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.

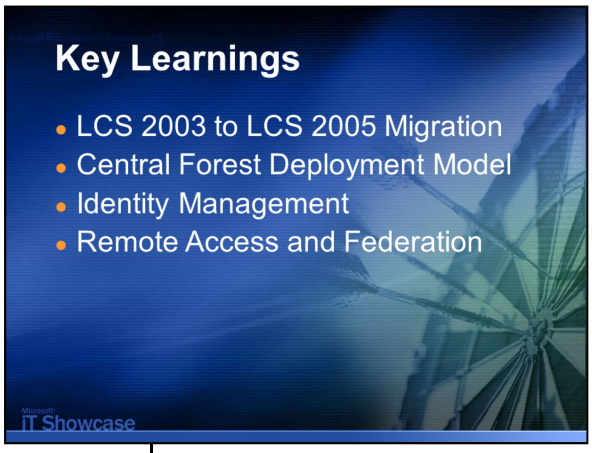
Given the existing Microsoft deployment of Live Communications Server 2003 and the updated and new features of Live Communications Server 2005, Microsoft IT and the Live Communications Server product group developed a strategy to enable the production deployment of an updated, real-time, person-to-person 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.

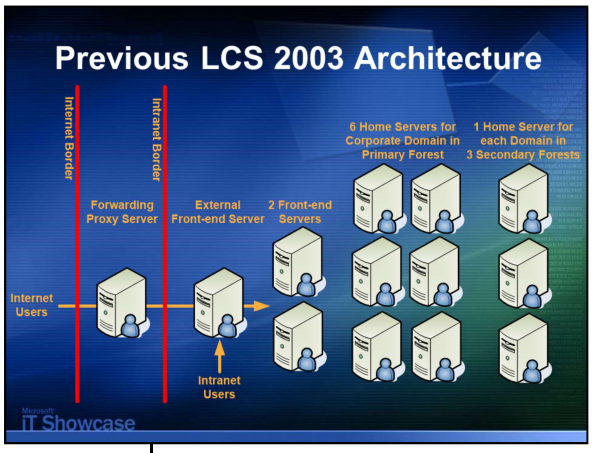
Note: *For security reasons, the names of forests, domains, and other internal resources do not represent real names used within Microsoft and are for illustration purposes only.*



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

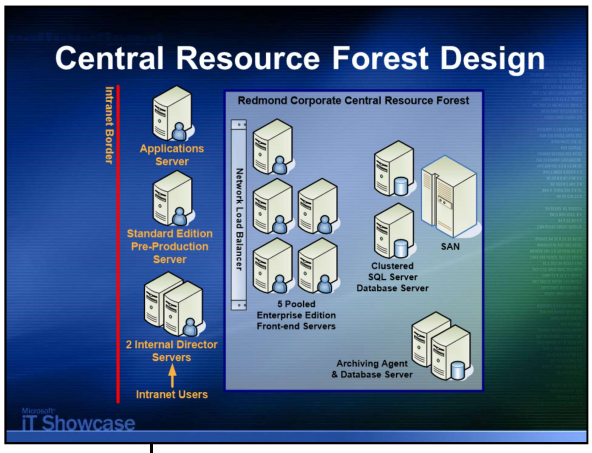


Previous Architecture (based on Live Communications Server 2003)

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.*

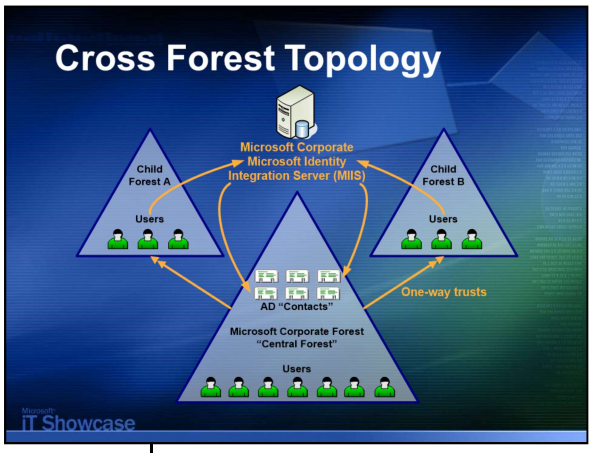
Live Communications Server 2005 Enterprise Edition introduces a highly scalable, high-availability deployment model based on the concept of server pools. *Live Communications Server 2005 Enterprise Edition supports multiple front-end servers per server pool and the use of clustered back-end SQL Server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



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.



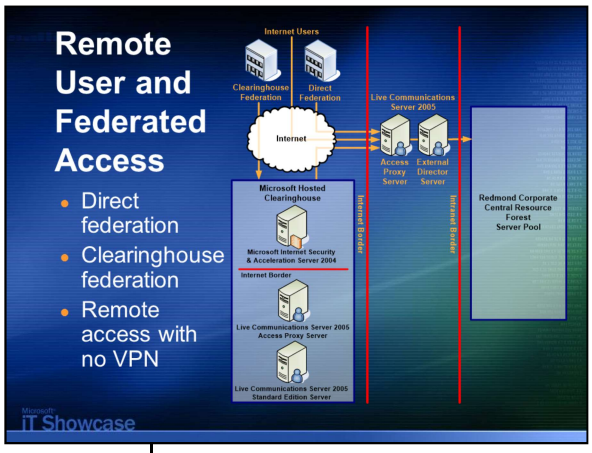
Central Resource Forest Deployment Model

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.



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.

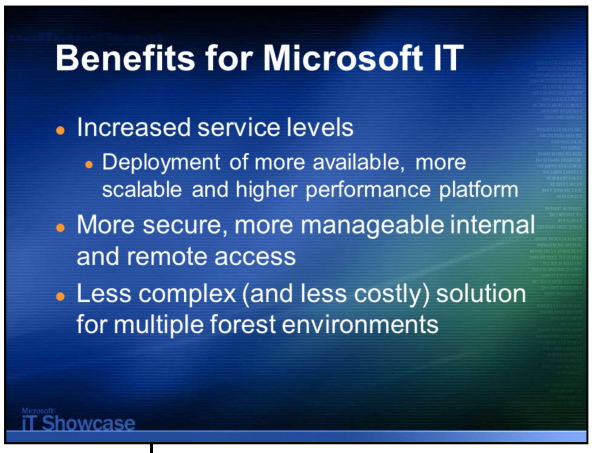
Direct Federation

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.



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.