying that you want to always include the PortICA service, when running a CDF trace, for example. The same goes for any clear text / verbose logging that you might enable. Fortunately we can enable the PortICA service by hand to be included in these kinds of traces / logs.

Enable logging

PortICA logging can be enabled in two ways; the first one is by hand. CTX118837 will tell and show you exactly what needs to be done. You will first need to create an XML file (PortICAConfig): copy and paste the content listed in the abovementioned CTX document, save it etc. Just follow the steps in the CTX doc and you will be fine. I probably make it sound harder than it actually is. The second method is by using Scout. This will basically automate the above steps for you.

There is no difference between the two except that Scout offers you a GUI and you won't have to manually create, or copy and paste anything. Again, it will depend on the type of issue you are troubleshooting whether this will work for you, you might want to enable PortICA logging by hand on one of your base images, for example. That would be a judgement call.

Anyway, this is how it's done using Scout. First you go into the Collect & Upload window, find the remote machine where you want to enable PortICA logging, and click on the settings icon. After that the 'WinRM/Service Log Settings' screen will appear and all you have to do is swipe the PortICA Service button to the right (On).

It is CDF in the background

Remember how I explained that Scout actually uses CDF control to run the CDF traces? What happens is that as soon as you click continue to start the trace, CDF control is copied over from the installation / utilities folder to the remote machine and is executed remotely. Once you click stop, CDF control will be deleted from the remote machine and all collected data will be copied over to the Delivery Controller from where Scout was originally started.

Read the following CTX article for more information on how to use Scout: CTX130147

CDF Control

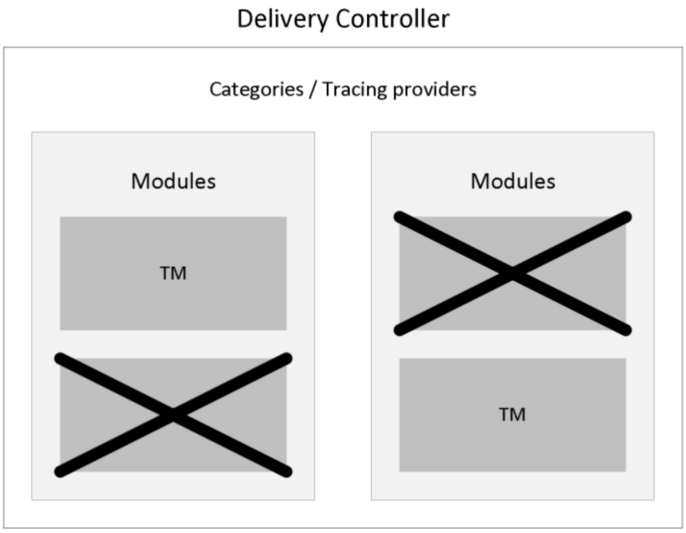
CDF stands for Citrix Diagnostic Facility: it has been around for over eight years and is still one of the most used diagnostic tool kits used today! While built into Citrix Scout it's also available as a stand-alone download and fully supports all new XenDesktop editions. It is an event tracing controller/consumer, geared towards capturing Citrix Diagnostic Facility (CDF) trace messages that are output from the various Citrix tracing providers (will be explained the next section). Note that you will need to have local administrative permissions to be able to start tracing. Here's where to get it and how to use it: CTX111961.

Consider it to be good practice to try and collect some CDF traces prior to opening up a support case with Citrix, since this is probably one of the first things they'll have you do, unless you are in doubt on where to start, of course.

Where does the information come from?

Every Citrix component (like a Delivery Controller) is split into a certain amount categories a.k.a. trace providers. A category can be everything related to USB, or ICA traffic, printing, FMA services, profile management, provision services, and so on and so forth: there are a few dozen in total. These categories are divided into several modules, and these modules consist of various so-called trace messages.

Now, when a CDF trace is run again, using Scout or CDF control, diagnostics information is collected by reading the trace messages from the various modules, and this is what actually gets logged as part of the trace. When a trace message gets called upon or is read, it will respond with its current state, which could be an error code telling us what's wrong.



CDF tracing modules

The number of modules, and thus trace messages, per Citrix component will differ. A Delivery Controller will hold a lot more modules / trace messages than a virtual machine as part of your VDI deployment, for example. If you open up CDF control on a Delivery Controller you'll see exactly what I mean.

Trace Message Format files

Once you have stopped the trace, either using the stand-alone CDF Trace tool or from within Scout, the collected information will be saved in the following folder:

AppData\Local\Temp\Scout\ of the logged-on user executing the trace.

All CDF traces will be saved with the .etl extension. At this time you could just grab the data, zip it, and send it over to CTX Support as (perhaps) requested.

Or maybe CTX isn't involved (yet) and you want to have a look for yourself; or both. As soon as you open the .etl file, perhaps using a tool like WordPad, you'll notice that the letters, numbers and other characters displayed won't make much sense to the human eye.

When a CDF trace is started and the trace messages are read from the modules, the information that gets logged is partly in the form of GUIDs. Which means that these (.etl) files will first need to be parsed, or translated if you will, before they will make any sense at all.

As mentioned, the .etl files first need to be parsed before they become readable. To be able to this you'll need at least two things: first, a tool that is able to do the parsing for you; and secondly, TMF files which hold the instructions for parsing and formatting the binary trace messages generated by Scout and/or CDF control. As you can read in the below statement / quote, TMF files aren't thought up by Citrix, it's more of a general approach: The trace message format (TMF) file is a structured text file that contains instructions for parsing and formatting the binary trace messages that a trace provider generates.

The formatting instructions are included in the trace provider's source code and are added to the trace provider's PDB symbol file by the WPP preprocessor. Some tools that log and display formatted trace messages require a TMF file. Tracefmt and TraceView, WDK tools that format and display trace messages, can use a TMF file or they can extract the formatting information directly from a PDB symbol file. In the Citrix world we would use CDF control and/or CDF Monitor for this.

There are two types of TMF files available, public and private. Public TMF files are the ones we use for personal file parsing. The private TMF files are for CTX Support eyes only, something to keep in mind. Public TMF files can be acquired in two ways, you can download them directly from the Internet by using CDF control, or you can contact an online TMF server, live parsing your .etl files.

I would advise to always try and download the TMF files whenever possible. When you try to parse large files directly from the Internet using an online TMF server and the connection fails, or perhaps you are on a high-latency line, or the TMF servers are, or go, offline at some point (which isn't unusual, by the way) you will have to start all over again. Of course you will first have to wait until the TMF servers are reachable again. Next to that, if you need to parse large traces: this could take a long time when applying the online parse method.

It also has to be noted that parsing, and especially reading CDF traces (.etl files), is something not to be taken lightly. With this I mean that, although the parsing of .etl files is a relatively easy process, the reading of these files, once they are parsed, is something else. You'll need some special skills to be able to actually find the error or fault causing your issue. Then again, it could be something you're into, or perhaps you're curious and just want to have a look to see what's in there: all are valid reasons to go and have a peek.

Citrix Support

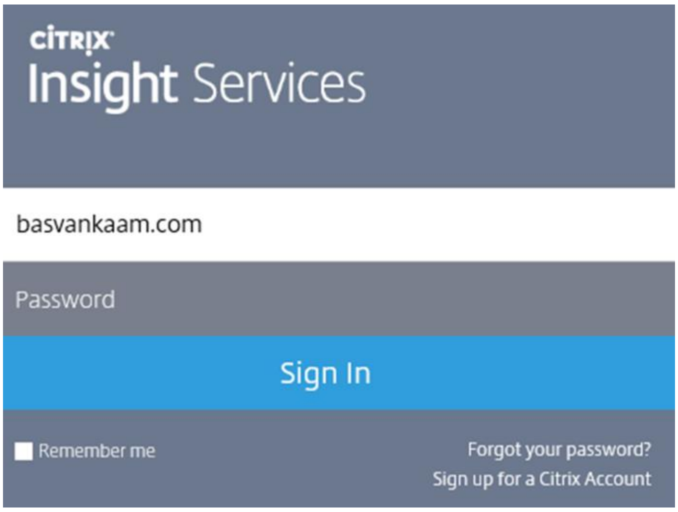
Imagine yourself digging deep into a CDF trace: you have narrowed it down to just a few specific modules and you know exactly what to look for and what is most likely causing your issue, whatever it may be. It could happen that the publicly available TMF files are not sufficient and that you need some of the private TMF files to parse a specific part of the trace that will expose your issue. What to do? That's right, you need to contact Citrix Support. Of course in a scenario like this you will probably be finished quickly since you will be able to pinpoint what needs to be parsed to find out what's wrong. But still, you'll need a support contract for this to happen.

Citrix Print Detective

This tool has been around for a few years now and as of version 1.2.1.5 it also supports XenDesktop 7. Print Detective is an information-gathering utility that can be used for troubleshooting problems related to print drivers. It enumerates all printer drivers from the specified Windows machine, including driver-specific information. It can also be used to delete specified print drivers. It allows for log file capabilities and provides a command-line interface as well. It supports all of Microsoft's desktop and server platforms. How to use Print Detective? Go to: CTX116474.

Insight Services

Insight Services is the glue binding it all together: here you can upload your log and trace files and link them to any support cases you might have registered earlier. Once you upload a file, Insight Services will automatically analyse your log files and scan them for hundreds of known issues. From their website: Citrix Insight Services reads log files from XenDesktop, XenServer, XenApp, NetScaler, PVS, ByteMobile, XenMobile, CloudBridge, CPBM and XD/XA Connector, and we'll be adding products to it over time. We're adding new plug-ins that capture known issues for these products all the time. So Citrix Insight Services will keep getting better.



Insight Services login

When Citrix Insight Services discovers any known issues in your environment, it suggests hotfixes, patches and updates with red/yellow/green prioritisation. It will also analyse your configuration and give you best-practice advice, with links to relevant articles or white papers.

Citrix Insight Services isn't just for troubleshooting. It's also a great way to give your infrastructure a quick Health Check, so you can spot any issues before they become real problems. Got to https://cis.citrix.com and make sure to read through CTX131233 for more information around Insight Services.

Call Home and CIS in Director

As it did before, Citrix Call Home performs periodic collections of your system and product configuration, plus performance, error, and other information. As of XenDesktop version 7.8 this information can now be automatically (this can be scheduled to your needs and/or preferences) sent to Citrix Insight Services for proactive analysis and resolution.

Also new in version 7.8 is the ability to access Citrix Insight Services instantly from Director by means of a drop-down menu. This way you can easily access all information collected through Call Home and Scout combined.

PowerShell

While PowerShell can be used in many ways to configure and troubleshoot XenDesktop and/or XenApp architectures, here I would like to focus on the main infrastructural services that make up the FMA. The states of your FMA services are best checked using PowerShell.

Using some of the PowerShell Get- commandlets when checking up on your FMA services will show you exactly what is going on, when and if something is wrong. It's much more detailed and reliable than using the Windows services.msc console.

If you have a central management server, or multiple I suggest you create a personal PowerShell profile and include some of the basic Get- FMA service checks in it. This way, every time you open PowerShell these basic checks will be done automatically before you continue. If you look at Director, on the main dashboard, there you also see your Delivery Controllers listed at the bottom of the screen. If all is well, green checkmarks pop up next to them. This is also PowerShell issuing Get-Commands in the background.

Here are a few examples to check some of the more important FMA services:

- Get-BrokerServiceStatus
- Get-ConfigServiceStatus
- Get-HypServiceStatus
- Get-AcctServiceStatus
- Get-ProvServiceStatus

Another thing to mention is that both Studio and Director run on top of the P owerShell SDK as well. Everything you can do within Studio can also be done through PowerShell, including a whole bunch of configuration options and tweaks that are not possible using 'just' Studio. When you check your Delivery Controllers in Studio, you'll see a number in minutes next to each Controller that indicates when the Delivery Controller has last registered itself with the Central Site database. This number should always be 0. By default, the Controller checks in every 20 seconds (they exchange heartbeat messages) which will then be valid (TTL) for another 40 seconds.

Old school

It's great that we have such an extensive toolset at our disposal, but let's not forget about the basics. A simple NetStat and/or firewall port check, a Ping to check network connectivity perhaps, Tracert, Telnet etc. Are all our services up and running, no errors or warnings, no time or sync issues, a quick and dirty manual event log check, and when you do, remember to check all components that might be involved, your Controller, StoreFront, Web Interface, VDA etc. You get my point, right? Of course this kind of functionality is built into most of the tools as well, but sometimes all you need is a simple DOS Prompt and you're good to go. No separate install or configuration steps needed.

Toolset collections

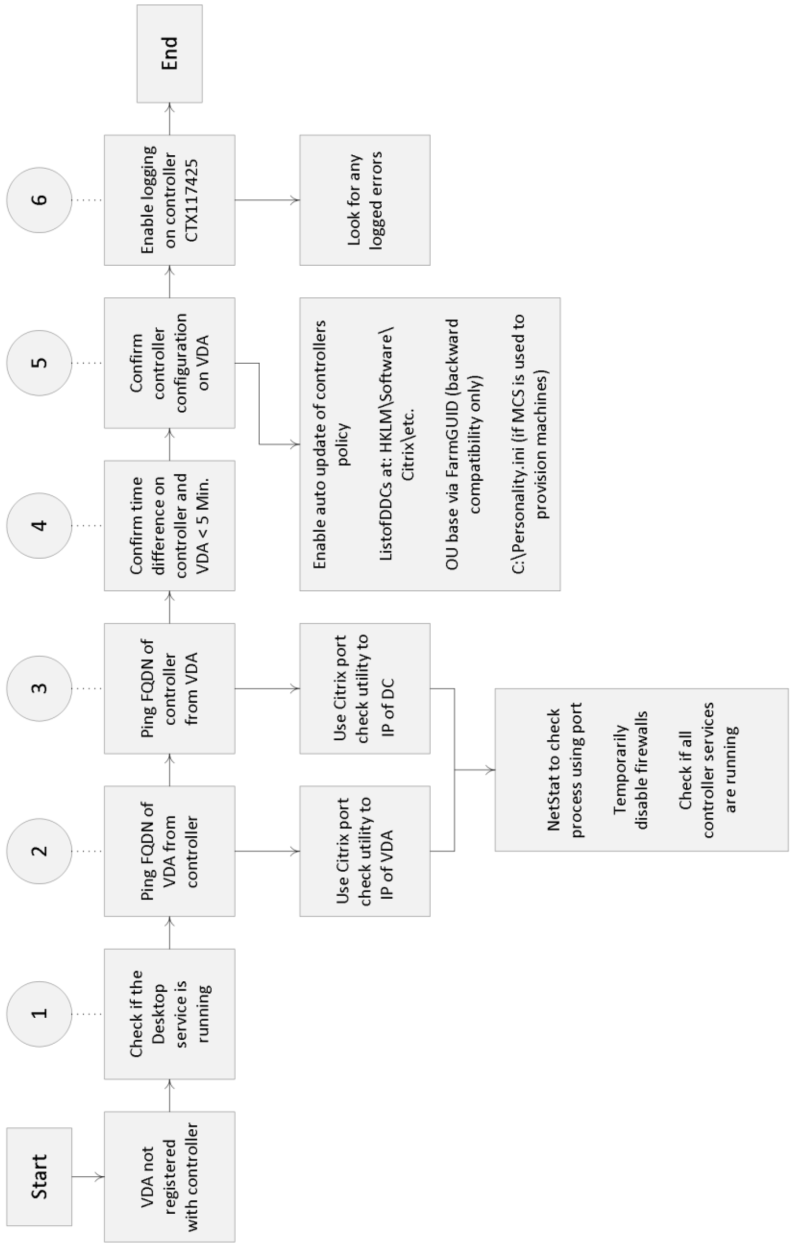
I could probably fill another 5 pages or so with separate troubleshooting tool descriptions, but in practice you will probably only use a handful, especially with tools like Scout, aggregating multiple into one.

However, to make sure I do not leave any potentially important tools out of scope, I will also include links to the Citrix Diagnostic Toolkit and the Citrix Supportability Pack. Both contain an enormous amount of Citrix (-related) tool sets, free for you to use. You will find that both will have an overlap, as do I in my troubleshooting tools mentioned throughout this chapter. The Citrix Supportability Pack has just been updated (April 2016) with a whole bunch of (very) useful and new tools like: The AppDisks diagnostics tool, Audio Volume Persistence Tool, Database Sizing Tool, Foreground Lock Timeout Tool, SmartHub, VDA Cleanup Utility, PreSCAN and more!

- You will find the Citrix Supportability Pack over at: CTX203082.
- The Citrix Diagnostic Toolkit is located at: CTX135075.

Troubleshooting VDA registration process

Within the FMA VDAs need to register themselves with a Delivery Controller, otherwise they won't be of much use. Follow the steps outlined in the CTX document below and/or have a look at the visual overview over at the next page to successfully troubleshoot the VDA registration process. CTX136668.


Start
VDA not registered with controller
1
Check if the Desktop service is running
2
Ping FQDN of VDA from controller
Use Citrix port check utility to IP of VDA
3
Ping FQDN of controller from VDA
Use Citrix port check utility to IP of DC
NetStat to check process using port
Temporarily disable firewalls
Check if all controller services are running
4
Confirm time difference on controller and VDA < 5 Min.
5
Confirm controller configuration on VDA
Enable auto update of controllers policy
ListofDDCs at: HKLM\Software\Citrix\etc.
OU base via FarmGUID (backward compatibility only)
C:\Personality.ini (if MCS is used to provision machines)
6
Enable logging on controller CTX117425
Look for any logged errors
End

VDA registration troubleshooting steps

Citrix Health Assistant

Version one (multiple will follow) of the Citrix Health Assistant focuses on VDA registration issues for both XenDesktop and XenApp. A series of health checks will be run in an automated fashion to identify any potential root causes for common VDA registration issues. It is a GUI based tool but also supports the use of command line commands. The following health checks are included:

1. VDA Machine Domain membership verification
2. VDA software installation and relevant services status verification
3. VDA communication ports status
4. VDA services status
5. Windows firewall configuration

6. VDA communication with Desktop Delivery Controllers (DDC)
7. VDA time sync with each DDC

Look up the following CTX document for some additional information and the actual Health Assistant download: CTX207624.

UPS print device certification tool

The Citrix UPS Print Driver Certification Tool can be used to test the compatibility of a print driver with the Citrix Universal Print Server. The tool checks for compatibility by using the print driver to simulate load, allowing a network administrator or print driver manufacturer to determine the following:

- Print driver is capable of handling the load normally seen with a Citrix Universal Print Server.
- Print driver meets the Citrix Universal Print Server performance requirement.
- Identifies potential print driver issues, allowing a network administrator or print driver manufacturer to further troubleshoot problem areas.

See the following CTX document for more detailed information: CTX142119.

StressPrinters

This tool can be used to compare various print drivers (CPU load, time required to successfully create a printer) as well as simulate multiple sessions' auto-creating printers using the same print driver. Have a look at the CTX document for an instruction video on how to use the StressPrinters tool: CTX129574.

Receiver Clean-Up tool

The Receiver Clean-Up utility is designed to assist with the following scenarios:

- When errors occur during upgrade from an earlier version of Receiver or Online Plug-in.
- When unexpected behaviour or performance is experienced after upgrade from an earlier Receiver or Online Plug-in.
- If Receiver upgrade is not possible due to feature incompatibility and/or a clean uninstall is required.

The Receiver Clean-Up Utility removes components, files, and registry values of Online Plug-in 11.x, 12.x, and Receiver for Windows 3.x, 4.x (Online Plug-in 13.x, 14.x). This includes the Offline Plug-in component if installed. See the accompanying CTX document for more information and to download the actual tool: CTX137494.

The Remote Display Analyzer

This is a tool for and by the community. It is developed and thought up by Bram Wolfs and Barry Schiffer and has been very well received. Although the concept behind it might sound simple, I can assure you the technology is not. The tool is somewhat special; first of all it will show you which HDX codec is being used, including all related and relevant information. Best thing is, it will only take you two mouse clicks (one double-click, actually) literally. No command prompts, no WMI queries, HDX Monitor or Director etc.

Secondly, and this is huge, it will let you change display settings on the fly and LIVE switch between the different codecs available, without needing to log out, reconfigure, reboot etc. Framehawk included. You could say it's an industry first, since even Citrix themselves have not been able to come up with something similar. All real-time statistics and related information can be viewed using a 'normal' user account, no admin permissions needed.

Below you will find a short but impressive list of what you as an admin can expect from the Remote Display Analyzer:

- It is meant as a tool for admins, not users. You don't always need admin permissions, though.
- It will give you a (real-time) indication of what the resource consumption is for a specific workload, which might come in handy for troubleshooting.
- It will show you the configured display mode right away, only seconds after launching the tool.
- It will only show you information that matters for the detected display mode, clear and crisp so no (more) confusion whatsoever.
- You can change display settings on the fly, see what works best under which circumstances.
- It is possible to switch between encoders by changing the settings and also possible to switch between DCR and ThinWire.

Make sure to check out their website at www.rdanalyzer.com and follow them on Twitter at @rdanalyzer.

Conclusion

This chapter should give you a good indication of what is out there. Of course I will never be able to list and highlight all the tools available today, but I am pretty sure that I have covered the most popular ones including all accompanying CTX articles, leading you to even more useful information and downloads.

Key takeaways

- Successful troubleshooting starts with understanding the environment, architecture and components you're working with.
- In times of 'peace' make sure you spend some time getting to know the various troubleshooting tools and methodologies out there. Assemble your own tool kit and/or come up with your own troubleshooting methodology /approach.
- Make sure to go over some of the tips I gave you at the beginning of this chapter: there are some useful pointers in there. Not much use in repeating them all here, the same applies to all the tools listed.