Microsoft

Microsoft Desktop Optimization Pack for Software Assurance

Microsoft® System Center Virtual Application Server

Branch Configuration Guide

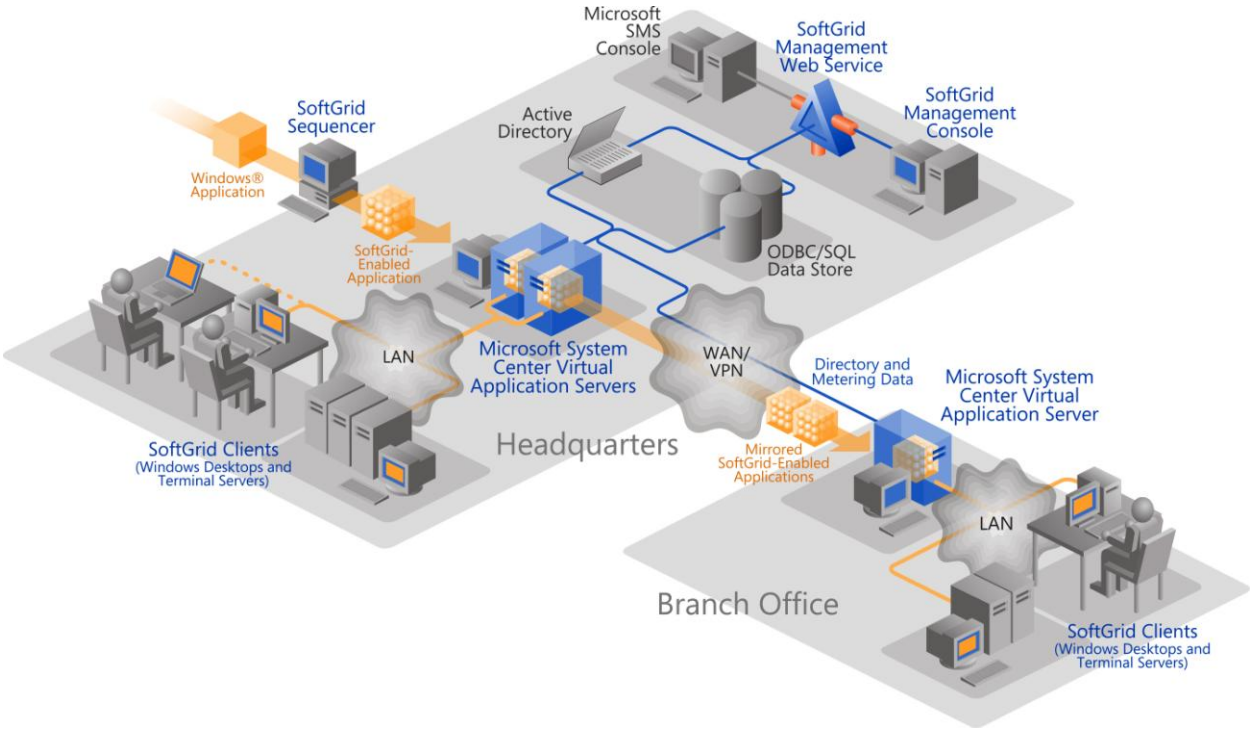
March 2007

Table of Contents

Introduction

As Microsoft® SoftGrid Application Virtualization is used to deliver applications directly to PCs with the SoftGrid for Desktop Client, it quickly becomes apparent that streaming multiple concurrent applications across a wide-area network results in less than optimal initial launch times for larger numbers of user. It also becomes clear that an entire remote office cannot wholly depend upon a WAN connection to be able to perform its functions. With this in mind, the need for a Microsoft SoftGrid Application Virtualization model that allows users to stream applications directly on the LAN, yet still allow centralized management across the WAN is necessary. This document will describe the current design and operation of a system to accomplish these goals, known as the Microsoft Systems Center Virtual Application Branch Server (SCVABS).

This document is designed to give the basic orientation of the components and considerations necessary in creating virtual application branch server architecture. It does not consider all possible scenarios, but should be a good primer for creating your own designs based on environmental requirements.



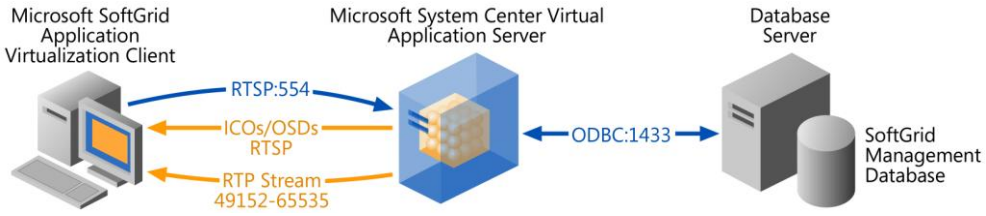
Microsoft SoftGrid Application Virtualization infrastructure

Microsoft System Center Virtual Application Server Components

The main purpose of a branch server is to allow for LAN-based streaming of applications, yet still retain centralized control of the applications. It is important to note that the full functions (AD, DNS, Database, etc.) described below may be combined onto a single branch server in order to conserve the use of hardware, however all design with these components should adhere to their respective best practice guidelines.

The Microsoft Systems Center Virtual Application Infrastructure

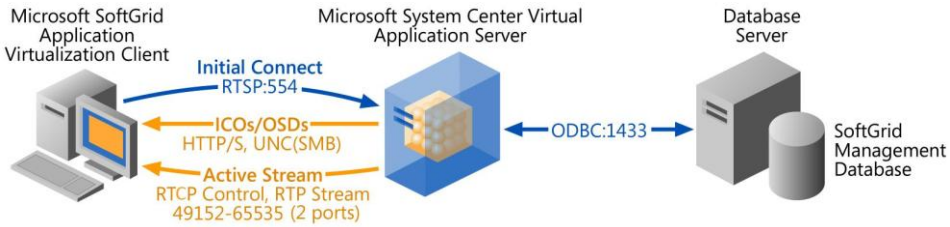
- **Microsoft Systems Center Virtual Application Server (MSCVAS)**
  The MSCVAS is the distribution point for streaming applications in the Microsoft SoftGrid Virtual Application infrastructure. This system has basic dependencies that are important to understand in order to properly design a branch scenario.
- **The MSCVAS SoftGrid Database**
  The MSCVAS relies on a database during startup for information about its configuration, the virtual applications it will host, licensing, and caches the Active Directory group identifiers used for application assignment. The database is also used for optional metering of the virtual applications.



Microsoft System Center Virtual Application Server Communication

- **The Content Folder**
  The MSCVAS relies on a folder where the virtual application content is stored. This folder contains the SPRJ (optional) OSD, ICO and SFT files which make up the virtual application. This folder is registered as part of the servers configuration and is required in order to properly stream. This folder can either be a local folder or a UNC path to a share.
- **The Virtual Application Record**
  The virtual application record contains the configuration information as well as the Active Directory group GUID which is used for application assignment. The OSD and ICO paths in this record typically contain HTTP/S or UNC paths to centralized repositories of application components.
- **Active Directory**
  Active Directory is the central repository responsible for virtual application assignment. However, Active Directory is rarely communicated with in the current MSCVAS system. Active Directory is read for groups when the application record is created, however in production, the group identifiers associated with the virtual application records are kept in the database and cached at the servers on server startup. When a user requests a Desktop Configuration request or an application authentication or authorization event, the users token is passed to the server where the user's group membership is checked against the cached group identifiers. This makes for fast and efficient checking of group membership without being chatty with Active Directory.

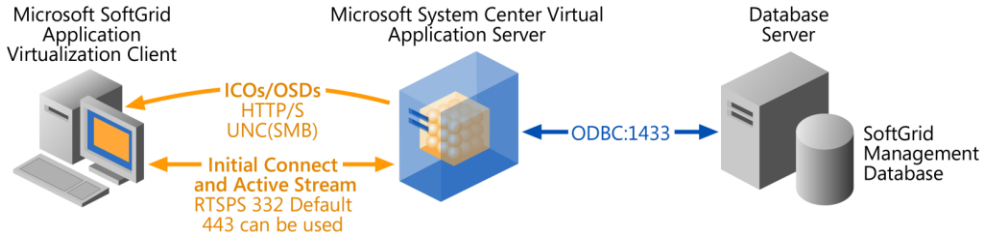
- **The streaming transport: Real-Time Transfer Protocol (RTP)**
  RTP is a suite of protocols used by the MSCVAS for the streaming delivery of virtual applications. By default the RTSP protocol listens on port 554 for requests from the Microsoft SoftGrid Application Virtualization Client and then dynamically connects to the client on two high ports (one for RTCP and one for RTP) in the range between 49,152 and 65,535. The RTCP port is then used for control messages, while the RTP is used for the actual data transfer.



Microsoft SoftGrid Application Virtualization Client Default Communication

RTSPS (TLS + Inline RTSP) may be used as an option where a single port is needed and an encrypted application stream is desired. The default port is 332 in RTSPS; however it can be redirected to 443. RTSPS uses a single port for both RTCP and RTP traffic for all connections to the MSCVAS and this can have an effect on performance.

While RTSPS is an option for delivering streamed content, it should not be viewed as a complete methodology for securing the communication stream between the server and the client. Microsoft recommends reading the security best practices document for streaming communication for more explanation on recommended security practices.



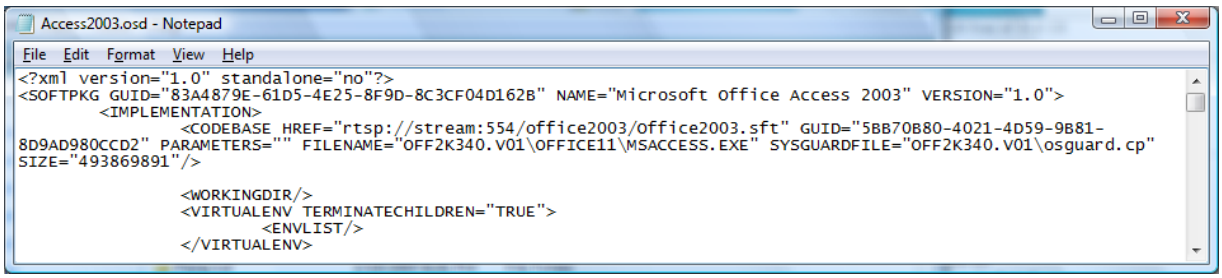
Microsoft SoftGrid Application Virtualization Client RTSPS Communication

- **The Desktop Configuration Service**
  In order to publish the virtual applications and properly configure the desktop for use, the MSCVAS possesses a Desktop Configuration service. The Desktop Configuration Service is optionally triggered through a logon event, a pre-set interval or manual operation performed by the user. The Microsoft SoftGrid Application Virtualization Client will check with the MSC Virtual Application Server to discover any applications assigned to the user. The MSCVAS will use the user's credentials and check the MSCVA Data Store for the application configurations.

  The MSCVAS will then return the location of the ICO and OSD files, along with the file associations and publishing locations from the application record to the client in XML. The client will use the protocol specified in the URI of the application record to then directly connect to each location and download the Icon and OSD files. Finally, the client will publish the shortcuts as directed by the server. Typically two different protocols may be used: HTTP/HTTPS or UNC Paths.

  The figures above represent the communication structure for the Desktop Configuration service.

- **The Microsoft SoftGrid Application Virtualization OSD File**
  The OSD file tells the client where to connect for the virtual application stream. It accomplished this through an RTSP or RTSPS URL inside of the `CODEBASE` tag as seen below:



Sample OSD File

The client uses the host name (“stream” in this example) in the RTSP or RTSPS to direct the connection request to a MSCVAS server. This name may be an IP Address or host name and can be directed to a third-party load balancer for connection distribution as well.
Optionally, this name can be replaced with a variable known as `%SFT_SOFTGRIDSERVER%`. If this variable is used in place of a host name, the client will use the entry for the environment variable of the same name on the local system. This environment variable may be set any number of ways including through login script.

Minimal Disconnected Operation Mode (MDO Mode)

MDO Mode is the capability for the client to run applications that are already in cache in the event the database, server or network ceases to respond. There is a time-out that is administrator configurable so the client can be offline for a number of hours but not for an extended period of time. This capability was provided so users may continue to execute in case of a down situation. While in MDO mode, the user may use existing applications in cache, however additional blocks, new applications and application updates will not be available until the server MSCVAS returns to proper operation.

When operating in MDO mode, when an application makes a request for additional blocks not in cache, a close message will be sent to the application. Typically, this application will bring up the save dialog box and the user may save their data before closing the application. The user may then launch the application again. However, if the application makes the request again for a component that is not in cache, the application will shut down again as previously described.

Network Latency and Connection Speed

Network latency and connection speed are factors which can affect the performance of the branch scenario. The performance of the protocols used by Microsoft SoftGrid Application Virtualization platform may be susceptible to varying degrees by high latency networks, low connection speed or both. Microsoft is working on determining latency thresholds and will publish this information as it becomes available.

Quality of Service (QoS)

In order to better ensure proper performance of protocol communication between the MSCVAS and the MSCVA database, Microsoft recommends looking into QoS configurations that prioritize SQL traffic on 1433.

Testing

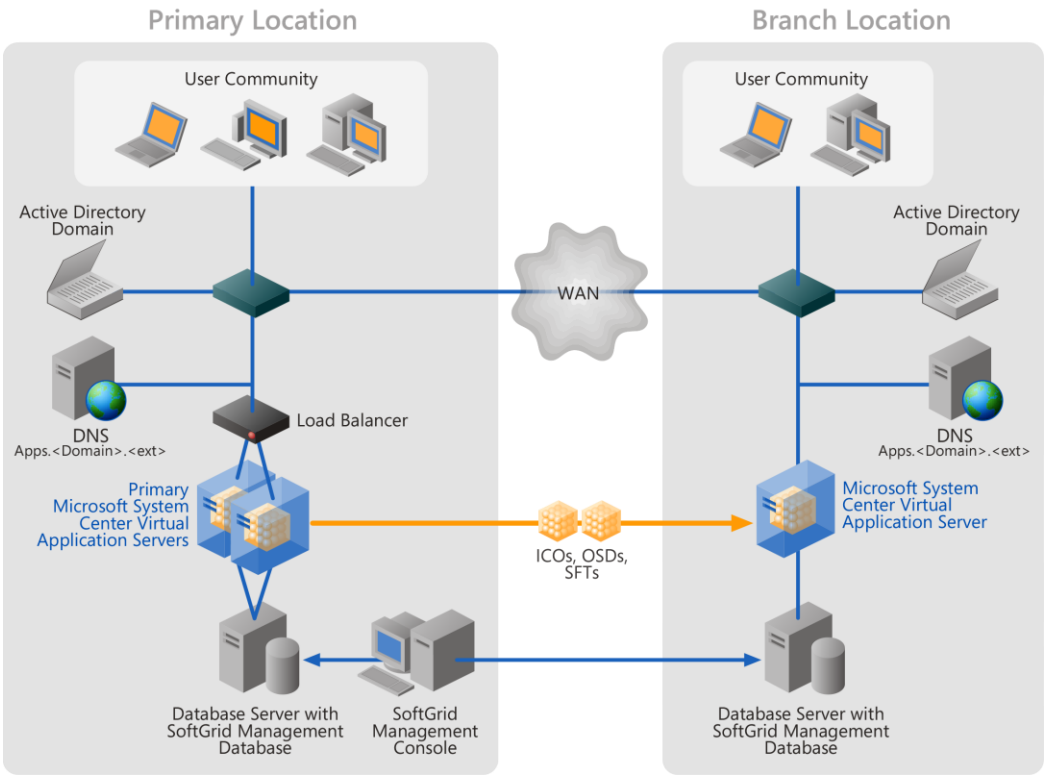
Since every network is different, it is important to thoroughly test the deployment scenarios either through WAN simulation or directly on similar network connections. This testing information can be used to further extrapolate the overall impact and therefore strategy used in which branch office model will be used.

Branch Models

There are essentially two designs that are supported inside of Microsoft SoftGrid Application Virtualization: the Non-Centralized Branch and the Centralized Branch Hub. The differences between these two models are simply where the database exists. The commonalities in key design areas will be discussed in the next section.

Non-Centralized Branch

A Non-Centralized Branch includes a local database and a replicated copy of the content, but is managed as separate entities from a central management console. The figure below shows a Non-Centralized Branch:



Non-Centralized Branch Architecture

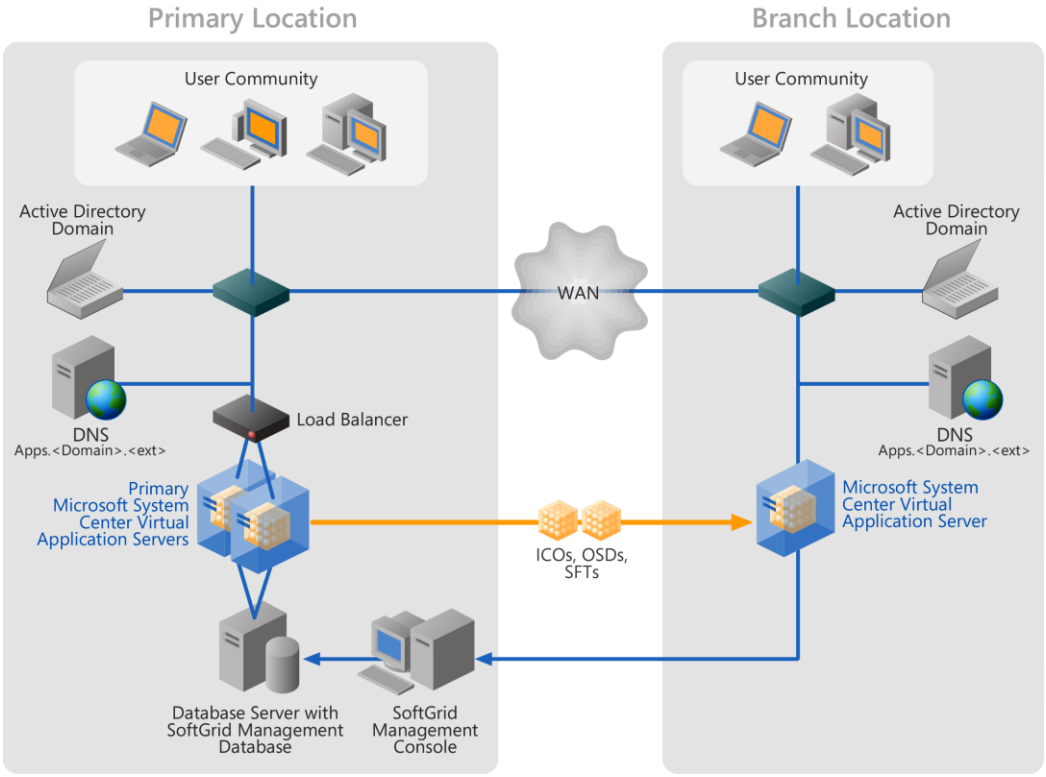
MSCVAS Database

Connection to the Microsoft SoftGrid database is a dependency for the MSCVAS and needs to be available when the server starts operation. Currently, the MSCVAS database does not support replication. In the Non-Centralized Branch model, the MSCVAS database is placed locally in the branch, either on the branch server itself or on another server if more than a single branch server is being used at the remote location. In this situation, the application records must be either directly imported or copied through the MSCVAS management console application record copy feature.

The metering database in this model will only collect data for the local applications that are connected to the server. Centralized metering in native Microsoft SoftGrid Application Virtualization is not supported for the Non-Centralized Branch model at this time.

Centralized Branch Hub

The Centralized Branch Hub is characterized by a single, centralized database which the branch servers use via a direct connection over the WAN. SoftGrid content is replicated to all sites. Since the database is centralized, all publishing information is centralized. The figure below shows a Centralized Branch Hub:



Centralized Branch Hub Architecture

Now that we have reviewed the two different types of supported branch models, let's take a look we will examine the enabling technologies.

MSCVAS Database

Connection to the Microsoft SoftGrid database is a dependency for the MSCVAS and needs to be available when the server starts operation. Currently, the MSCVAS database does not support replication. The centralized database model keeps the database at a foundation site and the remote servers connect over the WAN. In this model, only one database is maintained and the metering information is centralized. Due to the MDO capabilities of the Microsoft SoftGrid Virtual Application system, if the WAN link drops, the users may continue to use the applications already in cache.

Common Design Considerations

Content Replication

Since the MSCVAS is local to the client LAN, it is important to replicate the virtual applications to the remote locations. There are more than a few ways to accomplish this and we will explore a few of these options. Microsoft recommends replicating the virtual application files in after business hours where possible in order to WAN link service degradation for end users.

Please Note: It is important to make sure that the content is replicated to the remote MSCVAS before enabling the application in the MSCVAS database. Failure to do so will prohibit the client from getting the application.

Manual or Scripted Replication
This includes manually copying the virtual application files between content shares, delivering the Microsoft SoftGrid virtual applications via removable media (CD, DVD, USB drive, etc.) as well as creating a script to automate the copy process between content shares over the network...

RoboCopy
Microsoft RoboCopy is a robust copying tool that can perform file and folder differentiation and is easily scripted.

Third-Party File Replication
Third-party tools may be used to replicate virtual application files between locations. This includes NAS and SAN replication where the MSCVAS uses a UNC path to the NAS device or a mounted connection to the SAN location.

SMS 2003
An MSCVAS can be co-located on an SMS Distribution Point server. You can also utilize the package replication capabilities in SMS to move the virtual application assets as packages to the remote Distribution Points. The trick here is to make sure the content path for the MSCVAS is the same as the root share point for the SMS Distribution Point. This gives you the ability to use SMS to replicate the packages through BITS or other means, yet allows streaming to occur from the MSCVAS. However, SMS package distribution is not a solution for database replication. The database must either be present locally per the Non-Centralized Branch model or centralized with the connection over the WAN per the Centralized Branch Hub model.

Distributed File System Replication (DFS-R)
DFS is Microsoft's distributed file system where a generic host name and URL are presented as a generic alias for accessing local content. DFS has an automated replication capability that will keep the content folders synchronized while allowing the server to access a normalized UNC path.

Proximity Awareness through Multiple Naming Techniques

Microsoft SoftGrid Application Virtualization is designed as a web service and carries the same principles. In the case of location awareness, MSCVAS does not provide a service to automatically connect the client to the nearest server. However, there are a few options when looking at creating proximity awareness that involve different naming techniques. All of these techniques may be used by both the Desktop Configuration service and the streaming delivery of the application.

Location Specific OSD Files

Each .OSD file is configured with the appropriate branch server DNS name and replicated to the specific branch server it represents. When the client refreshes the desktop from the desktop configuration service, the location specific OSD files will be presented to the client and directed to the local MSCVAS on application stream request.

However, there are a couple drawbacks to consider. First, this is a manual process that requires keeping track of multiple .OSD files. Second, if the user is a traveling user between SoftGrid enabled LAN segments, the user may be using a WAN based branch server name when they connect off of the home network. This can cause slow response times.

Login Scripts and the `%SFT_SOFTGRIDSERVER%` Variable

The `%SFT_SOFTGRIDSERVER%` variable can be set with the server information by a login script. This script can be user specific; however, there is the ability in Active Directory to specify a script for a Site. These Active Directory Site scripts can set the specific server or DNS name tied to a load balancer. This allows the RTSP URL host name to remain generic with the `%SFT_SOFTGRIDSERVER%` variable and allows the local PC to be set with the proper local server name.

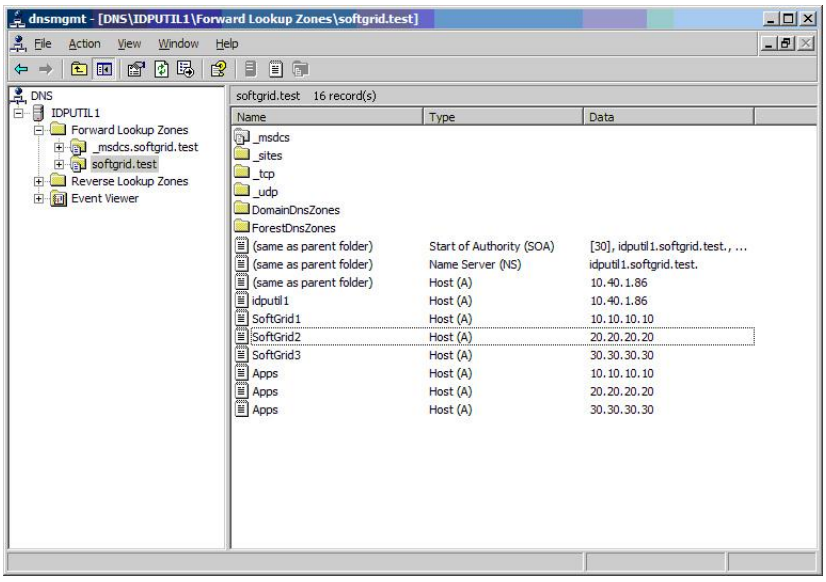
Third-Party Site Aware Load Balancers

Certain third-party load balancers can be site aware. This means they are aware of their counterparts in other locations and can route the request to the appropriate site. These load balancers are available from multiple vendors. When the request comes to the load balancer, the closest server can be determined and the request routed accordingly. Some of these products include a secondary list of next closest servers for connection fault tolerance. Each third-party vendor handles these requests differently so check with the specific products documentation for more information.

Microsoft DNS Based Proximity Awareness

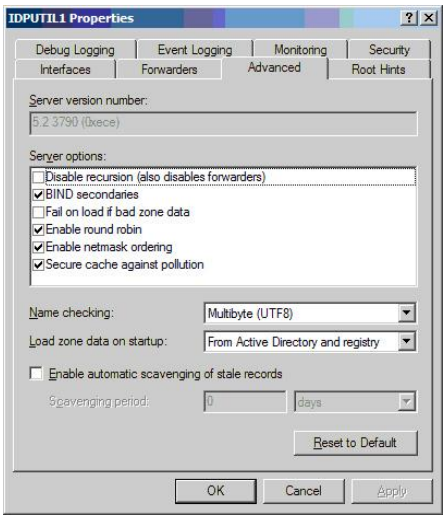
Netmask Ordering in DNS allows the same hostname to be assigned to the multiple IP addresses, including IP addresses on separate subnets. These records can represent a server or a virtual IP address of a load balancer. This generic name is now used in place of a local hostname in the RTSP URL. When the client begins the streaming process, the DNS name is resolved from the RTSP URL (unless an IP address is used directly). The DNS server will look for the local subnet first and return the address on the subnet to the client. The client will then connect to the local device on that subnet.

To enable Netmask Ordering, create a generic host name record (in the following example it is named “Apps”) for each MSCVAS that already exists in DNS Zone as shown below:



If there is a load balancer present that utilizes a virtual IP address, make sure to enter the virtual IP Address into the “Apps” host record. Once completed, replace the current HREF in the .OSD file with “`rtsp://apps.<domain>.<ext>`” leaving the rest of the line the same. Windows 2000 and above DNS server utilizes by default a function called “netmask ordering”. This essentially tells DNS to return an IP Address to the DNS query that is on the same subnet as the DNS Client. If one is not available then it will return the next closest address on the list. By adding the “Apps” record for each SoftGrid server and enabling Netmask Ordering, the client is returned the local MSCVAS.

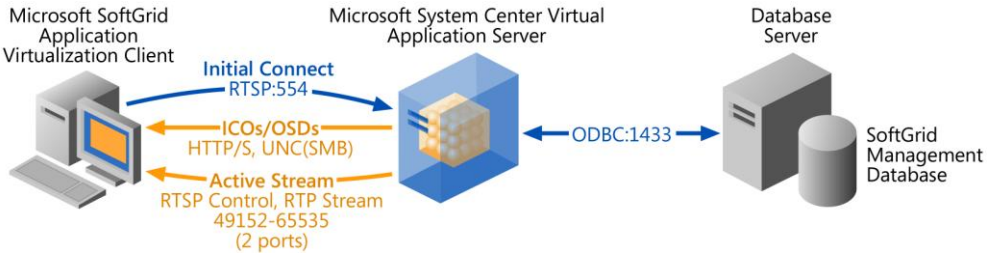
To ensure this operation functions properly, go to the DNS administration MMC, right mouse click on the SOA server for the Zone the SoftGrid servers are located, click properties then the Advanced tab. The figure below shows the “Enable netmask ordering” checkbox to be checked.



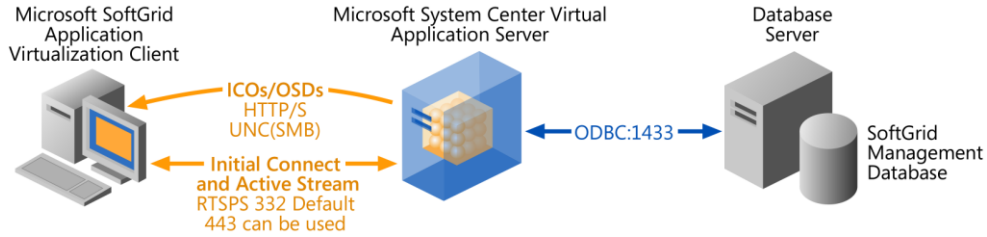
The SoftGrid clients will now look for a DNS record on each LAN segment that will point them to the proper Server no matter their location.

The Desktop Configuration Service

The Microsoft SoftGrid Desktop Configuration service relies on the MSCVA database to provide the assigned applications and their associated configurations to the client. In order to support this process, the MSCVAS must make multiple calls to the database over ODBC on port 1433. ODBC has a higher susceptibility to WAN latency. However, the delivery protocol for the OSD and Icons are specified in the application record. WAN optimized protocols such as HTTP/S and to a lesser extent SMB in a UNC path can be used to deliver these components. The figures below depict this communication.



Microsoft SoftGrid Application Virtualization Client Default Communication



Microsoft SoftGrid Application Virtualization Client RTSPS Communication

It is for these reasons that Microsoft recommends configuring the Desktop Configuration service source as a server or load balanced set of servers with a database that is on the same high speed network. In the case of the Non-Centralized Branch model, the server entry in the Desktop Configuration service should point to the local server. In the case of the Centralized Branch Hub model, the Desktop Configuration service at the client should point to the MSCVA servers in the centralized location. The paths in the Application Records may use the same name aliasing techniques to ensure the content is coming from the optimal servers on the network.

Naming Techniques and the Application Record

The Microsoft SoftGrid Client will check with the SoftGrid Server to discover any applications assigned to the user. The MSCVAS will use the user's credentials and check the MSCVA Data Store for the applications configurations. The MSCVAS will then returns the location of the ICO and OSD files, along with the file associations and publishing locations from the application record to the client in XML. The client will use the protocol specified in the URI of the application record to then directly connect to each location and download the Icon and OSD files. Finally, the client will publish the shortcuts as directed by the server. Typically two different protocols may be used: HTTP/HTTPS or UNC Paths.

There are no special considerations when using the HTTP or HTTPS protocols outside of normal IIS design considerations; however there is an issue when using alias naming with UNC paths.

Windows Server 2003 SP1 and above includes enhanced security features that result in Client SMB requests, such as attempts to access a shared directory on the server using a UNC path with a DNS alias rather than the server's actual computer name. It will fail even if the request contains the correct IP address of the server. For example: Attempting to access `\\apps.domain.net\content` from a client PC will fail even if the apps.domain.net FDQN is resolved by DNS to the IP address of the server.

Refer to the following Microsoft Support KB article for details: http://support.microsoft.com/kb/281308/en-us

Attempts from a user session on the server to access a shared directory on that server via a UNC path that uses a DNS alias rather than the server's actual computer name, will fail even if the request contains the correct IP address of the server.

For example: Attempting to access `\\apps.domain.net\Content` from a user session on the server will fail even if the apps.domain.net FDQN is resolved by DNS to the IP address of the server.

Refer to the following Microsoft Support KB article for details: http://support.microsoft.com/kb/914060/en-us

In order to use a Windows 2003 server (SP1 or later) as a MSCVAS with generic naming, the following two registry changes are necessary to enable the server to respond to requests that are made using a DNS alias such as apps.domain.net rather than the server's actual computer name:

- Create a new DWORD registry value as follows:
  `[HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters]`
  `DisableStrictNameChecking = 1`
- Create a new DWORD registry value as follows:
  `[HKLM\System\CurrentControlSet\Control\LSA]`
  `DisableLoopbackCheck = 1`

Active Directory

It is recommended that a Domain Controller/Global Catalog reside on the same LAN as the SoftGrid branch servers. This is to ensure the login time is kept to a minimum and adds a level of fault tolerance in case the WAN link becomes unavailable. This is not a requirement, but a recommendation per Microsoft best practices.

Online Resources

Microsoft Desktop Optimization Pack Resources:
http://www.windowsvista.com/optimizeddesktop

Microsoft SoftGrid Application Virtualization Knowledgebase:
http://support.microsoft.com/search/?spid=12357&adv=1

About the Author

Chad Jones (MCSE, CNE, CCEA, CCI, SCP, PMC) is a group product manager in the Windows Client Product Management group, where he is responsible for Microsoft SoftGrid and the Microsoft Diagnostics and Recovery Toolset. Before joining Microsoft, Chad helped create the Softricity second-generation platform, SoftGrid. As senior director of product strategy at Softricity, he contributed in several key areas, including strategic product planning, technical evangelism, companion product engineering, customer design reviews, and market definition and positioning. He was also responsible for the creation of the Return on Virtualization (ROV) Calculator, which Forrester Research approved as the first accepted return on investment (ROI) model for virtual applications.

Acknowledgements

Special thanks to the following people for helping to create the configurations presented here as well as reviewing this paper:

Julian Weinstock, SR Product Manager
Sean Donahue, Technical Evangelist
John Flanagan, Technical Evangelist
Steve Chadly, SR Consultant II
Chris Maher, Engagement Manager
Edwin Yuen, Engagement Manager
Roberto Cazzaro, Sustained Engineering Manager
Jeroen Van Eesteren, Support Team Manager
Microsoft SoftGrid Application Virtualization Development Team.