Inside Citrix chapter twenty eight – The one with Appendix B - Key Takeaways (per chapter)

Is this all still relevant?

- When talking about cloud computing remember that there are multiple cloud services to choose from: it is not a one-size-fits-all solution.
- Even when moving your entire on-premises infrastructure (or the biggest part) might be beneficial in the long run, it will still take careful planning and execution to get there.
- Start small and take it from there. Hybrid solutions are the way forward, think CWC, for example.
- A lot of companies benefit by leveraging the cloud for Burst Capacity and backup.
- Don't forget about printing and scanning when hosting your RDSH / VDI-based infrastructure in the cloud (bandwidth limitations).
- True VDI (or DaaS) from the cloud, and with this I mean virtual machines with a desktop Operating System installed, assigned on a one-to-one basis, are still hard to achieve. This is mainly because of Microsoft's licensing restrictions.
- Most DaaS solutions are based on RDSH / XenApp in the back-end, meaning you will share your 'desktop' with multiple users.
- The cloud will no doubt have a major impact on how we configure and manage our future infrastructures going forward. However, on-premises RDSH and VDI infrastructures are here to stay for at least another five to ten years, if not longer (my guess is longer).

The evolution of the FMA

- Both XenApp and XenDesktop are built and based on the FlexCast Management Architecture (FMA). And I am pretty sure it will stay like this for many more years to come.
- The FMA was first introduced with XenDesktop version 5.0 back in December 2010. Before that, XenDesktop was also based on the Independent Management Architecture (IMA).
- XenApp became part of the FMA on June 26 2013, which was the official GA date of XenDesktop 7.0.
- The FMA was initially built with VDI in mind.
- This also meant that XenApp was no longer available as a separate product and that they (Citrix) also decided to stop any further development regarding 6.5.
- Luckily, Citrix listened and reintroduced XenApp and XenDesktop as separate products with the release of version 7.5. I don't think they will make a mistake like that again.
- With the addition of XenApp to the FMA, a new (server) VDA was needed.
- The FMA was always meant to be the next generation architecture, providing enhanced scalability, robustness, flexibility and manageability over the IMA.

The FMA, its foundation

- The FlexCast Management Architecture is a Microsoft dot-net-based architecture built upon the WCF (Windows Communication Foundation) framework.
- The WCF framework itself is built using the Microsoft .NET framework
- Dot-net-based applications are executed in a software environment known as the Common Language Runtime, or CRL.
- The .NET Framework supports the following programming languages: Visual Basic, Visual C#, Visual F# and Visual C++.
- Citrix offers several SDKs and APIs, plus some additional tools and services to help you build and integrate custom-developed monitoring and management solutions.
- Citrix has its own Citrix Developer Visual Studio Extension free for you to download.
- Google for 'Citrix developer overview' and you are good to go.

Delivery Controller

- As mentioned, your Delivery Controllers have a lot of responsibilities and can therefore be seen as the heart of your FMA deployment.
- Always deploy at least two Delivery Controllers per Site, and if you can per Zone as well. A minimum of one is needed in the case of a WAN link failure.
- Virtualising your Delivery Controller makes them more flexible, especially in bigger environments. Adding extra DCs or compute resources will be a breeze.
- Almost all Site traffic goes directly through your Delivery Controllers over to the Central Site database and vice versa.
- Try to keep your Delivery Controllers physically close to your database server and any Host Connections you might have set up.
- Delivery Controllers are fundamentally different from Data Collectors: remember that. No LHC, direct database communication, no communication between Delivery Controllers, service- and agent (VDA)-based, and so on.
- StoreFront directly communicates with one of your Delivery Controllers during the user authentication, application enumeration and launch process. You can configure your StoreFront server with a NetScaler load balance VIP address, which will load balance the connections to the Delivery Controllers within the NetScaler VIP.

The virtual delivery agent

- 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 users 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 deinstall 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.

StoreFront

- You basically have two points of authentication within a XenDesktop / XenApp Site: StoreFront and NetScaler.
- When working with Zones always make sure to deploy at least one StoreFront server per Zone. Needed in the case of a WAN link failure.
- Users may need to subscribe themselves to resources they are allowed to start. These user subscriptions are synchronised between all StoreFront servers within the same StoreFront server group.
- The above is also referred to as the 'Self Service Store' setup, which is enabled by default. A bit more on this in the 'The Citrix Receiver' chapter.
- The 'Self Service Store' can be disabled, leaving you with the 'Mandatory Store' configuration. Using this setup all resources for which a user has proper permissions will be displayed by default, no subscriptions needed.
- Combined with the 'Self Service Store' approach you can configure Keywords in Citrix Studio to automatically subscribe your users to certain resources, like a standard desktop, for example. When a user logs in, the resources will be directly displayed on his or her welcome screen.

- If email based discovery is enabled and configured, you have the option to either advertise the Store or to hide the Store. When advertised the Store is presented as an option for your users to add. When you hide it, the user will need configure the Citrix Receiver him or her self using a setup URL or provisioning file, for example.
- When configuring and modifying your StoreFront deployment, especially when editing the web.conf file, make sure you are doing this only using one StoreFront server at the same time. Preferably the one you installed and configured first.
- You can manually propagate any changes you have made to StoreFront to your other StoreFront servers within the same server group.
- When dealing with multi-site deployments, you can configure specific user groups to be mapped to a preferred site.
- StoreFront multi-site configurations let us configure a Recovery site. This site will sit idle until all other StoreFront deployments stop accepting connections, whatever the reason may be.
- When using a Citrix NetScaler think about using it to load balance all external incoming traffic to your StoreFront servers.
- If you only publish a single desktop to a user, StoreFront will automatically launch it directly after the user successfully logs in to StoreFront. This behaviour can be changed by manually editing web.conf file. Have a look at the following CTX document: CTX139058.
- StoreFront plays an important part in configuring Citrix Receiver pass-through authentication a.k.a. Single Sign-on. Look for the support document CTX200157.

The Central Site database

- As of XenDesktop 7.x, only SQL is supported for the Central Site database.
- It contains all static as well as dynamic Site-wide information.
- Make sure you understand the differences between the IMA and FMA when it comes to your Controllers and the Central Site database.
- If your Site is spread over multiple geographically separated locations, or you have multiple Zones configured, your Central Site database should always be in the Primary Zone, or the main datacentre.
- So even with multiple Zones configured it is still one central database.
- Make sure to implement some form of HA solution for your Site databases, since Connection Leasing is only meant as a supplement.
- Your Delivery Controllers and the Site database are constantly communicating: for this, Windows authentication is required between the Delivery Controller and the database.
- When the database fails (even without Connection Leasing) existing connections will continue to work. New sessions cannot be established and Site-wide configuration changes are also not possible.
- It is not recommended to install SQL on the same machine as a Delivery Controller.
- Try to keep your database server physically close to your Delivery Controllers in the data centre.

- SQL software, server or Express, must be installed and configured before creating a XenDesktop Site after its initial installation.
- While SQL Express is primarily used for PoC and testing purposes it could be used for smaller production environments as well. No HA capabilities though. It's up to you.
- You must be a local administrator and a domain user to create and initialise the databases (or change the database location).
- To be able to create an empty database, to add Delivery Controllers to it, create and apply schema updates and so on, you will need to have the following server and database roles: dbcreator, securityadmin and db_owner.
- When using Citrix Studio to perform these operations, the user account must be a member of the sysadmin server role.

The Citrix Receiver

- No matter how you decide to deploy and configure Citrix Receiver, make sure to instruct your users.
- Don't forget to inform your helpdesk employees when planning configuration changes to Receiver.
- I briefly introduced you to the Web Access and Self Service modes. Remember, it does not have to be one or the other. They can be configured and used side-by-side.
- A couple of years ago the Self Service mode was released as a separate plugin; it is now built into Receiver.
- In fact, some of the most important modules that make up Receiver today are the ICA Client software, the Self Service plugin, and the Single Sign-on module for ICA.
- It all started with the ICA Client software back in 2009. Since then it has gone through a lot of name changes and of course the underlying technology also matured over time.
- The upcoming Receiver X1 is probably a great example of its evolution during the last decade.
- When upgrading to a newer version of Receiver, make sure to follow the step-by-step procedure as outlined by Citrix; have a look this CTX article: CTX135933.
- As it stands today, the Citrix Receiver version 4.4 should be able to upgrade from any of the older Receiver versions that might be installed without any issues.
- When upgrading to a version older than 4.4 and you run into any issues, have a look at CTX137494, the Receiver Clean-Up utility.
- Do not forget about the ICA handshake and the earlier mentioned virtual channels.
- The Citrix Receiver can be managed and configured using various methods, for example: using the command-line, registry settings, StoreFront account settings, or on a per application basis using Studio and Group Policy Objects.
- When viewing the Citrix Receiver Feature Matrix, remember that not all features are on there.
- By default, the HTML5-based and built-in (StoreFront) Receiver is not enabled: this needs to be done manually.

Studio / Zones

- Citrix Studio is THE management console that allows us to administrate, configure and manage our XenDesktop and/or XenApp Sites from a single pane of glass. It also provides us with access to real-time data collected through the Broker service running on the Delivery Controller.
- Studio also provides us with a range of basic troubleshooting tools and options.
- While Zones are not a new concept, you need to be aware that Zones within a 7.x deployment are not the same as with XenApp 6.5 – not yet anyway. There are some distinct differences between the two, as we have clearly seen in this chapter.
- Citrix is working on a phased approach with regard to the reintroduction of Zones; needless to say, this is phase one.
- Zones in the FMA still depend on the Central Site database: there is no LHC.
- The main focus of this first releases is to simplify overall management and keep traffic local.
- Make sure to keep an eye on the RTT between Zones; it needs to be below 250 milliseconds; less is more in this case. Consult the table for recommended values.

Director

- Director is a real-time monitoring and troubleshooting web-based tool.
- Citrix EdgeSight technology has been built into Director (primarily used for historical data reporting, trends and analyses). The EdgeSight software will no longer be available as a separate product. The latest version of EdgeSight was 5.4, which is still supported until 31-Dec-17 if you have a valid software maintenance and/or Subscription Advantage.
- To be able to make use of the built-in historical reporting fucntionality Platinum XenDesktop / XenApp licenses will be needed.
- To make use of the network analysis functionality you will need to have at least a NetScaler Enterprise or Platinum license.
- Depending on your XenDesktop / XenApp / NetScaler licenses, you will be able to store historical data for a certain period of time. See the overview.
- Director offers different views for administration and troubleshooting purposes, including the ability to configure delegated administration on a per role basis.
- Alerts and notifications are directly visible and accessible from the main dashboard.
- The main XenDesktop / XenApp infrastructural services are also being monitored by Director, these are visible from the main dashboard view. It uses PowerShell for this.
- SCOM alerts and notification can be configured and viewed from Director as well. Just recently, Citrix acquired the SCOM Comtrade management packs for Citrix environments.
- Insight Services can now be accessed directly from Director. It is fuelled with analytics data from Scout, as well as Citrix Call Home.
- Insight services can also be accessed directly by going to www.cis.citrix.com.

- Director can also be used with older IMA, XenApp 6.5 environments. It also supports older VDAs.

Citrix License Server and licensing

- Citrix Licensing relies on Flexera software, as do many other product vendors, by the way.
- The license server is a relatively light role and can easily be shared with other roles on a single virtual of physical server. A single license server is able to handle over 10,000 continuous connections.
- XenDesktop and XenApp licenses come in different forms. There are per user, per device and concurrent licenses available.
- A user license gives a single user the right to start sessions on an unlimited number of devices. The license is bound to the user and is device-independent.
- A device license works the other way around. A session can be started from a single device, but it does not matter by whom. It is user-independent.
- If a user/device license is issued, it is applied to a license token for both a XenDesktop and a XenApp license token, even if you only connect to just one or the other. They are always issued in pairs.
- Concurrent licenses are not bound to a user or device: you can use them for both. However, these are more expensive to purchase.
- If the license server becomes unavailable for some reason it will make use of a built-in grace period of 30 days. Everything will continue to function as before. This basically means you will have 30 days to get the license server up and running again.
- While products like XenDesktop and XenApp are both licensed through a central license server, a product like NetScaler, will need its license installed directly on the device itself.
- Citrix offers various forms of support and maintenance. Subscription Advantage allows you to upgrade to the latest versions, Feature Packs and so on. Software Maintenance, on the other hand, offers you 24x7x365 support. When purchasing either XenDesktop and/or XenApp you will need to also purchase at least one year of Subscription Advantage and/or Software Maintenance, which isn't that uncommon.
- Recently they released their Current Release (CR) and Long Term Service Release (LTSR) product support options. For each Long Term Service Release, the clock restarts, giving you 5 years of mainstream support and 5 years of extended support, plus more. Current Releases will provide access to the latest security, productivity and collaboration features to help keep your workforce competitive, plus extras.
- The 'new' CR release isn't really new; it is basically the way it has always been before they introduced the LTSR option.

Host Connection

- While in earlier releases of XenDesktop / XenApp 7.x Host Connections were limited to Hypervisor platforms, cloud environments are now supported as well.
- As it stands today, MCS can be used in combination with Azure, AWS and/or the Citrix CloudPlatform. However, PVS is not supported: it simply does not work. It also works

for, or with all Hypervisors mentioned. The Nutanix Acropolis Hypervisor will be added to the list shortly.

- MCS only works with virtual machines.
- You can add multiple Host Connections if you want, also combining cloud and on-premises Hypervisors.
- When adding Hypervisor Host Connections you will have to use the addresses of your System Center Virtual Machine Manager, Virtual Center or XenCenter.
- When using Zones make sure that the Host Connection configured for a Zone is close to, or actually physically located within, that Zone.

NetScaler

- The NetScaler can do more than 'just' provide secure remote access to XenDesktop and/or XenApp environments.
- All NetScalers are (almost) equal with regard to the functionality and features that they can deliver. Depending on the type of license you upload, certain functionalities and/or features will become available. Pay as you Grow.
- The main differences between the physical appliances can be found in the compute resources and the type of Cavium SSL accelerator card that they hold. This card is used to decrypt and encrypt SSL traffic. The more powerful the card, the more SSL transactions it will be able to handle.
- NetScalers can be physical (MPX and SDX), virtual (VPX), virtual on physical (VPX on SDX) and containerised (CPX).
- While not mentioned earlier (except for the license type) there is also a NetScaler Express edtion. It is free of charge and a potential great resource for smaller deployments, PoC's and test environments. The VPX Express edition offers the same features as the VPX standard edition. However, there are a few limitations to keep in mind like: no SSL Offload capabilities, max 5 Mbps throughput, licensed per year. Other than that it is definitely worth having a look at.
- There are three main ADC platform licenses available: Standard, Enterprise and Platinum. There is also a separate NetScaler Gateway license and a universal license.
- If you need to temporarily increase your network bandwidth think about purchasing and applying a Burst Pack.
- Remember the one is none rule? Well, it applies to NetScalers as well.
- NetScaler HA (2 nodes) is always set up as active-passive, with one NetScaler being the primary node of the two, and thus the active one. The secondary node(s) will send a continuous stream of heartbeat messages (interval is configurable), checking to see if the primary device is active and accepting connections. If it fails to respond, and after multiple retries, a secondary node will take over, which is referred to as a failover. NetScaler clustering, which is Active / Active using ECMO, can grow up to 32 nodes in total.
- When applying NetScaler HA be aware that different NetScaler models cannot be paired: the model and make of both NetScaler appliances must be equal and both NetScalers must run the same software version, licenses included.

- The NetScaler can also provide secure remote access to XenMobile web, SaaS and mobile applications. The latter is referred to as Micro VPNs. In fact, you need a NetScaler for this.
- Always start small and contact your Citrix sales representative when in doubt. Remember the Pay as you Grow model: you can't go wrong.
- When dealing with larger and more complex environments, consider having a look at the NetScaler Unified Gateway set-up.
- Make sure to apply SSL certificates to secure your in- and outbound connections.
- It is thought of as a best practice to use third-party certificates when dealing with external, inbound connections, and to use internal CA certificates for all internal SSL traffic, from your StoreFront Server to your Delivery Controllers, for example.
- When setting up a test lab or PoC environment, self-signed certificates can be helpful.
- NetScaler can secure remote access for both StoreFront as well as Web Interface.
- When implementing a Citrix NetScaler certain firewall ports will need to be opened. Always check the Citrix product documentation before implementing.

Provisioning Services

- Provisioning Services streams a base image over the network down to either virtual or physical machines.
- It works for both desktop as well as server Operating Systems.
- A device using a vDisk is also referred to as a Target Device.
- The machine used to create and maintain the vDisk is referred to as the Master Target Device.
- Target Devices are managed using Device Collections.
- Dozens, hundreds or thousands of Target Devices can share a single vDisk.
- The life cycle of a vDisk consists of creation, deployment, maintenance and finally retirement. For this we can leverage the built-in PVS Versioning mechanism.
- Give your write cache sizing and location some consideration: you will be glad that you did.
- Although PVS vDisks can also be streamed in Private Mode, where any changes made to the vDisk will be saved, this isn't a very popular approach.
- Provisioning Services can seem complicated and challenging at first. Take your time and take it step by step, you will be fine. There are many excellent resources out there to help you on your way.
- Make sure to make your PVS infrastructure highly available.
- While PvDs have their use, apply them wisely: it's not for everyone. And while this may be somewhat off topic, in many cases where VDI is being considered, RDSH might make more sense.
- Make sure to check out CTX117372 for some best practices around PVS networking.
- While in the past it was always considered a best practice to use physical machines for your Provisioning Servers, today virtual machines are almost always recommend by Citrix. This has a lot to do with the enhancements around standard networking.

- The same applies to isolating your PVS traffic, again mainly due to the advancements that have been made on the networking and virtualisation side of things during the last couple of years. Keep it simple. One of the main reasons why isolation might still make sense is because of security considerations.
- CTX131611 lists a bunch of Known Hardware Related Provisioning Services Issues.
- Check out CTX124185 for best practices around antivirus on PVS vDisks.

Machine Creation Services

- MCS is considered to be easy. It is managed and configured directly from Studio and you do not need any additional infrastructural components as you do with PVS.
- MCS is based on differencing disks technology.
- Your base or golden image will be copied over to all datastores, which are part of the virtual machine deployment. Take this into account when thinking about your storage needs.
- When application virtualisation is not an option, often forcing you to install applications into your base image, think about using application layering as an alternative.
- When using MCS, rollbacks are treated the same way as a new or updated base image: they will again need to be copied over to all datastores involved. Note that in some cases the previous image might still be in use by some machines. If so, than no full copy will be needed.
- Give your Idle and Disconnect session policies some thought. This will make it easier to reboot your machines during night-time, depending on company policy, of course.
- Go over the earlier mentioned list of storage implications a couple of times: there is a lot to consider.

The FMA core services

- FMA stands for FlexCast Management Architecture and, as of XenDesktop version 7, includes a Desktop as well as a Server VDA.
- It is the next generation architecture for XenDesktop and XenApp VDI and/or RDSH-based deployments.
- Over the years it has evolved from six up to eleven main services in total.
- Internal communication takes place over port 80 using Windows Communication Foundation end points.
- Each service runs complete separated from the other services, as a result each service also has its own separate database connection string: if one service fails it will not directly affect any of the other services.
- There is a distinct difference in architecture when compared to the IMA. All of the HDX / ICA bits and bytes are installed as part of the VDA on the Session Host and VDI based VMs while the Delivery Controllers primarily concerns itself with brokering, maintaining and optimizing existing sessions.
- All services run under the NT AUTHORITY \ Network account and use the local computer account for database authentication purposes. One of the benefits this brings

is that password are automatically changed every 30 days. This is a big deal, as service accounts are usually very dangerous.

- The Broker service includes the XML as well as the STA service.
- There are 18 active (sub) site services in total, all running within the Broker services, taking care of various Site housekeeping tasks.
- There needs to be a way that VDAs can track and contact the various Delivery Controllers within a Site to be able to register themselves. Citrix uses the auto-update feature for this.
- As we have seen, the PortICA, or picaSvc2.exe, service is an important one during the VDA launch and user login process.
- The PortICA a.k.a. PicaSvc2.exe and the Citrix Desktop Service a.k.a. BrokerAgent.exe services are the two main FMA services within the Desktop VDA.
- The Connection Brokering Protocol (CPB) plays an important role in the VDA registration process. It is basically a collection of WCF end points.
- The Server VDA does not have the PortICA service; however, it does have a Broker service.
- It basically uses the same ICA stack as with XenApp 6.5, but with a different management interface to make it compatible with the 7.x Delivery Controllers.
- Service groups make FMA services highly available.

The ICA / HDX protocol

- Edward Lacobucci founded Citrix in 1989.
- Initially they started developing a multi-user platform for Microsoft's OS/2.
- Citrix actually started out as Citrus.
- They licensed the OS/2 source code from Microsoft and started developing Multiuser, which would later become their first major release.
- ICA was introduced when Citrix Multiuser was launched, which was around 1990 / 1991.
- Shortly after Citrix launched Multiuser, Microsoft announced that they would drop OS/2 and move to Windows.
- With some help of other companies, Microsoft included, Citrix managed to stay in business.
- In the meantime Citrix patented ICA and they started working on a new and improved version of ICA.
- Eventually a new agreement was signed giving Microsoft access to the ICA source code. This is how the Microsoft RDP protocol came to exist.
- ICA supports most, if not all, standard protocols today.
- It uses TCI/IP port 1494 by default, and is tunnelled through port Nr. 2598 when Session Reliability is enabled.
- The ICA protocol consists of 32 virtual channels in total, 17 of which are reserved by Citrix.
- The client capabilities are negotiated at session launch time, also referred to as the handshake.

- Virtual channels consist of, and communicate through, virtual drivers at the client side and server-side applications on the server side.
- Customers and other third parties have the ability to develop their own virtual channels.
- Each virtual channel has a default priority assigned to it, ranging from 0 to 3, with 0 being the highest, or most important. A higher priority means more bandwidth.
- By editing the registry you can manually change priorities. Be careful with this, giving more priority to one VC means you also take away priority (bandwidth) somewhere else.
- Multi-Stream ICA works by assigning separate TCP/IP ports to groups of priorities, or streams, establishing true QoS.
- Session Reliability ensures that the user session is not disconnected and that the user's session freezes, while in the background the ICA traffic is buffered.
- All buffered ICA traffic will be flushed out to the user's device once the user session reconnects.
- Session Reliability can leverage the Auto client reconnect feature to enforce users to reauthenticate when a session is reconnected.
- HDX is an extension to the ICA protocol and is in no way intended to replace ICA. It works on top of the ICA protocol.
- The Citrix ThinWire technology has multiple names: it is known as ThinWire Plus, ThinWire Advanced, Legacy ThinWire and ThinWire compatibility mode. They all have one thing in common: ThinWire is all about compressing data and enhancing the overall user experience.
- ThinWire has a small CPU and memory footprint and doesn't need much bandwidth.
- Framehawk is all about packet loss and high latency connections, delivering a more than acceptable user experience under challenging circumstances.
- In general, Framehawk needs more CPU and bandwidth than ThinWire, although this has been greatly enhanced with the latest 7.8 release.

Application delivery

- Although I narrowed it down to three ways of application delivery, there are of course a lot more flavours to choose from, especially when talking virtualisation, layering and containerisation. Search for the Application Virtualization Smackdown whitepaper, or visit rorymon.com. You will be amazed by the options you have.
- AppDisks is Citrix's approach to application layering. But again, make sure to give the others some thought as well. Although with AppDisks you will be able to manage everything directly from Studio.
- AppDisks will be available for all licenses. AppDNA integration with AppDisks will be for Platinum customers only. When used in conjunction with AppDisks, AppDNA will automatically check your AppDisks, or any other applications you might have for that matter. It will tell you if they are good to go in combination (compatible) with the platform you want to deploy them on.
- Application layering is not meant as a direct replacement for application virtualisation: they go hand-in-hand. In practice you will probably use all three, base image-installed applications, virtualised and layered apps.
- Application layering does not isolate applications.

- Think of it as just another tool in the toolbox to make life a little easier.
- Remember that, although a single master image is great to have, it is also a utopia in most cases. Just don't go nuts: keep the number of images to manage to a minimum. Less is more.

The user login process

- There are two main authentication points within a Flex Management-based Architecture: NetScaler (optional) and StoreFront.
- Knowing the difference between the IMA and the FMA, how traffic flows throughout each component, and the way they are supposed to interact is or can be vital to successfully troubleshooting the FMA.
- As of version 3.0, StoreFront can also use the XML service for authenticating users.
- Note that there is a distinct difference between authentication and verification. Authentication is to make sure that somebody is who he or she claims to be. Verification is done to find out which resources are assigned (permissions) to the user, which will then be displayed in the user's store, ready for subscription.
- User authentication and resource enumeration basically go hand-in-hand.
- The STA only applies when connections are coming in externally through NetScaler.
- The STA service is part of the Broker server, and so is the perhaps better-known XML service.
- The HTML5-based Citrix Receiver, as part of your Internet browser, can offer the exact same functionality and features as a natively installed Receiver.
- The Windows authentication process is also involved when launching a Citrix published resource.
- Site policies allow us to exclude certain users or to apply certain policies when specific conditions are met. PowerShell can be used to manage and configure Site policies.

A deeper look into Citrix printing

- There are two main (Microsoft) print file formats, EMF and XPS.
- EMF print output is first rendered by the GDI – Graphics Device Interface – before being handed over to the spooler service.
- XPS was introduced as of Windows Vista. EMF development ended with Windows XP and Server 2003.
- EMF data is not compressed. XPS data does get compressed.
- With EMF, each image needs to be redrawn over and over again, even if the same image is used multiple times. XPS can reference a single image multiple times: think company logos, watermarks etc.
- To be able to use XPS, both your print device and the print driver need to support the XPS print file format. If not, it will fall back to EMF.
- High-level Print Spooling: Print output is received by the spooler service, print driver renders Metafile into raw data readable by print device (the actual print job), spooler service sends print job to physical print device.

- When spooled locally, local resources (CPU, memory) are leveraged. No network traffic is generated.
- When spooled remotely (print server) remote resources are leveraged. This will also produce additional network traffic between the XenApp and print server. Might be something to consider depending on your print architecture.
- Most print issues can be led back to badly written drivers. Not tested and/or optimised for multi-user environments.
- Main problems used to be (or still are): Spooler service crashes, CTX print manager service crashes, blue screens, auto-print creation failures, high CPU loads.
- Do NOT make use of kernel mode (version 2) print drivers.
- Use user mode (version 3 and 4) print drivers exclusively.
- Consider isolating your print drivers a.k.a. Print Driver Isolation introduced with Windows Server 2008 R2.
- But... only apply Print Driver Isolation where it makes sense.
- Version 4 modes print drivers: Designed for Metro-style applications (XPS), enhanced printer sharing, easier to install, maintain, manage etc.
- When a Citrix session starts, after the user logs in, it will, by default, try to map all printers known to the client device within the session.
- Change this behaviour to: map the client's default printer only. Configure the 'Auto-create client printers' policy for this. Of course you have multiple options to choose from.
- Tthe XenApp server will try to match the print driver (s) found on the client device. If the print driver cannot be found, the system attempts to install the driver from the Windows operating system. If the driver is not available in Windows it will (try and) use the Citrix Universal Print Driver (it will need to be enabled for this to work).
- Configure the 'Automatic installation of inbox printer drivers' to change this behaviour.
- Think about implementing 'printer driver mapping compatibility'. Print driver mapping is useful in situations where the print driver on the client is named differently than the print driver on the server (these need to match), but offer the exact same functionality. It can also be configured to create a whitelist: this way you can tell the XenApp server that it is ok to auto-install print drivers when not found on the system, but only if those drivers are on the (white) list.
- Use 'signed' drivers exclusively and always thoroughly test your print architecture set-up, no matter how convinced you may be that it will work.
- Limit the number of print drivers installed: less is more!
- Avoid upgrading print drivers. Always uninstall the old driver and install the new one.
- Always match the print server OS to that of the XenApp server OS.
- The Citrix Print Management Service communicates with the spooler service and the local ICA Client, it compresses print data before sending it over the ICA channel, and also manages the ICA virtual channel for client print mapping.
- Printing preferences (user) and properties will be stored on the client device by default. If this is not supported, they will be stored in the user profile within the server Operating System.

- Configure the 'Printer properties retention' policy to change this. Again, you have multiple options.
- A printing pathway defines how print traffic can or will be routed throughout your environment. It also tells us where a job gets processed, spooled, rendered etc.
- There are two Citrix printing pathways: the client printing pathway and the network printing pathway.
- Besides these pathways there is also a set-up named 'Server local printers', which is basically a physical print device directly attached to a XenApp server.
- When using the client printing pathway, application print output is spooled / rendered on the XenApp server (local from a client perspective) before it is sent back to the client device.
- With the client printing pathway the traffic between the XenApp server and the client device is sent through the ICA protocol, meaning it can be managed / compressed.
- When a (fat) client device has a local printer attached, the client printing pathway will always be used.
- When TCP/IP direct printers are added manually or by using / applying Group Policy Preferences, the printer is seen and treated as a locally attached printer. As such, print traffic will flow through the client printing pathway.
- Thin client devices (Linux-based) do not support the client printing pathway. They lack local printing capabilities. The network printing pathway (session printers) will need to be used instead.
- The network printing pathway will send the application print output from the XenApp server to the print server where it will be spooled / rendered. Spooling takes place remotely. From there it will send the print job to the physical print device.
- Using the network printing pathway all traffic sent between the XenApp server and the print server will be uncompressed / unmanaged, non-ICA.
- The Universal Print Server can help compress / manage traffic sent between the XenApp server and the print server.
- When a client device has a network-provisioned (print server) printer, Citrix will always try and route print traffic over the network printing pathway.
- I say 'try', because if the print server and the XenApp server are in different domains and they are unable to communicate, the client printing pathway will be used instead. The same applies when both machines are unable to communicate for other reasons.
- By disabling the 'Direct connection to print servers' policy, we can force the client printing pathway to be used, even when network-provisioned printers are leveraged.
- There is no 'one size fits all', period!
- Keeping the XenApp and print server close together isn't always the best solution.
- All this applies to XenApp as well as XenDesktop, and isn't IMA- or FMA-specific.
- The Universal Print Driver (UPD) is disabled by default.
- The UPD is installed as part of the VDA.
- There is an EMF as well as an XPS print file format UPD.
- The EMF UPD will be used by default. This can be changed through policy.
- Both the Universal Print Server and the Universal Printer use the Universal Print Driver by default.

- The Universal Printer is a logical / generic object created at the beginning of a session. It will be mapped to the client's default printer but this can be changed to any printer known to the client device.
- When using the Universal Printer, no print mapping / enumeration takes place, speeding up the logon / login process.
- The Universal Printer only works for Windows devices.
- It is potentially useful when the 'Wait for printer to be created' policy is used or when you need access to multiple printers, local & network.
- The Universal Print Server (UPS) consists of a client (UPClient) and server (UPServer) component.
- It uses the UPD by default but can be paired with Windows Native print drivers, again, for more enhanced printing capabilities.
- It's optimised for network printers and offers additional compression and QoS options.
- It supports both EMF and XPS-based print drivers.
- It also works for thin client devices and tablets, based on network (session) printers.
- The UPS does not support client side rendering / spooling, meaning that all application print output will be sent over to the print server (which has the UPServer component installed) right away.
- All traffic sent between the XenApp (UPClient component) and print server (UPServer component) can be managed / compressed when enabling the UPS.
- Network printers will leverage the UPS automatically through a process called auto-discovery.
- It can handle up to 50 print jobs per minute.
- Recommended for remote office scenarios. Please note that testing will be necessary to see if adequate compression ratios are achieved.
- Helps in managing a large number of network printers.
- Can be used for proximity printing. The UPS is a prerequisite.
- Use session (network) printers on fast(er) networks.
- Session printers are network printers that can be assigned and mapped to a specific user or user groups.
- With proximity printing, sessions are filtered based on IP addresses or subnets (there are some more options). This way a user will always connect to the closest printer (UPS is needed).
- When dealing with slow printing remember that it's not all about network bandwidth. Also check for congestion and latency.
- The 'simpler' the print driver, the less traffic will be generated. Use vendor drivers only when specific functionality is needed.
- Last-minute addition from the E-docs pages: XenApp and XenDesktop 7.6 FP3 include an Always-On logging feature for the print server and printing subsystem on the VDA. In order to collate the logs as a ZIP for emailing, or to automatically upload to Citrix Insight Services, use the PowerShell cmdlet (Start-TelemetryUpload) supplied with the VDA installer in 7.6 FP3.
- Citrix Printing Tool 3.1 helps configuring and troubleshooting the Citrix Printing subsystem on XenApp, XenApp Online Plug-in and XenDesktop.

- 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.
- All-purpose troubleshooting tool – Run Citrix Scout from a single XenDesktop controller (DDC) or XenApp server to capture key data points and CDF traces for selected computers followed by a secure and reliable upload of the data package to Citrix Technical Support.
- The Citrix UPS Print Driver Certification Tool can be used to test the compatibility of a print driver with the Citrix Universal Print Server.
- Not sure? Test your print drivers thoroughly using StressPrinters.
- Check out Microsoft's (MSDN) web page to find out more about Print Driver Isolation.
- Release data: February 2012, primarily focused on XenApp 6.5: XenApp Printer Driver Manager. Manage your XenApp print drivers. Update the Automatic Printer Replication List with a GUI.
- A collection of Citrix troubleshooting and diagnostic tools: CtxAdmTools.

Troubleshooting the FMA

- 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 tool listed.

Sizing and storage considerations

- When it comes to sizing your XenDesktop / XenApp infrastructures: there is no 'one size fits all'.
- You need to understand the workloads you have to deal with and size accordingly.
- There is more to it than 'just' compute resources: don't forget about your underlying storage platform.
- While sizing is important, try not to overdo it. Real-world testing will always be needed.
- Ask peers for help and/or advice, consult the Citrix XenDesktop Handbook, use Project Accelerator and test, test and test some more.
- Load testing can give us an indication of what might be possible, but remember that your users can be (very) unpredictable.
- When conducting load tests, always try to incorporate any exotic applications that you might have. These are the ones you should be most curious about.

- IOPS fundamentals help you in understanding what is going on under the hood. It will also help in understanding what other IT folks might be talking about in other articles / blogs.
- A random IOPS number on its own doesn't mean anything. What type of IOPS are we talking about: reads, writes, random, sequential, rereads and/or writes, single or multiple threads, block sizes and so on. And even more importantly, what is the latency number in MS?
- Storage providers should be able to provide you with at least the latency in MS, the reads vs. writes ratio, and the data block sizes used during testing.
- Remember that there is a big difference between steady state, boot logon, application launch and logoff storms.
- Storage throughput is not the same as IOPS. When dealing with large amounts of data that need to be processed and transmitted, storage throughput becomes more important.
- Reads are less intensive than writes. Also, today we have a lot of options when it comes to caching reads.
- While IOPS are important when it comes to sizing and forming a potential bottleneck, do not forget about CPU, memory and storage controllers. They can only handle so much..

The Citrix Workspace Cloud

- CWC offers customers the ultimate hybrid model and an easy way to get used to and migrate to the cloud.
- All the latest and greatest FMA features will first be made available to CWC before being built into the on-premises XenApp and XenDesktop products. And this also applies to both ShareFile as well as XenMobile.
- They use a unique, but very simple updating and testing mechanism for this, which unfortunately is still under NDA at the time of writing.
- Although when using the life cycle management service, you will still need to maintain and manage your VDAs, StoreFront and NetScalers to some extent, it will make life a lot easier. Take it for a test-drive.
- Resource Locations include: on-premises / your own datacentres, Azure, AWS and/or the Citrix CloudPlatform, and more will follow I'm sure.
- Ongoing management and monitoring are done from the CWC consoles; they have the exact same look and feel as the on-premises Studio and Director consoles.