Inside Citrix chapter seven – The one with the Virtual Delivery Agent

VDA in short, is a relatively small piece of software that gets installed on all virtual and physical machines running a Windows/Linux server and/or desktop operating system as part of our XenDesktop Site, making their resources remotely available to users.

The VDA communicates directly with the Delivery Controller (it registers itself) as well as with the Receiver software installed on the end point device. It is also referred to as the client-side component of the FMA.

> **FMA fact**: Prior to XenDesktop 7 the VDA was referred to as the Virtual Desktop Agent, while today we know it as the Virtual Delivery Agent, a subtle difference.

During session brokering the VDA is responsible for establishing and managing the connection between the virtual or physical RDSH / VDI machine and the user's end point device. During session initialization (after a user logs in) it also checks if a valid Citrix license is available and it will apply whatever policies have been configured for that particular session.

The VDA primarily consists of two main services, the Citrix ICA Service (picaSvc2.exe) and the Citrix Desktop Service (BrokerAgent.exe), which communicates directly with the Broker Service on the Delivery Controller.

The VDA Desktop Service consists of multiple plug-ins, like the Director plug-in, a WMI plug-in, the Monitor plug-in, and a few more.

In one of the upcoming chapters we will have a closer look at all that is taking place from a services interaction point of view.

They all communicate with the Delivery Controller through the Desktop Service as mentioned. Both services will be discussed in more detail as we progress.

New (VDA) kid in town

With the introduction of XenApp to the FMA, Citrix had to come up with a server-based Virtual Delivery Agent, since prior to XenDesktop 7.x the FMA was exclusively designed for VDI, meaning VDAs for desktop Operating Systems only.

And so they did. As of XenDesktop 7.x and forward there are now two types of VDAs, or four, depending on your point of view: one for Windows desktop Operating Systems, one for Windows server Operating Systems, and a VDA for Linux as well, which includes options for both desktop as well as various server Linux distributions.

As mentioned previously, the biggest difference between the two is the underlying (ICA) protocol stack. For desktop machines a single-user ICA stack (a.k.a. PortICA) is used, which

allows only one user session at a time. For server machines, Citrix now includes a multi-user ICA stack extending the Windows Remote Desktop Services with the HDX/ICA protocol.

This is basically the same ICA protocol stack as developed for Citrix XenApp 6.5 and earlier releases with some adjustments to make it compatible with XenDesktop / XenApp FMA Delivery Controllers.

The following server and desktop Operating systems are supported. Server VDA: Windows Server 2008 R2, Windows Server 2012 and R2, and Windows Server 2016 is supported as well. Desktop VDA: Windows 7 SP1 Professional, Enterprise and Ultimate editions, Windows 8 and 8.1 Professional and Enterprise editions, and as of XenDesktop 7.6 Feature Pack 3 Windows 10 Enterprise edition. Although do make sure to check out the Citrix E-docs since not all features are supported. And as for Linux, desktop and server: SUSE, Red Hat, CentOS and Ubuntu.

> **FMA fact**: You can configure multiple Machine Catalogs with different desktop and server Operating Systems within the same environment / Site.

As you probably remember, before the 7.x release we basically installed XenApp (full install) onto each server that would serve as a Session Host and/or Data Collector. In comparison, the Server VDA is supposed to be a much more lightweight approach, even when compared to the former 'Session only mode' in XenApp 6.5. It now solely consists of the components needed to host sessions, and, as such, it doesn't share any of the other components and services installed on the Delivery Controllers, which wasn't the case with 6.5 and before.

VDA registration

As soon as a Virtual Delivery Agent starts up, meaning the desktop or server Operating System boots, it will try and register itself with one of the Delivery Controllers (or cloud connectors) known within the Site. To make this happen there needs to be a mechanism in place that tells the VDAs which Delivery Controllers are part of the Site and how they can be reached.

For this Citrix introduced the 'auto-update' feature, which is enabled by default. It will keep all VDAs updated when Delivery Controllers are added or removed (go offline) from the Site. Each VDA maintains a persistent storage location to save this (Controller) information. When the auto-update feature is disabled, or does not supply the correct information the VDA will check the following locations (in this order):

- Through configured policies.
- The ListOfDDCs Registry Key.
- OU-based discovery (legacy).
- The Personality.ini file created by MCS.

> **FMA fact**: If a VDA is unable to register itself with a Delivery Controller or communication between the VDA and the Delivery Controller fails for any reason, the machine will stay in an unregistered state and won't be directly accessible or manageable through one of your Delivery Controllers.

In addition to the above, when installing the VDA manually you will be prompted for the locations of your Delivery Controllers. One of the options you have is to fill in a Delivery Controller FQDN by hand, or you can let the system do the searching for you. Also, after the Delivery Controller configuration part you have the ability to enable or disable a couple of specific features:

- Optimize performance: This is enabled by default. The optimization tool is used for VDAs running in a VM on a Hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. Note: do not enable this option if you will be using Remote PC Access.
- Windows Remote Assistance: This one is also enabled by default. When this feature is enabled, Windows Remote Assistance is used with the user-shadowing feature of Director, and Windows automatically opens TCP port 3389 in the firewall.
- Real-Time Audio Transport for audio: Again, enabled by default. When this feature is enabled, UDP is used for audio packets, which can improve audio performance. Personal vDisk: Disabled by default and only available for desktop Operating Systems. When enabled, Personal vDisks can be used with a master image.

The installation sequence and the options you have, have changed slightly throughout the past few years.

In 'The FMA core services' chapter we will have a closer look at how the registration process takes place and what some of the main differences between the (new) server and desktop VDAs are with regard to the services they host and how they interact.

> **FMA fact**: There is a separate HDX 3D Pro VDA for use with GPU acceleration for example. This type of VDA enables you to make use of hardware acceleration, including 3D professional graphics applications based on OpenGL and DirectX. (The standard VDA supports GPU acceleration of DirectX only.). It can be selected during VDA installation. Resources can either be assigned on a one to one basis (Passthrough) or shared amongst multiple VMs (vGPU).

Did you know about VDA in High-Availability mode?

Normally all connections run from your installed Agents through your Delivery Controllers. But what if your Controllers are not reachable? So, your database is fine, but your Controller(s) are not: hmm…

You can configure your Virtual Delivery Agents to operate in something called high-availability mode; this way your users can continue to use their desktops and installed applications. In high-availability mode the VDA will accept direct ICA connections from users instead of connections brokered by a Delivery Controller.

Although it's hard to imagine this ever happening, it's good to know what your options are. When enabled, if the communication with all Delivery Controllers fails high-availability mode is initiated after a preset period of time, which is configurable. By default, it kicks in after 300 seconds.

High-availability mode will be enabled for a maximum of 30 days in total. During this time the VDA will attempt to register itself with one of the Controllers while your users will continue to use their desktop and/or installed applications.

As soon as a Controller becomes available the VDA will try and register itself without any interruptions to the user. From then on, all other connections will be 'brokered' as usual. If during these 30 days the VDA is not able to register itself with one of the Controllers the desktop(s) will stop listening for connections and will be no longer available.

As per Citrix: High-availability mode is suitable only for use with dedicated desktops, where the mapping between the user and the VDA is known. You cannot configure high-availability mode for use with pooled desktops.

To enable high-availability mode you need to set / configure the High Availability and HaRegistrarTimeout registry keys. These keys need to be created manually after the Virtual Delivery Agent is installed. With the High Availability key, you enable or disable high availability for the VDA. Set it to 1 to enable or 0 to disable. The HaRegistrarTimeout key lets you configure the amount of time the VDA will try and register itself with a Delivery Controller if it loses its connection before initiating high-availability mode on the VDA.

Secondly, you need to provide your users with an ICA launch file that will enable them to make direct ICA connections. You have to create an ICA file for each user who requires this feature: Citrix does not create or distribute ICA files for this purpose.

Limitations

There are, however, a few limitations to using the VDA high-availability feature. These include: user roaming. If a user device is already connected to the desktop, users are unable to connect from a different user device.

Delivery Controller-originated policies. Policies originating on the Controller, such as those governing client drive mapping and access to the clipboard, will not work, as there is no connection to the Controller.

Policies originating from the Domain Controller and Local Group Policy are unaffected. Note that policies from a previous registration persist and are applied, so outdated policies might take effect. Power management. When the desktop powers up, it attempts to register, fails and, after the timeout, enters high-availability mode. NetScaler Gateway and Remote Access cannot be used.

Key takeaways

- VDAs communicate directly with your Delivery Controllers (Desktop service).
- On boot, VDAs register themselves with a Delivery Controller.
- The mechanism used to find a Delivery Controller to register with is referred to as 'auto-update' but can be achieved in other ways as well.
- Registration will be done through port 80 by default; customising your VDA settings through Control Panel can change this.
- VDA registration can be verified by restarting the Citrix Desktop Service on the VDA machine itself. After the restart, look for event 1012 stating it successfully registered with a Delivery Controller.
- A VDA consists of two main services, the Citrix Desktop Service and the Citrix ICA Service. The Desktop Service communicates with the Broker service on the Delivery Controller it registers with.
- The Delivery Controller will also power-manage the VDA, meaning it will (re)boot it when needed (works for desktop VDAs only). It will also tell it to listen for new connections when user's login to their VDI environment to ensure a successful connection.
- With the addition of XenApp to the FMA, Citrix created a new Server VDA. This will be discussed in more detail later on.
- Use the VDA in HA mode as a last resort. Hopefully it will never come to this.
- VDAs can be managed through policy.
- Different versions of VDAs can be mixed within the same environment (you can select the VDA used from Studio during configuration and install). Make sure to always check with Citrix to find out which configurations are supported.
- Using mixed versions of VDAs can lead to limited feature support. This includes management and monitoring features through Studio and Director.
- Always try to de-install the old VDA and install the new VDA.
- Before installing the latest VDA available, make sure to check with Citrix for any known issues that might have surfaced during testing (E-docs).
- Sometimes manually updating to the latest VDA (after reimaging) is recommended.
- For lab set-up purposes you can install the Delivery Controller software, the database, StoreFront, licensing etc. all on one server.