The magazine for professional system and network administrators

On test:

2X VirtualDesktopServer 9

Virtual desktops to spec

On test: 2X VirtualDesktopServer 9

Virtual desktops to spec

by Jürgen Heyer

The provision of individual applications or even entire workstations over a network via a virtual desktop infrastructure has long ceased to be the stuff of fantasy. However instead of simply offering one way of publishing applications, the 2X VirtualDesktopServer is at your disposal with an impressive range of features: Support for the terminal servers of Microsoft, Citrix, VDI and Public Desktops on a wide range of client platforms offers plenty of room for manoeuvre in setting up a customized configuration. IT-Administrator has placed the various variants under the microscope in a detailed test.

Many providers of virtualization solutions select only one of the leading hypervisors. By contrast 2X, as the developer of software for thin clients and server based computing, offers in a single product, i.e. its VirtualDesktopServer (VDS), multiple possibilities for providing applications and complete desktops on end-user terminals. It is not for nothing that 2X is promoting its application server, which is contained within VDS, but is also available as a stand-alone product, as the first alternative to Citrix. In combination with Windows Terminal Server and Citrix itself, the administrator has available comprehensive options for publishing individual applications and desktops.

The 2X flagship VDS also supports practically all current hypervisors, so that alongside terminal services, virtual desktops (VDI) can also be provided. Also very broadly configured is the client support with an impressive number of agents for different operating systems. If you need, for example, to publish Windows desktops on a Linux system or if you want remote access via your iPhone, then it's possible with 2X VDS.

At the start of the test, the highly advanced public beta of version 9 was available to us. Shortly before the end of the test, we were able to have a look at the officially released version. Ultimately, the aim of VDS is to provide different users with precisely the scope of applications or entire desktop environments on precisely the required platform, tailored and dimensioned to provide the required performance. Since VDS combines miscellaneous functionalities in one product, the administrator needs only operate one console. In addition, on the user side only

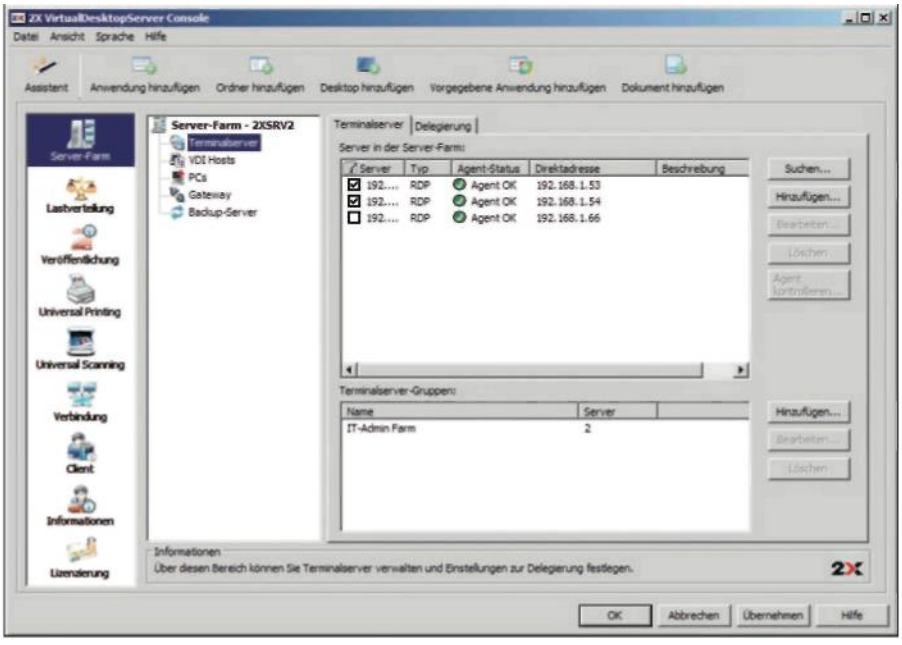

Figure 1: The VDS area is very clearly presented, showing where the servers belonging to the server farm are registered

regardless of which way the provision is made. This makes the solution very maintenance-friendly.

Publishing server redundancy

When setting up VDS, it should be noted that under Windows Server 2008 R2 this must take place while logged in as a local administrator. When we initially tried as a domain administrator, we were confronted by a program abort message, which unfortunately didn't provide enough information to determine the cause of the problem. In this respect, the manual states only general administrator

rights are required, and it was only after a call to technical support that we were able to progress. If you are installing under Windows Server 2003, you will not come up against this problem.

The server on which VDS is first installed, functions by default as the master publishing server (broker). This means that all client requests are first sent to this server, which then forwards them to the actual system, via which the desired application or desktop will be made available. However, this also means that upon failure of the publishing server the entire deployment would fail. To create redundancy here, one or more backup servers can be defined, which then take over the distribution. If the master publishing server fails permanently, then a backup server can always be upgraded to master status.

So that in normal mode the backup server does not just sit around idly waiting for the master to fail, it can also be used as a so-called secure client gateway. Its purpose is then, especially in environments with heightened security requirement and in networks segmented by firewalls, to tunnel the entire data traffic through one port (by default port 80) and, if required, additionally to encrypt it using SSL. By default SSL2 and SSL3 are supported, however a limitation to SSL3 is possible. The gateway access can additionally be filtered using MAC addresses, in which case the administrator must either maintain an exclusion list (all addresses except ...) or an inclusion list (only addresses ...).

Just one click to return to the default settings

Highly advantageous where the implementation of individual security requirements is concerned, is the possibility that all ports used for RDP, Citrix, the use of secure client gateways, the use of SSL/TLS and communication with agents can be modified. Also welcome is the feature which allows the administrator to return to the default configuration, wherever the the ports can be modified, simply by clicking the provided button - so if a system misconfiguration has occurred, returning to the default state is no problem.

The 2X publishing agent must be installed on all systems, on which VDS is to be used for the provision of applications or desktops. This can take place via a setup, or likewise remotely using the VDS console described in more detail below. This also allows the already installed agents to be checked for accessibility and function and, if necessary, deinstalled or updated to a later version.

One strength of VDS is the load sharing, optionally with a round robin approach or resource-based. Especially which using many different applications, it is generally more efficient to use a resource-based approach in which VDS uses the number of user sessions, the available RAM and the CPU loading as indicators and allocates new sessions accordingly. Nevertheless, if required VDS also creates separate sessions preferably again on the same server.

To maintain the number of sessions within limits, it is possible to limit them to one per user. Additionally, there are yet more options for special requirements for a customised distribution, the description of which would, however, take up too much space here. We liked the detailed overview provided by VDS of the current load distribution state and the distribution of sessions. In addition, we were impressed that the configuration program suggested the updating of the publishing agents on the terminal servers when, during the course of the test, the beta status was updated to the first officially released version.

Powerful control centre

We found the VDS console easy to understand thanks to its clear layout, which combines all the adjustment options in a single user interface. On the left side the administrator sees a menu with the main headings (server farm, load distribution, publishing, universal printing, universal scanning, connection, client information and licensing).

Groups for prioritising and availability The administrator must enter all the servers from which desktops or applications will be distributed under the "Server farm" heading. This could be terminal servers, either from Microsoft or Citrix, virtual desktop hosts (VDI-hosts) and dedicated PCs, so that these can be published using RDP. The administrator also enters the already mentioned Secure Client Gateway here as well as any backup servers. Within the entered terminal servers a grouping function is implemented in order to subdivide them, for example so that certain applications or desktops are only published through a fraction of the servers.

This also means that not all the terminal servers must be identically configured. Rather, the administrator can define a server group for a specific provision of an application and then only enable it for a particular user group. Consequently he has the possibility of improving control of licensing regulations and making more efficient use of licences. Also, if necessary, user groups can be prioritized in that the administrator only makes an application available to a group via a few terminal servers, but for another group makes it available over additional servers, so that they, even in the event of high loading, can always launch a

Publishing Server and Secure Client Gateway under Windows Server 2003/2008 (R2) Standard or Enterprise, Terminalserver-Agent under Windows Server 2003/2008 (R2) Standard or Enterprise with activated terminal services. The 2X-Client is available for Windows Server 2003, Windows XP, Vista, 7, CE Embedded, Mac from 10.5.x, also for the 32-bit Linux distributions Ubuntu 8.04/8.10/9.04/9.10, OpenSuse 11.1, Fedora Core 9/11, CentOS 5.2, VectirLinux 6.0 and Android as well as iOS.

session. Provided a user has authorisations to several server farms, he can, to all intents and purposes, connect to several simultaneously.

Flexible cooperation with hypervisors

Where VDI hosts are concerned, the 2X VDS is shown to be exceedingly flexible, as practically all current hypervisors such as Microsoft Hyper-V, VMware vSphere, ESX, ESXi, Parallels Virtuozzo Containers, Citrix XenServer and Oracle Vir-tualbox are supported. In the test we used the configuration for operation using VMware vCenter and ESXi. This is comparatively complex, but was in the end setup fairly quickly. For this purpose, 2X makes available a virtual appliance (vApp) with an Ubuntu installation for download, which is then to be imported via vSphere Client.

Further VDI agent appliances are available for Citrix XenServer and Virtual Iron. In the test itself, we didn't need to configure anything on the appliance itself, it automatically obtained suitable IP addresses via DHCP. When creating the VDI host in the console, diverse entries are necessary such as the hypervisor type, the precise version, the IP address, the port used and the access data (user/password), which can also be immediately tested. If the VDI agent is installed on the appliance, as in our test, then its IP address is also required. Also the administrator can specify the highest number of activated guests and specify the format of the RDP printer.

As, especially for configuration using a vCenter, not all running virtual machines should be used as a VDI guest, the administrator can block the use for each VM individually. Also, he has the possibility, by use of a pool definition, of grouping together several guests and then making the pools only available to certain user groups. When carrying out filtering based on users and groups, VDS accesses, upon request, the Active Directory, so that group administration is best carried out in the AD. Alternatively, filtering is available using clients and IP addresses. Overall, we were impressed by the level of flexibility available.

Figure 2: VDS and the application server are linked together in a setup, the licence determines the scope of use

Also interesting is the possibility of preventing the access both to the VDI host and also the terminal server for certain periods using a time scheduler. Here, current sessions can optionally maintain their status or be disconnected or reset. The connection times can be set permanently, daily, weekly, fortnightly, monthly or yearly. Therefore, for example, the definition of maintenance windows is problem-free.

A subordinate role may be played by the option of publishing dedicated PCs. For certain configurations, which, for example, cannot be visualized due to specific hardware requirements, this may make sense. In this case, RDP must be activated on the PC and the VDS agent installed.

Graphical view of the farm design

Of advantage in obtaining a general overview is the possibility of displaying a graphical view of the current farm design at any time. Additionally 2X offers the so-called Virtual Infrastructure Designer (VID), a tool for designing a VDS environment with graphical support. To operate the VID, Visio 2003 or higher must be installed. During the test VID would not initially start, rather always crashing on a range of systems with an error message. By working with technical support, the problem was quickly analysed and it quickly became apparent that the cause was the language version. We consistently used a German Windows version, 2X by contrast uses English versions internally. Thereupon, 2X resolved the problem within a few days and we were able to continue testing with a working VID.

When calling the VID, a wizard asks for the components which are to be used for application and desktop provision together with their IP addresses. From these a logical view is created. Using drag & drop, the administrator can add further components. A click on a component lists its properties so that they can be more precisely adjusted. The result is a configuration file, which can be imported into VDS. Likewise, it is possible to export the configuration of a running VDS environment, to load it in the VID, change it in VID and then reimport it into VDS.

Under the console heading "Publishing", the administrator can adapt the ports to the agents and control to what extent the calling of the application list requires a user authentication. Furthermore, VDS supports dual-factor authentication via Deepnet or SafeNet. Also integrated is authentication via SafeID, FlashID, MobileID, QuickID, GridID and SecureID. Nevertheless, of benefit at this point is the possibility, when using this feature, of again excluding certain users or clients from this process.

Complete desktops or individual applications

To publish resources, the administrator has available a toolbar in the VDS console with which there are various options plus a wizard which further simplify the setup. More detailed investigation shows that there is no great difference between using the wizard and the direct options to add an application, folder, desktop, specified application or document. In all cases, VDS conveniently asks for the required information over several windows. The administrator is guided in all cases.

The named publishing options are largely self-explanatory from the label. For the above mentioned applications, there are some system-orientated applications such as Internet Explorer or parts of the system control which are rigidly stored in VDS, furthermore the administrator can select from the installed applications or another individual application. Amongst the installed applications, VDS again publishes all the corresponding individual programs, as they are found in the start menu. More precise details are necessary for the publication of an individual application. Here, the administrator must directly specify the storage location of the executable file. From the console, the administrator can specify both colour depth and window size for both desktops and applications or make them dependent on client-side settings.

By default, alongside a menu structure in the 2X client described in more detail below, VDS sets up a shortcut in the start folder of the user PC. It is however possible to create shortcuts on the desktop or in the autostart folder. Insofar as the number of simultaneous calls of an application is limited, e.g. because of licence limitations, this number can be saved and in the event that the number of licences is exceeded, be linked with various actions such as "warn operator and do not start" or "Warn administrator and start". Of course, it is no problem to generally limit the calling of an application to one instance.

Instead of filtering accesses as previously described at the server level based on user, client or IP address, VDS also supports this at the resource level. Thus the administrator can individually specify, who should be able to call and who should not be able to call which application or which desktop. The displayed shortcuts are continuously correspondingly adjusted. In the test we have gone through the various options and were surprised how easily this functioned and what extensive opportunities the administrator has for individual configuration. As soon as something changes, this is adjusted on the client-side by updating the view.

It quickly became clear to us that in a production environment a precise pre-planning of the resources to be published is necessary, so that first of all a clearly understandable structure results and secondly different terminal servers and VDI hosts can be configured to match requirements. An important requirement in this respect is also a corresponding grouping, for example, via Active Directory. Particularly at the beginning, it certainly makes sense to start with the publication of fewer resources and then to successively expand the scope.

Wider client support

Particularly impressive is the client support of VDS: alongside the default Windows client, there is also a Linux and Mac client, which is authorised for various distributions (see "System requirements" box). Moreover clients for iOS (iPad, iPhone) and Android are available to enable smartphone access. In the Windows environment there is an XP embedded client as well as a version for Windows CE. Two further portable Clients for U3 and PortableApps complete the offering. The wide range of available clients permits, for example, the use of Windows desktops, published via VDS, on a Linux system or an iPad.

Client installation on various platforms is described in detail in the manual. The Windows client in particular has a multitude of settings so that its look and feel, such as window size or interaction with the local resources, can be individually matched. Where proxies are used, the settings are made here. In all cases, before first use at least one connection

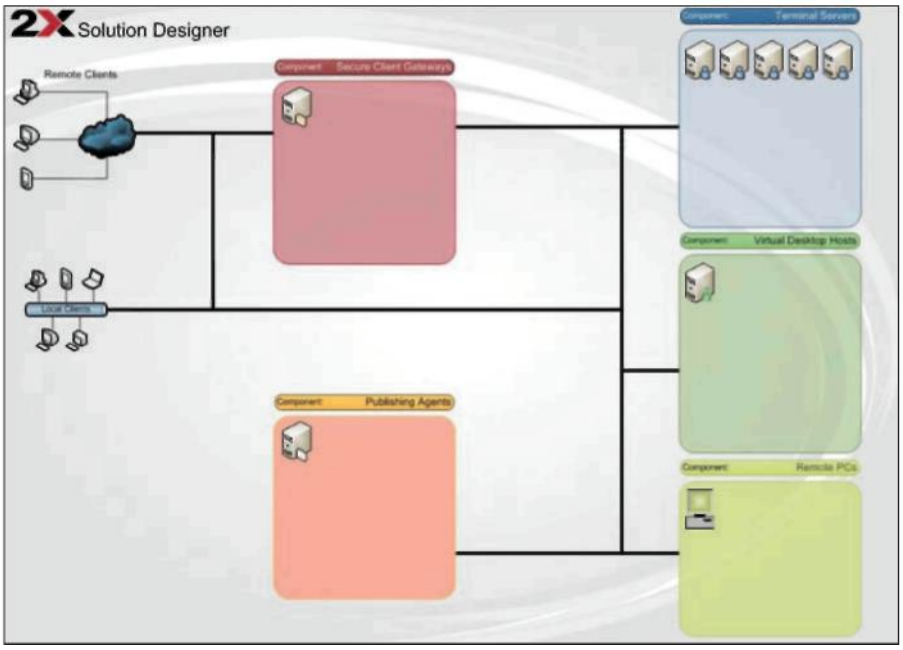

Figure 3: Upon request, VDS presents the current configuration in a clearly laid out graphical view. Clicking on a component displays the corresponding properties.

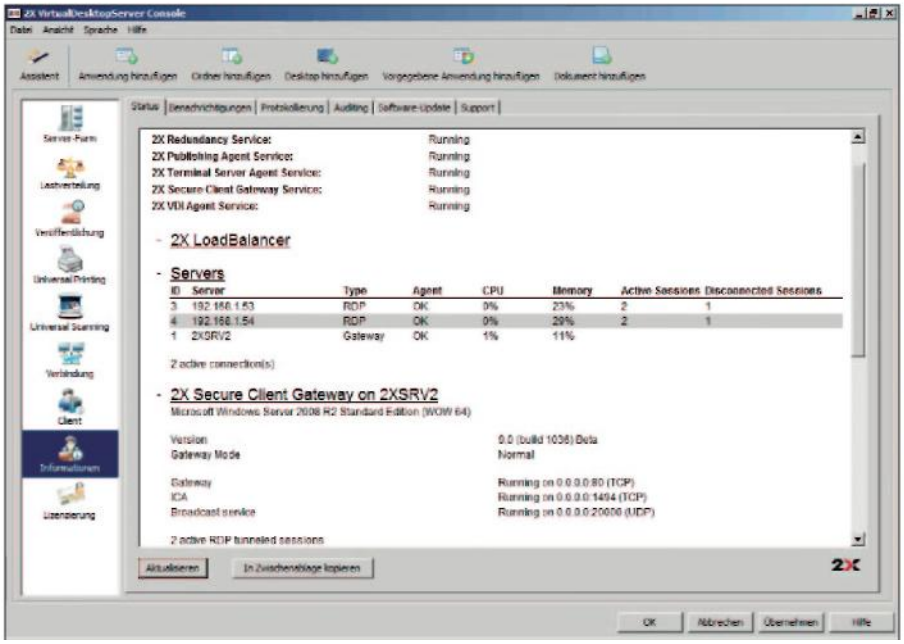

Figure 4: An informative overview reveals the current load and its distribution within the farm

to a VDS farm must be created so that the client knows where it can find a VDS server or a secure client gateway.

Where the connection properties are concerned, the client recognises three operating modes. With a direct connection, VDS has the least loading, because the client only briefly queries it and is then allocated a terminal server to which it connects directly. In "regular gateway" mode the entire communication runs over a secure client gateway, just as with the setting "SSL connection" under which there is however additional encryption. The client is so structured that several connections can be setup. In this way, several farms can be accessed, so that an administrator need not pack all publications in one farm, if this makes more sense.

When the client calls the system, the menu structure specified on the VDS console is displayed with the enabled applications and desktops. As already mentioned, the objects are also incorporated in the start menu or optionally incorporated on the desktop. A double-click on an application and it starts "seamlessly", i.e. without any delay, just like a locally called application. Ultimately the user scarcely notices that he is calling an application on a terminal server and not a local application.

Alongside the described normal clients, it is also possible to use thin clients with PXE boot. To achieve this, 2X offer a ThinClientOS for download, which then enables access to the resources made available by VDS over a secure client gateway. For this feature, it is important that PXE booting is activated on the Secure Client Gateway.

Alongside provision via the various clients, VDS offers access via a web portal, referred to as 2X Access Portal. Here also various farms can be registered. The Portal can be set up on a VDS server or at another point. We found the installation process not altogether smooth as although in the prerequisites only IIS and .NET-Framework 2.0 are named, during the setup on our Windows Server 2008 R2 it because apparent that some other role services such as ASP.NET, management scripts and static content were missing. Rather that just checking the requirements once and then providing a complete list of all the missing components, each one in turn resulted in an error message which each time required aborting and then restarting of the installation.

The user interface of the access portal is dynamically structured for the selection of applications and desktops and takes into account the filter options so that each user sees exactly those icons corresponding to the resources which he is authorised to see. Via an administrator login, authorised users access a page with settings which permit configuration of the portal.

Product
Program for server-based computing with terminal server and hypervisor support.

Developer
2X www.2x.com/de/

Price
VDS Small Business (one Server, 80 desktops, one gateway) costs € 900, VDS Professional (two servers, 160 desktops, two gateways) costs € 2,550 and VDS Enterprise (three servers, unlimited desktops and gateways) is available for € 5,150.

Technical data
www.it-administrator.de/downloads/datenblaetter

IT-Administrator scored as follows (max. 10 points)

Publishing of applications and desktops	**9**
Client support	**9**
Administration of access rights	**8**
Securing of data communication	**9**
Hypervisor support	**9**

This product is suited _____

Ideally to use in heterogeneous environments, where desktops and applications from a range of sources are to be made available to different user groups. The more complex the environment, the better VDS can exhibit its strengths.

With limitations for use in pure terminal server environments with uniform provision. Here also operation of a purely native Windows terminal server farm may be sufficient.

Not at all to environments which work solely with local resources where no applications or desktops must be published.

Value added terminal server

For the deployment of terminal servers VDS offers, in a manner analogous to Citrix, a value added beyond that possible with a native TS deployment. Naturally VDS supports the new functions of RDP7 such as redirection of the media player with video and audio as well as enhanced bitmap acceleration. Alongside the universal printing feature, VDS also offers universal scanning. Twain compatible applications can thus use scanning hardware on remote clients, without a necessity for device drivers to be installed on the server.

Also possible is multi-monitor operation and, in conjunction with a terminal server running under Windows Server 2008 R2 and a Windows 7 client, Aero Glass is supported. The various filters, based on users, groups and IP and MAC addresses have already been mentioned. These are primarily extremely useful with different user groups and complex environments. Logon is simplified by means of a configurable single sign-on. Alongside the automatic hand over of the system information any other user with a username can be added.

The available documentation is pleasantly comprehensive and easy to understand. Alongside the main manual there are miscellaneous additional documents as, for example, descriptions for setting up the VDI Agent Appliances, the web portal and the use of Deepnet for Two-factor authentication.

Summary

Overall 2X VDS was highly impressive on test. The producer has been successful in combining an extensive range of features with extremely easy operation. The VirtualDesktopServer from 2X combines the publishing of applications and desktops via Microsoft Terminal Server and Citrix with the provision of virtual desktops in a single product. In addition the desktops of stand-alone PCs can be published. Impressive also is the very wide hypervisor support for nearly all well known products. At least as impressive is the client pallet, which alongside Windows and Linux systems also includes a general Java client as well as providing support for Android and iOS.

The central console, through which administration steps are executed, appears highly effective to us. We also like the fact that using VDS several terminal server farms and VDI hosts can be administered simultaneously and grouped for different user accesses. Consequently the support of an exceedingly heterogeneous environment with different requirements for the individual users from one central point is possible. The setting up of several publishing servers according to a master/backup principle ensures high availability. The use of secure client gateways, with which the entire data traffic is tunnelled over one port and as necessary encrypted, predestines the product for use in environments with heightened security requirements.