The Complete Guide to Migrating from Citrix XenApp/XenDesktop 6.5 to 7.x and Replacing EdgeSight

A technical guide to planning the migration to Citrix XenApp/XenDesktop 7.x and replacing EdgeSight

By Goliath Support Team

Table of Contents

Introduction

Migration to Citrix 7.x

This document will cover the process of migrating from Citrix XenApp 6.5 to XenApp/XenDesktop 7.x. One of the first topics to cover is the change in architectures from Citrix Independent Management Architecture (IMA) in 6.5 to Citrix FlexCast Management Architecture (FMA) in 7.x. FMA is a service-oriented architecture that provides the underlying framework for application delivery, provisioning, and management across Citrix Technologies. FMA in 7.x completely replaces the IMA utilized in XenApp 6.5 and previous versions.

Below is a listing of key architectural differences between IMA and FMA that must be considered when transitioning to XenApp/XenDesktop 7.x:

> **Delivery Controllers** – In the IMA architecture Zone Data Collectors acted as the brokering service and were the only servers to have read/write access to the data store. The data collector role was not a dedicated role by default and should the ZDC become unavailable, an election would be conducted to elect the replacement. In larger environments, it was recommended that the ZDC and secondary ZDC were dedicated and defined via policy. FMA fully delineates between Controllers and Workers. Site and user session management is handled by the Controllers. A Controller cannot offer resources (published apps) to users. In addition, there is no dedicated zone master. FMA evenly distributes this role across all Controllers in the site. Remote Desktop Services (RDS) and/or Terminal Services roles are no longer needed on Delivery Controllers. Licensing for RDS including RDS CALs would be required on servers providing applications and desktops.
>
> **Microsoft SQL Server Database instead of IMA Data Store** – The IMA data store of 6.5 could be deployed as a MS SQL or Oracle database. Each XenApp server in the farm also contained a local read-only copy of the database as it pertained to it, stored as an MS Access file. FMA replaces the data store with a Microsoft SQL Server database as a central repository for configuration information relating to the Citrix XenApp/XenDesktop environment. Support for the Oracle database was also dropped in version 7.x. This database handles messages between Delivery Controllers and is crucial to the operation of the environment including user logon. Citrix supports Mirroring, Cluster and AlwaysON to ensure availability of this database to all Delivery Controllers. Only the Delivery Controllers in an environment connect to this database. With XenApp/XenDesktop 7.12 and newer, the local host cache was reintroduced for the delivery controllers to add a layer to resiliency. The new local host cache is SQL Express rather than Access and only resides on the delivery controllers, not each session host.
>
> **VDA –** The Virtual Delivery Agent is deployed on both XenApp session host servers and virtual desktop VMs. In the IMA architecture, any session host server could act in any role (delivery server, XML, broker, STA server etc.) and all services were installed on all of the servers in the farm. The FMA architecture distributes the roles in a defined fashion. Management and brokering services such as XML and STA are installed and run on the delivery controller server. Application and desktop delivery services and functions are deployed on the VDAs. A XenApp session host with the VDA deployed cannot perform management or brokering functions and the delivery controller cannot deliver application or desktop resources. This makes for a more streamlined and efficient environment with less resources wasted on services and functions that are not leveraged.

Citrix Director – This web-based tool offers support and monitoring of the Citrix Environment. Based on permissions, this allows functions like shadowing users and troubleshooting the Citrix infrastructure.

Citrix Studio – The AppCenter and Delivery Services Consoles have been replaced by Citrix Studio which allows administrators to configure the environment.

Active Directory – All XenApp Controllers, Workers, and Users must be members of the underlying Microsoft Active Directory.

Delegated Administration – Permissions within the Citrix XenApp 7.x environment can be applied based on roles and scopes. Roles can be defined based around job functions of administrative staff. Scopes allow grouping of objects to organize them in a way that makes the most sense for a deployment.

Architectural Considerations for Transition – Design vs. Build

Design vs. Build

As we move through the process of building the new environment, we can start to consider the methods with which we will move from "what do we have" to "what do we want." One common mistake is to start the design with the hardware first without understanding what load we will be placing on it, what the entire environment will look like, what will be required from a Citrix perspective as far as support systems, what we will need from a high availability perspective, or what kind of user densities we will be able to achieve. No matter what we are doing, it's all based on data from previous environments, learning from prior mistakes and what your application impact will be and where we have to adjust accordingly.

The top layers of this diagram are more logical, the foundation of understanding what your users look like and will require for their daily needs. Then we look further into understanding your users - are they remote, full-time users? Will they need a dedicated resource for computing, or will they be accessing from various devices including mobile platforms? We also need to gain an understanding of the entire application footprint. You will need to obtain a full inventory of what the users require, how they use it, what the applications require from the environment, and how the users will be accessing it. Will they utilize a Gateway/StoreFront, VPN, NetScaler, or Direct Access? Also at the User Access Layer, what will they interface with to access their resources, laptops, macs, thin client etc.? This defines the Access Layer of your design plan.

From there, you will begin to structure delivery at the Desktop Layer. Will users be accessing a specific application or set of applications, or will it be a published desktop, or VDI environment? How will that tie back to the users?
The Control Layer is next where we will design the mechanisms, the delivery controllers, the NetScaler Gateways, StoreFront, and Provisioning Servers, among other aspects of the environment. We will also need SQL as part of the Control Layer. This is the layer where you will plan around any high availability and redundancy that will be required in your environment.

At this point we can then begin to think about the hardware. What is it going to take to run all of this properly from storage, processing, RAM, networking, and other perspectives?

Architecture Differences

The table below shows an overview of the main differences (and similarities) between the XenApp and XenDesktop 6.5 and 7.x architectures. Many of the underlying concepts are similar to prior versions of Citrix while terminology may have changed with the new versions:

XenApp 6.5	XenApp/XenDesktop 7.x	Definition
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)	Underlying platform for application delivery & management
Farm	Delivery Site	Top-level Object in a Citrix Environment hosting applications & desktops for delivery to groups of users
Worker Group	Machine Catalog Delivery Group	Group for managing applications, load-balancing, & server software
Worker, Session Host, XenApp Service, Remote Desktop Services (RDS), Terminal Services Machine	Virtual Delivery Agent, Server OS VDA, Desktop OS VDA	Runs the applications & desktops that are published to the user
Zone Master / Zone Data Collector [1]	Delivery Controller	Distribute & handle connection requests
Delivery Services Console	Citrix Studio	Configure and manage user permissions, applications, & desktops within the environment
Delivery Service Console	Citrix Director	Monitor the environment, shadow, & troubleshoot
Publishing applications	Delivering applications	Prepare applications for delivery to users
Data store	Database	Storage for configuration & session information
Load Evaluator	Load Management Policy	Measure load on a machine, balance based on policy
Administrator	Delegated Administrator, Role, Scope	Define permissions for managing the Citrix environment
Local Host Cash (LHC)	Connection Leasing [2] Local Host Cache [2]	Supplements the SQL Server database to enable connection or reconnection
EdgeSight	No Longer Available [3]	Monitoring of the XenApp & XenDesktop Environment
Web Interface [4] / Storefront	StoreFront	Manages delivery of desktops & applications via Citrix Receiver or a website
Single Sign-On	StoreFront, Receiver, & Policies	Allow users to access resources without signing in multiple times

1 – In Citrix versions 7.x prior to 7.7, there is no direct equivalent to Zones in Citrix XenApp and XenDesktop 7.x. In 6.5, zones allowed you to aggregate servers and replicate data across wide area connections. In 7.x, applications can traverse WANs and locations. Delivery Sites can be designated for specific data centers or geographical locations. Users can access multiple Delivery Sites. App Orchestration allows management of many sites across geographic boundaries. The zone master role itself is now distributed across controllers in a site. Citrix re-introduced a feature called Zones in 7.7, but it is not a direct correlation to the Zones that were available in 6.5. The concentration of the zones feature in 7.7 is surrounding the reduction of management complexities and to improve consistency across zones.

2 – Connection Leasing is the answer to LHC in FMA before 7.12, but should not be considered a replacement. It is the closest equivalent when considered along with the site database. Connection Leasing supplements the SQL Server and allows users to connect or reconnect to their most recently used applications and desktops if the site database is offline. Connection Leasing caches assigned personal resources. In versions of Citrix XenApp and XenDesktop 7.12 and beyond, LHC now replaces Connection Leasing. More information on LHC / Connection Leasing is in the SQL section of this document.

3 – Citrix Studio and Director have a minimum amount of functionality compared to what was formerly available with EdgeSight. Replacing EdgeSight is covered in detail in section 8 of this document.

4 – Citrix Web Interface is end-of-life, but is still available in some versions of 7.x. It is highly recommended to use StoreFront instead of Web Interface.

Planning Considerations

Preparing for Migration

Proper design and planning of the XenApp 7.x infrastructure is crucial to a successful deployment and upgrade. A successful upgrade and implementation is crucial to user acceptance and of course user acceptance is crucial for any successful Citrix migration.

It is generally recommended that organizations migrate using a phased approach and a parallel environment. This approach entails building an environment to run in parallel and be fully configured and tested without affecting user connectivity. Phased rollout to the user base allows designation of test users and groups that can ensure an environment is ready for full migration. Additionally, if there are problems in the new environment only a smaller number of users will be affected. As part of this phased approach and utilization of parallel environments, roll-back planning is also easier to implement in case of major issues with the new infrastructure.

Infrastructure components in XenApp 7.x such as Delivery Controllers will need to be newly created and deployed. StoreFront (or Web Interface) can present applications and desktops from existing 6.5 and 7.x sites.

It is important to verify that existing server and desktop operating systems are compatible with Citrix technologies, required applications, and other aspects of the environment. In addition to ensuring the existing applications work in the parallel environment, you might also consider upgrading to newer operating systems versions or new application versions such as Microsoft Office as well. Microsoft's policies regarding the support lifecycles of Windows operating systems and/or applications might also need to be added to the discussion as part of the Citrix deployment project. Any additional changes such as version levels of Office should be fully tested to ensure the new environment operates to expected standards and user requirement levels.

Generate a roadmap to perform this roll-out successfully. Use the roadmap throughout the migration project to ensure you are meeting technology, user and business expectations.

We use logon simulation, in the form of the Goliath Application Availability Monitor, to test users and groups to ease migration and fully test the end-to-end connectivity, performance, and operation of the new XenApp 7.x environment before any end users attempt to connect. The Goliath Application Availability Monitor can be used on an ongoing basis to ensure accessibility of the Citrix deployment.

Understanding Application Requirements

Compatibility Requirements

Citrix has defined compatibilities with the underlying version of Windows Server installed in various elements of the environment. For application compatibility requirements, we will examine the versions of Microsoft Operating Systems for Server and Desktop Operating System VDAs. The table below shows a general overview of these compatibilities.

Windows Version	Citrix Server OS VDA Product/Version					
	7.13	7.11	7.6 LTSR	6.5	6	5 and FP
Windows Server 2016	X	X				
Windows Server 2012R2	X	X	X			
Windows Server 2012	X	X	X			
Windows Server 2008R2 SP1	X	X	X	X	X	
Windows Server 2008R2				X	X	
Windows Server 2008 64-bit						X
Windows Server 2008 32-bit						X
Windows Server 2003 64-bit						X
Windows Server 2003 32-bit						X

Windows Version	Citrix Desktop OS VDA Product/Version				
	7.13	7.11	7.6 LTSR	5.x	4
Windows 10	X	X	X		
Windows 8.1 Pro/Ent	X	X	X		
Windows 8 Pro/Ent			X		
Windows 7 SP1 Pro/Ent/Ult	X	X	X	X	X
Windows Vista				X	X
Windows XP 32-Bit				X	X
Windows XP 64-Bit				X	X

When planning your Citrix deployment, a very important part of the process is gathering an inventory of the applications that your user community will require. As part of this inventory, consider the legacy application requirements surrounding Windows, SQL and other environmental configurations. Additionally, determine the requirements of each application with regard to connectivity and infrastructure requirements. During the inventory, collect details about what groups of users utilize which applications. This will help with mapping users to Active Directory Groups, Group Policy and other aspects of the environment. This documentation and user mapping will be useful later in the setup and transition process.

You can take advantage of the process of inventorying the applications running in your environment to consolidate and reduce the application inventory list based around criteria such as application versions, non-business related applications, legacy applications, management applications (such as antivirus, inventory, monitoring, and backup solutions), and application functionality. Here are some other changes to consider to coincide with the roll-out :

- Migrate toward new and consistent versions of applications across your installation footprint.
- Eliminate non-business related applications while activating security settings that prevent users from reinstalling them.
- Upgrade management applications such as antivirus software to corporate standards.
- Evaluate and eliminate redundant applications which perform a similar function so that administration of multiple applications is streamlined (PDF Viewers, web browsers, word processing, etc.)

While performing the inventory and audit of applications, keep track of applications in the environment that may be considered technically challenging to install or implement. These applications may need additional effort to properly implement within the Citrix deployment. Additionally, you can use testing within the parallel environment to gain an idea of what workload various applications will place on your server and networking infrastructure.

Keep track of user peripheral requirements such as printers during the inventory process. This will provide the appropriate information when the time comes to configure the Citrix and Active Directory environments for handling deployment of the required devices to the appropriate users.

While conducting your inventory, pay close attention to licensing requirements for all of your applications (not just Citrix) to ensure that the new XenApp or XenDesktop environment will not run afoul of any application licensing restrictions. Track what users will have access to an application so this can be used for future adjustments to or to determine any necessary increases in application licensing. In addition, special steps can be taken in order to isolate users who should or should not have access to certain applications in the interest of conserving licenses of costly or limited applications. This same criteria can also be used to determine security groups for user access to applications within the Citrix environment.

Additionally, some applications will experience issues when running within a shared Citrix infrastructure, or within an environment that contains other apps with incompatible registry settings, DLL or other files.

Legacy Apps

You may encounter legacy applications that have certain requirements regarding the Windows environment on which they are run. Some of these requirements may drive the configuration of sections of the Citrix environment.

For example, a 16-bit application code (or an application with any internal 16-bit architecture) will not run within a 64-bit Windows operating system. Applications of this nature can be installed within a separate XenApp 5.0 farm running on 32-bit Windows Server 2008. Applications running in this environment can be published via StoreFront. This environment will run in parallel to the XenApp 7.x installation. Note that 32-bit installations of Windows are limited to addressing 4 GB of RAM. This limitation will affect the maximum user density of a server. XenApp 5.0 is the last version of XenApp supporting an underlying 32-bit operating system.

An alternative approach is to install the 16-bit application in a 32-bit Windows environment delivered as a VM Hosted App. In this method of delivery, the application is installed on a virtual machine running 32-bit versions of Windows operating systems. In this setup, only one user can connect to each VM at a time, so this solution may not be sustainable for applications accessed by many users simultaneously. If this solution is attractive to you, but you require higher numbers of users accessing the legacy application, you may also consider deploying a VDI environment utilizing desktop operating systems that can support the legacy application. For example, if VDI endpoints will be under 4 GB of RAM a 32-bit operating system may be suitable and may also be able to support the 16-bit legacy application.

Performance Requirements

If workloads require vGPU in order to deliver graphic workloads via HDX 3D Pro, your hosts need to conform to specific requirements for hardware and graphics cards. Citrix maintains a compatibility list with the most up to date information regarding the supported hardware platforms. HDX 3D Pro allows Citrix users to utilize solutions like NVIDIA GRID cards that are installed on the host server. In this deployment scenario, users will experience high-end graphics capabilities within their Citrix XenApp session. Certain graphics intensive applications such as CAD will perform well when delivered via vGPU enabled hosts. There are three methods of mapping GPU to users.

- Pass-Through GPU requires one GPU for each XenDesktop instance (single user) or XenApp session (multiple users).
- Another option is to use Hardware Virtualized GPU where an NVIDIA GRID's power card can be shared between multiple machines.
- You can also use Software Virtualized GPU in which sessions do not have direct access to the GPU. Software Virtualized GPU is not a recommended option.

If delivery of the Microsoft Office platform has been identified as part of your application requirements for your Citrix XenApp 7.x environment, it is important to note the effects on overall user density per server. Microsoft Office 2010 gives the greatest amount of user density per server while Microsoft Office 2013 reduces this by approximately 20%. Microsoft Office 2016 single server user densities are generally 25% less than a comparable Microsoft Office 2010 installation.

There are additional considerations in a Microsoft Office 365 deployment.

Special considerations surrounding Outlook Cached mode should be taken in an Office 365 installation where Microsoft Hosted Exchange is utilized. You will need to make decisions about persistence of user profile files and the potential for additional space requirements. Additionally, utilizing online (non-cached) Exchange mode may result in a slower user experience. Please refer to the following table below for some of the considerations relating to Microsoft Hosted Exchange configurations in a shared Citrix XenApp or XenDesktop environment. If it is decided to use Outlook Cached mode, it's recommended that the Outlook cache file is stored outside of the user's universal profile folder to avoid lengthy synchronization and file copy procedures.

	Offline Cached Exchange Mode	Online Non-cached Mode
Drive Space	High disk space requirements per user, full size of mailbox will be stored in user profile location. Special considerations for profile management	Much lower drive space requirements per user
Storage Performance	Higher IOPS requirements, each user will be accessing a large file stored within their user profile	Lower IOPS requirements
User Experience	Faster access	Higher latencies possible during Access
Network Requirements	Each user requires constant connection to the hosted Exchange environment	Periodic synchronizations to the Exchange environment allowing higher network latencies and greater bandwidth requirements
Search	Higher IOPS requirements to service local cache search	"Instant Search" is unavailable
User Profiles	Profile must follow user, user profiles will potentially be very large and take much longer to synchronize (depending on profile management solutions)	Non-persistent configuration is acceptable

There are additional considerations regarding Skype for Business / Lync implementations. The majority of presence and messaging features of Skype / Lync work perfectly in a XenApp or XenDesktop environment. However, it can become a challenge when considering the Video and Audio solutions present in Skype / Lync. Citrix publishes the "Citrix HDX Real-time Optimization Pack" which helps enable the best functionality of Skype / Lync across Citrix clients.

OneDrive for Business is another part of the Office 365 platform. Microsoft indicates that the OneDrive for Business Sync agent is unsupported in Terminal Services/Citrix XenApp and XenDesktop environments. If you are running Sync in a non-persistent VDI or XenApp session, this will result in a large amount of data transfer during user logon. One workaround is to require users to access their OneDrive via a web browser. Citrix makes the recommendation to utilize Citrix ShareFile instead of OneDrive Sync for corporations that may be entitled to this via existing licensing or those who choose to purchase it separately.

Office 365 licensing can be a challenge inside an environment where users may log into multiple unique desktops or where one machine may host multiple users. Microsoft has addressed this via the "Shared Computer Activation" licensing methodology. In this configuration, the Office 365 installation will contact the Office Licensing Service via the internet. This methodology stores the licensing information in the user profile, if a user logs into a machine they've already used, the cached license is utilized. In this scenario, licenses for a machine will only last a brief period of time before licenses must be reactivated. In order to reactivate licensing, an internet connection is required. If a user cannot be properly licensed, Office will operate in a reduced functionality mode. This "Shared Computer Activation" licensing method requires the Office Deployment Toolkit in order to be properly configured.

Planning the Delivery Method

Shared Desktop

This is a high-density solution sharing a server operating system among many simultaneous users. This is currently XenApp, but has been referred to as other names throughout the history of Citrix. Some of the older names include MetaFrame, Presentation Server, or ICA. In this type of environment user permissions are generally restricted. Users will not be able to reboot, change certain Windows settings, or install applications. When utilizing XenApp, all users are sharing a single operating system and it's possible that one user can adversely affect other users' experiences when connected to the same server. Some applications can become difficult to administer in this type of environment due to application requirements, conflicts with permissions applied, and issues with sharing underlying operating system or application files. The potential problems in a Shared Desktop environment can be amplified when utilizing badly architected or legacy applications.

Despite the inherent challenges, a Shared Desktop environment is traditionally one of the main ways that administrators implement Citrix solutions. There are benefits to user mobility, accessibility from varying endpoints, low bandwidth or high latency network connections, simplification/consolidation of administrative and management tasks, and centralization of the environment.

Virtual Desktop: Persistent and Non-Persistent

The use of the term persistence of data in this document refers to the persistence of user data, not the persistent unchanging nature of the desktop image. This is in-line with documentation from Citrix. Therefore, a persistent virtual desktop continues to contain user data between subsequent logins of that user. Non-persistent virtual desktops would not store user data.

This style of Citrix solution is generally referred to as XenDesktop or VDI. In this deployment methodology, each user has their own desktop which is not shared. In other words, only one user logs into each desktop. This can increase application compatibility and prevent issues with users potentially affecting the performance and usability of the environment for other users. There are also higher requirements on the underlying infrastructure including storage space and throughput. The underlying shared system image must be based around a Desktop version of an operating system. Server versions of operating systems are not supported. Desktops of this style can be deployed in two modes, Non-Persistent or Persistent. In Non-Persistent mode, users connect to a single master image that is provisioned via either Provisioning Services (PVS) or the newer Machine Creation Services (MCS). The administrator has the choice of allowing users to connect to the same desktop on subsequent connection attempts or being randomly assigned to a different desktop on each connection. In both of these modes, changes to the desktop are lost on disconnect/reboot. In Persistent Mode, users will reconnect to the same desktop and have their changes stored to a Personal vDisk file that is retained between reboots. Dedicated Virtual Desktops are also considered persistent. It is required that the Personal vDisk files be stored on shared storage.

Published Applications

Instead of publishing an entire shared desktop, you can also choose to publish an individual application. A server hosts this application and multiple users can connect to that single server. In situations where applications are complex to install, this method of deployment can save efforts surrounding updates to the application or struggling with installation of the application on many workstations. This deployment method is preferred when the underlying application has few requirements on other applications running in the same Windows environment. This can also provide greater security than deploying a full desktop as users will only have access to the single application that is published.

App-V vs. Direct Install

In a Citrix VDI environment, application streaming reduces the applications installed into the gold image by managing applications from a central location and pushing them to appropriate VDI sessions. Citrix Application Streaming is now considered end-of-life and is only supported on operating systems prior to Windows Server 2012 and Windows 8. For new installations, Microsoft App-V is the preferred technology. Microsoft App-V can also be a solution for applications that have technical issues or compatibility issues with some operating systems.

Applications are packaged on the App-V Management Server for distribution via an App-V Publishing Server. The App-V Management server houses the package repository and associated configurations. Publishing Servers connect to a Management Server. Publishing Servers are registered with the Management Server and obtain metadata from it for publishing application requests. The App-V Client installed on the virtual desktop communicates with the Publishing Server to procure the appropriate virtualized apps.

If your application utilizes DLLs that work within DLLHost.exe, or utilize COM+, it will not work via App-V distribution methodologies if they are:

1) part of the operating system
2) prerequisites
3) requirements for other applications to start or start services or require device drivers to function.

App-V version compatibilities with Citrix technologies:

App-V	XenApp and XenDesktop Version	
	Delivery Controller (DDC, ZDC)	VDA
5.0 including SP1	XenApp 7.5 and Up XenDesktop 7 and Up	7.0 and Up
5.0 SP2	XenApp 7.5 and Up XenDesktop 7 and Up	7.1 and Up
5.0 SP3	XenApp and XenDesktop 7.6 and Up	7.6.300 and Up

To support App-V in a Citrix environment, the Citrix VDAs must have both the Microsoft App-V Client and the Citrix App-V components installed. This is in addition to having a properly deployed Microsoft App-V environment.

Direct Installation of applications into the base disk image that is distributed to Citrix VDI sessions is another method of managing application footprint. In this scenario, applications are manually installed within the base image. The preferences, settings and drivers required for endpoints would also be installed into this image. Considerations regarding endpoint hardware, software licensing, application security, and user location will drive portions of the image creation.

Application footprint and endpoint hardware platform will drive elements of the image that is deployed. If different users will require different applications or be running on different client hardware, it may be required to publish multiple images.

When an image has been fully tested, and confirmed to be operational, it is published to the environment as a “gold image.” Changes to this gold image should be carefully controlled as it will affect all users of the image. Only select environments will have a single gold image for distribution to the entire user base. Most will have multiple gold images depending on user, hardware, or application requirements.

Deciding on a Delivery Method

It’s important to understand the user base who will be accessing the environment and how they work on a daily basis. You will need to investigate what applications are utilized and how those applications behave. Additionally, you will want to spend time concentrating on how the user wants to work - including mobility and what endpoints they will be accessing from. A proper plan in the beginning of your migration process will result in a Delivery Method decision that will increase user acceptance and enable an environment to be built that will sustain growth, be easy to manage and administer, and reliable for the user base.

It’s entirely possible that multiple Delivery Methods may need to be implemented in a blended fashion in order to meet the requirements of the applications, server environment, network infrastructure, or users.

User Management Considerations

Profile Management Overview

User management, or more commonly known as profile management, is an incredibly vital part of the application and desktop delivery infrastructure. It really can be thought of as the glue that ensures a consistent and usable user experience. This is especially true for environments where users may be accessing resources from a combination of resources such as published apps and virtual desktops.

The user profile contains all the configuration, personalization and data for a specific user. Items such as documents, desktop, favorites and application settings, all reside within the user profile. HKEY\CurrentUser registry settings are also part of the user profile. On a standard PC or persistent virtual desktop, profile management is easy – log in, load your settings, and go. All the data is stored on the local operating system and doesn’t need to be accessed from any other resource. However, in a virtualized environment where all the components are abstracted, that isn’t the case. A user could log in to a different resource every time they access the environment, and if they must reconfigure their settings every time they access a session, it would be unusable. This means that profile settings and data need to be stored centrally and be accessible from multiple resources, adding potential complexity and pitfalls to the already complex concept of application and desktop delivery.

Poorly designed profiles are also major contributors to many of the common issues that users experience in a Citrix XenApp or XenDesktop environment. These include slow logons, loss of user settings, profile corruption and are often a result of not having a sound profile management design (or worse, no profile management at all). Even in scenarios where there isn't a use case for storing user settings or data, profile management is still needed to ensure that logon performance is not impeded.

The following section covers the considerations that should be made when choosing, designing and deploying a user profile management solution. These concepts apply to both Citrix XenApp 6.5 as well as Citrix 7.x, but understanding what you have now and where you want to be from a user management standpoint is crucial to ensuring a successful migration.

Types of User Profiles

There are three native types, or models when it comes to determining how you want to deliver profiles to users. Each have advantages and disadvantages, and the best choice is generally determined by the applications and/or types of desktops that are being delivered.

1. **Local Profiles** – These profiles are stored locally on the resources (Citrix XenApp server or Citrix XenDesktop Virtual Desktop Machine). A single profile is stored on a single machine and it is not accessible from any other resource than the machine it's installed on. These require little to no configuration and are generally very stable. They are only ideal when users have dedicated persistent virtual desktops and have no other resources that they will access.
2. **Mandatory Profiles** – This profile type is a preconfigured profile that resides on the local machine. They are completely static and any changes that a user makes are saved or retained. As a result, they are the most stable form of profile and virtually impervious to corruption. They do require configuration and setup to set the parameters of what is included in the profile configuration. These profiles are ideal for scenarios where users are accessing published applications that do not require personal user storage or the saving of personal settings. Mandatory profiles are also often leveraged in published and virtual desktop scenarios where they are deployed as kiosks.
3. **Roaming Profiles** – The roaming profile is stored in a central network location for every user and is designed to be available to a user regardless of the session host server or virtual desktop accessed. The intention is for the user's data, settings and personalization to follow them wherever they log in. Roaming profiles allow for the most flexibility since the user's experience is consistent, regardless of the delivery mechanism or application they access. However, the flexibility does come with some additional complexity and challenges. Roaming profiles work by copying the user's data and settings down to the session host during logon and then copy it back to the server at logoff. The very nature of this operation can be problematic, especially if the profile is large or if there are a significant number of files that need to be copied.

Each of the three basic models of profile delivery, as stated above, have pros and cons when it comes to deciding on what model to deploy. As a result, there are additional advanced methods for profile management to deliver profiles in a more stable and efficient manner.

1. **User Folder Redirection –** While technically speaking folder redirection is not a type of user profile, it is often used for centrally storing user data on the network. Desktop, documents,

Internet Explorer favorites, application data and downloads, start menu, links, and searches all can be redirected. When a redirection policy is configured, the local folders are pointed to a network share (determined by the administrator) and the files are accessed across the network. To the user, the data is local. From an overall perspective, this is an efficient way to keep user data consistent and backed up regardless of where they log in. From an application and desktop delivery perspective, it also helps to make profile management easier. These folders are often the largest folders and contain the largest amount of data from a user perspective. Utilizing redirection means that the data does not have to be uploaded and downloaded as part of a roaming profile.

2. **Citrix User Profile Management –** UPM is an enhanced version of standard roaming profile. It is designed to overcome many of the shortcomings that are inherent with roaming profiles while delivering the same benefits. It is more flexible and configurable from a folder management perspective, and it is designed to overcome the “last write wins” issue by not writing the entire profile back during logoff. Additionally, UPM functions as a service that runs on all XenApp and XenDesktop session hosts. By operating as a service, profile management is far more consistent and stable than available with native Windows roaming profiles.
3. **Third-Party Solutions –** Third-party solutions such as RES and AppSense also exist to ease the burden of profile management. These solutions often rely on separate architectures and Microsoft SQL server for data management. Although they come with complexity resulting from this, the added benefits provide a considerable amount of additional flexibility and performance with profiles. In most cases, a third-party solution is chosen because of scale, or the need to have a custom configuration that is outside the scope of Windows or Citrix Profile Management technologies.
4. **Hybrid Profiles** – Hybrid profiles are a combination of two or more profile management solutions. They are useful for making the delivery of profiles either more efficient/easier to manage and/or stable. An example of this would be combining roaming profiles with folder redirection (detailed in this section), and mandatory profiles. The mandatory profiles would dictate files and folders that are consistent and do not change between users. Folder redirection allows for user data files such as the Documents folder and the Desktop folder to be accessed directly from a CIFS share, rather than having to copy the files up and down. This is useful because is eliminates the need to roam the profile components with the largest footprint. Overall, this example makes the profile load time much faster and more stable by having less data to load at login, and less to copy off at logoff. Additionally, by having a smaller footprint it greatly reduces the risk of profile data corruption, resulting in much less administrative overhead.

The following chart breaks down the key differences in profile types.

Feature	Local	Roaming	Mandatory	Hybrid
Central Management/Roams with User	×	✓	[1]	✓
User Settings are Stored Persistently	✓	✓	×	✓
Granular Configuration	×	×	×	✓
Logon Performance and Stability Enhancements	×	×	×	✓

“ [1]”: Can be used in conjunction with Roaming Profiles as part of a Hybrid Profile

Determining the Right Solution for Your Environment

To determine the right solution, there are several considerations that must be analyzed. As with everything related to application and desktop delivery, it starts with the applications and what their requirements are. But in addition to the applications, the migration parameters must be deeply considered as well. Just because the existing profile management strategy works in your 6.5 environment, this doesn't mean it will when moving to 7.x. This is especially true if you are introducing a single image management technology (PVS or MCS) or if you are adding VDI to the mix. On top of that, portability must be considered, especially in the instance where users have locally stored profiles in the 6.5 environment. To help analyze and determine the overall user management architecture, the following considerations should be made:

- □ What is the profile management configuration in the existing Farm, and is it effective?
- □ Where is user data stored for the applications delivered by the environment?
- □ Where are user settings stored for the applications delivered in the environment?
- □ Will users have a need to personalize and save their settings (Windows or applications)?
- □ Will users have a need to store personal data?
- □ How are printers made available to users and how will the printer settings be stored?
- □ How are applications delivered (installed directly on published desktops or VDI, published, App-V, etc.)?
- □ Are applications delivered via session host silos or are there multiple applications delivered from the same session host(s)?
- □ Are PVS or MCS being used in the Site(s)?
- □ Is personal vDisk in use?
- □ Is there a multi-site or farm configuration? Will users access resources from multiple physical locations?

In addition to understanding the above questions that define some of the potentially unique aspects of your environment, there are also some general guidelines that are applicable based on how resources are going to be delivered to users. They are listed as follows:

	Local	Roaming	Mandatory	Hybrid
User Setting Persistence Required (Personalization Characteristic: Basic / Complete)				
Hosted VDI – Random	×	•	×	✓
Hosted VDI – Dedicated / Static with PVD	•[1]	•	×	•[2]
Hosted Shared	×	•	×	✓
XenClient	✓	•	×	•
User Setting Persistence Not Required or Not Desired (Personalization Characteristic: None)				
Hosted VDI – Random	✓	×	•	×
Hosted VDI – Dedicated / Static With PVD	×	×	✓	×
Hosted Shared	×	×	✓	×
XenClient	×	×	✓	×

"✓": Recommended, "•": Viable, "×": Not Recommended

"•[1]": Recommended for users who use a single virtual desktop only

"•[2]": Recommended for users who use more than one virtual desktop

Another key consideration when making the determination of how profiles are going to be delivered is folder management. As highlighted earlier, folder redirection should be used to reduce the profile footprint while also making its operation more efficient. Based on the advantages of folder redirection the initial thought would be to redirect everything that can be, and in many cases that is the right approach. However, before we decide what folders should be redirected, evaluating what folders are unnecessary is key. If users do not need to save local documents or do not need to save data on the desktop (if only published apps are being used for example) then the most efficient method of managing them is to exclude them.

There are also folders where the decision isn't cut and dry. The best example of this is the Application Data folder. By nature, the data in the AppData folder can be quite large. As a result, the initial instinct would be to redirect the AppData folder. However, accessing this data across the network may result in applications performing slowly. In those cases, it may become necessary to roam the AppData folder.

This decision will then drive how your roaming profiles are managed. If using Citrix Profile Management, it is likely that you will want to configure active write back if you need to roam a folder that is large such as the AppData folder. Overall the AppData conundrum must be handled on a case-by-case basis and as with everything else, will be driven by your applications' requirements.

The chart below provides guidance on what folders are recommended for redirection based on the profile type in use.

Folder	Local	Roaming	Mandatory	Hybrid
Application Data	×	×	×	×
Contacts	×	✓	×	•
Desktop	×	✓	×	•
Downloads	×	✓	×	•
Favorites	•[1]	✓	•	✓ *
Links	×	✓	×	•
My Documents	•[1]	✓	•	✓ *
My Music	•[1]	✓	•	•
My Pictures	•[1]	✓	•	•
My Videos	•[1]	✓	•	•
Saved Games	×	✓	×	•
Searches	×	✓	×	•
Start Menu	×	✓	×	•

"✓": Recommended, "•": Viable, "×": Not Recommended

Profile management is a necessary component to Citrix application and desktop delivery. In many ways, it is the glue that keeps user experience consistent and reliable end-to-end. Even though, it is critical and important, it is often overlooked and not configured optimally. Migrating to XenApp/XenDesktop 7.x introduces an excellent opportunity to evaluate your current profile management method and to optimize or architect it to enhance user experience.

Resource Planning

CPU and CPU Ready, RAM, Disk IOPS and Capacity

In Citrix XenApp and Citrix XenDesktop environments, proper allocation of hardware resources is crucial to gaining and maintaining user acceptance.

If you are publishing a Citrix XenDesktop environment via dedicated virtual machines, make sure you assign at least 2 vCPUs to each machine. The end user multitasking experience can be drastically affected if there is only one vCPU. If a user will only be performing simple tasks using a minimal number of programs a single vCPU may suffice. Tasks and applications of this light nature may be more suitable for XenApp deployments like a Shared Desktop or Published Application.

In a Citrix XenApp server based environment it is recommended to start with four vCPUs on Windows Server 2008 R2 platforms. With Windows Server 2012 and 2012 R2 the recommendation is to move to eight vCPUs. Windows Server 2012 and 2012 R2 can support nearly double the user density of Server 2008 R2 with the same hardware specifications in some deployments.

If you chose to oversubscribe or over-commit CPU in your environment, the guidelines have changed in the newest processor and operating system technologies. In XenApp 6.5 on Windows Server 2008 R2 (running on VMware ESXi 4.x and 5.x) it was generally recommended to oversubscribe at a ratio of 1.5x (or 150%) for XenApp workloads. This number was based on Intel Sandy Bridge and Ivy Bridge chips. XenApp 7.x on Windows Server 2012 R2 running on VMware ESXi 5.x and 6.x can be oversubscribed at a higher level of up to 2x or 200% based on Intel Haswell and later chip technologies.

Additionally, Citrix utilizes Thinwire H.264 as a default graphics codec. If you are running a recent Microsoft Operating System such as Windows 10 or 2012 R2, it may be better to switch codecs to the newer HDX Thinwire (automatic H.264). This protocol is also known as Thinwire Plus, Enhanced Thinwire or Next-Gen Thinwire. Features within the protocol have been called SuperCodec, Deep Compression, Thinwire Advanced and Thinwire H.264. Thinwire H.264 uses more CPU power than the non-H2.64 Thinwire protocol. This results in lower server scalability (user density per server) and also utilizes more bandwidth. Citrix versions 7.9 and beyond now have the HDX Thinwire / Thinwire Plus (non-H.264) enabled by default. For earlier versions, use Citrix's built-in policy templates to make the change in codec.

If a server does not have proper RAM assigned to it, excessive paging will occur. Paging will adversely affect performance of your storage environment due to unnecessary additional IOPS load.

Network Requirements (WAN, LAN, and Remote)

In Citrix XenApp and XenDesktop 7.x, the bandwidth requirements have changed from prior versions. As with prior iterations of Citrix XenApp and Citrix XenDesktop versions, modifications have been made in attempts to reduce the bandwidth requirements while delivering the best possible end user experience. This also extends to latency as Citrix continually improves their protocols to handle underlying network latency without adversely affecting the end user wherever possible.

That said, proper network connectivity is crucial to deliver applications in a fashion that will be most acceptable to the end users who will be utilizing the platform. General user acceptance of the Citrix environment can be drastically affected by bad performance of the environment.

Some general rules of thumb for LAN deployments, you should use a high quality managed network switch preferably delivering gigabit to the desktop while offering backbone or fabric interconnectivity between switches at speeds higher than gigabit. VLAN configurations can be utilized to isolate traffic by business need. One common configuration is to isolate printer and server subnets/VLANs from the workstation VLANs. Additionally, switches that provide QOS or other traffic management can be useful to ensure proper and timely delivery of Citrix traffic. Generally speaking, Citrix streaming protocols should be handled by underlying network infrastructure in a fashion similar to VoIP traffic. It's a real-time protocol that is highly latency sensitive.

Selecting a Carrier

If you are deploying to branch offices over a WAN, MPLS circuits are excellent in their ability to maintain delivery quality, privatize your bandwidth, increase security, and prioritize traffic end-to-end. MPLS circuits are generally recommended over more costly point-to-point connections as they offer most of the benefits of a dedicated point-to-point connection without as much of the expense. VPN connections are also potential candidates for delivery of Citrix workload but duplicate some of the functionality of products like Citrix NetScaler. It's important to understand the underlying connection quality in both VPN and MPLS circuits. User performance and experience will be directly impacted by latency, packet loss, jitter and bandwidth of underlying connections. Certain "commodity" connections like Cable and consumer-grade fiber (i.e. Fios) do not offer Service Level Agreements (SLA's) surrounding uptime, time to restoration in case of outages, latency, packet loss or jitter. Performance guarantees such as this are usually dedicated to higher cost enterprise grade telecom circuits.

In large Citrix deployments the higher costs of these enterprise grade circuits can be easily justified to guarantee end user performance. We've also seen excellent success in aligning with one primary telecom carrier for network connection acquisition. This can prevent off-network hops and telecom peering points between carriers which are notorious for adding latencies and uncontrollable aspects to your deployment. Unfortunately, these off-network hops and peering points will be a continual source of contention between carriers when support calls happen.

As a customer you will have little power to affect any change when it comes to these telecom pain points. As such, if you can align with one carrier across all of your network installation points, this affords you the ability to negotiate much tighter SLA requirements and allows the carrier much greater control over the quality of the circuits they deliver to you. Additionally, look for carriers that own their own equipment and have national footprints to allow for growth. Once you are invested with a particular carrier, contract term length, MPLS configurations, and installation lead times can make it very difficult to change to another carrier. You should ensure you've properly tested all aspects of the carrier you are considering.

You should also give additional thought regarding network connection redundancy. The ability of branch office and remote users (accessing via HQ connections) to communicate over these connections is likely 100% mission critical to their ability to perform their job. Generally speaking, you should consider other carriers than your main telecom partner. Be sure to discuss what network points are shared (if any) between the various carriers you may be considering. This is one place that commodity carriers such as cable and consumer-grade fiber (Fios) may be considered. The key reason for this is that most of these commodity carriers completely own their networks and equipment and are wholly disparate from other installed telecom carriers in a particular geographic region. Again, it's crucial to have the discussion with all carriers so you can understand what (if anything) may be shared between them and their competition. Generally speaking, it's been helpful to communicate exactly what you are trying to accomplish with all carriers that are involved. For example, admit to the commodity carrier that you are using them as backup connectivity and discuss with your primary carrier this same aspect. The quality levels of the commodity-grade connections are not as much of a concern when it comes to backup connectivity as even the worst circuits can still be better than being down entirely.

Another option to consider is wireless for backup connectivity. The speeds of most wireless networks are now usually high enough to sustain some enterprise traffic. There are options to combine multiple wireless connections for even greater bandwidth. The major drawback to wireless is that most of these circuits have a bandwidth limitation per billing cycle or charge for overages on a metered basis. This can become costly in an enterprise environment, but again these costs should be weighed against the potential costs of downtime.

As far as Citrix technologies themselves, if you are delivering Desktop OS VDAs, you can use Desktop Composition Redirection or DCR. (This has been renamed from Aero Redirection in prior versions of XenDesktop.) In Windows 8 and beyond, this setting is now default because Aero is always enabled on these operating systems. If this redirection to the client is not enabled, processing of the Aero environment happens in the data center and costs additional CPU (or GPU). DCR only works in a VDI environment.

You can also utilize the HDX Thinwire HDX Policy Templates to customize your Citrix environment for exactly what you need for your XenApp or XenDesktop deployment. These templates allow you to deploy optimal settings for your preferred use case. You can deploy templates for High Server Scalability (HSS), Very High Definition User Experience (VHDX), and Optimized for WAN. The High Server Scalability template gives the greatest user density per server, lower CPU requirements on the server along with a good end user experience. This template changes color depth, frame rates and prevents the use of the H.264 video codec. This still allows videos to be played but optimizes them less. The Very High Definition User Experience (VHDX) settings makes the end user experience the best it can be with the caveat of less scalability per server. This setting will give users better audio, animations, printing and a high end user experience. The Optimized for WAN setting is for remote users that have high latency or low bandwidth connections. This setting is very similar to the High Server Scalability (HSS) setting but is tighter with bandwidth surrounding things like audio, printing, and file sharing. This setting also disables the H.264 video codec.

If you are utilizing legacy operating systems before Windows 8 or Server 2012 R2, Citrix provides policy templates that are labeled “Legacy OS” in order to get the best results on these platforms

The newer HDX Thinwire adapts to lower bandwidth networks more efficiently than those in prior versions of XenApp and XenDesktop.

For XenDesktop in high bandwidth LAN or WAN deployments where endpoints will support it, utilize DCR. If you are delivering XenApp on a LAN or WAN, the choice is HDX Thinwire. Load settings customization profiles to modify these protocols as appropriate for your deployment.

Most LAN connections will handle Citrix protocols well. If you are delivering desktop images to your workstations it is important to have high bandwidth to the desktop.

Image and Delivery Planning

There are several considerations that need to be made when it comes to resource/image management in a Citrix XenApp/XenDesktop 7.x environment. With Citrix XenApp 6.5 and earlier there were far fewer options, making the decision-making process far easier. For one, published apps and published desktops were the only options for user experience delivery overall. From an image standpoint, Citrix XenApp servers were deployed and in most cases a virtual machine template was used to perform the initial provisioning of the session host resource. After that, all the machines were managed on an individual basis. With the Advent of Citrix XenDesktop Provisioning Services (PVS) became an option for Citrix XenApp infrastructures. This allowed Citrix XenApp administrators to manage a single image and single server instance, while streaming up to thousands of session host server resources from that single image. This was an incredible advancement in infrastructure management for the Citrix XenApp admin. However, PVS introduced complexity by having its own dedicated infrastructure, database, and networking requirements. As a result, only larger deployments found the technology to be practical from a deployment standpoint. As detailed in a previous section of this eBook, the introduction of Citrix XenApp/XenDesktop 7.x combined both platforms into a single architecture, FMA. With the new unified architecture came significantly more options for user experience delivery and image management. The following section will detail the options available for image management in a 7.x deployment, the pros and cons of each, as well the impact each will have from a resource and migration standpoint.

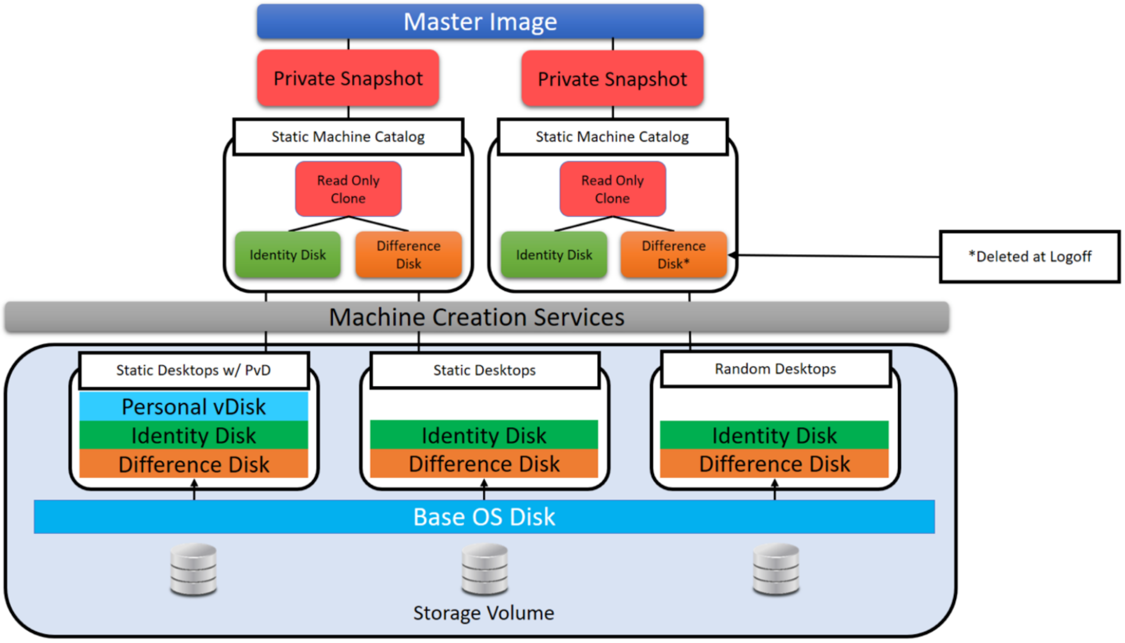
Image Delivery Platforms

Stand-alone or Installed – This is the traditional provisioning method for provisioning server and desktop resources. A machine is built either from scratch or from a base virtual machine template. From there, the resource is a stand-alone machine with resources that must be managed on an individual basis.

Each machine is patched, updated and has applications installed individually. In order to ease the administrative burden of having to manage each session host resource on an individual basis, tools such as SCOM or other tools for software deployment and patch management are often used. This is the easiest method for deployment, but overall comes with the highest levels of administrative overhead. There are also no efficiency gains from a performance or storage capacity standpoint. Stand-alone VMs are recommended in small environments, less than 5 Citrix XenApp Session hosts and/or VDI. Environments where apps are siloed and each server has a unique configuration is also a use case where stand-alone servers would be recommended.

Machine Creation Services – MCS is a single image management technology imbedded directly into Citrix XenApp/XenDesktop. The technology was originally introduced in 5.x and was only available to use with virtual desktops until XenApp was fully integrated into FMA. As of version 7.x, MCS is available as an image management services for both XenApp and XenDesktop delivery resources.

Machine creation services leverages APIs available in vSphere, XenServer and/or Hyper-V to leverage snapshot capabilities for creating linked clones from a single master image. Each machine provisioned with MCS has a differencing disk, identity disk and an optional personal vDisk. MCS provisioned images are configured via machine catalogues from the delivery controller. A stand-alone VM is designated when the MCS catalog is created, the resource pool is then provisioned from snapshots of the master VM. Machine Creation Services create unique ids for each of the provisioned VMs, creates and manages their Active Directory accounts. To update the VMs in an MCS pool an administrator makes changes to the master VM and selects the update option in the delivery controller console. New snapshots of the update master are provisioned replacing the originals. All changes made to the pooled virtual machines are destroyed during the update process.



Machine Creation Services provide several advantages to administrators from an administrative and resource standpoint. Using linked clones allows for a smaller overall storage footprint by only having one instance of the base operating system. It also is a relatively low overhead service to manage and requires zero additional configuration to deploy. It is recommended that thin provisioning storage technology (NFS is the most preferred) is leveraged with MCS. MCS is a virtual machine technology and does not support provisioning with physical resources.

Provisioning Services – PVS is a single image management technology that like MCS, allows you to provisioning multiple machine resources from a single image saving disk capacity. However, being a single image management technology is where the similarities end.

PVS is a separate technology that integrates with Citrix XenApp XenDesktop. Rather than leveraging the hypervisor and API integration, it delivers operating system resources to machines by streaming the image over the network. The Provisioning Services architecture consists of a server (usually two minimum for HA) that is used for managing the environment. It has a Microsoft SQL back-end and uses a file share for storage of image files. A gold image is made from a master machine (physical or virtual), and is stored in the image file repository. These image files can be stored in multiple locations and replicated for high availability. Provisioned resources or target devices are generated from a template VM that is configured without a virtual hard disk. These target devices can be created from a utility on the PVS server or from the delivery controller directly when a machine catalog is configured for PVS. The wizard and/or the delivery controller creates the machine accounts in AD and all unique machine information is stored in the PVS database. Target devices are configured to PXE boot and receive a configuration file from a TFTP server. The virtual machines then boot over the network from the PVS image configured on the PVS server. Image updates are done by booting a virtual machine to the master image in private mode. From private mode, the disk is editable and changes are saved. Target devices are rebooted to the new version of the disk image to receive updates. PVS target devices are 100% read-only and all changes are destroyed upon reboot.

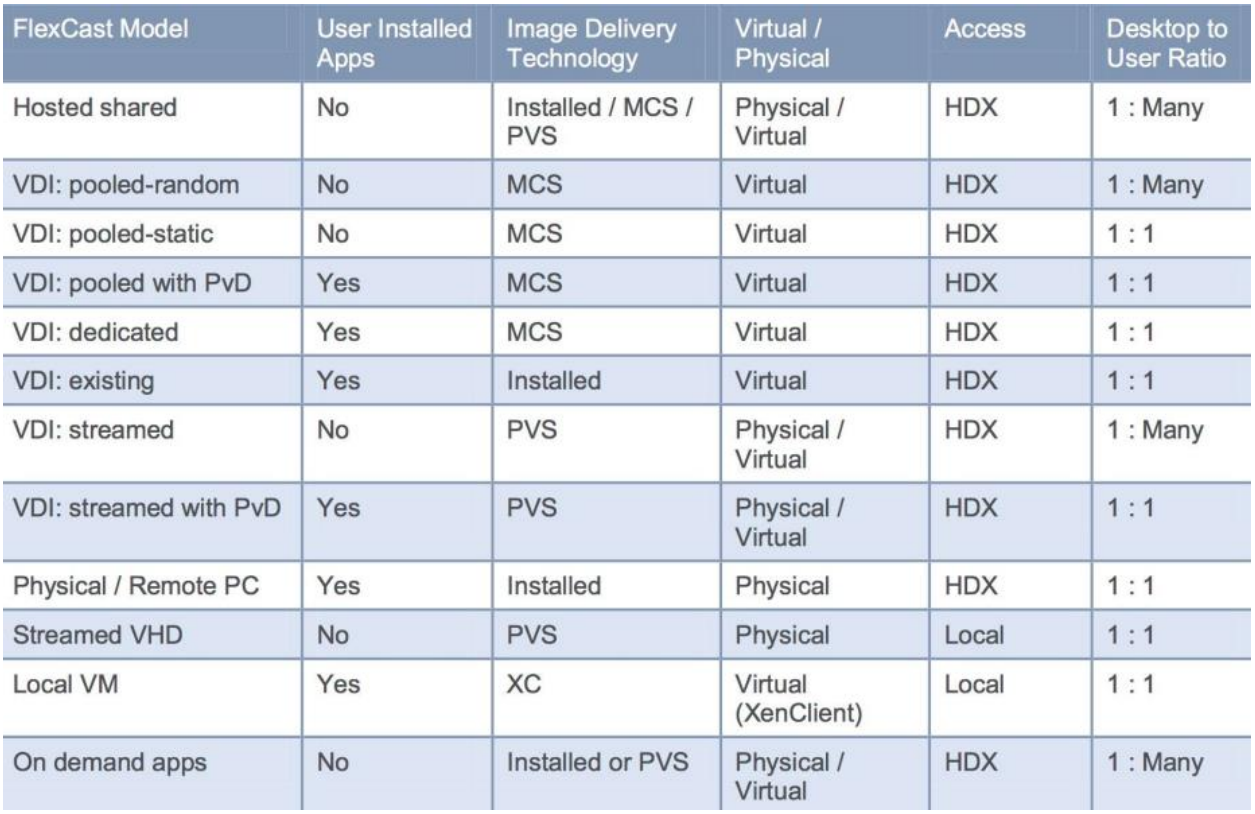
There are several significant advantages beyond management ease and capacity savings for deploying PVS as an image management solution. The greatest benefit is performance by leveraging RAM for disk operations. Read IOPS are mitigated by configuring the PVS server with adequate RAM. When an initial read of data happens it is then cached in the RAM of the PVS server. In other words when an operating system is booted the files are stored in memory. When the subsequent target devices are booted, they boot from RAM rather than the disk. This concept applies to all read operations during the run cycle of all target devices. Mitigating RAM I/O is significant and can greatly improve the overall performance of the delivery infrastructure without having to make a significant investment in storage. This benefit is especially useful for mitigating issues such as boot storms. From a read IOPS perspective there are several options. Write cache can happen on either the server disk, the local disk of the VM or RAM. If local disk is used, different storage locations can be chosen to distribute the write IO across multiple LUN. If RAM is used the virtual machine’s memory resources are leverage for writes, mitigating the impact of write I/O. With PVS 7.9 and up memory spillover is also available to help ensure that RAM is accidently depleted by writes. PVS also can support physical and virtual target device resources, eliminating the requirement that MCS has for virtual machine resources only.

MCS or PVS what is the best option?

When making the decision as to what image management solution is best for you there are several considerations to make. The first is based on what you are using today. If you have PVS deployed in your Citrix 6.5 environment, that is an important variable because it is already in place and if configured optimally, likely doing the job for you.

The next consideration is based on what you are planning on delivering to your users. The specifics around the following delivery models for applications and desktops are detailed in a different section.

However, the method chosen impacts the options available from an image management perspective, and therefore are key components to making the determination of what image management model is best for your environment.

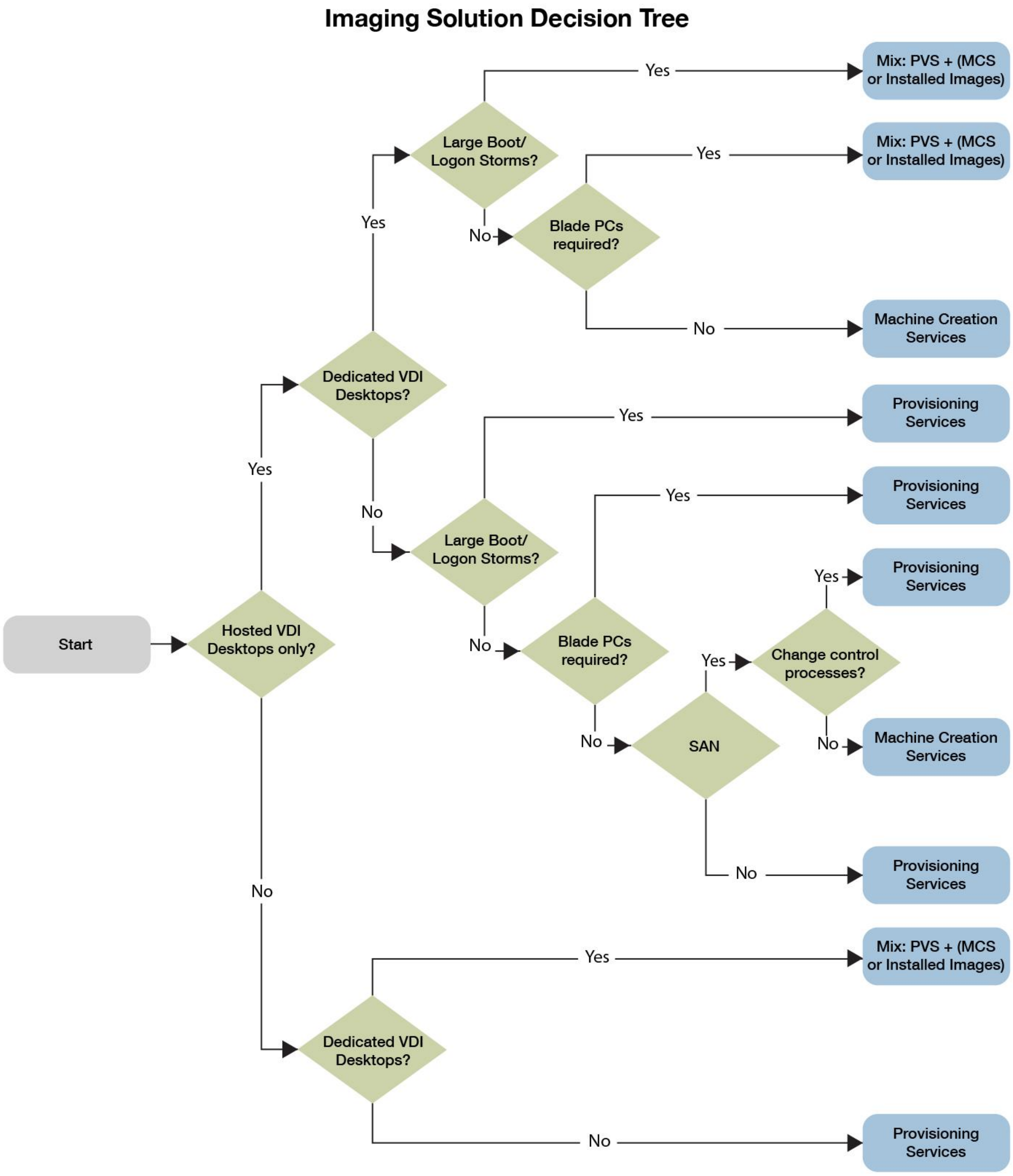


FlexCast Model	User Installed Apps	Image Delivery Technology	Virtual / Physical	Access	Desktop to User Ratio
Hosted shared	No	Installed / MCS / PVS	Physical / Virtual	HDX	1 : Many
VDI: pooled-random	No	MCS	Virtual	HDX	1 : Many
VDI: pooled-static	No	MCS	Virtual	HDX	1 : 1
VDI: pooled with PvD	Yes	MCS	Virtual	HDX	1 : 1
VDI: dedicated	Yes	MCS	Virtual	HDX	1 : 1
VDI: existing	Yes	Installed	Virtual	HDX	1 : 1
VDI: streamed	No	PVS	Physical / Virtual	HDX	1 : Many
VDI: streamed with PvD	Yes	PVS	Physical / Virtual	HDX	1 : 1
Physical / Remote PC	Yes	Installed	Physical	HDX	1 : 1
Streamed VHD	No	PVS	Physical	Local	1 : 1
Local VM	Yes	XC	Virtual (XenClient)	Local	1 : 1
On demand apps	No	Installed or PVS	Physical / Virtual	HDX	1 : Many

Once you have ascertained what works in your environment now, and evaluated what resource types are going to be delivered, the following considerations should also be assessed:

- Although boot and logon storms are not as prevalent as they used to be, IOPS and disk performance are still the biggest Achilles heel of application and desktop delivery. The overall performance capabilities of your storage infrastructure is important and needs to be assessed to make the best decision. If disk performance isn't an issue, or if you are using a technology such as IntelliCache, then MCS is a viable option. If there is a question, PVS is the better option.
- Thin provisioning isn't a requirement of MCS, but without it, many of the storage gains afforded by linked clones will be logs. PVS doesn't need thin provisioning to fully take advantage of the capacity savings that it provides.
- Physical vs. Virtual. If your session hosts are physical, then MCS cannot be used. Also, some environments find that for local users, physical "fat" desktops are more useful. In that case PVS is capable of having physical target devices. This is a great way to use physical desktops but still get the benefits of VDI out of it.
- Ease of use, if there aren't IOPS considerations, and thin provisioning is available then MCS is probably the better option. MCS is fully integrated into the delivery controller, and does not require any additional configuration. It also does not require additional maintenance, scaling and database maintenance. For smaller environments (50 or less XenApp session hosts or 100 or less VDI) MCS is the likely better option.

Daniel Feller created a PVS vs. MCS decision tree chart that is an excellent resource for making the determination.


Imaging Solution Decision Tree
Start
Hosted VDI Desktops only?
Yes
No
Dedicated VDI Desktops?
Yes
No
Large Boot/ Logon Storms?
Yes
No
Mix: PVS + (MCS or Installed Images)
Blade PCs required?
Yes
No
Mix: PVS + (MCS or Installed Images)
Machine Creation Services
Large Boot/ Logon Storms?
Yes
No
Provisioning Services
Blade PCs required?
Yes
No
Provisioning Services
SAN
Yes
No
Change control processes?
Yes
No
Provisioning Services
Machine Creation Services
Provisioning Services
Dedicated VDI Desktops?
Yes
No
Mix: PVS + (MCS or Installed Images)
Provisioning Services

Overall, Citrix PVS provides significant advantages from a performance and optimization standpoint. It also supports physical and virtual machines. These factors make it a powerful solution, this comes with complexity and several components that need care and feeding. The other thing to keep in mind is that is doesn’t have to be an all or nothing approach when it comes to image management.

Like every other aspect of XenApp and XenDesktop, taking advantage of the multiple options can be the best path as use case drives everything. If your VDI deployment is all persistent desktops and there are only 250 of them, then MCS may work best for the desktops. If your XenApp is 500 servers that all reside on spinning disk, then PVS may work better for them, and for your lab stand-alone may be the best option.

High-Availability and Disaster Recovery Planning

Ensuring availability for a mission-critical application delivery mechanism is a must. As with most aspects of planning for the migration from IMA to FMA, there are significant changes when it comes to High-availability (HA) and/or Disaster Recovery (DR) planning.

For clarification, HA and DR are not necessarily one in the same. High-availability in the context of this discussion refers to local resource availability - in other words, component redundancy. Disaster Recovery refers to multi-site availability, and while there is some overlap in the technology components used to achieve both, they are different concepts.

Citrix XenDesktop Site Level HA

As with IMA, the SQL data store is critical to ensuring that brokering sessions for users can happen. All data related to the Site (Farm in IMA) including configuration, access rights, and resource load among others are stored in the database and subsequently, without it, resources are not available to users.

In an IMA deployment, each server has a local host cache making database resiliency native to the platform by having a read-only copy of the database hosted on each session host server that is accessed should the primary SQL database become unavailable. As one can imagine, this made ensuring that resources are accessible relatively easy as HA was built in. The only limitation was that administering and/or making configuration was not possible if the primary data store was unavailable. The local host cache gave administrators great flexibility with how they wanted to architect SQL HA, as the biggest consideration was the availability of administration.

When the FMA architecture was first introduced, there was no mechanism built for FMA. If the database was down, new sessions could not be established and effectively the entire environment was down. This necessitated the deployment of HA at the database level, and in larger environments it required a POD or modular architecture.

Connection Leasing

Citrix began to build in resiliency with the release of Citrix XenApp/XenDesktop 7.6 which introduced the concept of Connection Leasing. This capability allows the delivery controller to cache user connections to the most recently used applications and desktops when the database is available. These connections are cached for a two week period, and the lease is replicated across all site delivery controllers to ensure that apps and desktops are available regardless of the broker. These leased connections are stored on the local disk of the delivery controller and if the DB becomes unavailable, the cached resources will be presented to the user when they connect.

While connection leasing does help overcome the all or nothing availability challenge with database access it does have limitations, starting with the fact that a lease is only two weeks. In other words, if a user needs to launch an application or desktop that they haven't used in more than two weeks, it will not be available to them should the database be unavailable. Furthermore, connection leasing is only available for server-hosted (published) desktops, published applications and statically assigned VDI desktops. If you are delivering pooled desktops, caching is not an option unless the desktops are assigned to specific users prior to the database going down.

Other considerations with Connection Leasing are listed as follows:

- VDA's must also be at a minimum version of 7.6.
- Site database size will increase.
- Additional disk capacity will be required for your delivery controllers when implementing connection leasing.

Connection Leasing, while limited, is a useful feature that can ease the pain of having a database outage. It is recommended that administrators migrating to Citrix 7.6 through 7.11 take advantage of it if moving to 7.12 and up is not an option. It also does not replace the need for a stable and reliable SQL HA deployment.

Local Host Cache

With the release of Citrix XenApp/XenDesktop 7.12, the local host cache was reintroduced into the technology. This capability brings back a critical component of the IMA architecture for resiliency. It also eliminates the limitation of only being able to launch previously accessed applications from no more than two weeks previous. Like connection leasing, only server-hosted (published) desktops, published applications and statically assigned VDI are supported with the local host cache. The local host cache is also read-only and therefore environmental changes cannot be made to the environment when sessions are being brokered from the local host cache.

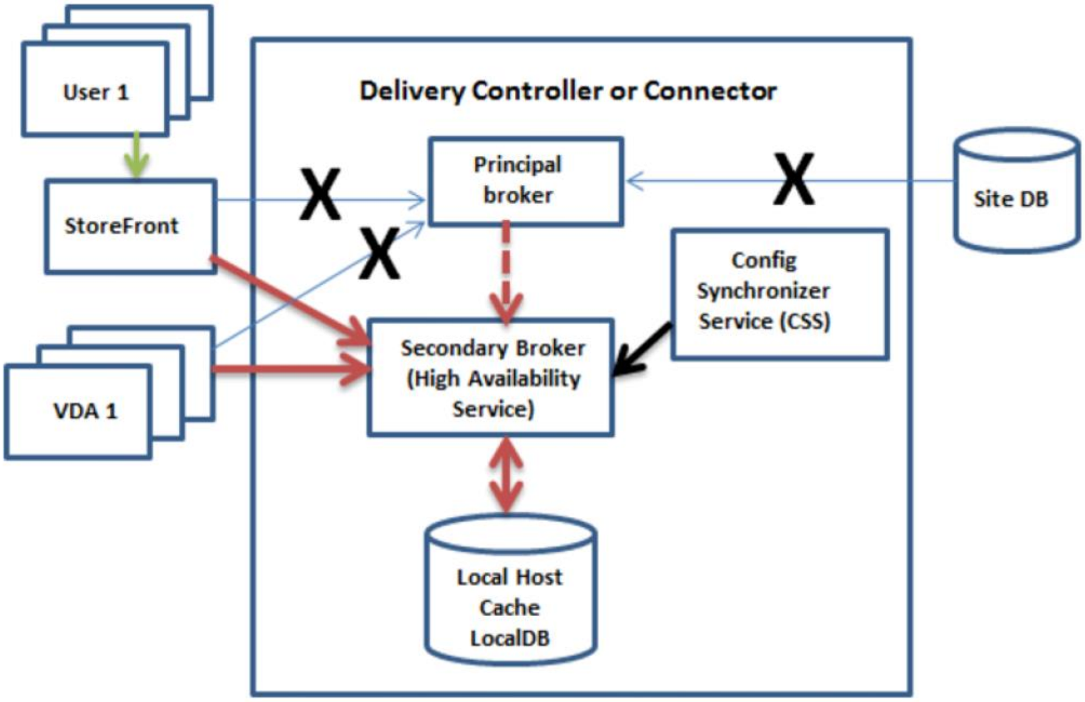
The Local Host Cache in concept is like the version found in Citrix XenApp 6.5. However, there are significant improvements to stability and less of a need to constantly run the diskmaint command. As depicted in the diagram on the next page, the local host cache consists of several components listed as follows:

Principal Broker – This is the primary session broker server that accepts connections from the storefront, communicates with the site DB and sends users to the appropriate VDA.

Citrix Config Synchronizer Service – This service copies changes made to the primary broker to the secondary controller. These changes consist of anything related to site configuration.

Secondary Controller – The secondary controller copies information received from the primary broker to a local SQL express instance. Following the completion of data transfer to the SQL express database, the Config Synchronizer Service is reengaged and performs a check to ensure that the primary data store and the Local Host Cache match.

If a failure occurs, the principal broker detects that the Site DB is no longer available and stops listening for new connections and VDA status. At that time re-registration occurs and the Secondary Broker begins receiving and listening for VDA status messages. During this time, the Secondary Broker handles all incoming connections from StoreFront and the Principal Broker continuously polls the site database for availability. Once the connection to the site DB is reestablished, the Secondary Broker stops listening for new connections and the VDAs re-register with the Principal Broker. This process is depicted in the image below.


User 1
StoreFront
VDA 1
Delivery Controller or Connector
X
X
X
Principal broker
Config Synchronizer Service (CSS)
Site DB
Secondary Broker (High Availability Service)
Local Host Cache LocalDB

The local host cache has been a useful capability that traditionally has eased the burden of HA with the SQL data store. It also provides protection from issues related to DB failover and fail back on the SQL Server side of things. The re-introduction of the capability in XenApp/XenDesktop 7.12 is a welcome enhancement that is improved from the IMA version, and will provide the needed extra layer of resiliency for FMA deployments. However, relying on local host cache alone is not recommended and while it should be deployed it should be leveraged to augment and enhance your database HA design.

SQL High Availability – SQL Server High Availability is recommended to ensure full data store availability and resiliency in a Citrix XenApp/XenDesktop environment. All delivery controllers connect to a Site database. This database contains all the configuration, user and VDA registration for a Citrix XenApp/XenDesktop site.

One controller can be shut down or removed from service without affecting other controllers in a site. While this allows for fault tolerance and high availability at the controller level, it means that the database is a single point of failure. As detailed in the above subsections, some caching capabilities are built into the technology for resiliency, but they do not fully replace the need to have a highly available SQL environment. As such, Citrix supports the following Microsoft SQL HA configurations.

- **VM level HA –** As the name implies, this is only supported with SQL servers that are virtual machines. This is predicated on the Hypervisor platform’s support of HA. It allows for automatic restart of a virtual machine on a different server should a failure occur. VM level HA is the most cost-effective form of HA from a resource and licensing perspective. However, there is also guaranteed downtime between the time the server goes down and the time it becomes available again. Furthermore, it provides no protection against any type of corruption at the OS and/or application layer.
- **Mirroring –** Mirroring increases availability with instantaneous failover. This form of HA requires replication of database data between different SQL server instances. Mirroring can be synced synchronously or asynchronously. With XenDesktop, high-safety mode is recommended which requires a separate witness server to validate availability and to confirm a failover event. With database mirroring, the witness server can be a single point of failure and should have VM level HA implemented at a minimum.
- **SQL Clustering –** Also known as failover clustering, SQL clustering provides HA for the entire SQL instance not just the database. This allows for the redundant servers to appear as a single instance on the network. If one become unavailable for any reason, failover is seamless, instant and invisible to the end user. SQL clustering requires shared SAN storage.
- **AlwaysOn –** AlwaysOn Availability Groups are the newest enterprise HA model for SQL server. This capability introduced with SQL Server 2012 is in many ways a combination of SQL mirroring and SQL Clustering. It allows for OS and instance level HA by using a single virtual IP/instance on the network. However, at the database level, the data is replicated across a network connection. This capability removes the dependency on SAN storage that is found with SQL clustering.

  Furthermore, SQL AlwaysOn nodes allow for scaling out, because the secondary nodes can be used for incoming read-only requests, backup or integrity checks. With XenDesktop the read-only capability is not support because there can be data lag with read-only nodes.

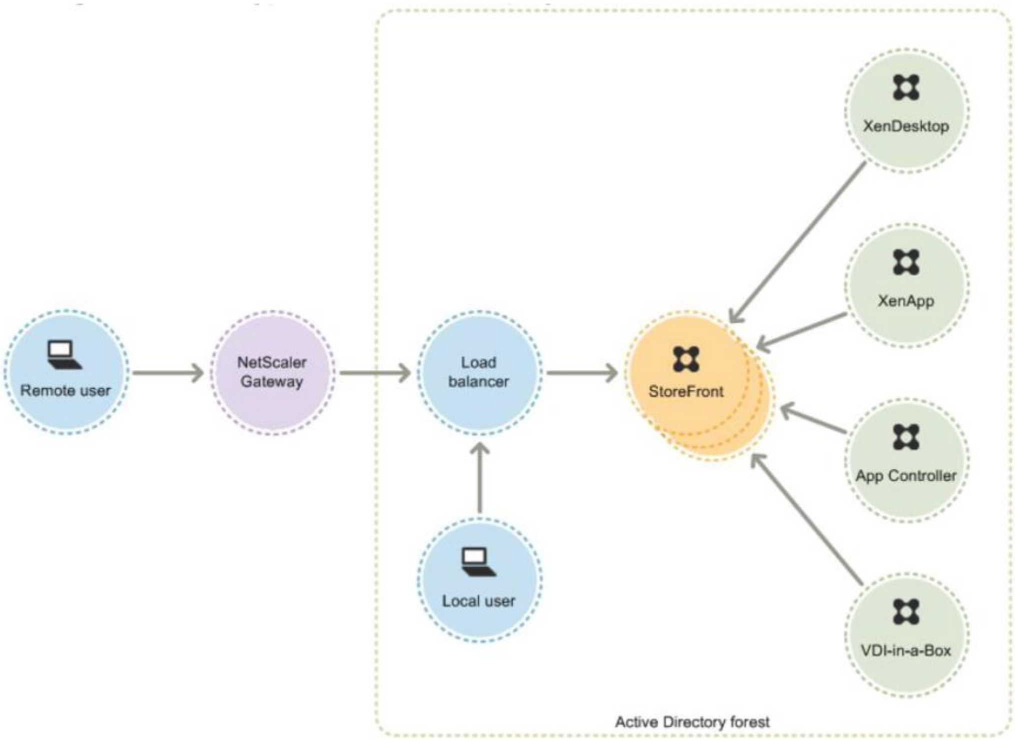
The recommended type of SQL HA varies based on the XenApp/XenDesktop component. Overall leveraging connection leasing or local host cache (depending on version) will ease the demand and overall HA requirement. The chart below depicts each database component and the supported availability types.

Component	VM-Level HA	Mirroring	Failover Clustering	AlwaysON Availability Groups
XenApp/XenDesktop Site Database	Test Only	Preferred	Supported	Supported
XenApp/XenDesktop configuration logging database	Test Only	Preferred	Supported	Supported
Provisioning Services Farm Database	Test Only	Preferred	Supported	Not Supported

Provisioning Services

In addition to HA planning for the Citrix XenApp/XenDesktop site database(s), provisioning services HA must also be considered. PVS is configured in a Farm-based architecture that also relies on an SQL database for storing configuration data, image data and target device attributes such as GUID information and Active Directory computer names. Beyond the SQL database PVS requires storage of the target device images to be available. Images are stored on a CIFS share that require availability for provisioned virtual machines and physical machines to operate. Furthermore, several network services are also required for operation, TFTP, PXE, DCHP and overall network connectivity to target devices.

PVS Farm Availability is dependent on connectivity to the SQL database. As depicted in the previous chart, SQL mirroring is recommended, but SQL failover clustering is also supported. From a PVS server perspective, it is recommended that multiple servers are deployed to ensure availability at the server perspective. It is also recommended that offline database support is enabled at the farm level from the PVS console. Like session caching and local host cache, offline database support allows for limited functionality of the PVS environment should the farm database become unavailable. This feature works by using a snapshot of the PVS database that is created when the server starts. The stream process continually updates the snapshot with information related to the PVS server and target devices. When running in offline mode, farm management functions and the console are not available. Should a failover occur, any new information pertaining to the server or target devices during the outage is synced back to the database once it becomes available again. The image below depicts how PVS offline database support works.



In addition to ensuring farm availability, consideration must be made to image availability. PVS images can be configured in an active/active (load balanced) configuration where OS streaming is balanced across multiple PVS server or can be configured in an active/passive failover configuration.

When configuring high availability for vDisk, version control is a critical consideration that must be planned for and maintained to ensure consistency within the environment. For basic active/passive failover, Windows Clustering may be configured using shared storage. If failover is configured in conjunction with load balancing across servers (active/active), each PVS must have its own local vDisk copy to deliver services. To ensure consistent version control between servers, it is recommended that DFS-R is implemented as described below.

Replication can be managed directly from the PVS console to monitor and ensure availability. Beyond replication it is also recommended that subnet affinity is properly configured to ensure accessibility to target devices from all networks should a failover scenario occur.

StoreFront Services and Multi-Site HA – StoreFront is the primary component for providing entry to the Citrix delivery infrastructure and as such, it is the key component for managing HA, this is especially true when configuring a multi-site architecture.

From an HA perspective, StoreFront server groups should be configured that allow for the configuration data to be replicated across multiple storefront servers. A minimum of two servers is recommended. StoreFront servers should be load balanced using Citrix a Citrix NetScaler VIP to ensure that resources are maximized and availability as depicted below.

Storefront also serves a key role in a multi-site HA deployment architecture. Multi-Site can refer to multiple physical locations or multiple XenApp/XenDesktop sites in the same physical location. In either scenario, the StoreFront acts as the internal load balancing and failover mechanism for the environment. With versions of StoreFront prior to 3.6, configuring multi-site HA was done by making modifications to the Web.config file on the StoreFront server. As of version 3.6, the configuration can be found in the GUI in the manage delivery controllers screen.

When designing your deployment, there are several considerations that need to be made as detailed below:

Active/Active vs. Active/Passive: This is the overarching question. How are resources going to be accessed? Active/Active means that resources will be load balanced across multiple sites and while this is the best way to ensure that you are getting optimal performance it doesn't necessarily provide much benefit beyond that. As a matter of fact, it can be very problematic if you are not careful.

The first challenge is to not overrun resources. Although it seems tempting to leverage all of the available resources for production use, a failover will still dictate that a single site can handle all of the connections from the other site(s) should there be an outage. It is easy to unintentionally starve one site out of rescues if you are not careful.

The second consideration is proximity and bandwidth when it comes to applications and users. Are the apps able to support an active/active configuration? If not, then you need to statically deploy them and balance the load based on the application. Profile access also plays a role in this. If you are using DFS to replicate profile data from one site to another, that does not mean that the profiles can be accessed from both sites at the same time. As a matter of fact, that is the path to rampant profile corruption. Profiles must be configured in an active/passive manor to ensure the integrity of the data. This means that users will likely have to access the data across a WAN if the sites are in two physical locations. If the bandwidth isn't there, there could be significant performance issues with pulling profile data across the WAN.

Application and Desktop Names: When configuring multiple sites, the naming convention for apps and desktops is critical. They need to be identical in order to be invisible to the user once the sites are aggregated in Storefront. If they are not, the applications will appear as duplicates. During the configuration phase, the preferred Site is configured for users based on AD group membership. If the primary site is not available, users will fail over to the secondary site to consume their applications.

From a disaster recovery standpoint, profile data also needs to be redundant and highly available. The method for providing the availability overall will vary based on the profile management solution that is deployed.

Replacing EdgeSight

One of the key components to ensuring a quality Citrix end user experience for users is having visibility into the delivery infrastructure. This is especially true when planning for and executing a migration. First, it is critical to have a complete understanding of the health, user experience quality and resource utilization of the existing environment. Without having a baseline, it will be next to impossible to accurately determine the sizing requirements for the new infrastructure. It is also necessary to understand the quality of the experience that users have in the old environment to understand if the new meets or exceeds the existing user experience standards. Moving into the new environment it is equally important to have the same level of visibility to ensure that users are successfully transitioning to the new resources, as well as ensuring that resource consumption and user experience is as expected as the transition commences.

As you can see, visibility is key in both the existing environment and the new to ensure the success of your migration. Citrix does have basic tools for monitoring the environment that many customers leverage for gaining this visibility. However, they tend to lack key functionality to troubleshoot and resolve Citrix related issues for one simple reason: they do not have visibility outside of the Citrix environment and it is the supporting infrastructure that many times is the root cause of the end user performance issues. Our team can definitively state that the majority of “Citrix is slow” complaints are a result, not of Citrix, but due to IT elements that have nothing to do with Citrix other than supporting the Citrix application.

WE STRONGLY RECOMMEND USING MONITORING FOR BOTH THE CURRENT 6.5 AND 7.x ENVIRONMENTS DURING MIGRATION. THE ARCHITECTURE OF THE PRODUCTS HAS CHANGED AND IT IS ESSENTIAL FOR A SUCCESSFUL MIGRATION TO RESOLVE ISSUES QUICKLY. FAILURE TO DO SO CAN SLOW MIGRATION AND INCREASE PAIN FOR ADMINISTRATORS. Most vendors will allow a rental on one of the environments during the process.

There are some organizations that find EdgeSight to be a capable solution for monitoring their Citrix XenApp environments. However, even those organizations will need to transition to a new solution as it is no longer supported in 7.x. Outside of the end-of-life challenge there are other considerations for replacing EdgeSight. These include the need to monitor the entire infrastructure beyond the Citrix delivery components, having the ability to have deeper metrics related to end user experience, and having better alerting, reporting and dashboarding capabilities. In short, the move away from Citrix EdgeSight is inevitable as you transition your environment, and the new tools Citrix provides with 7.x (Director, Insight and Comtrade) are collectively less capable. Regardless, there will need to be a technology change even if you are satisfied with EdgeSight, and this presents an opportunity to implement a more powerful, capable and cost-effective (when comparing Enterprise vs. Platinum) technology.

Breaking Down Monitoring Requirements

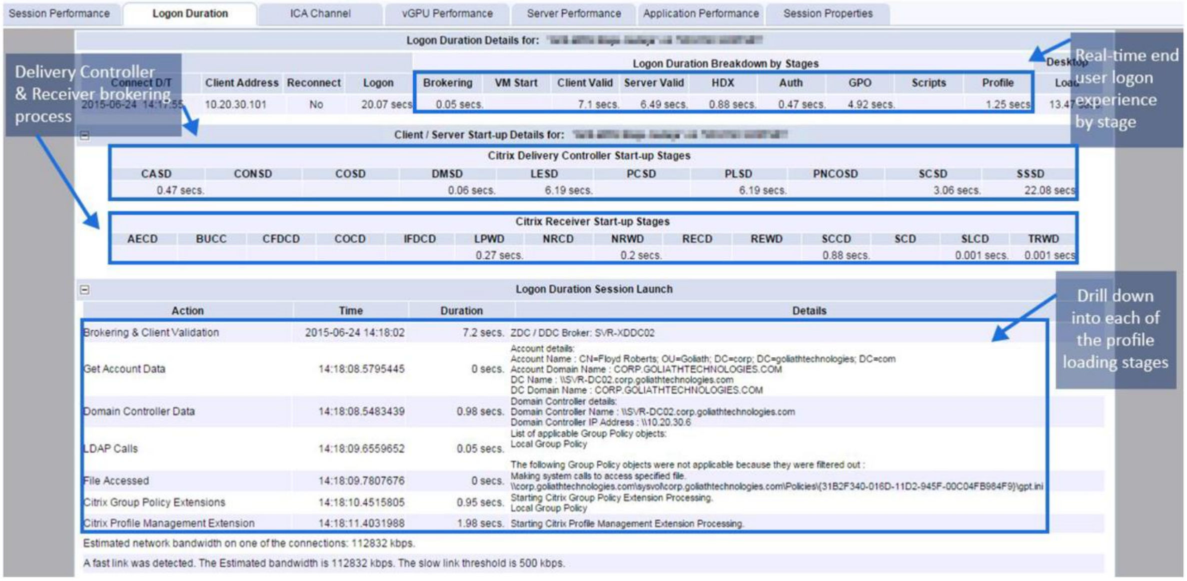
We are going to begin with understanding the monitoring requirements for a XenApp/XenDesktop monitoring solution. As previously stated, many environments run EdgeSight today, and are quite happy with it. So the first question that needs to be answered is, what are the features that matter the most to me in a monitoring solution? Am I simply looking for a feature by feature replacement for EdgeSight so when I migrate I have the same capability, or am I looking for more?

When is the best time to deploy a new solution for monitoring? This is other question to ask as you are moving through the process of deciding what the replacement solution is. Although this seems like an obvious answer on the surface, it is not, and as you will read, migrating to the new solution sooner than later is likely the best course of action.

The following breaks down the key capabilities that we recommend for a replacement solution.

1. **Logon Duration Drilldown for Troubleshooting** – When it comes to end user experience there are three components that make-up the vast majority of issues, -- logon availability, logon duration and session performance. As you can clearly see, logon is a major source of pain for many Citrix deployments and when moving to a new version that is further emphasized as carrying logon issues from the legacy environment forward to the new 7.x infrastructure can easily occur if you do not have insight into the entire logon process.

Having a complete picture of the entire logon process is important as the entire operation is complex with many moving parts. As depicted below, Goliath Performance Monitor provides the complete picture of what happened during a user's logon from the initial connection, through all of the components to the launch of the desktop or application.


Session Performance
Logon Duration
ICA Channel
vGPU Performance
Server Performance
Application Performance
Session Properties
Delivery Controller & Receiver brokering process
Real-time end user logon experience by stage
Drill down into each of the profile loading stages

Logon Duration Details for: [redacted]

Logon Duration Breakdown by Stages

Connect D/T	Client Address	Reconnect	Logon	Brokering	VM Start	Client Valid	Server Valid	HDX	Auth	GPO	Scripts	Profile	Desktop Load
2015-06-24 14:17:55	10.20.30.101	No	20.07 secs	0.05 secs.		7.1 secs.	6.49 secs.	0.88 secs.	0.47 secs.	4.92 secs.		1.25 secs	13.47 secs.

Client / Server Start-up Details for: [redacted]

Citrix Delivery Controller Start-up Stages

CASD	CONSD	COSD	DMSD	LESD	PCSD	PLSD	PNCOSD	SCSD	SSSD
0.47 secs.			0.06 secs.	6.19 secs.		6.19 secs.		3.06 secs.	22.08 secs

Citrix Receiver Start-up Stages

AECD	BUCC	CFDCD	COCD	IFDCD	LPWD	NRCD	NRWD	RECD	REWD	SCCD	SCD	SLCD	TRWD
					0.27 secs.		0.2 secs.			0.88 secs.		0.001 secs.	0.001 secs

Logon Duration Session Launch

Action	Time	Duration	Details
Brokering & Client Validation	2015-06-24 14:18:02	7.2 secs.	ZDC / DDC Broker: SVR-XDDC02
Get Account Data	14:18:08.5795445	0 secs.	Account details: Account Name : CN=Floyd Roberts; OU=Goliath; DC=corp; DC=goliathtechnologies; DC=com Account Domain Name : CORP.GOLIATHTECHNOLOGIES.COM DC Name : \\SVR-DC02.corp.goliathtechnologies.com DC Domain Name : CORP.GOLIATHTECHNOLOGIES.COM
Domain Controller Data	14:18:08.5483439	0.98 secs.	Domain Controller details: Domain Controller Name : \\SVR-DC02.corp.goliathtechnologies.com Domain Controller IP Address : \\10.20.30.6
LDAP Calls	14:18:09.6559652	0.05 secs.	List of applicable Group Policy objects: Local Group Policy The following Group Policy objects were not applicable because they were filtered out :
File Accessed	14:18:09.7807676	0 secs.	Making system calls to access specified file. \\corp.goliathtechnologies.com\sysvol\corp.goliathtechnologies.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
Citrix Group Policy Extensions	14:18:10.4515805	0.95 secs.	Starting Citrix Group Policy Extension Processing. Local Group Policy
Citrix Profile Management Extension	14:18:11.4031988	1.98 secs.	Starting Citrix Profile Management Extension Processing.

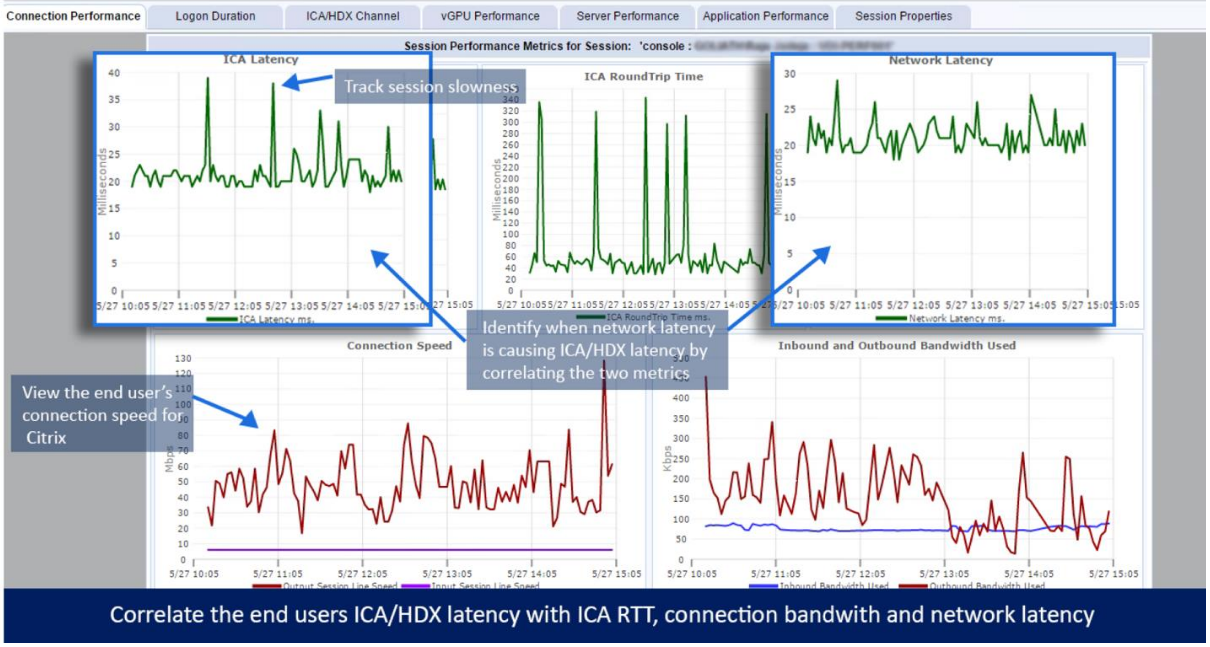
Estimated network bandwidth on one of the connections: 112832 kbps.

A fast link was detected. The Estimated bandwidth is 112832 kbps. The slow link threshold is 500 kbps.

If logon issues stem from brokering, StoreFront, Receiver of Windows components such as group policy having the insight to identify and resolve logon issues is paramount to ensuring a quality end user experience. A solution that provides visibility and the capability to find root cause quickly will ensure success. Furthermore, as detailed in the section of this document about user profiles, abstracting the user (their profile) from the XenApp environment is recommended to ease and automate the migration process. If user logon issues are not discovered and resolved before migration, the issues will certainly carry forward into the new environment. This alone is problematic, but if there are additional issues that compile on top of the old, it could mean that resolving the logon issues is unsurmountable. Understanding and resolving any logon issues no matter how minor prior to migration is ideal to ensure a smooth transition to XenApp/XenDesktop 7.x.

2. **ICA Monitoring and Session Performance Monitoring** - Understanding session performance and how it impacts user experience begins with the ICA/Protocol. Visibility into metrics such as Network latency, ICA latency, ICA RTT and connection speed are critical to understanding what is causing user experience issues with users.

As depicted below, each of the connection metrics are useful for understanding if users are experiencing session related issues due to connection issues, activity-related issues or resource constraints.



Session Performance Metrics for Session: 'console : [redacted]

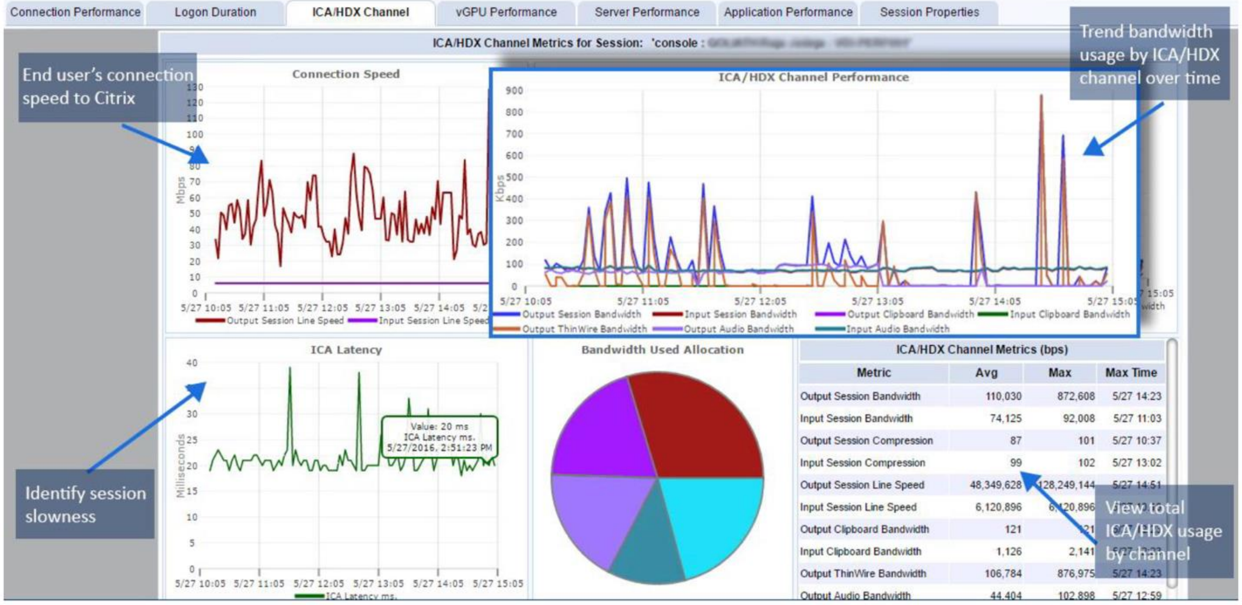
Track session slowness

Identify when network latency is causing ICA/HDX latency by correlating the two metrics

View the end user's connection speed for Citrix

Correlate the end users ICA/HDX latency with ICA RTT, connection bandwith and network latency

In addition to the overall connection related metrics, understanding how user activity in-session impacts performance as well. ICA channels are used to segment traffic based on the type of activity being conducted - video, clipboard, USB, audio, and printing among others are some examples of ICA channels. Each channel and its subsequent activity can be identified, parsed out and measured for any given session. This data is important to understanding how user activity impacts the overall performance a user's session and should be a requirement of any Citrix monitoring solution.



ICA/HDX Channel Metrics for Session: 'console : [redacted]

End user's connection speed to Citrix

Trend bandwidth usage by ICA/HDX channel over time

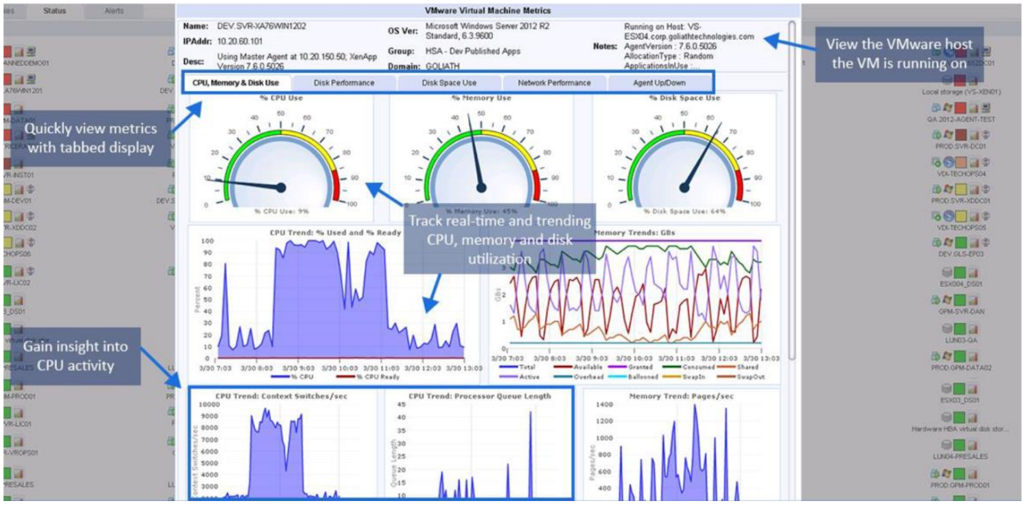
Identify session slowness

View total ICA/HDX usage by channel

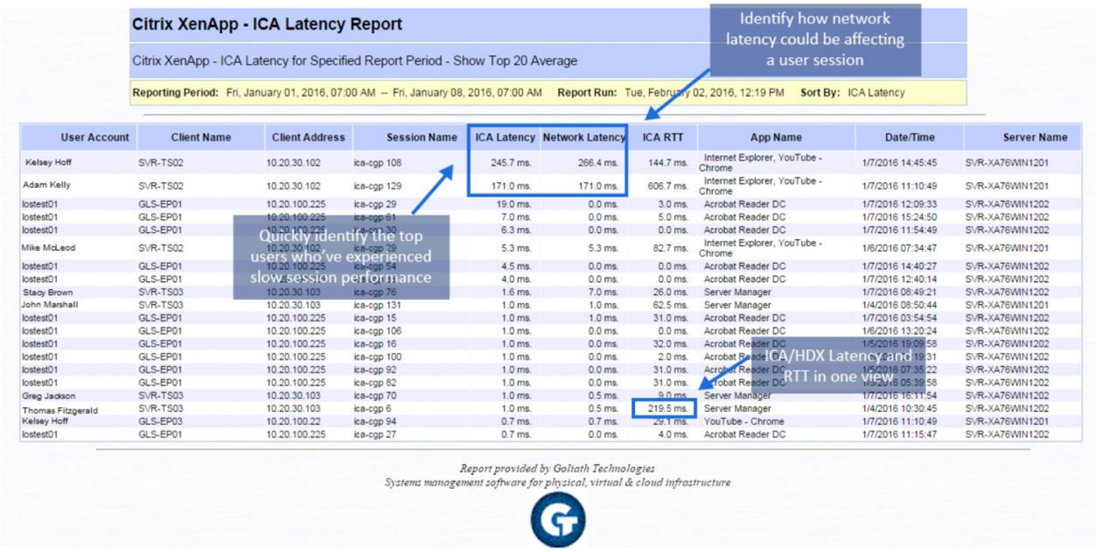
ICA/HDX Channel Metrics (bps)

Metric	Avg	Max	Max Time
Output Session Bandwidth	110,030	872,608	5/27 14:23
Input Session Bandwidth	74,125	92,008	5/27 11:03
Output Session Compression	87	101	5/27 10:37
Input Session Compression	99	102	5/27 13:02
Output Session Line Speed	48,349,628	128,249,144	5/27 14:51
Input Session Line Speed	6,120,896	6,120,896	[illegible]
Output Clipboard Bandwidth	121	121	[illegible]
Input Clipboard Bandwidth	1,126	2,141	[illegible]
Output ThinWire Bandwidth	106,784	876,975	5/27 14:23
Output Audio Bandwidth	44,404	102,898	5/27 12:59

Citrix Supporting Infrastructure and Component Monitoring and Alerting - It goes without saying the underlying components of a XenApp/XenDesktop environment such as the session hosts, StoreFront/Web, ZDCs/Delivery Controllers and PVS are critical to the entire end user experience picture. Having visibility into these components is a basic requirement for any XenApp/XenDesktop monitoring solution. Monitoring the Infrastructure System resource utilization on any of the Citrix infrastructure components is critical because high usage can result in delayed logons or user experience issues such as high ICA latency and round-trip time (RTT).


VMware Virtual Machine Metrics
Name: DEV.SVR-XA76WIN1202
IPAddr: 10.20.60.101
Desc: Using Master Agent at 10.20.150.50; XenApp Version 7.6.0.5026
OS Ver: Microsoft Windows Server 2012 R2 Standard, 6.3.9600
Group: HSA - Dev Published Apps
Domain: GOLIATH
Notes: Running on Host: VS-ESXi04.corp.goliathtechnologies.com AgentVersion: 7.6.0.5026 AllocationType: Random ApplicationsInUse
CPU, Memory & Disk Use
Disk Performance
Disk Space Use
Network Performance
Agent Up/Down
% CPU Use
% Memory Use
% Disk Space Use
CPU Trend: % Used and % Ready
Memory Trends: GBs
CPU Trend: Context Switches/sec
CPU Trend: Processor Queue Length
Memory Trend: Pages/sec
View the VMware host the VM is running on
Quickly view metrics with tabbed display
Track real-time and trending CPU, memory and disk utilization
Gain insight into CPU activity

4. **Historical Reporting and Analysis -** Having the ability to view the environment in real-time is important, but having data available historically is equally important for several use cases including root cause analysis, performance trending over time and validating SLAs. Having a complete and robust reporting engine is central to being able to parse and use historical data effectively for any need.



Citrix XenApp - ICA Latency Report

Citrix XenApp - ICA Latency for Specified Report Period - Show Top 20 Average

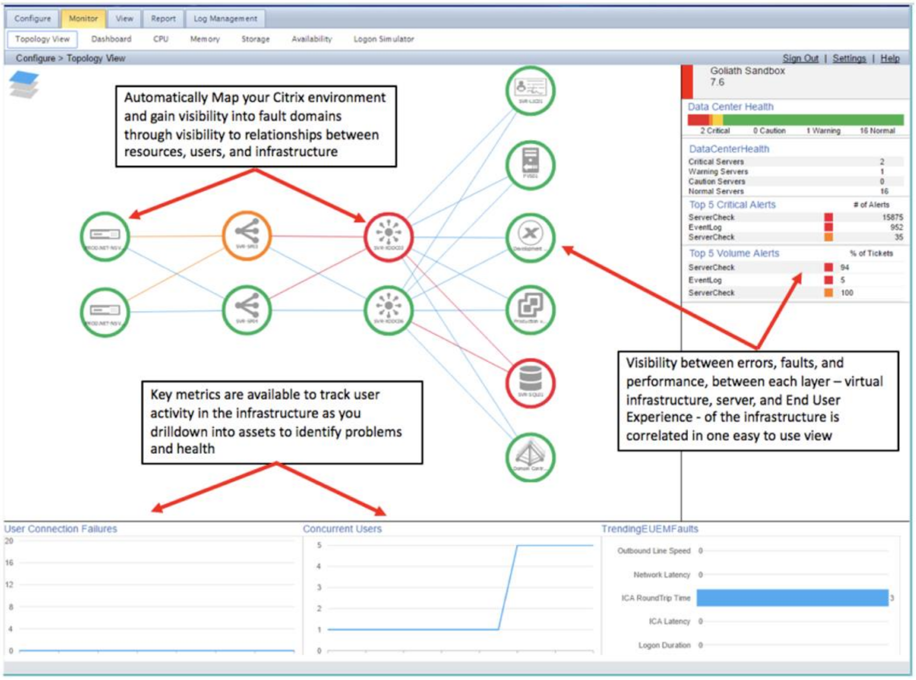
Reporting Period: Fri, January 01, 2016, 07:00 AM -- Fri, January 08, 2016, 07:00 AM **Report Run:** Tue, February 02, 2016, 12:19 PM **Sort By:** ICA Latency

User Account	Client Name	Client Address	Session Name	ICA Latency	Network Latency	ICA RTT	App Name	Date/Time	Server Name
Kelsey Hoff	SVR-TS02	10.20.30.102	ica-cgp 108	245.7 ms.	266.4 ms.	144.7 ms.	Internet Explorer, YouTube - Chrome	1/7/2016 14:45:45	SVR-XA76WIN1201
Adam Kelly	SVR-TS02	10.20.30.102	ica-cgp 129	171.0 ms.	171.0 ms.	606.7 ms.	Internet Explorer, YouTube - Chrome	1/7/2016 11:10:49	SVR-XA76WIN1201
lostest01	GLS-EP01	10.20.100.225	ica-cgp 29	19.0 ms.	0.0 ms.	3.0 ms.	Acrobat Reader DC	1/7/2016 12:09:33	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 61	7.0 ms.	0.0 ms.	5.0 ms.	Acrobat Reader DC	1/7/2016 15:24:50	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 30	6.3 ms.	0.0 ms.	0.0 ms.	Acrobat Reader DC	1/7/2016 11:54:49	SVR-XA76WIN1202
Mike McLeod	SVR-TS02	10.20.30.102	ica-cgp 29	5.3 ms.	5.3 ms.	82.7 ms.	Internet Explorer, YouTube - Chrome	1/6/2016 07:34:47	SVR-XA76WIN1201
lostest01	GLS-EP01	10.20.100.225	ica-cgp 54	4.5 ms.	0.0 ms.	0.0 ms.	Acrobat Reader DC	1/7/2016 14:40:27	SVR-XA76WIN1202
lostest01	GLS-EP01	[illegible]	[illegible]	4.0 ms.	0.0 ms.	0.0 ms.	Acrobat Reader DC	1/7/2016 12:40:14	SVR-XA76WIN1202
Stacy Brown	SVR-TS03	10.20.30.103	ica-cgp 76	1.6 ms.	7.0 ms.	26.0 ms.	Server Manager	1/7/2016 08:49:21	SVR-XA76WIN1202
John Marshall	SVR-TS03	10.20.30.103	ica-cgp 131	1.0 ms.	1.0 ms.	62.5 ms.	Server Manager	1/4/2016 08:50:44	SVR-XA76WIN1201
lostest01	GLS-EP01	10.20.100.225	ica-cgp 15	1.0 ms.	1.0 ms.	31.0 ms.	Acrobat Reader DC	1/7/2016 03:54:54	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 106	1.0 ms.	0.0 ms.	0.0 ms.	Acrobat Reader DC	1/6/2016 13:20:24	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 16	1.0 ms.	0.0 ms.	32.0 ms.	Acrobat Reader DC	1/5/2016 19:09:58	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 100	1.0 ms.	0.0 ms.	2.0 ms.	Acrobat Reader DC	[illegible]	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 92	1.0 ms.	0.0 ms.	31.0 ms.	Acrobat Reader DC	1/5/2016 07:35:22	SVR-XA76WIN1202
lostest01	GLS-EP01	10.20.100.225	ica-cgp 82	1.0 ms.	0.0 ms.	31.0 ms.	Acrobat Reader DC	1/5/2016 05:39:58	SVR-XA76WIN1202
Greg Jackson	SVR-TS03	10.20.30.103	ica-cgp 70	1.0 ms.	0.5 ms.	9.0 ms.	Server Manager	1/7/2016 16:11:54	SVR-XA76WIN1202
Thomas Fitzgerald	SVR-TS03	10.20.30.103	ica-cgp 6	1.0 ms.	0.5 ms.	219.5 ms.	Server Manager	1/4/2016 10:30:45	SVR-XA76WIN1202
Kelsey Hoff	GLS-EP03	10.20.100.22	ica-cgp 94	0.7 ms.	0.7 ms.	29.1 ms.	YouTube - Chrome	1/7/2016 11:10:49	SVR-XA76WIN1201
lostest01	GLS-EP01	10.20.100.225	ica-cgp 27	0.7 ms.	0.0 ms.	4.0 ms.	Acrobat Reader DC	1/7/2016 11:15:47	SVR-XA76WIN1202

Report provided by Goliath Technologies
Systems management software for physical, virtual & cloud infrastructure

Identify how network latency could be affecting a user session
Quickly identify the top users who've experienced slow session performance
ICA/HDX Latency and RTT in one view

5. **Enterprise Dashboards with Troubleshooting Drilldown –** Dashboards and high-level views are valuable ways to quickly identify potential issues and to trend performance over time. From a historical perspective, dashboards provide an executive summary view that delivers health and trending information over time. Real-time dashboards as depicted below allow administrators to quickly address and track problem areas in the environment.



Automatically Map your Citrix environment and gain visibility into fault domains through visibility to relationships between resources, users, and infrastructure

Key metrics are available to track user activity in the infrastructure as you drilldown into assets to identify problems and health

Visibility between errors, faults, and performance, between each layer – virtual infrastructure, server, and End User Experience - of the infrastructure is correlated in one easy to use view

DataCenterHealth	
Critical Servers	2
Warning Servers	1
Caution Servers	0
Normal Servers	16

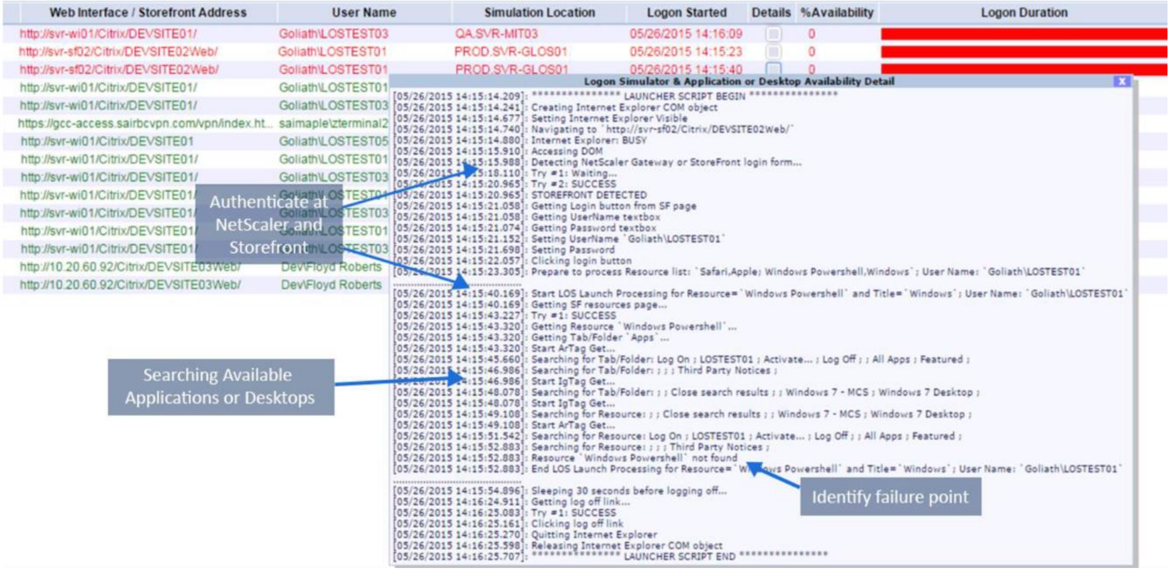
Top 5 Critical Alerts	# of Alerts
ServerCheck	15875
EventLog	952
ServerCheck	35

Top 5 Volume Alerts	% of Tickets
ServerCheck	94
EventLog	5
ServerCheck	100

Going Beyond EdgeSight

The five areas highlighted above are the primary components that an EdgeSight replacement should have for feature parity. However, having a truly comprehensive monitoring and troubleshooting solution for Citrix XenApp/XenDesktop is critical and even more emphasized during a migration. As a result, the ultimate goal should be to go beyond what EdgeSight offers. Below are some of the key components to ensure the highest quality user experience as well as a successful migration.

1. **Preemptive Application Availability Testing** – While EdgeSight did have some synthetic transaction capabilities it was not designed to be a true advanced warning system for logon. The Goliath Application Availability Monitor is a technology that allows administrators to test availability and logon/launch performance using a real ICA session, generated by a real test user. The logon simulation technology acts as a real user would sitting at a desk logging into the environment, launching applications and validating its success.



Web Interface / Storefront Address	User Name	Simulation Location	Logon Started	Details	%Availability	Logon Duration
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST03	QA.SVR-MIT03	05/26/2015 14:16:09	□	0	🟥
http://svr-sf02/Citrix/DEVSITE02Web/	Goliath\LOSTEST01	PROD.SVR-GLOS01	05/26/2015 14:15:23	□	0	🟥
http://svr-sf02/Citrix/DEVSITE02Web/	Goliath\LOSTEST01	PROD.SVR-GLOS01	05/26/2015 14:15:40	□	0	🟥
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST01					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST03					
https://gcc-access.sairbcvpn.com/vpn/index.ht...	saimaple\zterminal2					
http://svr-wi01/Citrix/DEVSITE01	Goliath\LOSTEST05					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST01					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST03					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST01					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST03					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST01					
http://svr-wi01/Citrix/DEVSITE01/	Goliath\LOSTEST03					
http://10.20.60.92/Citrix/DEVSITE03Web/	Dev\Floyd Roberts					
http://10.20.60.92/Citrix/DEVSITE03Web/	Dev\Floyd Roberts					

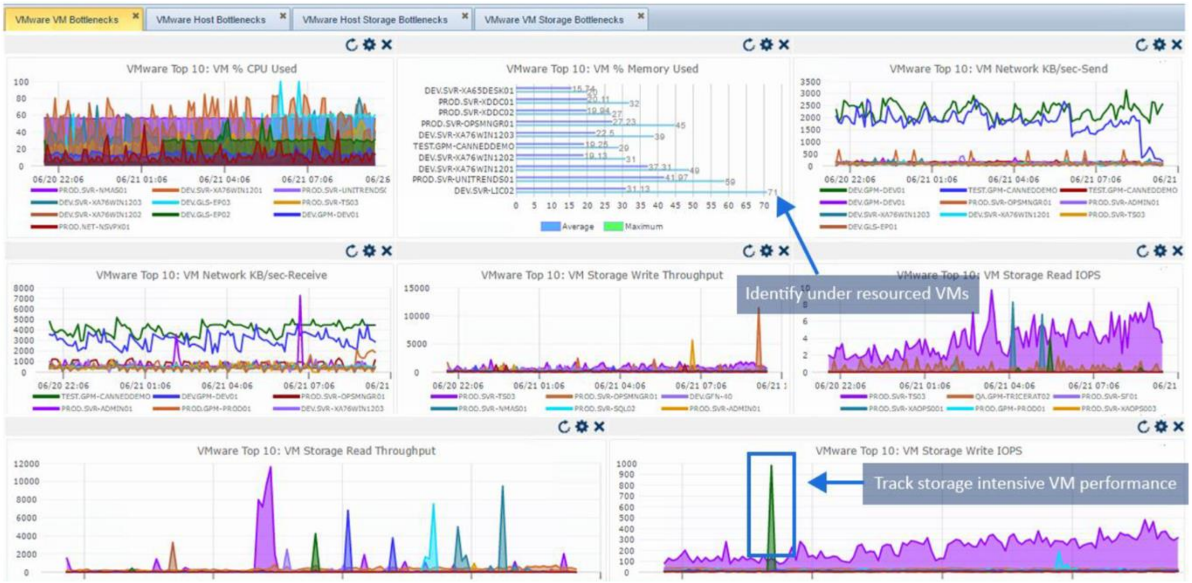
Logon Simulator & Application or Desktop Availability Detail

```
[05/26/2015 14:15:14.209]: *************** LAUNCHER SCRIPT BEGIN ***************
[05/26/2015 14:15:14.241]: Creating Internet Explorer COM object
[05/26/2015 14:15:14.677]: Setting Internet Explorer Visible
[05/26/2015 14:15:14.740]: Navigating to `http://svr-sf02/Citrix/DEVSITE02Web/`
[05/26/2015 14:15:14.880]: Internet Explorer: BUSY
[05/26/2015 14:15:15.910]: Accessing DOM
[05/26/2015 14:15:15.988]: Detecting NetScaler Gateway or StoreFront login form...
[05/26/2015 14:15:18.110]: Try #1: Waiting...
[05/26/2015 14:15:20.965]: Try #2: SUCCESS
[05/26/2015 14:15:20.965]: STOREFRONT DETECTED
[05/26/2015 14:15:21.058]: Getting Login button from SF page
[05/26/2015 14:15:21.058]: Getting UserName textbox
[05/26/2015 14:15:21.074]: Getting Password textbox
[05/26/2015 14:15:21.152]: Setting UserName `Goliath\LOSTEST01`
[05/26/2015 14:15:21.698]: Setting Password
[05/26/2015 14:15:22.057]: Clicking login button
[05/26/2015 14:15:23.305]: Prepare to process Resource list: `Safari,Apple; Windows Powershell,Windows` ; User Name: `Goliath\LOSTEST01`
..........................................
[05/26/2015 14:15:40.169]: Start LOS Launch Processing for Resource=`Windows Powershell` and Title=`Windows` ; User Name: `Goliath\LOSTEST01`
[05/26/2015 14:15:40.169]: Getting SF resources page...
[05/26/2015 14:15:43.227]: Try #1: SUCCESS
[05/26/2015 14:15:43.320]: Getting Resource `Windows Powershell` ...
[05/26/2015 14:15:43.320]: Getting Tab/Folder `Apps` ...
[05/26/2015 14:15:43.320]: Start ArTag Get...
[05/26/2015 14:15:45.660]: Searching for Tab/Folder: Log On ; LOSTEST01 ; Activate... ; Log Off ; ; All Apps ; Featured ;
[05/26/2015 14:15:46.986]: Searching for Tab/Folder: ; ; ; Third Party Notices ;
[05/26/2015 14:15:46.986]: Start IgTag Get...
[05/26/2015 14:15:48.078]: Searching for Tab/Folder: ; ; Close search results ; ; Windows 7 - MCS ; Windows 7 Desktop ;
[05/26/2015 14:15:48.078]: Start IgTag Get...
[05/26/2015 14:15:49.108]: Searching for Resource: ; ; Close search results ; ; Windows 7 - MCS ; Windows 7 Desktop ;
[05/26/2015 14:15:49.108]: Start ArTag Get...
[05/26/2015 14:15:51.542]: Searching for Resource: Log On ; LOSTEST01 ; Activate... ; Log Off ; ; All Apps ; Featured ;
[05/26/2015 14:15:52.883]: Searching for Resource: ; ; ; Third Party Notices ;
[05/26/2015 14:15:52.883]: Resource `Windows Powershell` not found
[05/26/2015 14:15:52.883]: End LOS Launch Processing for Resource=`Windows Powershell` and Title=`Windows` ; User Name: `Goliath\LOSTEST01`
..........................................
[05/26/2015 14:15:54.896]: Sleeping 30 seconds before logging off...
[05/26/2015 14:16:24.911]: Getting log off link...
[05/26/2015 14:16:25.083]: Try #1: SUCCESS
[05/26/2015 14:16:25.161]: Clicking log off link
[05/26/2015 14:16:25.270]: Quitting Internet Explorer
[05/26/2015 14:16:25.598]: Releasing Internet Explorer COM object
[05/26/2015 14:16:25.707]: *************** LAUNCHER SCRIPT END ***************
```

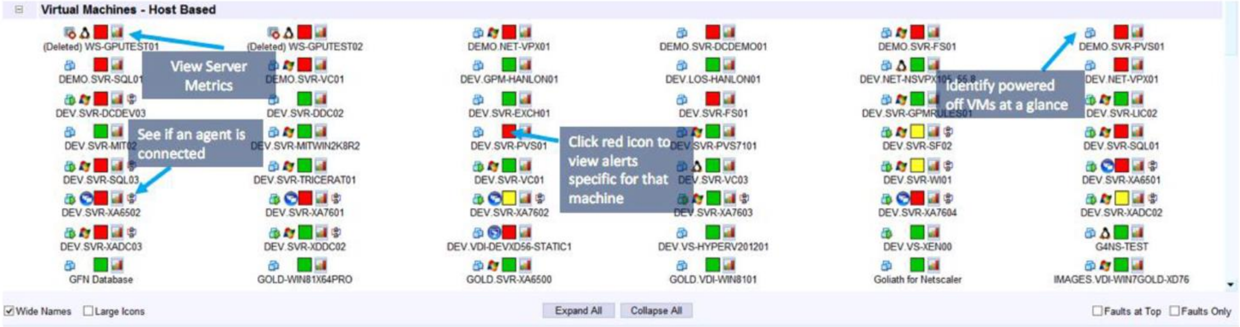
X
Authenticate at NetScaler and Storefront
Searching Available Applications or Desktops
Identify failure point

The Application Availability Monitor not only identifies if a logon is successful or not, it can also provide information on the duration of logons as well. Beyond that, it is able to identify where in the process logon failures occur by performing validation checks at each stage of the logon. This allows the logon simulator provide advanced warning to logon issues before real users are impacted.

2. **Hypervisor Monitoring and Alerting –** Obviously when monitoring a Citrix solution, having visibility into the Citrix infrastructure is a must-have. However, there are so many more components outside of Citrix that can result in a user ultimately having a poor experience. One of those is the underlying Hypervisor host servers and storage. Having visibility into these components is critical to ensuring that all issues no matter how low level are identified. Additionally, when planning a migration these levels are critical to having visibility into for the purpose of baselining and planning for the resources that will be needed for the new environment.



3. **Windows/Linux Application and Infrastructure Servers –** As previously stated, a large variety of Citrix issues do not stem from Citrix at all. Outside of underlying issues with the supporting infrastructure, service-related issues around DNS, DHCP, Active Directory etc. and application related issues with apps such as MS SQL, Exchange, and SharePoint can be the root cause of many problems as well. Having a tool that can also provide insight into other applications and the hosting servers will also ease the burden of ensuring that users are able to work efficiently.



View Server Metrics

See if an agent is connected

Click red icon to view alerts specific for that machine

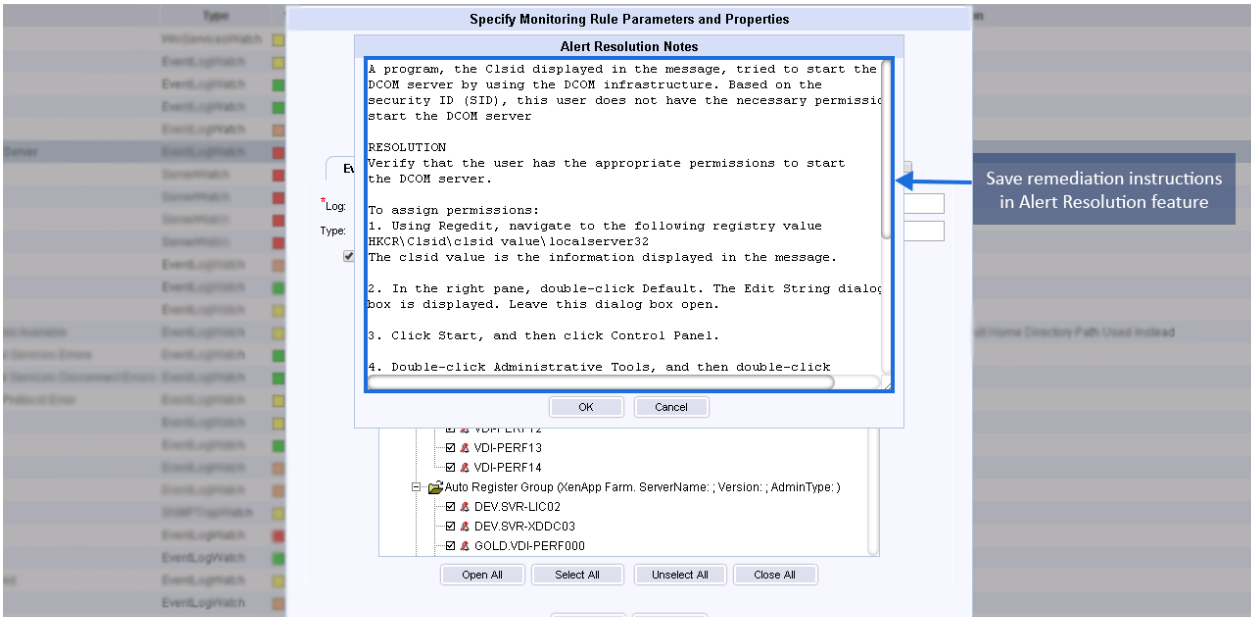
Identify powered off VMs at a glance

4. **Intelligent Alerting –** Being proactive is a critical component to ensuring a quality end user experience, and alerts are the foundation to that. All aspects of the delivery infrastructure should be able to be monitored for both up/down and thresholds where applicable. Alerts need to be flexible and cover all of the following aspects of the delivery infrastructure.

   a. ICA User Experience Monitoring
   b. Hypervisor Resource Monitoring
   c. Data store Resource Monitoring
   d. Windows Event Logs
   e. Syslog
   f. Performance Counters
   g. Process Thresholds and Availability
   h. Windows and Linux Services
   i. File Watch
   j. SNMP Traps

5. **Alert Resolution** – This feature allows an organization to reduce support costs and gain consistency and speed in resolving alerts when they arise. This feature allows senior engineers to put instructions and even executables in the product so when an alert is triggered, the help desk personnel or lower support technicians can resolve the issue. This is a significant help in transferring knowledge between engineers and techs. Alert Resolution Notes allow for knowledge transfer to be recorded easily, and allows the individual addressing the issue to have information available right at their fingertips with the alert itself. Alert resolution notes integrate a knowledge base with the monitoring technology, eliminating the need to perform unneeded research, and prevents having to "hunt" down someone with the requisite knowledge.

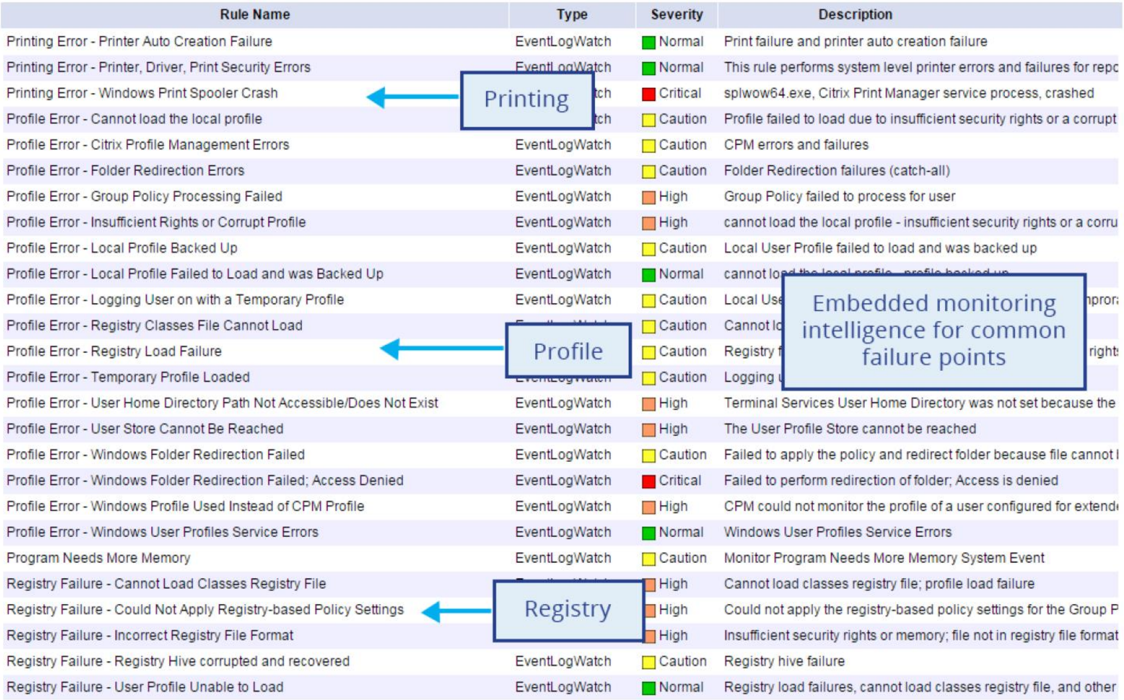
Product Screenshot: Alert Resolution Feature



```
A program, the Clsid displayed in the message, tried to start the
DCOM server by using the DCOM infrastructure. Based on the
security ID (SID), this user does not have the necessary permissio
start the DCOM server

RESOLUTION
Verify that the user has the appropriate permissions to start
the DCOM server.

To assign permissions:
1. Using Regedit, navigate to the following registry value
HKCR\Clsid\clsid value\localserver32
The clsid value is the information displayed in the message.

2. In the right pane, double-click Default. The Edit String dialog
box is displayed. Leave this dialog box open.

3. Click Start, and then click Control Panel.

4. Double-click Administrative Tools, and then double-click
```

Save remediation instructions in Alert Resolution feature

The EdgeSight Replacement solution should also be able to monitor the Citrix XenApp/XenDesktop deployment immediately out-of-the-box as depicted below with pre-built rules specific for monitoring delivery components and their dependencies.



Rule Name	Type	Severity	Description
Printing Error - Printer Auto Creation Failure	EventLogWatch	🟩 Normal	Print failure and printer auto creation failure
Printing Error - Printer, Driver, Print Security Errors	EventLogWatch	🟩 Normal	This rule performs system level printer errors and failures for repc
Printing Error - Windows Print Spooler Crash	tch	🟥 Critical	splwow64.exe, Citrix Print Manager service process, crashed
Profile Error - Cannot load the local profile	tch	🟨 Caution	Profile failed to load due to insufficient security rights or a corrupt
Profile Error - Citrix Profile Management Errors	EventLogWatch	🟨 Caution	CPM errors and failures
Profile Error - Folder Redirection Errors	EventLogWatch	🟨 Caution	Folder Redirection failures (catch-all)
Profile Error - Group Policy Processing Failed	EventLogWatch	🟧 High	Group Policy failed to process for user
Profile Error - Insufficient Rights or Corrupt Profile	EventLogWatch	🟧 High	cannot load the local profile - insufficient security rights or a corru
Profile Error - Local Profile Backed Up	EventLogWatch	🟨 Caution	Local User Profile failed to load and was backed up
Profile Error - Local Profile Failed to Load and was Backed Up	EventLogWatch	🟩 Normal	cannot load the local profile - profile backed up
Profile Error - Logging User on with a Temporary Profile	EventLogWatch	🟨 Caution	Local Use npror
Profile Error - Registry Classes File Cannot Load		🟨 Caution	Cannot lo
Profile Error - Registry Load Failure		🟨 Caution	Registry f rights
Profile Error - Temporary Profile Loaded		🟨 Caution	Logging u
Profile Error - User Home Directory Path Not Accessible/Does Not Exist	EventLogWatch	🟧 High	Terminal Services User Home Directory was not set because the
Profile Error - User Store Cannot Be Reached	EventLogWatch	🟧 High	The User Profile Store cannot be reached
Profile Error - Windows Folder Redirection Failed	EventLogWatch	🟨 Caution	Failed to apply the policy and redirect folder because file cannot l
Profile Error - Windows Folder Redirection Failed; Access Denied	EventLogWatch	🟥 Critical	Failed to perform redirection of folder; Access is denied
Profile Error - Windows Profile Used Instead of CPM Profile	EventLogWatch	🟧 High	CPM could not monitor the profile of a user configured for extend
Profile Error - Windows User Profiles Service Errors	EventLogWatch	🟩 Normal	Windows User Profiles Service Errors
Program Needs More Memory	EventLogWatch	🟨 Caution	Monitor Program Needs More Memory System Event
Registry Failure - Cannot Load Classes Registry File		🟧 High	Cannot load classes registry file; profile load failure
Registry Failure - Could Not Apply Registry-based Policy Settings		🟧 High	Could not apply the registry-based policy settings for the Group P
Registry Failure - Incorrect Registry File Format		🟧 High	Insufficient security rights or memory; file not in registry file format
Registry Failure - Registry Hive corrupted and recovered	EventLogWatch	🟨 Caution	Registry hive failure
Registry Failure - User Profile Unable to Load	EventLogWatch	🟩 Normal	Registry load failures, cannot load classes registry file, and other

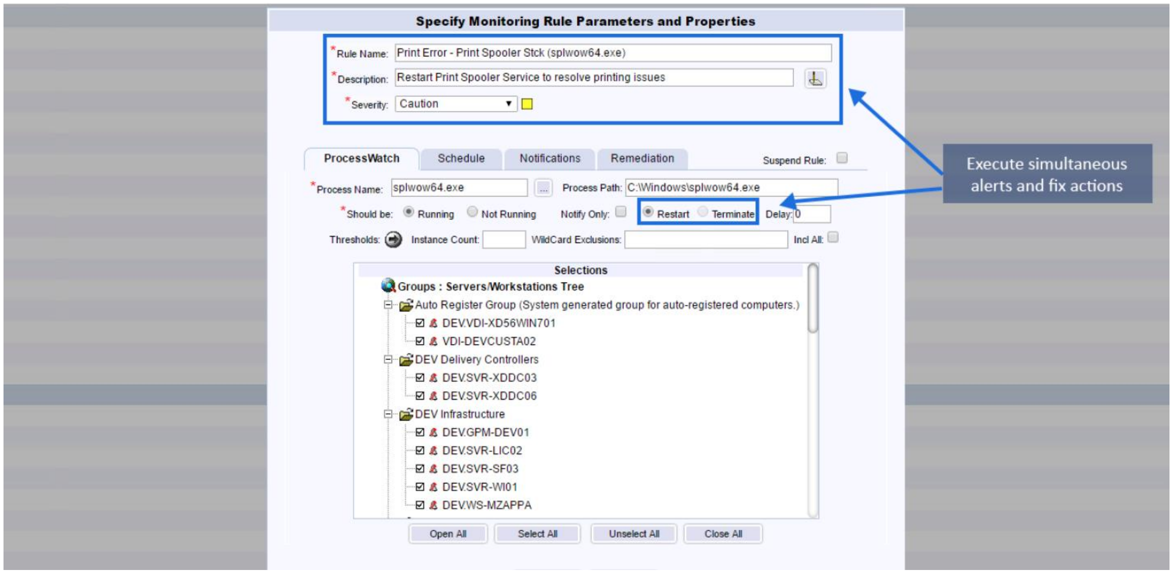
Printing

Profile

Registry

Embedded monitoring intelligence for common failure points

Beyond the simple ability to notify admins when a threshold has been breached or when a component is down, a sophisticated solution should also be able to take action where applicable and perform remediation actions to resolve issues on an automated basis as depicted below.



Specify Monitoring Rule Parameters and Properties

*Rule Name: Print Error - Print Spooler Stck (splwow64.exe)

*Description: Restart Print Spooler Service to resolve printing issues

*Severity: Caution ▾ 🟨

Suspend Rule: □

*Process Name: splwow64.exe

Process Path: C:\Windows\splwow64.exe

*Should be: ● Running ○ Not Running Notify Only: □ ● Restart ○ Terminate Delay: 0

Thresholds: Instance Count: WildCard Exclusions: Incl All: □

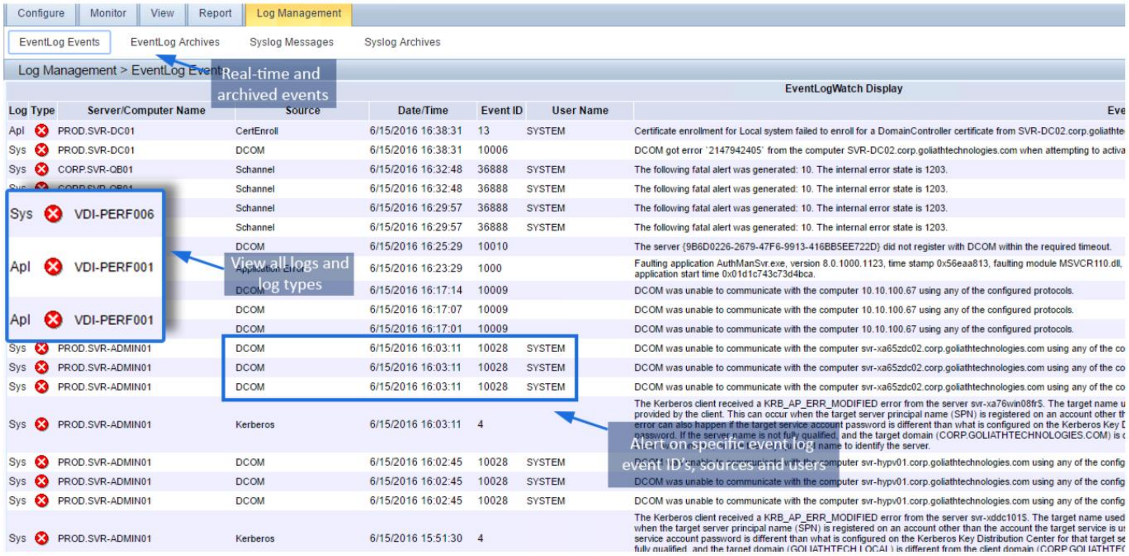
Selections

Groups : Servers/Workstations Tree

- Auto Register Group (System generated group for auto-registered computers.)
  - ☑ DEV.VDI-XD56WIN701
  - ☑ VDI-DEVCUSTA02
- DEV Delivery Controllers
  - ☑ DEV.SVR-XDDC03
  - ☑ DEV.SVR-XDDC06
- DEV Infrastructure
  - ☑ DEV.GPM-DEV01
  - ☑ DEV.SVR-LIC02
  - ☑ DEV.SVR-SF03
  - ☑ DEV.SVR-WI01
  - ☑ DEV.WS-MZAPPA

Execute simultaneous alerts and fix actions

6. **Event Log Management –** The final component for achieving a truly comprehensive tool for Citrix XenApp/XenDesktop is event log management. In the end, all root cause analysis ends with the event logs. The event log is the diary of a system and is a treasure trove of information that more often than not, leads to the root cause of most issues. However, with complex delivery infrastructure such as Citrix XenApp and XenDesktops there are many components that work together to deliver user experience. As a result reviewing the logs of an individual server may prove useless, but having a tool to aggregate and parse the logs from many sources, at many points in time is powerful. An effective event log tool will provide the capability to archive logs for historical analysis, alert on logs for proactive response and to parse current logs for root cause discovery.



Real-time and archived events

View all logs and log types

Alert on specific event log event ID's, sources and users

EventLogWatch Display

Log Type		Server/Computer Name	Source	Date/Time	Event ID	User Name	Eve
Apl	⊗	PROD.SVR-DC01	CertEnroll	6/15/2016 16:38:31	13	SYSTEM	Certificate enrollment for Local system failed to enroll for a DomainController certificate from SVR-DC02.corp.goliathte
Sys	⊗	PROD.SVR-DC01	DCOM	6/15/2016 16:38:31	10006		DCOM got error '2147942405' from the computer SVR-DC02.corp.goliathtechnologies.com when attempting to activa
Sys	⊗	CORP.SVR-QB01	Schannel	6/15/2016 16:32:48	36888	SYSTEM	The following fatal alert was generated: 10. The internal error state is 1203.
Sys	⊗	CORP.SVR-QB01	Schannel	6/15/2016 16:32:48	36888	SYSTEM	The following fatal alert was generated: 10. The internal error state is 1203.
			Schannel	6/15/2016 16:29:57	36888	SYSTEM	The following fatal alert was generated: 10. The internal error state is 1203.
			Schannel	6/15/2016 16:29:57	36888	SYSTEM	The following fatal alert was generated: 10. The internal error state is 1203.
			DCOM	6/15/2016 16:25:29	10010		The server {9B6D0226-2679-47F6-9913-416BB5EE722D} did not register with DCOM within the required timeout.
			Application Error	6/15/2016 16:23:29	1000		Faulting application AuthManSvr.exe, version 8.0.1000.1123, time stamp 0x56eaa813, faulting module MSVCR110.dll, application start time 0x01d1c743c73d4bca.
			DCOM	6/15/2016 16:17:14	10009		DCOM was unable to communicate with the computer 10.10.100.67 using any of the configured protocols.
			DCOM	6/15/2016 16:17:07	10009		DCOM was unable to communicate with the computer 10.10.100.67 using any of the configured protocols.
			DCOM	6/15/2016 16:17:01	10009		DCOM was unable to communicate with the computer 10.10.100.67 using any of the configured protocols.
Sys	⊗	PROD.SVR-ADMIN01	DCOM	6/15/2016 16:03:11	10028	SYSTEM	DCOM was unable to communicate with the computer svr-xa65zdc02.corp.goliathtechnologies.com using any of the co
Sys	⊗	PROD.SVR-ADMIN01	DCOM	6/15/2016 16:03:11	10028	SYSTEM	DCOM was unable to communicate with the computer svr-xa65zdc02.corp.goliathtechnologies.com using any of the co
Sys	⊗	PROD.SVR-ADMIN01	DCOM	6/15/2016 16:03:11	10028	SYSTEM	DCOM was unable to communicate with the computer svr-xa65zdc02.corp.goliathtechnologies.com using any of the co
Sys	⊗	PROD.SVR-ADMIN01	Kerberos	6/15/2016 16:03:11	4		The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server svr-xa76win08fr$. The target name u provided by the client. This can occur when the target server principal name (SPN) is registered on an account other th error can also happen if the target service account password is different than what is configured on the Kerberos Key D password. If the server name is not fully qualified, and the target domain (CORP.GOLIATHTECHNOLOGIES.COM) is d [illegible] name to identify the server.
Sys	⊗	PROD.SVR-ADMIN01	DCOM	6/15/2016 16:02:45	10028	SYSTEM	DCOM was unable to communicate with the computer svr-hypv01.corp.goliathtechnologies.com using any of the config
Sys	⊗	PROD.SVR-ADMIN01	DCOM	6/15/2016 16:02:45	10028	SYSTEM	DCOM was unable to communicate with the computer svr-hypv01.corp.goliathtechnologies.com using any of the config
Sys	⊗	PROD.SVR-ADMIN01	DCOM	6/15/2016 16:02:45	10028	SYSTEM	DCOM was unable to communicate with the computer svr-hypv01.corp.goliathtechnologies.com using any of the config
Sys	⊗	PROD.SVR-ADMIN01	Kerberos	6/15/2016 15:51:30	4		The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server svr-xddc101$. The target name used when the target server principal name (SPN) is registered on an account other than the account the target service is us service account password is different than what is configured on the Kerberos Key Distribution Center for that target se fully qualified, and the target domain (GOLIATHTECH.LOCAL) is different from the client domain (CORP.GOLIATHTEC

In summary, visibility is key. XenApp and XenDesktop are both complex multi-layered technologies that require both deep and wide insight into the ICA/HDX protocol and the underlying infrastructure. Citrix EdgeSight, while not perfect, satisfied the most basic requirements of administrators for years. However, with the end of EdgeSight support and the introduction of less capable tools for monitoring XenApp/XenDesktop 7.x, there is a true need to find a new solution. Goliath Performance Monitor delivers a solution that surpasses the depth of logon and session insight and adds further dimension with visibility into support infrastructure components and enhanced capabilities such as logon simulation, intelligent alerts and event log management.

The process of executing a migration also further emphasizes the need for a more complete solution. While EdgeSight can monitor XenApp 6.5, it cannot monitor 7.x. This is problematic for managing the migration as two different solutions with different capabilities will be needed. Additionally, it cannot baseline the entire infrastructure from the bottom up, also introducing difficulty with understanding the requirements for ensuring success. To guarantee the greatest level of success, the monitoring solution should be able to provide the ability to baseline your existing environment, identify root cause of existing issues, test access and availability of the new environment before migrating production users, and provide insight and management into the migration as it occurs.

Conclusion

A successful migration from XenApp 6.5 to 7.x brings complexity and many challenges with it. However, it also brings opportunity to improve the health, resiliency and overall performance of your application and desktop delivery infrastructure.

It is all about visibility at the end of the day. In an environment as complex as a Citrix delivery infrastructure, “good visibility” is the difference between success and failure. All aspects of the process from the initial baselining through to facilitating the migration requires a comprehensive and capable monitoring platform. Many of 6.5 environments today use Citrix EdgeSight and will be forced to deploy a new monitoring platform when they move to 7.x. This fact alone creates the need to replace EdgeSight as early in the process as possible. Not only is having complete visibility into every aspect of the infrastructure key, but consistency is equally important. A solution that supports both 6.5 and 7.x equally will provide the stability and consistency to ensure that every part for the process, including data collection, troubleshooting, issue resolution, monitoring, testing, QA and migration is successful. The right EdgeSight replacement is the engine for planning, testing, anticipating, troubleshooting, resolving and ultimately preventing user experience issues.

Good luck and let us know if this was helpful by emailing to support@goliathtechnologies.com. We are the team that collaborates on these documents in between answering your technical product questions.