Microsoft iT Showcase

Best practices, experiences, and global solutions from Microsoft IT.

Deploying Office Live Communications Server 2005 at Microsoft

How Microsoft IT deployed and operates a reliable, enterprise-wide real-time presence and instant messaging infrastructure

Technical White Paper

Published: October 2004

Microsoft

CONTENTS

EXECUTIVE SUMMARY

Situation

Previously, Microsoft IT upgraded its real-time presence and instant messaging solution from Exchange Instant Messaging to Live Communications Server 2003. While Live Communications Server 2003 provided the immediate business value users had expected, Microsoft IT wanted to deploy the solution in a high-availability configuration with improved manageability, scalability, and improved multiple forest support.

Solution

To provide increased service levels and manageability of its instant messaging and presence solution, Microsoft IT used Windows Server 2003 and SQL Server 2000 to deploy Live Communications Server 2005 using a pooled front-end server and clustered back-end database server configuration.

Benefits

- Increased service levels by deploying a more available, more scalable, and higher-performance front-end server and back-end database server configuration
- More secure internal and remote access that is easier to set up and manage
- Less complex (and less costly) deployment and management options for the multi-forest network environment at Microsoft

Products & Technologies

- Microsoft Office Live Communications Server 2005
- Windows Messenger 5.1
- Windows XP Professional Service Pack 2
- SQL Server 2000
- Windows Server 2003 with Active Directory directory services
- Microsoft Operations Manager 2005
- Microsoft Identity Integration Server 2003 for cross-forest directory synchronization

Increasingly, companies regard real-time presence and communications—such as instant messaging (IM), audio/video conferencing, data collaboration, whiteboard sharing, remote assistance, and file transfer—as key services for connecting employees and improving their productivity. Today, Microsoft employees are more mobile than ever. To increase their personal productivity, they frequently work from remote or home office locations, with little face-to-face contact with fellow employees, and collaborate with people they have never met in person. Microsoft® Office Live Communications Server 2005 enables Microsoft information workers to take advantage of real-time communications and presence to increase productivity without compromising security and manageability.

Previously, Microsoft had deployed Microsoft Exchange 2000 Server instant messaging services to support employee needs for basic presence information and instant messaging.

In the spring of 2003, Microsoft Information Technology (Microsoft IT) deployed Live Communications Server 2003 to replace the original deployment of Exchange 2000 Server instant messaging services. Designed for tighter presence integration into Microsoft Office System applications, and built using the industry-standard Session Initiation Protocol (SIP), Live Communications Server 2003 was the replacement for Exchange 2000 Server instant messaging services.

In the summer of 2004, Microsoft began deploying early releases of Live Communications Server 2005 to test the product in a large, worldwide enterprise environment. When fully deployed, five front-end servers and a two-node database cluster will support more than 80,000 enabled instant messaging accounts at Microsoft.

The focus of this paper is the experiences of the Microsoft IT Communications Operations team in planning, deploying, and operating its upgraded, security enhanced, real-time, person-to-person communications solution based on Live Communications Server 2005 Enterprise Edition.

This paper was specifically written for enterprise business and technical decision makers, IT architects, and operations managers who are considering an upgrade (or initial deployment) of a real-time presence and instant messaging infrastructure.

INTRODUCTION

Customers frequently ask Microsoft IT about the methods employed and lessons learned when Microsoft products and technologies are deployed internally. In 1999, Microsoft IT deployed Microsoft Exchange 2000 Server instant messaging services to support its employees' needs for basic presence information and instant messaging. In the spring of 2003, Microsoft IT deployed Live Communications Server 2003 to improve the ability of Microsoft employees to find and communicate with each other in real time.

In addition to running the global IT service internally, Microsoft IT is also committed to testing Microsoft enterprise products in production before they are released to customers to ensure that products will scale to meet the business challenges of other large enterprises. As part of that mission, in the summer of 2004, Microsoft IT worked together with the Live Communications Server product development group to deploy Live Communications Server 2005. Microsoft IT identified six business needs related to real-time communication:

- High-availability deployment
- Improved reporting
- Support for Microsoft SQL Server 2000 in addition to Microsoft SQL Server 2000 Data Engine (MSDE)
- Multiple forest management
- Internet access without a virtual private network (VPN) connection
- Federation of real-time communications services with external organizations

Given the existing Microsoft deployment of Live Communications Server 2003 and the updated and new features of Live Communications Server 2005, Microsoft IT and the Live Communications Server product group developed a strategy to enable the production deployment of an updated, real-time, person-to-person communications solution before the final version of the product was released to customers.

Deployment planning began in the first quarter of 2004. Proof-of-concept testing completed in the spring of 2004, and full production deployment completed in the fall of 2004.

Because every organization is unique, each IT organization must develop its own plan for deploying Live Communication Server 2005. There were tasks in the Microsoft deployment plan that other organizations may never encounter, or that may need to be completed at different times in the process. For example, at the same time that Live Communications Server 2005 was being deployed, Microsoft IT was also implementing network domain isolation based on Internet Protocol Security (IPSec), and deploying Windows® XP Professional Service Pack 2 (SP2). This affected the overall timing of the migration to Live Communications Server 2005.

Although this paper is not intended to serve as a step-by-step guide for deploying Live Communications Server 2005, Microsoft is sharing this information to assist its customers in deploying this product in their own environments. Additional information about Live Communications Server 2005 is available at http://www.microsoft.com/office/livecomm.

Note: *For security reasons, the names of forests, domains, and other internal resources do not represent real names used within Microsoft and are for illustration purposes only.*

SITUATION

In 2003, Microsoft deployed Live Communications Server 2003 to provide a more secure, standards-based, real-time presence and instant messaging solution for its employees. The Live Communications Server 2003 configuration deployed by Microsoft IT appears in Figure 1.

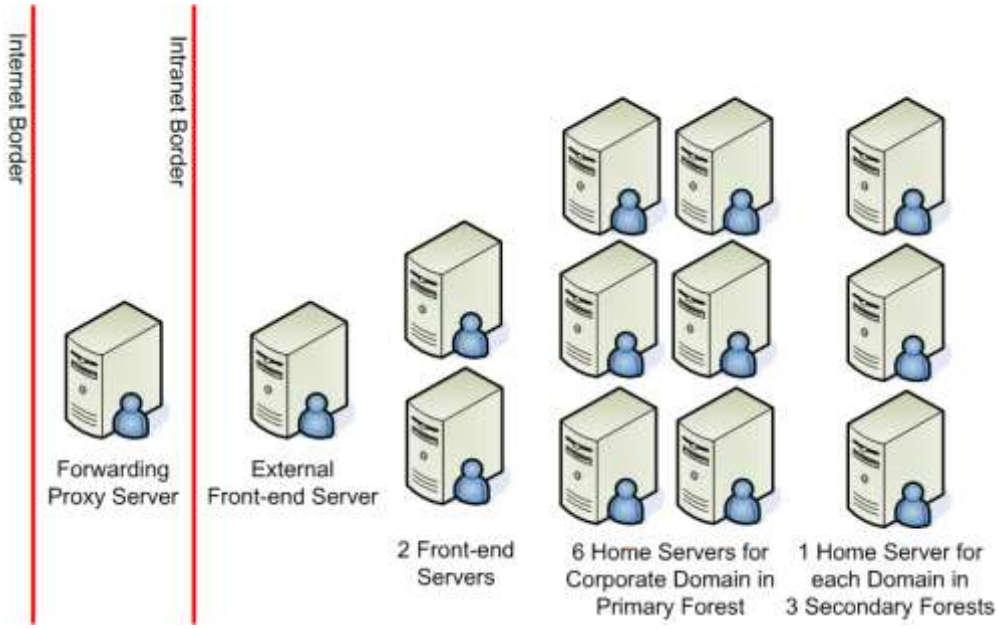

Figure 1. Previous Live Communications Server 2003 physical architecture

Nine Live Communications Server 2003 Standard Edition home servers were required, primarily because each forest was required to have one or more home servers to host the users in that forest. Live Communications Server 2003 Standard Edition was not designed for the high-availability requirements of large organizations like Microsoft. In addition, it was difficult to configure and support external Internet access for Microsoft employees to access their home servers without establishing a VPN connection. Lastly, configuring and enabling the federation of real-time presence and communications services at Microsoft with those of selected organizations and customers was not supported by Live Communications Server 2003.

Note: *In Live Communications Server 2003, the servers that hosted the real-time communications services were called home servers. Live Communications Server 2005 Standard Edition is based on a similar design where the MSDE is used to store user data on each local server.*

Live Communications Server 2005 Enterprise Edition introduces a highly scalable, high-availability deployment model based on the concept of server pools. *Live Communications Server 2005 Enterprise Edition supports multiple front-end servers per server pool and the use of clustered back-end SQL Server 2000 database servers. A large enterprise deployment can mix multiple Standard Edition servers and Enterprise Edition server pools.*

Microsoft Office Live Communications Server System Components

In its simplest terms, three components need to be deployed to create a security enhanced, real-time, person-to-person communications solution:

- Real-time communications-enabled client application
- Real-time communications server
- Operating system and networking infrastructure

Windows Messenger

In March 2003, Microsoft IT began deploying Windows Messenger 5.0, the real-time communications client application that is compatible with three protocol stacks:

- Session Initiation Protocol (SIP) to support Live Communications Server
- Rendezvous Protocol (RVP) for backward compatibility with Microsoft Exchange 2000 Server instant messaging services
- Mobile Status Notification Protocol (MSNP) supported by .NET Messenger Server public instant messaging service and used by the MSN Messenger consumer instant messaging client

The deployment of Windows Messenger, with its triple-protocol stack ("triple-stack"), enabled Microsoft employees to make more readily the transition from using Microsoft Exchange 2000 Server instant messaging services to Live Communications Server. The current version of Windows Messenger is version 5.1 (October 2004).

Key elements of the Windows Messenger user interface can be customized based on the Live Communications Server namespace that the user is logged on to. A list of the customizations used by Microsoft IT is provided in Appendix A – Windows Messenger 5.1 Client Branding.

Microsoft Office Live Communications Server 2003

Live Communications Server provides user authentication, device registration, presence, invitation, and encrypted instant messaging services between users. Once authenticated, a Windows Messenger user can interact with another user by using instant messaging, file transfer, whiteboard, voice and video, or multiple users by using the multi-party IM feature.

Figure 1 is a diagram of the physical architecture used by Microsoft IT to deploy its original Live Communications Server 2003 environment. Nine home servers were hosted in the Redmond, WA data center: six to serve the needs of the corporate domain users in the primary forest; and one server for each of the three product group development and testing domains.

In addition, two Live Communications Server 2003 front-end servers were deployed in the Redmond data center to route corporate users to their assigned home server.

This Live Communications Server 2003 configuration supported approximately 80,000 user accounts.

Live Communications Server 2005 Enterprise Edition

Live Communications Server 2005 Enterprise Edition is designed for large-scale deployments supporting over 100,000 users. This includes support for high scalability and

availability with a load-balanced Windows Server 2003 front-end server pool and a SQL Server 2000 SP3a back-end database server that can be clustered for high availability.

Live Communications Server 2005 is dependent on the following Windows Server 2003 services:

- Transport Layer Security (TLS) for client/server encrypted communications
- Mutual Transport Layer Security (MTLS) for server-to-server encrypted communications
- Active Directory® directory services for user authentication (including Kerberos and NTLM authentication)
- Directory forest and domain management
- Live Communications Server management console (with Microsoft Management Console)
- Domain Name Service (DNS) support for SRV (service) records enabling automatic configuration of connections between Windows Messenger 5.1 (or 5.0) and Live Communications Server 2005.

Active Directory Forests and Domains

When the first Active Directory server is created in an organization, the installation process creates the first (primary) domain in the first (primary) forest.

A forest consists of one or more domains that share a common schema, site and replication configuration, and global catalog. Domains within the same forest are automatically linked with two-way, transitive trust relationships. For one forest to trust another forest, an explicit trust relationship must be created.

A domain is a collection of computer, user, and group directory objects that share a common directory database, security policies, and security relationships with other domains. A domain is identified by a Domain Name System (DNS) domain name and each domain requires one or more domain controllers. If an organization requires more than one domain, multiple domains can be created in the primary forest (or a secondary forest).

Network and Active Directory Structures

Microsoft IT deployed an Active Directory design based on a primary forest as the container of user accounts, groups, and resources in the corporate domains controlled by Microsoft IT.

Domains within the primary corporate forest have multiple external trusts to child domains in the product development and test secondary forests. The child domains and secondary forests are used, for example, for developing and testing updated versions of Active Directory and Exchange Server in a production environment.

All of the forests are based on Windows Server 2003 except for one forest that is used for testing backward-compatibility with Microsoft Windows 2000 Active Directory services. Because of this backward compatibility requirement, the trust relationship between the domains in this forest and domains in the primary corporate forest must be configured on a domain-by-domain basis. Kerberos transitive trust exists between the primary corporate forest and the other Windows Server 2003 secondary forests.

The multiple-forest design allows Microsoft IT to centrally manage the network users and resources in the corporate, development and testing forests; while at the same time isolate each environment from Active Directory schema changes being made in the other forests.

Because of the mixed forest environment and the Microsoft IT decision to deploy Live Communications Server 2005 Enterprise Edition using a high-availability configuration in a central resource forest, Microsoft IT needed to configure the new Live Communications Server 2005 director servers to use NTLM authentication.

Background

To better appreciate how Live Communications Server 2005 was deployed at Microsoft, it is useful to understand the background information that drove the planning, design and deployment decisions.

Microsoft Information Technology

Microsoft IT is responsible for driving global operations and delivering information technology services to the entire Microsoft organization. The IT group directs all activities related to running and maintaining Microsoft information systems worldwide: technology infrastructure

and corporate and marketing information systems including production, distribution, and other key internal systems. Microsoft IT works to provide a world-class utility and excellence in business operations through its leadership in the design and integration of company strategies, processes, and architecture.

Microsoft IT provides a full range of services including server- and end-user support, telecommunications management, network operations, and information security. They are responsible for managing connectivity for more than 300,000 devices worldwide. Microsoft IT also ensures that more than 50,000 employees and 20,000 contractors and vendors in over 400 Microsoft locations are able to access corporate network services and resources 24 hours a day, seven days a week, from around the world.

Because the primary business of Microsoft is software design, Microsoft IT has an additional responsibility that is unique among global providers. In addition to running the company's IT utility, Microsoft IT is an early adopter of Microsoft technologies. They are responsible for testing and deploying Microsoft products such as Windows Server 2003, Microsoft Exchange Server 2003, and Microsoft SharePoint® Products and Technologies before these products are released to customers. This process is known by those within Microsoft as "eating our own dog food" or simply "dog-fooding."

Previous Experiences in Deploying Live Communications Server 2003

The Microsoft IT experience in deploying and managing Live Communications Server 2003 greatly influenced how it chose to deploy Live Communications Server 2005.

With Live Communications Server 2003, users were statically assigned to a single home server, and user profile and presence information was stored in the MSDE database on each home server. When a home server was unavailable, users assigned to that server needed to wait for the server to come online before the service was restored. This made it difficult for Microsoft IT to provide a high-availability service.

In addition, the recommended maximum number of users supported per server needed to scale beyond the limit of 10,000 to enable large deployments. Reducing the number of servers is a key factor in reducing overall hardware, software, and operating costs.

Lastly, employees, external organizations, and customers were looking for improved Internet access to the real-time person-to-person communications solution that Microsoft IT operated inside the Microsoft corporate firewall. Real-time presence provides its greatest value when it is easily available all of the time, regardless of whether an employee is connected to the Internet or the corporate network.

The Live Communications Server 2003 setup process also made it difficult for the Active Directory management team to independently plan and deploy the schema extensions required by Live Communications Server. The Live Communications Server 2005 setup program solves this by separating the Live Communications Server 2005 schema extension, installation and activation tasks into distinct, installer-controlled steps.

Microsoft uses multiple forests to separately manage the product divisions, sales and marketing, and product support teams. Implementing multi-forest scenarios with Live Communications Server 2003 was a tedious process requiring schema changes in all forests, and custom identity synchronization solutions to be built using Microsoft Identity Integration Server 2003 (MIIS). More information on the Microsoft IT deployment of MIIS can be found in the IT Showcase white paper *Enabling Cross-Forest Identity Management with Microsoft*

Identity Integration Server 2003 available at http://www.microsoft.com/technet/itsolutions/msit/deploy/cfimwiis.mspx.

Benefits of Deploying Live Communications Server 2005

Microsoft IT was able to address the above issues by deploying the Enterprise Edition of Live Communications Server 2005. The following Enterprise Edition features were key to the successful deployment of a new large-scale, high-availability real-time communications solution at Microsoft.

High Availability Deployment Scenarios

With the release of Live Communications Server 2003, each user was assigned to a specific home server with no support for load balancing or fail-over should one of the home servers become unavailable due to scheduled maintenance or a hardware or software failure.

Live Communications Server 2005 Enterprise Edition provides a new option of configuring multiple front-end servers into a server pool with load balancing and fail-over. Server pools also enable server software upgrades to be implemented on a server-by-server basis without interrupting end-user services.

Support for SQL Server In Addition to MSDE

Live Communications Server 2005 Enterprise Edition uses SQL Server-based databases to maintain user profile information, including a person's contact list and blocked users list. In the 2003 release of the product, database server support was limited to MSDE, which was not scalable, could not be clustered, could not be administered remotely, and was more tedious to backup and restore. Live Communications Server 2003 automatically installed MSDE, and SQL Server was unavailable as a database server option.

Microsoft IT wanted the option of deploying either SQL Server or MSDE. Live Communications Server 2005 Enterprise Edition provides this option by including support for clustered, highly available database servers.

Multiple Forest Management

Deployment of Live Communications Server 2003 in a multi-forest environment like the one at Microsoft presented a number of challenges, including the inability to manage multiple forests from a single administrator logon, and difficulties in moving users from one forest to another.

The 2005 release of Live Communications Server was specifically designed to remove the cross-forest deployment and management barriers found in the earlier version of Live Communications Server through its support of a central resource forest model for large-scale deployments.

External Internet Access without needing a Virtual Private Network Connection

Another lesson learned from the Microsoft IT experience with Microsoft Exchange Server is the need to support remote access to selected messaging services without requiring a user to first establish and log on to a VPN connection.

In Microsoft Exchange Server 2003, this feature is referred to as "RPC over HTTP" (remote procedure call over HTTP"). In Live Communications Server 2005, this is referred to as the "remote user" scenario.

Reduced use of VPN services reduces hardware, software, and operating costs. More importantly, accessing real-time presence information without requiring a VPN provides true real-time indication of availability of the people on a user's contact list.

Project Goals

Microsoft employees are active instant messaging users. They provide a model environment for the Live Communications Server product group to test updated releases of Live Communications Server in a large, worldwide, enterprise setting. A partial list of goals for this deployment of Live Communications Server included:

- Product stability and availability, as measured by days without a priority one failure, and actual versus planned server uptime.
- Usage as measured by number of enabled users, number of concurrent logged-on users, number of concurrent active users, and number of servers deployed or upgraded.
- Manageability, which includes the ability to migrate user information using in-the-box tools and Microsoft Operations Manager (MOM) 2005 support.

In addition, a matrix of tracking metrics is maintained that includes, for example, the total message traffic categorized by the number of messages and data volume, the number of help desk calls, and the number of product group software updates.

A detailed description of the Microsoft IT deployment of Live Communications Server 2005 is provided in the Solution section of this white paper. For readers unfamiliar with the new features found in Live Communications Server 2005, they are described in the next section, Understanding Live Communications Server 2005.

UNDERSTANDING LIVE COMMUNICATIONS SERVER 2005

To understand how Microsoft IT deployed its security enhanced, real-time communications solution, it is important to understand the new deployment and management features in Live Communications Server 2005.

Readers already familiar with these features may choose to skip to the Solution section, which specifically addresses the Microsoft IT deployment of Live Communications Server 2005. Additional information can also be found on the Live Communications Server 2005 Web site at http://www.microsoft.com/office/livecomm.

The previous release of Live Communications Server focused on five key attributes:

- Increase individual productivity using presence, IM and real-time communication capabilities
- Familiar tools for managing users, client software, servers, and network settings
- Extensible, real-time communications platform for custom client- and server-side solution development
- Standards-based signaling and communications protocols based on Session Initiation Protocol (SIP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) protocols
- Integration with the Microsoft Office System

Live Communications Server 2005 builds on these key capabilities to provide new connectivity features and high-availability and scalability options to support large enterprise deployments.

Live Communications Server 2005 is designed to improve business efficiencies by enabling information workers to find and communicate with their colleagues in real time with a security enhanced enterprise-grade environment that is integrated with the Microsoft Office System.

Live Communications Server 2005 is available in two product configurations: Standard Edition and Enterprise Edition. Live Communications Server 2005 Standard Edition is installed as a single-server configuration using MSDE as the local database server; Enterprise Edition offers high-availability and scalability options using multiple front-end servers and SQL Server 2000 as the back-end database server, optionally clustered for high database server availability.

Availability and Scalability

Live Communications Server 2005 Enterprise Edition provides the following enterprise deployment and scalability options:

- Distributed, two-tier architecture for fault tolerance
- Ability to use clustered or unclustered SQL Server 2000 back-end database servers
- Resilient client connectivity that enables Window Messenger clients to automatically reconnect to a different front-end server should the original server become unavailable due to planned or unplanned outages
- Third-party backup and restore support
- Scale-out support from a single server supporting 15,000 users, to server pools supporting more than 100,000 simultaneously active users

- Bandwidth-optimized protocol support
- Storage Area Network (SAN) interoperability

Figure 2 is representative of a typical high-availability Live Communications Server 2005 Enterprise Edition server pool solution that is capable of supporting over 100,000 simultaneously active users. There are three primary server roles in an Enterprise Edition server pool: director servers, front-end servers, and database servers. Additionally, to support external Internet access and inter-organization federation of real-time communications services, one or more Live Communications Server 2005 access proxy servers may be deployed in the perimeter network.

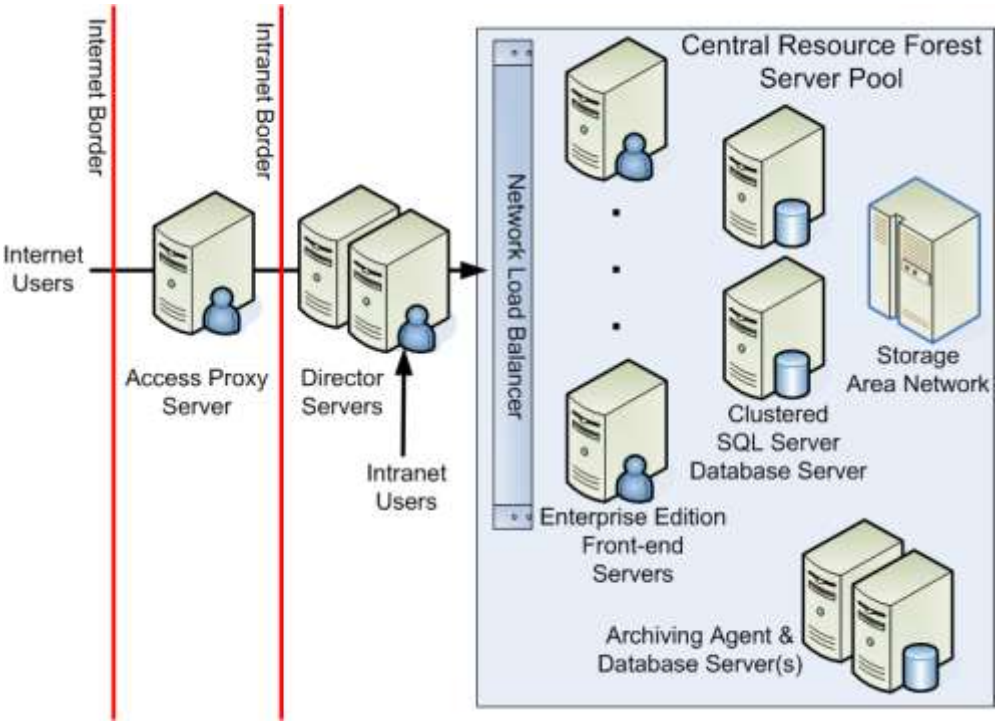

Figure 2. Live Communications Server 2005 high-availability server pool example

SIP and SIMPLE

Session Initiation Protocol (SIP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) are the core protocols used by Microsoft Office Live Communications Server and Windows Messenger for exchanging presence information, initiating real-time audio, video, text, and telephony-based communications sessions; and for exchanging instant messages. SIP and SIMPLE are emerging standards defined by the Internet Engineering Task Force (IETF).

Director Servers

In the high-availability server pool example depicted in Figure 2, the director servers are the first servers to receive SIP message streams from Windows Messenger intranet users or, via a Live Communications Server 2005 access proxy server, Windows Messenger remote users. For intranet requests, the director server redirects users to the server pool. For Internet requests, the director server forwards the SIP message to the appropriate server because Internet users do not have a direct connection to servers in the intranet. During migration to Live Communications Server 2005, director servers enable users to communicate with a mixed Live Communications Server 2003 and Live Communications Server 2005 environment without changing their Windows Messenger configuration.

Front-End Servers and Server Pools

Previously known as “home servers” in Live Communications Server 2003, a front-end server is responsible for handling all communications for a particular group of users. A server pool is a group of front-end servers that appear as a single virtual IP address resource. This is

achieved with a hardware network load balancer. When a director server directs a user to a server pool, it directs the user to the virtual IP address of the network load balancer; which in turn selects the available front-end servers to handle the user connection.

Additional front-end servers can be added to a server pool as required during a phased deployment of Live Communications Server 2005 (or as an organization grows). In addition, the hardware network load balancer enables selected front-end servers–usually one at a time–to be temporarily taken out of service for maintenance or replacement without affecting service levels. Often an additional front-end server is added to the server pool to provide additional capacity to support fail-over in the event of planned or unplanned server outages.

Database Servers

With Live Communications Server 2005 Standard Edition, the database is a local MSDE database service running on each home server. With Live Communications Server 2005 Enterprise Edition, in a typical enterprise configuration, the database server is a SQL Server 2000 server that is both logically and physically separated from the front-end servers. In a high availability scenario, the database server is configured as a two-node active-passive clustered SQL Server database server connected to a shared storage device; typically, a storage-area network (SAN). The latter scenario is depicted in Figure 2.

Access Proxy Servers

Similar in function to Live Communications Server 2003 forwarding proxy servers, the role of an access proxy server in a Live Communications Server 2005 configuration is to act as a secure connection point for remote users as well as users from other selected organizations who have been configured for federated access. A single proxy server can be deployed, or, for a more scalable and highly available remote access solution, multiple access proxy servers can be placed behind a network load balancer.

Access proxy servers check that the inbound message headers are valid (including the destination domain) and mark each message as originating from outside the firewall. Messages from an access proxy server are sent to a director server. Messages are then forwarded to a Live Communications Server Standard Edition server or Enterprise Edition server pool. This deployment model can support very large traffic volumes more easily and provides for authentication on the access proxy server.

Archiving Agent and Database Servers

Microsoft IT configured one archive agent server and one archive database server as part of its production Live Communications Server 2005 environment. The archiving database server uses the SAN environment to store statistics collected by the archiving service. Microsoft IT chooses not to archive message content.

Microsoft IT uses the data to analyze the Live Communications Server 2005 environment. The archived data is not stored for long-term retrieval. In addition, deployment of the archiving infrastructure was an important part of the Live Communications Server testing effort.

Internet Access and Federation between Organizations

Many enterprise users and users of public instant messaging services use IM to communicate and stay in touch with fellow employees, customers, friends, family members,

and other associates. Live Communications Server 2005 helps IT departments manage these diverse needs by supporting:

- More secure, inter-enterprise federation of real-time presence and communications
- Managed access to public instant messaging services
- Real-time communications clearinghouses.

Federation enables a trust to be established between two organizations that allow presence and instant messages to be freely but more securely exchanged between the Live Communications Server 2005 infrastructures running in each organization. Access proxy servers run in the perimeter network to verify each incoming request. Depending on whether a server pool or individual home server approach is used to deploy Live Communications Server 2005, the incoming request will be directed to a director server or front-end server.

Performance and Capacity Planning

Microsoft IT found that Live Communications Server 2003 was able to support a maximum of 10,000 active users on a single home server using MSDE. The Microsoft IT goal was to support 15,000 active users per server using the front-end server pool and clustered back-end database deployment model available in Live Communications Server 2005 Enterprise Edition.

Using Live Communications Server 2005 Enterprise Edition, a single server running with a separate SQL Server back-end database server can be expected to support approximately 15,000 to 20,000 active users; or over 100,000 simultaneously active users in a server pool consisting of five front-end servers and a separate clustered SQL Server back-end database server. Product group testing has found CPU utilization is typically much lower with Live Communications Server 2005 and user logons execute much faster because of protocol optimizations that reduce the number of round trips to the server.

In addition, the support for real-time communication services that is built into Microsoft Office 2003, Windows SharePoint Services, and SharePoint Portal Server 2003 must also be considered. After the deployment of Live Communications Server, Microsoft Office System users are able to see presence information for other enterprise users and can send an instant message from within an Office application such as Microsoft Outlook and Microsoft Word, and from within Web sites created through Windows SharePoint Services. This causes additional load on the front-end servers and needs to be taken into account during capacity planning (the 15,000 active users per Enterprise Edition server accounts for this additional load).

SOLUTION

The planning and deployment of Live Communications Server 2005 to create a security enhanced, real-time, person-to-person communications solution occurred in six stages. In addition to the project goals discussed earlier, Microsoft IT defined the following four objectives for this project:

- Deploying Live Communications Server 2005 using a central resource forest deployment model.
- Ensuring that previous versions of Live Communications Server can co-exist and interoperate with Live Communications Server 2005 Standard Edition servers and Live Communications Server 2005 Enterprise Edition server pools. This objective is important for many Microsoft customer upgrade and co-existence scenarios and is a specific requirement for upgrading the Microsoft IT Live Communications Server 2003 deployment.
- Giving users the ability to retain their individual contacts list and a blocked users list after migrating from the 2003 to the 2005 release of Live Communications Server.
- Reusing existing server hardware that continued to meet the Live Communications Server 2005 prerequisites.

The six major stages that Microsoft IT used to plan its deployment of Live Communications Server 2005 were based on the work that needed to be accomplished, and the effect that the work would have on the groups of users targeted by each stage. As exit criteria, each stage needed to be executed completely and successfully before the project could advance to the next stage. The following is a brief description of each of the six stages that Microsoft IT used for the deployment phase of this project:

1. **Preparation.** The basic components of the new Live Communications Server 2005 environment were put in place. These included: deploying a central resource forest to host the Live Communications Server 2005 server pool; deploying the 2005 Active directory schema extensions; installing and configuring the SQL Server database server cluster (including a dedicated SAN); and installing a single Live Communications Server 2005 Enterprise Edition front-end server. Selected users from Microsoft IT were enabled for this environment so they could test each of the 2003 and 2005 interoperability scenarios.
2. **Server Pool Deployment.** Extend the server deployment to add Live Communications Server 2005 Enterprise Edition servers in the server pool as users were migrated from Live Communications Server 2003 infrastructure. Users from three of the smaller Active Directory forests were migrated to the Live Communications Server 2005 central resource forest during this stage.
3. **User Mass Migration.** Having tested and verified the interoperability between the 2003 and 2005 releases of Live Communications Server, the migration of the remaining large forests was undertaken.
4. **Live Communications Server 2003 Cleanup.** This stage involved: removal of the remaining Live Communications Server 2003 environment; updating of the performance log data monitoring and gathering processes; and updating the installation, disaster recovery, and troubleshooting and operations guides for the new Live Communications Server 2005 environment.

5. **Test Server Deployment.** In preparation for production testing of the ongoing deployment of product updates, a Live Communications Server 2005 Standard Edition server was deployed. Selected users from Microsoft IT and the Live Communications Server product group were migrated from the Enterprise Edition server pool to the new Standard Edition production test server.

6. **External Internet Access.** An external director server dedicated to the access proxy server was deployed to provide remote access for employees and selected external customers and contacts, without having to go through a VPN.

Overall, the strategy consisted of a side-by-side installation and configuration of Live Communications Server 2005 with the predecessor release followed by the migration of successive groups of users to the new platform.

Planning

To provide continuous instant messaging service during the deployment of Live Communications Server 2005, and to accommodate the new two-tier, server-pool deployment model, Microsoft IT was required to deploy the Live Communications Server 2005 server pool and then migrate the 2003 users. When no longer needed, the 2003 servers would then be erased, rebuilt, and redeployed within one of the data centers at Microsoft.

Active Directory Planning

Live Communications Server requires that Active Directory provide optimal security and manageability of servers and clients. Live Communications Server supports Active Directory on either Windows 2000 Service Pack 3 (SP3) or Windows Server 2003. However, for multiple-forest organizations, all forests must be pure Windows Server 2003 forests to provide cross-forest Kerberos authentication.

If an organization does not have all Windows Server 2003 domain controllers in a forest, the initial authentication from the Windows Messenger client may fail. The solution is to configure Live Communications Server to use NTLM authentication on director servers. In this scenario, after the client is authenticated as an end user through NTLM, the front-end server directs the client to the appropriate server pool server.

The Live Communications Server database minimizes the impact on domain controllers. The only cases in which Live Communications Server communicates with a domain controller are as follows:

- Full Active Directory synchronization during initial server start-up
- Incremental synchronization when Active Directory is updated. Active Directory is checked approximately every five minutes and has little impact on domain controllers after the initial server start-up
- When a user is provisioned for real-time communications services
- At initial logon to the Live Communications Server service, when the client is authenticated

With Live Communications Server 2005 Enterprise Edition, Microsoft IT was able to deploy its internal real-time communications service as a high-availability solution in the central corporate forest. This implied that Microsoft IT was able to limit the deployment of the Live Communications Server 2005 Active Directory schema extensions to the central corporate

forest (and not deploy the schema extensions across the secondary product development and test forests).

Domain Name Service Planning

Microsoft IT used automatic, rather than manual, configuration of Windows Messenger clients. Microsoft IT set up automatic configuration at the time Windows Messenger was installed, and then configured the Domain Name Service (DNS) service to support the use of automatic configuration for the Live Communications Server namespace.

When an organization uses automatic configuration of the client, the client looks up a DNS service location (SRV) record for the Live Communications Server service. The DNS SRV record has the effect of mapping the namespace of the Live Communications Server service to a specific server name and TCP/IP port number.

When the Windows Messenger 5.1 client starts, it performs a DNS SRV record lookup based on the namespace in the user's SIP communications server account. For example, for a user logging into the contoso.com namespace, Windows Messenger uses the following convention to look up the name of the Live Communications Server DNS SRV record:

```
_sip._tls.contoso.com
```

The DNS SRV record lookup returns the DNS name of the server, server pool, or director server that the Windows Messenger user is to connect to as well as the TCP/IP port to be used (typically, port 5061 for encrypted TLS connections and port 5060 if unencrypted TCP/IP connections are used).

If the DNS SRV record is not available, the client performs a conventional DNS lookup for a server name comprising "sip." followed by the namespace of the user's account. Using the above example, the DNS "A" record would be named:

```
sip.contoso.com
```

Once the DNS name and port have been resolved, Windows Messenger is then able to connect to the Live Communications Server 2005 services.

Automatic configuration gives greater flexibility in managing the servers to meet the needs of the users and the environment while decreasing client management and operations costs.

Configuring DNS for Remote User and Federated Access

To support federated access via a Live Communications Server 2005 access proxy, a conventional DNS "A" record for the access proxy server needs to be configured in the organization's external DNS server. Typically, the name of the DNS record is same as the internal name (for example, sip.contoso.com). TLS (and MTLS) encrypted connections are established using the default port 5061.

To support remote user connections to the central resource forest server pool at Microsoft, Microsoft IT chose a slightly different approach. Microsoft employees are often mobile users working from customer offices and home offices. In these environments, port 5061 is often blocked by the local firewall while port 443, the default port used for Secure HTTP (HTTPS) access, is left open. To address this situation, Microsoft IT configured the Live Communications Server 2005 access proxy server (and the corresponding external DNS SRV record) to use port 443 rather than the default port 5061. TLS is used to encrypt these remote user connections.

Certificate Services

To ensure that TLS can be used as the transport protocol by Live Communications Server 2005, an organization must have a public key infrastructure (PKI) available. Certificates are used to initiate a TLS connection between the server and the client. Because Microsoft already deployed an internal PKI based on Windows Server 2003 certificate services, Microsoft IT used the automatic enrollment features of Microsoft Windows to obtain certificates for the servers running Live Communications Server. Automatic enrollment allows each server to automatically request and receive its certificate from the enterprise certificate authority (CA) as soon as the server joins the domain.

Because every server and every client at Microsoft is automatically enrolled and receives a certificate when it joins a Microsoft IT-controlled domain, no additional work was required for certificates. That is, Live Communications Server does not require the explicit creation of special certificates. Live Communications Server uses certificates that meet the following requirements:

- The certificate must enable client and server authentication.
- The certificate must contain the fully qualified domain name (FQDN) of the server.

In the Live Communications Server architecture, the underlying operating system caches certificate information for the clients and servers.

Network Capacity Planning

Live Communications Server consumes, on average, 1.6 kilobits per second (Kbps) of network bandwidth per user over an eight-hour period for presence and instant messaging traffic. Microsoft IT arrived at this value based on previous Live Communications Server product group testing. This value was sufficient to convince Microsoft IT that it was able to centralize the deployment of its Live Communications Server servers, because the high-bandwidth connections between the Redmond data center and the regional data centers had sufficient capacity to handle the traffic across wide area network (WAN) links. Network data compression helped reduce the bandwidth used by the real-time communications services.

Microsoft IT recognized that a centralized model would increase overall logon time when a user logged on to a server. However, the measured increase in logon time was a fraction of a second and was not noticeable to users. The centralized model offered more tangible cost savings benefits through simplified management.

Security Planning

Microsoft IT increased the security of the Live Communications Server service by deploying Windows Messenger 5.1 with high-security mode enabled, and by disabling all transport modes except for TLS.

With the preceding settings and high-security mode on the client, behavior in the Microsoft environment is as follows:

- TLS encrypts information between servers and clients across TCP/IP ports. The default communications protocol in Live Communications Server is unencrypted TCP.

  Note: *On the server side, Microsoft IT configured mutual TLS (MTLS) to encrypt information that travels between servers.*

- Live Communications Server requires Kerberos or NTLM authentication. Kerberos is the default authentication method for Live Communications Server. For backward compatibility with Windows 2000–based computers maintained by Microsoft test and product support teams, Microsoft IT uses NTLM for authentication on front-end servers. If only Kerberos were used on the front-end servers, security would be improved but users in a Windows 2000 forest would not be authenticated.
- Universal Plug and Play for network translation tables, which is dependent on unauthenticated HTTP protocols, is disabled on the client.
- Peer-to-peer connections are disabled for all IM sessions. This forces all communications, including audio/video and data collaboration session invitations, to be routed through Live Communications Server. Allowing instant messages to go directly from one client to another creates a security risk because instant messages cannot be archived and cannot be scanned for inappropriate uses.
- Audio/video conferencing and data collaboration sessions themselves still use peer-to-peer connections after the initial invitation has been accepted.

High-security mode contains optional features, such as disabling connectivity to the .NET Messenger Service and Exchange IM. However, Microsoft IT did not disable the .NET Messenger Service on the client pending the selection of alternative means for providing Microsoft employees with access to family members on public instant messaging networks.

In addition to the preceding security considerations, an organization can use Group Policy to require audio and video encryption. Microsoft IT did not use this configuration because audio and video encryption increases the time needed to set up a conference. In this case, Microsoft IT was more concerned about the user experience than the security of the connection. Because the data traverses only the internal network, there is little risk of someone being able to reconstruct individual network packets for an audio or video communication.

This is in addition to the Microsoft IT deployment of IPSec to support network domain isolation. For more information on the enterprise wide deployment of IPSec at Microsoft, refer to the Microsoft IT Showcase white paper Improving Security with Domain Isolation: Microsoft IT Implements IP Security (IPSec) available at http://www.microsoft.com/technet/itsolutions/msit/security/ipsecdomisolwp.mspx.

Communications Plan

All Microsoft IT employee communications regarding the ongoing software deployments are coordinated by and originate from a dedicated client services team in Microsoft IT. This ensures that employees receive e-mail messages from Microsoft IT that are of a consistent quality, and are properly timed and coordinated with other Microsoft IT projects that also need to communicate their plans and needs to Microsoft employees.

For the Live Communications Server 2005 migration, e-mail notifications were used to advise employees when the migration would affect them individually, the location of the end user support help page, and how to contact Helpdesk if they have any further questions or issues.

Microsoft IT creates an end-user support Web page for each product it supports (including Windows Messenger and services provided by the deployment of Live Communications Server 2005). This Web page includes a list of frequently asked questions (FAQs), additional self-help and troubleshooting information, and a link to the internal software distribution

servers where Microsoft employees can download and install the latest version of Windows Messenger.

Architecture

Microsoft IT took advantage of a key enterprise deployment feature in the release of Live Communication Server 2005: the ability to deploy a high-availability server pool using a central resource forest deployment model.

Central Resource Forest Deployment Model

From an Active Directory perspective, the Live Communications Server 2005 server pool was deployed into a central resource forest (the Microsoft corporate forest). This is where the greatest number of user objects had been created. Microsoft IT enabled Live Communications Server features for every user object that was e-mail enabled. If the e-mail enabled user object was already in the central resource forest, the central resource forest user object was enabled for real-time communications services.

If an e-mail enabled user object is in one of the secondary forests, Live Communications Server 2005 supports using an Active Directory contact object in the central resource forest as a user principal. Microsoft IT used Microsoft Identity Integration Server 2003 (MIIS) to automate the creation and synchronization of the central resource forest contact objects with the user objects in the secondary forests.

Previously known as Microsoft Metadirectory Services (MMS), MIIS is a centralized service that stores and integrates identity information for organizations with multiple directories. The goal of MIIS is to provide organizations with a unified view of all known information identifying users, applications, and network resources. MIIS helps improve productivity, reduce security risk, and reduce the total cost of ownership associated with managing and integrating identity information across the enterprise.

The process flow for exporting secondary forest/child domain user objects and the creation of the corresponding central resource forest contact objects is illustrated in Figure 3. MIIS selects the user object information from the secondary forests and creates the contact objects in the central resource forest. One-way trusts must be created from the central resource forest to each of the secondary forests if they do not already exist.

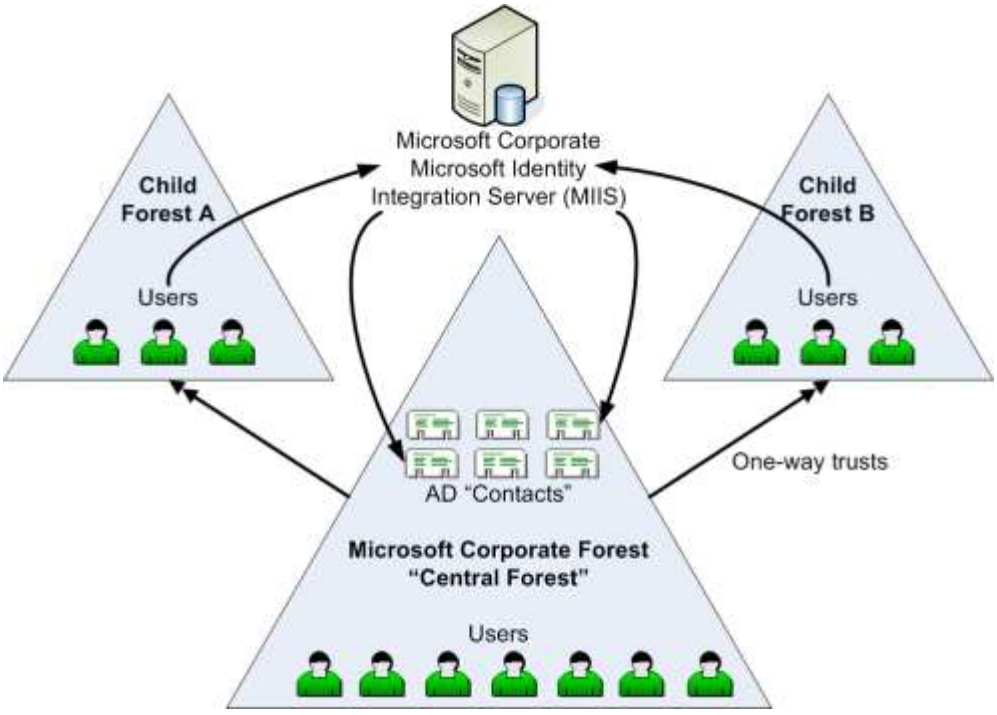

Figure 3. Microsoft IT Live Communications Server 2005 cross-forest topology

Server Pool Architecture

The Live Communications Server 2005 server pool architecture deployed by Microsoft IT is illustrated in Figure 4. Having all Microsoft employees and contractors configured in the central resource forest as either local user objects or imported contact objects is sufficient for Live Communications Server 2005 to provide security enhanced, real-time presence and communications services to all users regardless of their home domain. This centralized, highly scalable design eliminated the need to deploy separate Live Communications Server servers into each secondary forest or child domain.

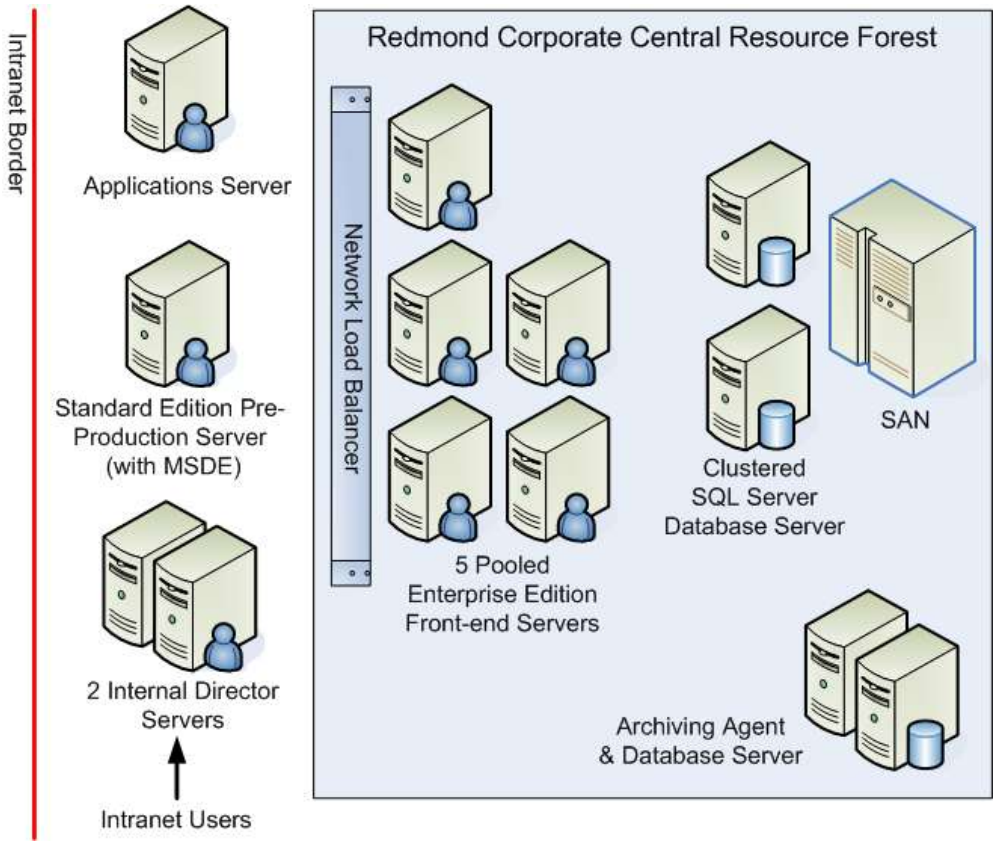

Figure 4. Microsoft IT Live Communications Server 2005 server pool architecture

The Live Communications Server 2005 applications server included in Figure 4 hosts custom server-side code that allows applications to intercept and reroute IM messages intended for application agents (rather than the Windows Messenger client). Microsoft IT developers use the Standard Edition applications server to test and support new applications.

Remote User Access and Federation between Organizations

To support the communication of presence information and instant messages between Microsoft employees working inside the Microsoft firewall with employees and other contacts working outside the firewall, Microsoft deployed the Live Communications Server 2005 remote user and federated access architecture depicted in Figure 5.

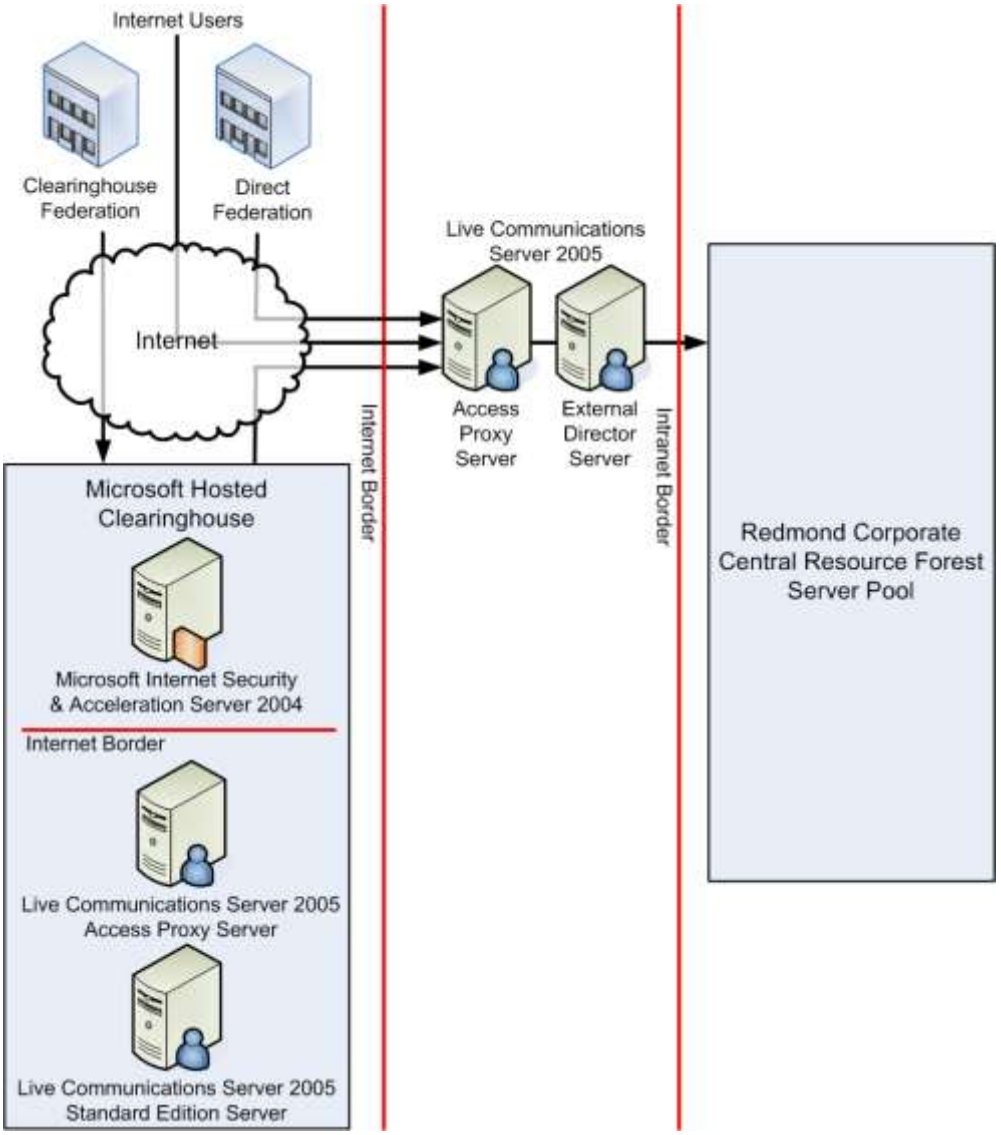

Figure 5. Remote user and federated access physical architecture

This environment supports three types of external communications:

- External Internet access by Microsoft employees working at customer and other business locations and home offices using a conventional personal computer.
- Direct federation enabling the deployments of Live Communications Server 2005 in selected Microsoft customer and other external organizations to exchange presence information and instant messages directly with the Microsoft IT Live Communications Server 2005 access proxy server. Microsoft IT configures direct federation with specific organizations based on business needs.
- Clearinghouse federation enabled through the deployment of a Live Communications Server 2005 clearinghouse on the Internet. Microsoft piloted a clearinghouse for organizations running pre-release versions. Ultimately, third-party service providers may

choose to provide instant message and presence services based on the clearinghouse federation model.

Remote User Access

Remote access by Microsoft employees is enabled using direct TLS access to the Microsoft IT Live Communications Server 2005 access proxy server shown in Figure 5. The access proxy server forwards presence information and instant messages generated by Windows Messenger to the external director server. The external director server then forwards these messages to the two internal director servers in the central resource forest server pool (Figure 4).

Direct Federation

With direct federation, the Live Communications Server 2005 access proxy servers from two different organizations are configured to use a trusted MTLS connection to connect their internal deployments of Live Communications Server 2005.

To simplify configuration of the Live Communications Server 2005 access proxy servers in each organization, Microsoft used server certificates from a public certificate authority (CA) to configure the MTLS connections. In addition, Microsoft IT ensured that the access proxy and external director servers were configured as follows:

- The Windows Server 2003 servers were installed as "workgroup" servers (and not members of a domain) to avoid any issues that might result from auto-enrollment.
- For security reasons, port 5061 (the port that Live Communications Server uses for exchange SIP messages) and port 443 were the only TCP/IP ports enabled on the access proxy server network interface cards.

Clearinghouse Federation

When several organizations want to federate their Live Communications Server 2005 environments, the pair-wise configuration of each MTLS connection between the access proxy servers in each organization can be tedious to set up and manage. Clearinghouse federation is an alternate Live Communications Server 2005 deployment strategy that simplifies the configuration and maintenance tasks when several organizations want to exchange real-time presence information and instant messages.

A Live Communications Server 2005 clearinghouse is an external Live Communications Server 2005 deployment that is directly connected to the Internet. The clearinghouse hosted at Microsoft consisted of one Live Communications Server 2005 Standard Edition server, one access proxy server, and one Microsoft Internet Security and Acceleration 2004 server.

Once the clearinghouse infrastructure was deployed, Microsoft IT configured its Live Communications Server 2005 access proxy server to trust incoming connections initiated by the clearinghouse. Similarly, the clearinghouse was configured to trust connections initiated by the Microsoft IT access proxy server. Selected external contacts and customers were then invited to configure their access proxy servers to connect to the clearinghouse. To configure the clearinghouse access proxy server, Microsoft created the trusted connections for each organization using the server certificates provided by each organization. As Microsoft IT found with its experience with direct federation, the simplest approach was for each organization to request its server certificates from the same public CA. This eliminated the additional step of insuring that the appropriate root certificates had been installed in the access proxy server in each organization.

Controlling Federated Access

Control over whether a particular organization or clearinghouse is allowed to access the Microsoft IT Live Communications Server 2005 access proxy server is established when the federated connection is created by Microsoft IT. After an external organization is configured for direct federation with the Microsoft IT Live Communications Server 2005 access proxy server, each user in the organization's namespace that is enabled for federated access is allowed to add Microsoft employees to their contact lists, exchange presence information and send instant messages to each other. External contacts must know the SIP address of the Microsoft employee they want to contact; they are not permitted to search the internal directory of Microsoft employees.

Similar to the direct federation scenario, when a clearinghouse is configured for federation with the Microsoft IT Live Communications Server 2005 access proxy server, all of the federation-enabled users of organizations federated with the clearinghouse are allowed to interact with federation-enabled employees at Microsoft. However, it is possible for Microsoft IT (or any organization federated with the clearinghouse) to configure their Live Communications Server 2005 access proxy server to block specific namespaces (Internet domains) from connecting through their local access proxy server. This is especially useful in the clearinghouse scenario where an organization might want to block access from one or more of the clearinghouse participants.

Deployment

This section describes the Microsoft IT experience deploying the Live Communications Server 2005 server pool architecture depicted in Figure 4, and migrating from the existing Live Communications Server 2003 to Live Communications Server 2005.

The key steps that Microsoft IT included in its Live Communications Server 2005 deployment process can be summarized as follows:

- Select the forest to be used as the central resource forest, and extend the Active Directory schema using the Live Communications Server 2005 setup wizard
- Set up the Live Communications Server 2005 front-end server pool, initially with one front-end server, and the clustered SQL Server back-end database server and SAN
- Configure MIIS Live Communications Server synchronization
- Export users' Live Communications Server 2003 data from secondary forests
- Import users' data into central resource forest contact objects
- Rehome contacts in central resource forest
- Disable Live Communications Server 2003 user object in secondary forests
- Decommission and recycle existing Live Communications Server 2003 servers
- Clean up Active Directory contact objects and Live Communications Server 2003 attributes from secondary forest user objects

Server Hardware

Microsoft IT used server hardware configurations that were based the Microsoft IT standard configurations that most closely matched the hardware requirements for Live Communications Server 2005.

Table 1. Microsoft IT Deployed Server Hardware

Server Role	Configuration
Access Proxy Server	Dual Intel Xeon 3.06 GHz, 1 MB Cache, 533 MHz FSB 2 GB DDR 266 MHz RAM 2 x 18 GB HDD (15,000 RPM SCSI), 2 GB Network Interface Card (NIC) Windows Server 2003 Service Pack 1* Live Communications Server 2005 (Access proxy server setup option)
Director Server	Dual Intel Xeon 3.06 GHz, 1 MB Cache, 533 MHz FSB 2 GB DDR 266 MHz RAM 6 x 18 GB HDD (15,000 RPM SCSI) 100 MB Network Interface Card (NIC) Windows Server 2003 Service Pack 1* Live Communications Server 2005 Standard Edition
Pooled Front-End Server	Dual Intel Xeon 3.06 GHz 1 MB Cache 533 MHz FSB 2 GB DDR 266 MHz RAM 4 x 18 GB HDD (15,000 RPM SCSI), 100 MB NIC Windows Server 2003 Service Pack 1* Live Communications Server 2005 Enterprise Edition
Back-end Database Server Node	Quad Intel Xeon 2.3 GHz 1 MB Cache 533 MHz FSB 5 GB DDR 266 MHz RAM 2 x 34 GB HDD (15,000 RPM SCSI), 1 GB NIC Windows Server 2003 Server Pack 1* SQL Server 2000 Server Pack Service Pack 3a
Archiving Database Server	Quad Intel Xeon 2.3 GHz 1 MB Cache 533 MHz FSB 5 GB DDR 266 MHz RAM 2 x 34 GB HDD (15,000 RPM SCSI), 1 GB NIC Windows Server 2003 Service Pack 1* SQL Server 2000 Service Pack Service Pack 3a (connected to SAN for storage)
Archiving Agent Server	Dual Intel Xeon 3.06 GHz 1 MB Cache 533 MHz FSB 2 GB DDR 266 MHz RAM 2 x 18 GB HDD (15,000 RPM SCSI), 2 GB NIC Windows Server 2003 Service Pack 1* Microsoft Message Queuing (MSMQ) Services

*** Microsoft IT was beta testing a pre-release version of Service Pack 1 for Windows Server 2003 as part of its deployment of Live Communications Server 2005. Windows Server 2003 Service Pack 1 is not required for customer deployments of Live Communications Server 2005.**

Central Resource Forest Active Directory Synchronization

The following table is the list of Live Communications Server 2005 directory attributes that required synchronization between the secondary forests and the central resource forest.

Table 2. Live Communications Server 2005 Active Directory Attributes

Active Directory Attribute	Description
msRTCSIP-UserEnabled	User is enabled for live communications services
msRTCSIP-FederationEnabled	User is enabled to communicate with users in other organizations that have established a Live Communications Server federated trust
msRTCSIP-InternetAccessEnabled	User is enabled for Internet access (without a VPN connection)
msRTCSIP-PrimaryHomeServer	Domain name of server and service for this user: single server (Standard Edition) or server pool (Enterprise Edition)
msRTCSIP-PrimaryUserAddress	SIP URI (SIP universal resource identifier)
msRTCSIP-OriginatorSid	NTLM authoritative object security identifier SID (maps contact or disabled user account in central resource forest to the authoritative user principal account)
proxyaddresses	Proxy addresses

Microsoft IT used MIIS to perform the synchronization of user objects in the secondary forests with the MIIS database and subsequently, from the MIIS database to the Active Directory contact objects in the central resource forest.

Operations

The Communications Operations group performs routine tasks for maintaining Live Communications Server. For example, Communications Operations collects daily counters that monitor key functions of servers to determine the load on those servers. Other routine maintenance tasks include backing up the servers and examining available disk space, memory usage, and processor performance. These tasks are similar to the operations of other IT services deployed at Microsoft.

Support Structure

When a problem with a server running Live Communications Server is identified at Microsoft, the problem is escalated through the Microsoft organization as follows:

- **Tier 1, Helpdesk.** Most issues are discovered through the MOM infrastructure. However, if the server owner or a user identifies the problem, he or she contacts Helpdesk.
- **Tier 2, Support Services and Client Services.** Support Services uses MOM alerts proactively to monitor servers for problems so that it may identify a problem before Helpdesk is notified. However, if the server owner or a user identifies server or client problem and contacts Helpdesk, Helpdesk then contacts client services for further action. A service request can then be opened and managed through to resolution.
- **Tier 3, Communications Operations.** Communications Operations receives server and client issues that are not covered by the support materials used by Tier 2. In addition, Communications Operations resolves problems and closes service requests for issues that are covered by—but cannot be resolved by—Tier 2.

- **Tier 4, Infrastructure Engineering.** Communications Operations can contact Infrastructure Engineering if resolving the problem involves modifying the IT architecture, or hardware or software standards. If necessary, Infrastructure Engineering can in turn contact the product development group to discuss possible improvements to the product.

Microsoft has four service level agreement (SLA) response times in place to resolve issues for any service. These response times, shown in the following table, apply across all tiers of support.

Table 3: SLA response times for resolving service issues at Microsoft

Priority	Definition	Time to resolve
Immediate	Meets one or both of the following criteria: Any unplanned outage that affects 50 percent or more of a site, IT service, or non-redundant critical IT device. Any unplanned outage that affects 50 or more clients/customers.	4 hours
High	Meets one or more of the following criteria: Any unplanned outage that affects less than 50 percent of a site, IT service, or non-redundant critical IT device, but is not a single user issue. Any unplanned outage that reduces the redundancy of an IT service or server/device by 50 percent or more. Any unplanned outage that affects fewer than 50 clients or customers but is not a single user issue.	12 hours
Normal	Meets one or both of the following criteria: Any unplanned outage that reduces the redundancy of an IT service or server/device by less than 50 percent. Any unplanned outage that affects a single client or customer.	72 hours
Low	A task and/or preventive maintenance that can be completed as time permits because user impact may not exist. Examples include requests for information, scheduled work, and preventive maintenance that is invisible to the customer.	No limit

Training of Client Support Personnel

During the early-adopter deployment of Live Communications Server at Microsoft—before training material for client support personnel was released to the public—Communications Operations held training sessions with the client services team for the issues unique to Tier 2 of the escalation hierarchy. In general, client services deals with account problems (such as issues in Active Directory) that prevent a user from using services such as Live Communications Server.

To ensure that Helpdesk personnel were prepared to handle user issues related to Windows Messenger 5.1, the Communications Operations group held a separate training session with Helpdesk subject matter experts (SMEs). The SMEs then trained their own staff to support Windows Messenger 5.1.

Communications Operations created a troubleshooting guide for Tier 1 and Tier 2 Helpdesk staff to use in handling client-side issues.

Operations Support

Once fully deployed, the Live Communications Server central resource forest consisted of seven servers and supported approximately 80,000 enabled accounts at Microsoft. The solution is monitored and maintained by a senior operations analyst on the Microsoft IT Communications Operations team. The senior operations analyst relies on the Microsoft IT data center infrastructure for server backup services, first- and second-level Helpdesk services, and basic server monitoring.

The senior operations analyst uses the Live Communications Server 2005 Microsoft Operations Manager 2005 (MOM) management pack to configure a MOM console for monitoring and tracking key operational metrics. All third-level support problems and solutions are documented on an internal Microsoft IT site available to Tier 1 and 2 Helpdesk personnel.

Server Monitoring

At Microsoft, Microsoft Operations Manager (MOM) is used to manage the server tier of a computer infrastructure, including core services such as Active Directory, DNS, and dynamic host configuration protocol (DHCP). MOM collects, in a central SQL Server database, predefined events from event logs on thousands of servers. MOM also runs health-monitoring scripts on many servers. In response to the most important events, MOM creates alerts that are routed to central consoles. In addition, MOM collects performance data from all managed servers and raises alerts for performance threshold exceptions.

Live Communications Server 2005 includes a Microsoft Operations Manager 2005 (MOM) management pack that allows the service to be centrally monitored in a similar manner through the MOM application. MOM provides useful operations manageability information. For example, it provides alerts when a server goes offline and can show the number of users logged on to the Live Communications Server service at a given time.

Note: *To obtain the MOM management pack for Live Communications Server, an organization must license both MOM and Live Communications Server. The management pack is then available from the download area of the MOM Web site: http://www.microsoft.com/mom/downloads/default.asp.*

Most of the time, MOM catches potential problems and sends alerts to the server support team; the server support team escalates issues to Communications Operations when the Tier 1 and 2 support documentation doesn't list a resolution for a particular issue.

Public views provide a graphical representation of the health of home servers, which affects how the service functions. The MOM management pack for Live Communications Server contains three public views:

- **Logged-On End Points.** This view is represented by one counter, which shows the number of users currently logged on to the service.
- **Machine Health.** This view is represented by two counters, which provide processor data and paging data. The processor data indicates how much load the processor is handling, which can help MOM operators determine whether more users can be added to the server. The paging data indicates whether the server has sufficient RAM.
- **Connection Health.** This view is represented by three counters: Flow-Controlled Connections, Queue Depth, and Average Holding Time for Incoming Messages. Flow-

Controlled Connections is the number of client connections for which the server is restricting messages, which (if it ever exceeds zero) can indicate the need to reduce the number of users assigned to that server. Queue Depth indicates whether the server is queuing requests, which can cause delays in the service and is an area of concern if the value is greater than zero for an extended period (in general, more than 30 seconds). Average Holding Time for Incoming Messages shows the average number of seconds that each incoming message spends in the server until it is handled, which can indicate delays in the clients and the need to reduce the number of users assigned to that server.

Communications Operations also works with teams that support and manage elements of the Microsoft environment that are not usually directly related to Live Communications Server, but that can be in certain situations. For example, when the network group receives a MOM alert for a major network outage between two data centers, it notifies Communications Operations about that alert because the Live Communications Server service may be affected.

Similarly, if the infrastructure support team encounters an issue in which replication of information in Active Directory is taking longer than the SLA requires, it sends that alert to the Communications Operations team. Even though the Active Directory issue may not affect Live Communications Server service immediately, this kind of communication can prepare Communications Operations for service requests that may appear in the near future, when people who were enabled for the service are unable to log on. Proactive communication throughout an organization helps maintain the services that employees use regularly.

The MOM management pack for Live Communications Server does not provide server statistics such as the number of text messages, audio messages, video messages, short- and long-distance communications at a given time. As part of Microsoft IT 's role of testing and troubleshooting Microsoft products, Microsoft IT uses alternative methods such as Windows performance monitor and the Live Communications Server archive logs to collect and analyze performance and operation data from services that are being tested. Product development groups, such as the one for Live Communications Server, use this data to improve their products.

Backup, Restore and Recovery

Performing regular backups is an important part of Live Communications Server daily operations and is the first step in the preparation for a disaster recovery scenario. An organization must also plan for, and practice, restoring and recovering those backups. The following sections represent the backup, restore, and recovery procedures in place for the components of the Live Communications Server 2005 architecture at Microsoft.

Live Communications Server 2005 Access Proxy Servers

Access proxy servers do not maintain any application state or user data. Backup procedures are limited to backing up the machine system state. Outside access from the Internet to the internal IM environment is not considered a mission-critical service. In a worst case scenario, recovering an access proxy server involves Microsoft IT re-imaging a replacement Windows Server 2003 server, re-installing Live Communications Server 2005 using the access proxy server setup option, and then restoring the machine system state. This approach assumes that the replacement server has the same server machine name as the previous server.

Live Communications Server 2005 Director Servers

Director servers maintain a database of user information to enable user authentication of new user sessions. No additional application or session data is maintained on the server. During a recovery scenario, the director server automatically rebuilds this database when it is installed and configured into the existing environment. Microsoft IT only backs up the machine system state on its director servers.

Live Communications Server 2005 Enterprise Edition Server Pools and Database Servers

All Live Communications Server 2005 application state and user information is maintained by the clustered SQL Server database servers, and the SQL Server database file resides in the dedicated partition on the server pool SAN.

Microsoft IT uses SQL Server 2000 to schedule a snapshot daily backup of the individual Live Communications Server 2005 databases. The backup files are written to another partition on the server pool SAN where they are subsequently backed up from disk to tape by the standard Microsoft IT backup service.

A front-end server running Live Communications Server 2005 Enterprise Edition in the central resource forest pool can be recovered by simply replacing it with a newly installed front-end server and configuring into the hardware load balancer and the central resource forest server pool. As mentioned earlier, Microsoft IT included an additional front-end server in the central resource forest server pool (beyond what was indicated from a capacity planning perspective) to provide additional capacity for planned and unplanned outages (including rolling upgrades of the individual front-end servers).

In addition, a custom script is scheduled to run each morning and each evening that uses the Live Communications Server 2005 DBImpExp utility to back up each user's contact list to an XML file. This enables a single user's contact list to be quickly restored without having to do a full database restore from tape.

Live Communications Server 2005 Archiving Agent and Database Servers

The role of the archiving agent and database servers is primarily for metrics gathering and are not considered mission-critical by Microsoft IT Communications Operations. Except for the machine system state, no other data is backed up on the archiving servers.

CONCLUSION

The Microsoft IT deployment of a security enhanced, real-time, person-to-person communications solution based on Live Communications Server 2005, Windows Server 2003, Active Directory, and Microsoft Identity Integration Server has provided Microsoft employees, Microsoft IT, and the Live Communications Server 2005 product group with specific benefits listed in the next section.

Benefits

The deployment of Live Communications Server 2005 Enterprise Edition at Microsoft resulted in the following benefits.

Increased service levels by deploying a more available, more scalable, and higher-performance real-time communications solution

The most significant change between Live Communications Server 2003 and Live Communications Server 2005 is the Enterprise Edition support for higher-availability and large scale deployments. This comes from an architecture based on a two-tier, load-balanced pool of front-end servers and a clustered SQL Server back-end database server. With moderate increases in hardware and installation costs, Microsoft IT was able to provide Microsoft employees with increased service availability at equal or reduced management and operations costs.

Microsoft IT now has a real-time presence and instant messaging solution that can scale up on the fly, and that allows for removal of a single server machine for applying updates, service packs, or product upgrades – with minimal interruption of service. Further, there is a single point of control for managing all Live Communications Server 2005 users and servers. Lastly, with the centralized, clustered database server solution, there is one set of storage volumes that need to be backed up on a nightly basis (instead of the individual instances of Microsoft SQL Server 2000 Data Engine (MSDE) that previously ran on each Live Communications Server 2003 home server in the Redmond data center).

Internal and remote access that is more secure and easier to set up, manage, and track

Remote user access from the Internet with no VPN connections

Many Microsoft employees are mobile users traveling from building to building for meetings or working from remote locations and home offices. Access to real-time presence information without a VPN connection makes service seamless whether a user is connected to the Internet or the Microsoft corporate network by wire or by wireless.

Encrypted Communications

The ability to encrypt content within an enterprise is an important security consideration. When using Exchange 2000 Server instant messaging services and the public instant messaging networks, all communications are transmitted in clear text. Clear text communications through a firewall can provide an entry point for viruses and other attacks, and make it possible for someone to eavesdrop on an instant messaging conversation.

Live Communications Server 2005 includes enhanced security features, such as encryption across network hops using the Transport Layer Security (TLS) protocol, and full authentication using Active Directory. The ability to encrypt and decrypt traffic between the

clients and servers helps prevent attempts to capture and read communications that are traversing the network.

All communications between Live Communications Server 2005 and Windows Messenger 5.1 as well as all server-to-server communications are encrypted through the enforcement of high-security mode on the client and the configuration of TLS and MTLS protocols on the server. The benefit is substantial, especially for Microsoft employees accessing the service from the Internet.

Less complex (and less costly) deployment and management options for multi-forest network environments

Restricting Active Directory schema extensions to a single forest

Using the central resource forest deployment model, the Active Directory schema extensions for Live Communications Server 2005 no longer needed to be applied to every forest that needs to participate in enterprise instant messaging. Only the forest selected as the central resource forest needs to have its Active Directory schema extended, simplifying the initial deployment, replication, and maintenance of the schema changes.

User Account Lifecycle Management

With MIIS, managing contact object creation or deletion when employees are hired or leave the company is automated. This allows for more efficient use of IT resources and lower ongoing management costs.

Single Namespace across Forests

With Live Communications Server 2005, an organization must deploy a live communications service in each forest that contains users who want to use the service.

As long as directories between forests are synchronized, Live Communications Server uses a single namespace across forests to help provide more secure cross-forest communications. For example, at Microsoft, the SIP address of users in any forest consists of an alias combined with the "microsoft.com" namespace. A user can search by first name, last name, or account name in the Windows Messenger and easily find someone in a secondary forest.

In addition, rather than putting all users in a parent domain to support users in two child domains, an organization can host all the Live Communications Server users in one of the child domains. This ability reduces the number of servers that Microsoft administrators need to manage, because they can use the infrastructure set up in one child domain to support users in the other child domain. Although the Microsoft environment consists of multiple forests and domains, Microsoft IT did not need to place servers in every forest and domain.

Lessons Learned and Best Practices

During the planning and deployment of Live Communications Server 2005, Microsoft IT encountered and addressed a number of new situations resulting in the following lessons learned and best practices.

Use High-Security Mode

Use the registry setting that enables high-security mode client connections. The high-security mode implies the following changes: enabling TLS and MTLS to encrypt information between servers and clients, requiring Kerberos and NTLM authentication, disabling

Universal Plug and Play, and disabling peer-to-peer connections for all instant messages and for invitations to other features of Windows Messenger. High-security mode provides increased levels of security in key parts of the service through a single setting.

The key benefit is the end-to-end encryption of all client/server and inter-server communications including logon credentials, text of instant messages, and presence information. For other features such as audio and video conferencing and file transfer, Windows Messenger establishes direct network connections between each user. These features use peer-to-peer protocols once the audio/video conferencing or file transfer session has been established between the users.

Be Aware of Seemingly Unrelated Infrastructure Changes

Overlapping with the deployment of Live Communications Server 2005, Microsoft IT was also completing or starting several projects that could potentially affect the deployment of Live Communications Server. Examples of these projects include the deployment of Windows XP Service Pack 2, network domain isolation based on IPSec, upgrading the wireless networking infrastructure, testing of new server operating system service packs, and the deployment of alternative load-balancing solutions.

During the deployment of Live Communications Server 2005, the Microsoft IT Communications Operations team worked to resolve minor issues involving each of the above technologies. This was facilitated by broad, open, electronic communication across the Microsoft IT service organizations.

Deployment Planning

When planning a deployment of Live Communications Server, an organization should be aware that the phases of deployment, and the number and configuration of servers running Live Communications Server, depend on a number of factors, such as:

- Size of the organization, including the number of forests, locations of data centers, number of expected users, and number of expected messages per user per session.
- Behavior of users, including frequency of sessions, number of contacts, and proportion of text message traffic to audio, video, and data collaboration traffic.
- Whether the deployment consists of a migration from an existing solution (such as Live Communications Server 2003 or Exchange 2000 Server instant messaging services) or whether Live Communications Server 2005 is the first real-time communications solution being deployed by the organization.

Additional information on planning for the deployment of Live Communications Server 2005 can be found at http://www.microsoft.com/office/livecomm.

Educate Users

Answer common questions in advance through e-mail and through an internal Web site that contains a list of frequently asked questions (FAQs) and pointers to other sources of information.

Most of the questions that Microsoft IT received during the pilot deployment of Live Communications Server at Microsoft were client-oriented. For example, users asked why some contacts were repeated in their contact lists, or whether they could chat with non–Live Communications Server contacts through the Windows Messenger 5.1 client.

Centralize the Live Communications Server Architecture

If you install servers allocated for Live Communications Server 2005 in a central location and if your organization has multiple forests, you can create one DNS entry and replicate that entry among all the corporate forests. A centralized model simplifies the management and maintenance of DNS records required for the service. However, if data centers are widely dispersed—for example, on different continents—you must ensure that there is sufficient bandwidth (at least 1.6 Kbps per user over an eight-hour period) in the connections between data centers to support a centralized model.

A centralized model may increase the time needed for users to log on to the service. You can determine the impact by measuring the current network delay. As a basic example of how to measure the network delay, you can use the PING protocol to send 100 1-kilobyte packets between the server and a computer in the target location. For Microsoft, the delay was approximately 107 milliseconds. This small delay was not sufficient for Microsoft IT to consider a distributed server deployment strategy. Other network environments that experience significantly longer delays may choose to distribute one or more of their home servers.

Summary

The Microsoft IT deployment of Live Communications Server 2005 Enterprise Edition served a dual purpose: testing of the product in a large, real-life enterprise environment with more than 80,000 accounts, and providing Microsoft employees with real-time communication features such as presence and instant messaging.

Live Communications Server 2005 Enterprise Edition is a complete enterprise solution because it offers:

- Improved security through TLS encryption, Windows authentication, and message archiving.
- Increased end-user productivity and reductions in the time needed to make decisions using real-time presence and more secure instant messaging.
- Manageability by being easy to deploy and administer through existing enterprise infrastructure assets that reside on the customer's premises and that do not rely on non-secure or possibly unreliable public services.
- Extensibility through application program interfaces (APIs) that enable the creation of innovative applications and customized solutions.

Deploying Live Communications Server 2005 can decrease costs in an organization by helping users communicate more efficiently and more securely—thereby increasing worker productivity—while minimizing the complexity of managing an instant messaging service. Live Communications Server 2005 also provides long-term value as a platform for applications and solutions (such as custom real-time communications, Voice over IP (VoIP) telephony applications and the Microsoft Office System) that use SIP to extend communications beyond instant messaging.

FOR MORE INFORMATION

Microsoft Office Live Communications Server

- Microsoft Office Live Communications Server Web site, http://www.microsoft.com/office/livecomm.
- Microsoft Office Live Communications Server Development Center, http://msdn.microsoft.com/office/understanding/livecomm/default.aspx.

Related Microsoft IT Showcase White Papers

- Improving Security with Domain Isolation: Microsoft IT Implements IP Security (IPSec), http://www.microsoft.com/technet/itsolutions/msit/security/ipsecdomisolwp.mspx.
- Enabling Cross-Forest Identity Management with Microsoft Identity Integration Server 2003, http://www.microsoft.com/technet/itsolutions/msit/deploy/cfimwiis.mspx.

Other Related Information

- Microsoft Operations Manager Web site, http://www.microsoft.com/mom.
- Microsoft Identity Integration Server Web site, http://www.microsoft.com/miis.

Microsoft Sales Information Center

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:
http://www.microsoft.com
http://www.microsoft.com/technet/itshowcase

For any questions, comments, or suggestions on this document, or to obtain additional information about Microsoft IT Showcase, please send e-mail to:
showcase@microsoft.com

APPENDIX A – WINDOWS MESSENGER 5.1 CLIENT BRANDING

Before Microsoft IT distributed the Windows Messenger 5.1 client to all users, it used the branding features of the client to assist pilot users. For example, to assess the user experience, Microsoft IT created a survey and made it available by clicking on the banner image displayed in Windows Messenger 5.1.

Microsoft IT client services team uses the Windows Messenger 5.1 branding features, such as the banner image that appears at the bottom of a conversation window, to display specific employee communications. The branding registry settings described below are installed by a custom script when an employee installs Windows Messenger 5.1. Microsoft IT can then change the content pointed to by the branding registry settings and cause a change to appear on all clients the next time users log on.

For Microsoft IT, branding consists of five main components. All of these were written to the client's registry at the time of client installation. The registry entry names are as follows:

Table 4. Windows Messenger 5.1 Client Branding Registry Settings

Registry Setting	Description
BannerURL	URL for location of the image that is visible at the bottom of a conversation window. The user can also click this area to go to a destination defined by BannerLinkURL. The BannerURL image and BannerLinkURL link were used by the Microsoft IT services team to communicate IT and non-IT-related messages to Windows Messenger 5.1 users.
BannerLinkURL	URL for the location of the page to which Windows Messenger 5.1 would redirect the user. For example, BannerLinkURL can redirect users to a Web page where a client update is located, or to a Web page that provides information about a feature of the service. During the pilot deployment, BannerLinkURL redirected users to the feedback survey. By using redirection on the Web server, the client-side registry setting can remain constant while still enabling Microsoft IT to control the page that would be displayed when a user clicked on the banner image.
HelpURL	The HelpURL is visible to the user on the Help menu. Microsoft IT configured this entry to point to the Microsoft IT Web page for Windows Messenger 5.1 where users can get answers to frequently asked questions (FAQs) and other information, including server status information.
Providername	The text of the menu item entry that appears on the Help menu. Clicking on this menu item causes the Web page associated with the HelpURL to be displayed.
TabURL	Registry entry that defines a URL where the Extensible Markup Language (XML) manifest file containing the configuration information for the custom tabs that are to appear along the left side of the Windows Messenger 5.1 application.