Abstract

This twenty-four slide presentation is based on a thirty-seven page technical white paper, published in October 2004, that describes how Microsoft IT deployed Microsoft Office Live Communications Server 2005 to provide its employees with a real-time communications and instant messaging solution. The Microsoft installation of Live Communications Server 2005 is redundant, scalable, highly available, capable of operating across multiple forests, and provides encrypted communication with contacts outside the corporate firewall. In addition, the Microsoft Operations Manager management pack provides reporting capabilities that facilitate maintenance and support of the service.

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.

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 presentation 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.*

Solution Overview

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.

Microsoft IT wanted to deploy a high-availability solution that had improved:

- Manageability
- Scalability
- Multiple forest support

Solution

Microsoft IT used Windows Server 2003 and SQL Server 2000 to deploy Live Communications Server 2005 using a pooled front-end server, clustered back-end database 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

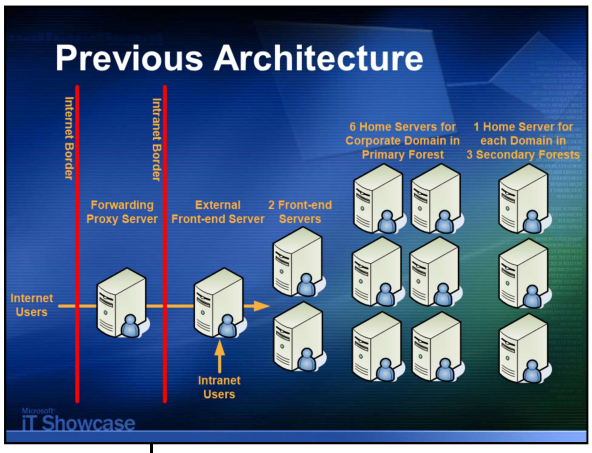
Products and Technology

- 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 services
- Microsoft Operations Manager 2005
- Microsoft Identity Integration Server 2003 for cross-forest directory synchronization

Features

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



Previous Architecture (based on Live Communications Server 2003)

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.*

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 was 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.

Solution

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

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.

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.

Active Directory Forests and Domains

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.

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.

Planning

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.

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. 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.

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.

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.

Planning, continued

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:

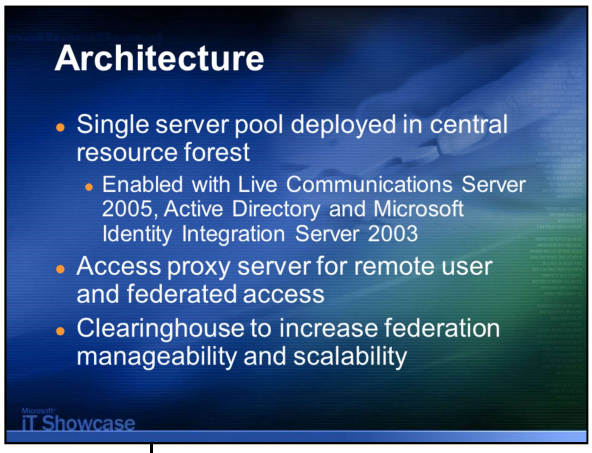
- TLS encrypts information between servers and clients across TCP/IP ports. The default communications protocol in Live Communications Server is unencrypted TCP.

  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. 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 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. Audio/video conferencing and data collaboration sessions themselves still use peer-to-peer connections after the initial invitation has been accepted.

Communications Plan

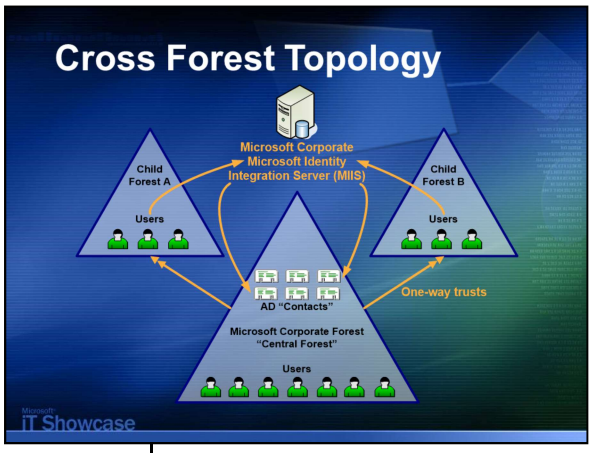
For the Live Communications Server 2005 migration, e-mail notifications were used to advise employees when the migration would affect them individually, the location of the end user support help page, and how to contact Helpdesk if they have any further questions or issues.



Architecture

Microsoft IT took advantage of a key enterprise deployment feature in the release of Live Communication Server 2005 Enterprise Edition: the ability to deploy a high-availability server pool using a central resource forest deployment model. In addition, remote and federated access capabilities were considered in the architecture design.

- Single server pool deployed in central resource forest
  - Enabled with Live Communications Server 2005, Active Directory and Microsoft Identity Integration Server 2003
- Access proxy server for remote user and federated access
- Clearinghouse to increase federation manageability and scalability



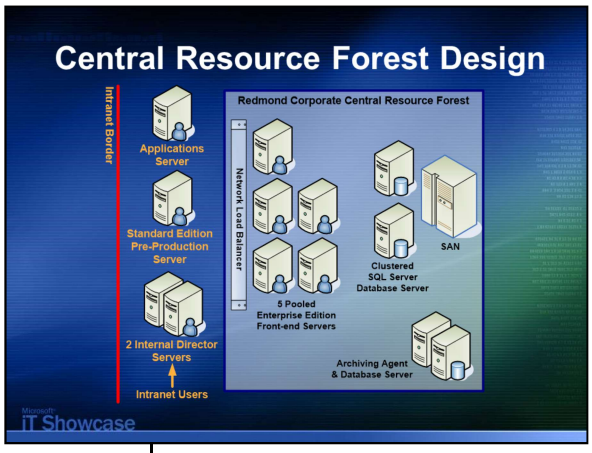
Central Resource Forest Deployment Model

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.

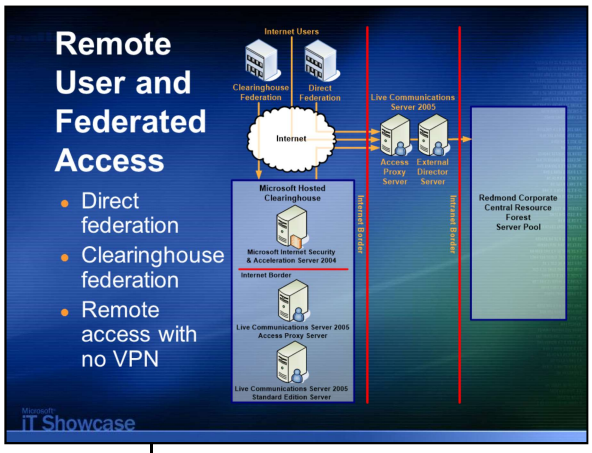
The process flow for exporting secondary forest/child domain user objects and the creation of the corresponding central resource forest contact objects is illustrated on this slide. MIIS selects the user object information from the secondary forests and creates the contact objects in the central resource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



Central Resource Forest Server Pool Architecture

The Live Communications Server 2005 server pool architecture deployed by Microsoft IT is illustrated on this slide. 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.

The Live Communications Server 2005 applications server on this slide 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 on this slide.

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 on this slide.

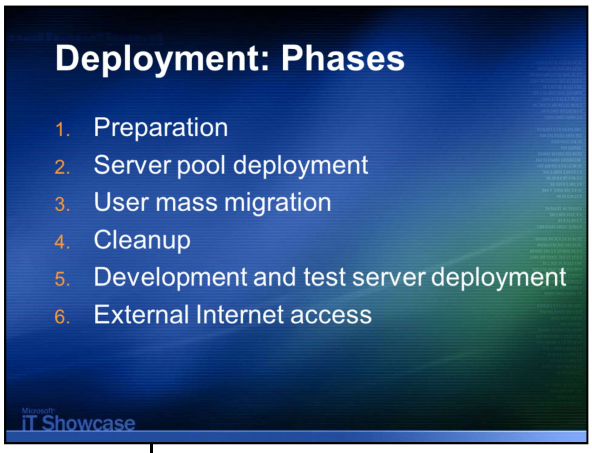
Direct Federation

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.

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.



Deployment: Phases

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:

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.

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.

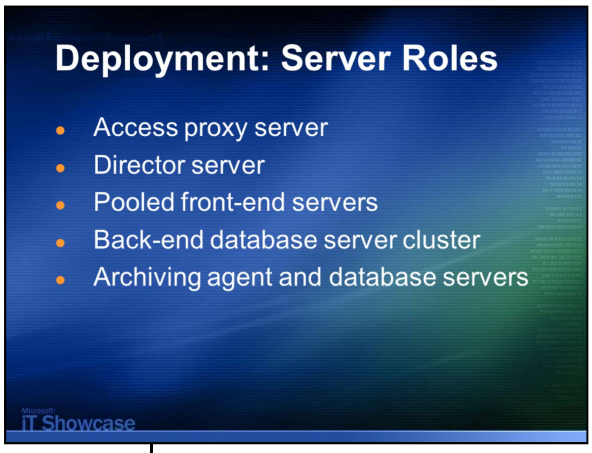
User Mass Migration. Having tested and verified the interoperability between the 2003 and 2005 releases of Live Communications Server, the migration of the remaining large forests was undertaken.

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.

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.

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.



Deployment: Server Roles

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. For more information on the specific server hardware configuration, see Table 1 in the white paper.

Operations

Four-tier support team

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.

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.

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.

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.

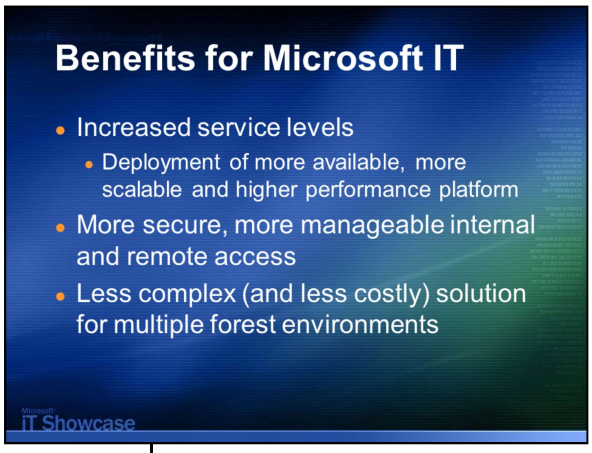
Microsoft IT uses SQL Server 2000 to schedule a snapshot daily backup of the individual Live Communications Server 2005 databases. The backup files are written to another partition on the server pool SAN where they are subsequently backed up from disk to tape by the standard Microsoft IT backup service.

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.

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.



Benefits

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

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. 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.

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

Restricting Active Directory schema extensions to a single forest

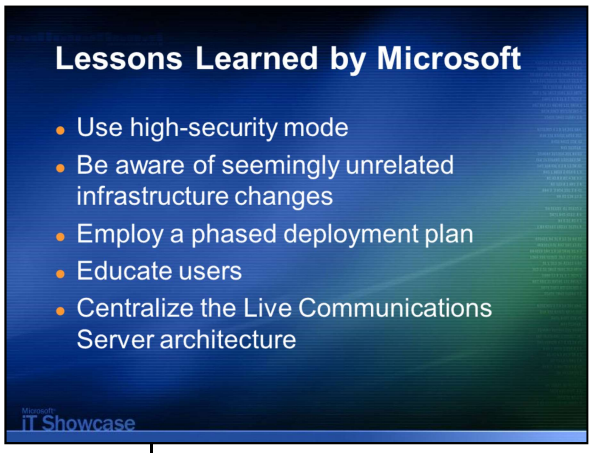
Using the central resource forest deployment model, the Active Directory schema extensions for Live Communications Server 2005 no longer needed to be applied to every forest that needs to participate in enterprise instant messaging. Only the forest selected as the central resource forest needs to have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

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.



Lessons Learned

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.

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.

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 or whether Live Communications Server 2005 is the first real-time communications solution being deployed by the organization.

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.

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.

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.
- Enterprise-grade availability, scalability and manageability.
- 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 Web site: http://www.microsoft.com/office/livecomm.
- Additional content on Microsoft IT deployments and best practices can be found on http://www.microsoft.com.
  - TechNet: http://www.microsoft.com/technet/itshowcase
  - Microsoft Services: http://www.microsoft.com/itshowcase
- E-mail IT Showcase: *showcase@microsoft.com*

About Microsoft IT Showcase

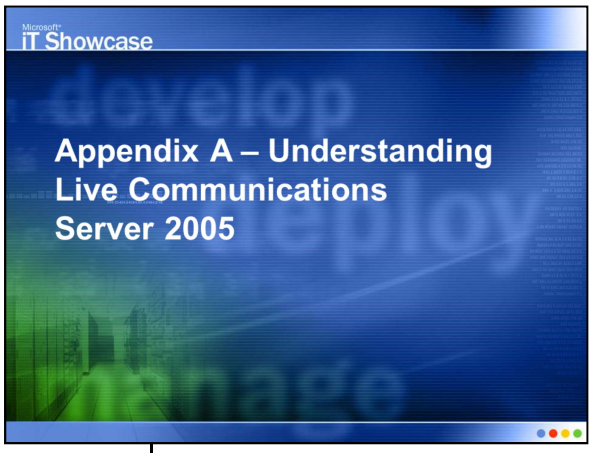
Microsoft IT Showcase is a collection of key business applications, deployment strategies, early adopter experiences, best practices and leading-edge initiatives direct from the Microsoft IT organization.

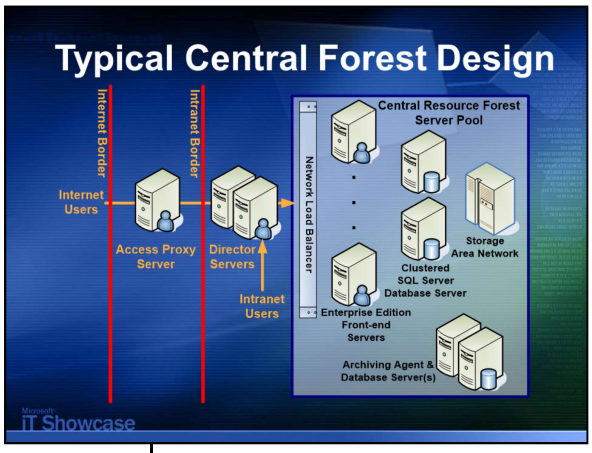
IT Showcase features case studies, white papers, presentations and multimedia presentations that illustrate internal business applications, product deployment experiences and other key IT initiatives being implemented within Microsoft.

Microsoft IT's Experience

Early adopter: Microsoft IT is often the first to implement new Microsoft® products in a production environment - and to develop line-of-business applications based on Microsoft technologies. Knowing what challenges we've faced and how we dealt with them can help you as you plan and execute similar projects.

Large-scale deployments: Microsoft IT oversees worldwide deployments, both of Microsoft's products and those of other vendors. The issues we have to deal with and the lessons we learn along the way can help you as you gear up for your own large rollouts.


Microsoft
IT Showcase
develop
deploy
manage
Appendix A – Understanding Live Communications Server 2005



Typical Central Forest Design

This slide 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.

Director Servers

In the high-availability server pool example depicted on this slide, 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

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).

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.