



ENOVIA SmarTeam

Deployment Guide

© Dassault Systèmes, 2008, 2010. All rights reserved.

CATIA, ENOVIA, SMARTEAM and the 3DS logo are registered trademarks of Dassault Systèmes or its subsidiaries in the US and/or other countries.

PROPRIETARY RIGHTS NOTICE: This documentation is the property of Dassault Systèmes. This documentation shall be treated as confidential information and may only be used by employees or contractors of the Customer in accordance with the terms of the End-User License Agreement accepted by Customer.

Any use of the Licensed Program contained in this media or accompanying it, is subject to the terms of the End User License Agreement accepted by Customer. The Licensed Program is protected by international copyright laws and international treaties. Unauthorized use, reproduction and/or distribution of any of the Licensed Program, or any part thereof, may result in severe civil and/or criminal penalties, and will be prosecuted to the maximum extent possible under the law. Company names and product names mentioned herein are the property of their respective owners and certain portions of the Licensed Program contain elements subject to copyright owned by these entities. See the Documentation CD provided with the Licensed Program for details and/or additional terms and conditions relating to these entities.

Part Number: GEN-A1-200210

Contents

Contents i

| | |
|--|-----------|
| Chapter 1: Introduction | 1 |
| Purpose of this Document | 1 |
| SmarTeam Components | 2 |
| Server Components Requirements | 3 |
| Default Port Assignments | 4 |
| Related Documentation | 5 |
| Internet Site | 6 |
| Chapter 2: General Deployment Recommendations | 7 |
| Component Dependencies | 7 |
| Minimal Deployment | 8 |
| Basic Single Site Deployment | 9 |
| Typical Enterprise Deployment | 9 |
| Chapter 3: Deployment Solutions For a Distributed Environment | 10 |
| Recommended Deployment Guidelines | 10 |
| Plan for Growth during Initial Deployment | 10 |
| Network Utilization | 11 |
| Offload Viewing Capabilities to a Dedicated Server | 12 |
| Remote Site | 12 |
| Terminal Server | 12 |
| Multi-Site Deployment | 13 |
| Replications | 13 |
| Deploy with Hardware and Software Recommendations | 14 |
| Sample Configurations | 14 |
| Chapter 4: SmarTeam – CATIA Web Integration | 16 |
| Local Site Implementation | 16 |
| Off-Site Location | 17 |
| Conclusion | 17 |
| Chapter 5: Capacity Planning, Sizing and Tuning | 18 |
| Capacity Planning | 18 |

| | |
|--|-----------|
| Sizing | 19 |
| Tuning | 19 |
| Appendix A: Database Specific Details | 20 |
| Oracle | 20 |
| MS SQL Server | 20 |
| IBM DB2 | 20 |
| Appendix B: System Specific Configuration Options | 21 |
| How to Enable Remote Copy Mode | 21 |
| SmarTeam Web Viewer Server Configuration | 21 |
| SmarTeam Session Management and System Configuration | 22 |
| Configuration Settings Path | 22 |
| SmarTeam Online Help Configuration | 22 |
| Appendix C: High Availability and Failover | 23 |
| Load Sharing | 23 |
| Generic Deployment Sample | 23 |
| Enterprise Deployment Samples (Security) | 24 |
| Clustering | 25 |
| Cluster Configuration | 26 |
| Appendix D: Deployment Questionnaire | 27 |
| Appendix E: Implementing the LUM Server over a Firewall | 29 |
| Network Configuration Requirements | 29 |
| Network Topology | 30 |
| Firewall Configurations | 30 |
| LUM Server Configuration | 30 |

Chapter 1: Introduction

Purpose of this Document

This document describes the distributed deployment guidelines recommended by SmarTeam. SmarTeam is a very flexible solution that can be deployed in various configurations and usage scenarios to address the needs of a large variety of organizations that differ in size (from 5 to 3000 defined users), required functionality, geographical deployment, working environment and so on. This document focuses on issues pertaining to the infrastructural aspects of the SmarTeam solution and explains how SmarTeam addresses issues such as:

- Enterprise requirements for scaling from the small to large environment
- Use of Web or Windows environment
- Deployment in one location or in multiple locations across the globe

Also, this document is targeted at implementers of SmarTeam Web Applications. Readers of this document should be familiar with SmarTeam Web Applications components and with common network topologies and terminology. Specifically, readers should be familiar with the concepts of a network Firewall.

SmarTeam Components

SmarTeam comprises a collection of components that work in conjunction to support SmarTeam applications. The configuration of the machines on which the components are installed depends upon the size, number of users, site locations and the network characteristics of the enterprise.

| Component | Definition |
|-------------------------------------|--|
| DB Server | Data storage for all SmarTeam-related information, including user information, application-level information and, most important, the customer's object model representation and storage (not including the working files themselves). |
| Vault Server | A server providing specific security constraints to the File Storage, allowing customers to manage their file objects by means of Check Out, Check In and Release operations. |
| Core Services | <p>SmarTeam Core Services consist of two key modules:</p> <ul style="list-style-type: none"> • System Configuration service • Session Management service <p>Both services enable all SmarTeam applications to retrieve and set configuration keys and execute session-based operations.</p> <p>Part of the SmarTeam Session Management service is the Authentication Module, which is responsible for integrating SmarTeam authentication with the enterprise's existing authentication solution (i.e., LDAP, Active Directory).</p> |
| Workflow Server | Provides management of all flow-related products and processes. |
| Viewer Server | Provides SmarTeam - Editor and SmarTeam - Web Editor with unified, cross-brand viewing technology for viewing CAD formats. |
| SmarTeam - Editor | SmarTeam rich client, enabling all of the licensed SmarTeam functionality. |
| SmarTeam - Web Editor (WED) Server | SmarTeam - Web Editor Server provides SmarTeam functionality over the Web for thin clients (web browser). There are two modes of work for the Web Editor Server - regular mode (all of SmarTeam functionality is available) and Navigator mode (only viewing functionality is available). |
| SmarTeam CAD Integration | Unique module of SmarTeam, allows smooth integration of SmarTeam PLM into key CAD applications (CATIA, SolidWorks, Solid Edge, AutoCAD, etc). |
| License Use Management (LUM) Server | Based on IBM technology, allows SmarTeam to control licensed applications. The LUM Server enforces license policies and enables the system administrator to monitor the usage of the various SmarTeam applications. |

Server Components Requirements

| Component | Description |
|------------------------|--|
| Core Services | <ul style="list-style-type: none"> The SmarTeam Session Management Service must be accessible to the SmarTeam Web application and the SmarTeam – Editor clients using the configured protocol (default TCP port 5606). For more details, see Appendix B. The SmarTeam System Configuration Service must be accessible to the SmarTeam Web application and the SmarTeam – Editor clients using the configured protocol (default TCP port 5607). For more details, see Appendix B. If the NLS Data Files are resident in a shared network location, these files must be accessible (SMB/CIFS) by SmarTeam Web application and by SmarTeam – Editor clients (It may be necessary to replicate the NLS Data files for use both within the internal network and on the Web). For detailed information about configuring the NLS Data files, please refer to SmarTeam – Editor Online Help. |
| Web Application Server | <p>The Web Application Server process must be able to communicate with the Database Server. The exact method and requirements for this communication depends on the type of database, see Appendix A for additional details.</p> <p>The Web Application Server process must be able to communicate with the Vault Server using http/s protocol using specific ports.</p> |
| Vault Server | <p>The Vault Server process must have access to the Database Server machine. The exact method and requirements for this access depends on the type of database, see Appendix A for additional details. Also, the Vault Server process must have access to shared file system (SMB/CIFS).</p> <p>Note: When you are implementing reverse proxy it is highly recommended that the Vault Server IP address will be configured as FQDM (e.g. vault.org.com). This insures that external users will access the Vault Server through the proxy server and internal users will continue to work in LAN. In addition the Vault Server should be configure as any other Web application over a proxy server.</p> |
| Markup Monitor Server | <p>The Markup Monitor Service must be deployed on the Vault Server machine. It must have access to shared file system (SMB/CIFS) and have read/write permissions to the markup directory on the Viewer Server machine.</p> <p>Note: The markup directory is the directory in the SmarTeam - Web Viewer Server that has details on a document and its possible markup (for more details, see SmarTeam - Web Viewer Installation Guide).</p> |

| Component | Description |
|---------------------|--|
| Viewer Server | The Viewer Server machine must be accessible by a specific single IP address to ALL SmarTeam Web clients whether on internal LAN or external from the Internet. |
| Flow Server | The Flow Server process must have access to the Database Server machine. The exact method and requirements for this access depends on the type of database, see Appendix A for additional details. |
| SmarTeam Web Client | <p>All SmarTeam - Web client machines must be able to access Web Application machine, Vault Server machine and the Viewer Server machine, using the following ports:</p> <ul style="list-style-type: none"> • TCP port 80 (if HTTP tunneling is used) • TCP port 443 (for HTTPS) <p>Note: For Viewer Server when not using HTTP tunneling, a TCP port which is defined by Viewer Server configuration (default port 5099) should be used.</p> |
| Licensing Server | A separate LUM server must be present for each subnet that has machines using its services. There should not be any restrictions on communication between the SmarTeam – Editor client or Web Application Server and the LUM server being used by them. |

The Proxy server and internal user will continue to work on the LAN.

Default Port Assignments

| Components | Communications | Protocol | Port |
|-----------------|---|----------|---|
| DB Server | Serves incoming connections | TCP | Default according to DB provider: Oracle - 1521 & 1526 SQL Server - TCP 1433, UDP 1434 DB2 - 523 & 50000 |
| Vault Server | Serves incoming connections | HTTP/s | In: HTTP (80) or HTTPS(443) |
| Core Services | Serves incoming connections, communicates with the DB servers | TCP | In: .NET Remoting 5606 & 5607 Out: DB ports |
| Workflow Server | Communicates with the DB servers | TCP | DB ports |

| Components | Communications | Protocol | Port |
|------------------------------------|--|------------|---|
| Viewer Server | Serves incoming connections, communicates with the vault server | HTTP/s | In: HTTP (80) or HTTPS(443) Out: Vault Ports |
| Authentication Module | Communicates with LDAP, Active Directory and DB servers | TCP | LDAP & Active Directory port - 389 DB Ports |
| SmarTeam - Editor | Communicates with DB, Core Services and LUM | TCP | Out: DB Ports .NET Remoting (5606 & 5607) LUM - 1515 |
| SmarTeam - Web Editor (WED) Server | Serves incoming connections, communicates with vault, Core Services, DB Servers, LUM | TCP/HTTP/s | In: HTTP(80) or HTTPS (443) Out: DB Ports .NET Remoting (5606 & 5607) LUM - 1515 |
| SmarTeam CAD Integration | Communicates with DB, Core Services and LUM | TCP | Out: DB Ports .NET Remoting (5606 & 5607) LUM - 1515 |
| LUM Server | Serves incoming communication | UDP | In: 1515 Out (Authentication Port): 1516 |

Related Documentation

The following documents are referenced in this guide. All the documents are available on the SmarTeam Program Directory CD unless specified otherwise.

| Name of Document | Remarks |
|--|--|
| Hardware and Software Requirements | Details the hardware and software required for a successful deployment of SmarTeam applications. |
| SmarTeam - Multi-site Administration Guide | Provides administration procedures to successfully setup, customize and maintain a SmarTeam - Multi-site system in a corporate environment |

Internet Site

You are highly recommended to frequently visit our Website for the latest updates and plug-in products, including the latest Service Packs, Program Directory (Release Notes), Hotfixes and technical support at <http://www.3ds.com/support>.

Chapter 2: General Deployment Recommendations

SmarTeam is deployed in different configurations, depending on the size and location of the organization's sites, network characteristics, and the functionalities required from licensed SmarTeam applications. The SmarTeam components can be installed together in one location, or may be distributed across multiple locations.

SmarTeam can be deployed in organizations with a few seats (10-20 concurrent users working with system) or many seats (up to 500 SmarTeam - Web Editor concurrent users/1000 SmarTeam - Editor concurrent users working in one site with the system).

The common ratios in the market are:

- 1:5 for concurrent Web implementation users to total number of users working in the system, e.g. 500 concurrent users equals 2500 defined users.
- 1:3 for concurrent windows client users to total number of users working in the system, e.g. 1000 concurrent users equals 3000 defined users.

Depending on the size and configuration of your system, you may need to install multiple instances of certain components. For more information on specific deployment solutions, refer to the Multi-site deployment section.

Component Dependencies

When deploying SmarTeam, certain dependencies must be taken into consideration:

- The vault server may need additional disk space for actual vault directories, if these reside on the same computer.
- Vault directories must be deployed on an NTFS partition if they reside on a Windows Platform. Vault directories may also be deployed on UNIX/Linux platforms. For UNIX/Linux usage, Samba 2.2.8a emulation for NTFS must be used.
- It is highly recommended that the following components be installed on separate dedicated machines:
 - Vault Server
 - Core Services
 - Workflow Server
 - WEB Server(s)
 - CMT Server
 - Viewer Server

Note: This recommendation is a general guideline to avoid performance degradation. In some cases (based on analysis of the expected load of each component) it is possible to install several of the above components on one machine, e.g., Vault Server and Viewer Server..

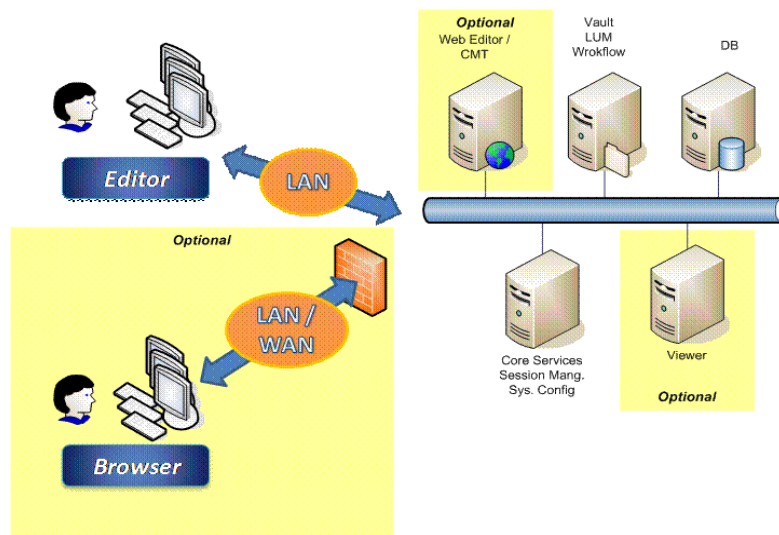
- Performance of SmarTeam - Editor Operations may vary according to network latency and bandwidth limitations. In a WAN deployment, some of the SmarTeam operations include interaction with remote servers (for example, DB, LUM).
- SmarTeam - Editor includes Microsoft® Word and Excel integrations.
- For e-mail sending capabilities, SmarTeam - Editor supports SMTP.

Minimal Deployment

The SmarTeam system allows deployment both for small units as well as enterprises. However, when the total usage of the system is low (as in small companies), the following deployment may apply:

The following diagram describes a minimum configuration. Three of the servers - the Vault/LUM/Workflow server, the DB server, and the Core Services/Session Management/System Configuration Server - are mandatory. The Viewer and SmarTeam - Web Editor/SmarTeam - Community Workspace (CMT) servers are optional, depending upon the functionality required.

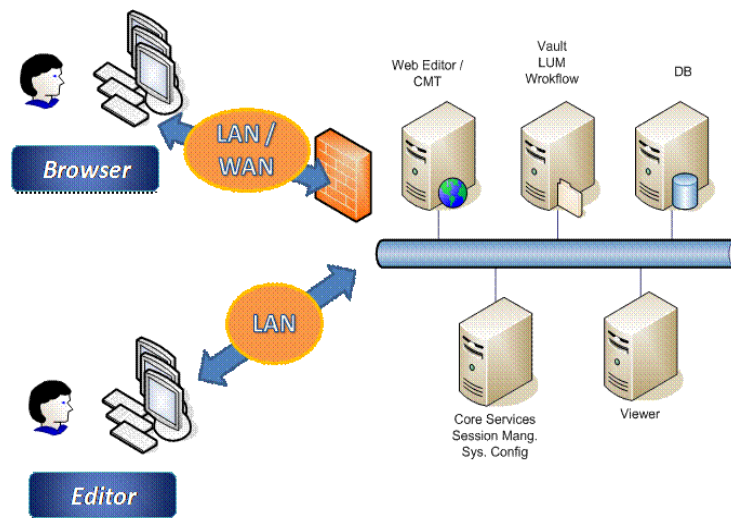
Note: You cannot install SmarTeam - Web Editor and SmarTeam - Community Workspace on the same server.



Basic Single Site Deployment

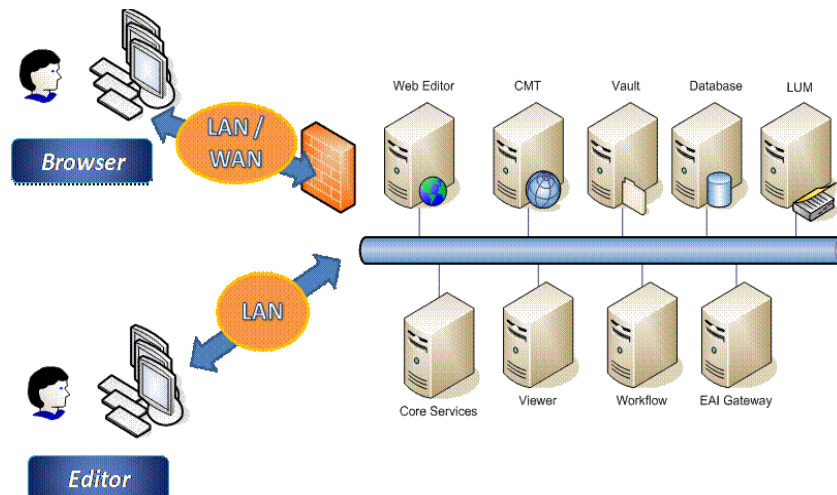
In the case of a single-site deployment, SmarTeam services and applications can be hosted on one or more servers, depending upon the user load and usage scenarios that must be supported by the system. Users are connected to the system using the SmarTeam Editor Client application and/or SmarTeam - Web Editor, which is the front-end Web application for the SmarTeam system. All access is via a Local Area Network (LAN): all SmarTeam servers are connected via LAN as well.

Note: You cannot install SmarTeam - Web Editor and SmarTeam - Community Workspace on the same server.



Typical Enterprise Deployment

The typical enterprise deployment is similar to the single-site deployment described above. However, in this deployment some of the users (for both SmarTeam - Editor and SmarTeam - Web Editor) access SmarTeam back-end services over a Wide Area Network (WAN). The Enterprise environment can potentially pose another challenge to the SmarTeam backend system as inter-SmarTeam services/servers may be connected over a WAN as well. For example, a LUM server can be located at the headquarters site while all other servers are located at a remote engineering site.



Chapter 3: Deployment Solutions For a Distributed Environment

The distributed (multi-site) environment involves enterprises with small, medium or large sites. The deployment of SmarTeam varies according to enterprise topology.

Recommended Deployment Guidelines

When deploying SmarTeam in the enterprise, we recommend using the following general guidelines.

- [Plan for Growth during Initial Deployment](#)
- [Network Utilization](#)
- [Offload Viewing Capabilities to a Dedicated Server](#)

Plan for Growth during Initial Deployment

The SmarTeam system is fully scalable for the enterprise, allowing for gradual growth of the system and its usage. However, at the time of deployment, it is strongly recommended that you plan for growth by considering the following points:

- Number of users
 - Plan the number of Web Application Servers that will be needed. The general recommendation is 100 concurrent users per server.
 - Plan the number of Core Services components that will be needed: for peak-hour calculations, the general recommendation is up to 500 concurrent connections per server.
- Number of Sites
 - Plan the location of backend servers (Vault, LUM, DB) in order to serve all sites with maximum performance.
- Multi-site place holders
 - "Multi-site planning enables the IT manager to prepare the distribution of the database load among sites; the default involves an equal distribution of objects among all sites. If a particular site, such as the headquarters site, needs additional storage, SmarTeam is able to assign objects from that site to a remote, predefined site with available space.
Example: For a current customer, SmarTeam maintained over 125,000,000 objects per super-class per range, as all of the customer's 16 sites were preconfigured.
- Data size (number of objects within the database and the number of files within the vault):
 - Default number of objects in the database: two billion per super-class.

- Total volume of database: in accordance with the database vendor specifications.

Note: It may be necessary to improve hardware.

- Disk space, dependent upon the type of system usage: a CAD-centric scenario requires relatively large amounts of disk storage space at the start, while other working scenarios (e.g., Microsoft® Office documents) require planning according to the number of users and number of documents inserted into the vault.
- Network constraints (latencies and bandwidth limitations)

Network Utilization

SmarTeam components can inter-connect using the underlying network infrastructure. Verifying the correct network configuration at the time of the initial deployment assures the most efficient performance and network utilization by SmarTeam.

There is a linear influence of the Network characteristic (Latency and Bandwidth) on the performance of SmarTeam actions. This influence should be taken into account in order to predict the expected performance of the system based on the network information.

The following should be considered at the time of initial deployment:

- "Database access characteristics"
 - "Low in bandwidth resources"
 - "High in number of transactions"
- "Core Services characteristics"
 - "Low in bandwidth resources"
 - "Medium number of transactions"
- "Vault access characteristics"
 - "High in bandwidth resources"
 - "Medium number of transactions"

SmarTeam – Editor Client (Also Relevant for CAD Integration)

A thick client enables performance improvement for heavy operations by using the client side processing capabilities. However, in order to retrieve and send data, the SmarTeam client connects to the Core Services, Vault and Database. In light of this, it is recommended to plan a deployment in which the clients will work on the LAN with the vault and the core services, while having the DB on the LAN is optional.

SmarTeam – Web Editor

The SmarTeam system can offer a Web client that is based on browser capabilities and interacts with the SmarTeam - Web Editor server using Standard HTTP protocol (or HTTPS for secure connection to the Web Server). This improves network utilization by having all client-based traffic handled via HTTP, with all SmarTeam components connected on a LAN, allowing optimal performance.

Offload Viewing Capabilities to a Dedicated Server

The viewer server might place a great strain on the SmarTeam – Web Editor server. We recommend moving the Viewer Server during the initial deployment. It is recommended that you deploy the viewer server together on the same LAN with the vault server.

Remote Site

The SmarTeam deployment scheme allows access and usage from one site to another remote site based on the following options:

1. Based on SmarTeam - Web Editor: Remote site users access SmarTeam by using SmarTeam - Web Editor/Navigator via standard Internet browser (e.g., Internet Explorer).
2. Based on SmarTeam - Editor: While deploying SmarTeam - Editor on a Windows client application for end-users on remote sites, the SmarTeam administrator can easily configure SmarTeam - Editor to work with its server on another site.

Note: This also applies to SmarTeam Multi-CAD integration products.

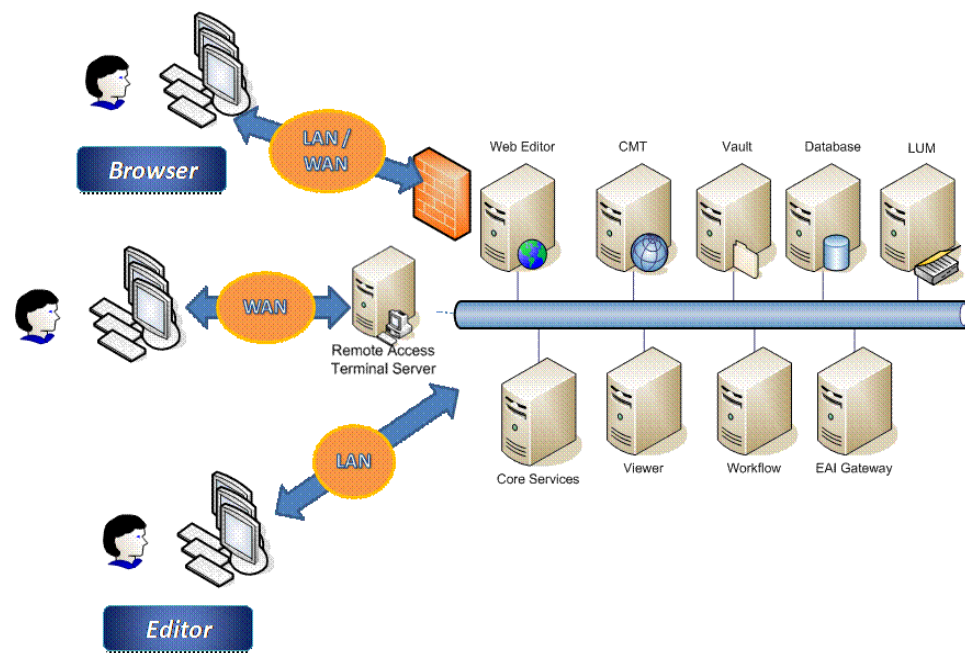
3. Remote access using a dedicated terminal server located on the organization central site.

Terminal Server

A Terminal Server (e.g., Microsoft Windows Terminal Server) enables users to run SmarTeam - Editor, Windows client application on a remote computer, located close to SmarTeam back-end servers. This option provides the following benefits:

- End users enjoy good performance of the SmarTeam - Editor client. Via the WAN, only UI performance is affected.
- The IT system administrator can easily manage, control and deploy SmarTeam - Editor clients for mass usage in medium/large sites.

Note: Terminal Server is recommended for up to 10 users per server.



Multi-Site Deployment

In today's organizations, the distributed enterprise faces huge challenges related to data management, different business hours according to time zones, different working methodologies in each site, and consolidation of companies due to mergers and acquisitions. SmarTeam - Multi-site was created to address these challenges, allowing distributed teams to work on a unified database, with unified vaults.

Replications

SmarTeam - Multi-site techniques and methodology are based on replicated databases, replicated vaults, or a combination of both.

Creation and modification of data in SmarTeam result in transactions in the database and, in some cases (such as lifecycle operations) vault updates.

Replication Intervals

Database Replication

In an asynchronous replication environment, the replication can be set to occur at intervals. Replicating data places a certain amount of load on the network. Network traffic implications depend on the number of transactions performed in the local and remote databases. The database replication mechanism is based on Oracle, which uses minimal-communications technology, sending changes only; therefore replication in most cases can be performed rather often. SmarTeam - Multi-site assumes the replication interval to be two minutes as a default (excellent communication), while 15-20 minutes is a normal variant. Setting the replication interval to hours or days may cause the accumulation of large transactional data volumes, resulting in an extended replication process. As expected, another implication of a longer replication interval is that the sites are not fully synchronized for longer periods. For more information on database replication, refer to SmarTeam - Multi-site Administration Guide.

Vault Replication

In general, file replication is a bandwidth consuming activity (more than Database replication). It is recommended to define the file replication interval based on the specific work scenario of the customer, and to define specific vaults for files in shared projects (high-frequency replication) and specific vaults for local-based vaults (low-frequency replication). For more information on file storage replication, refer to SmarTeam - Foundation Administration Guide.

Independent Site Projects

In a scenario where each site works on its own set of data and replication is performed for the purpose of overall company centralization of data, reusability of parts and sharing of standard component definition, it is sufficient and cost effective to replicate overnight, once a day, when the load on the network is minimal.

Collaboration

In cases when users from different sites need to work in collaboration and work on the same project-related data, it may be necessary to perform replication at shorter intervals. These intervals will have to be defined and fine-tuned according to network bandwidth, other critical enterprise systems that are using the network, other applications' usage patterns (synchronous or asynchronous updates) and the amount of data replicated.

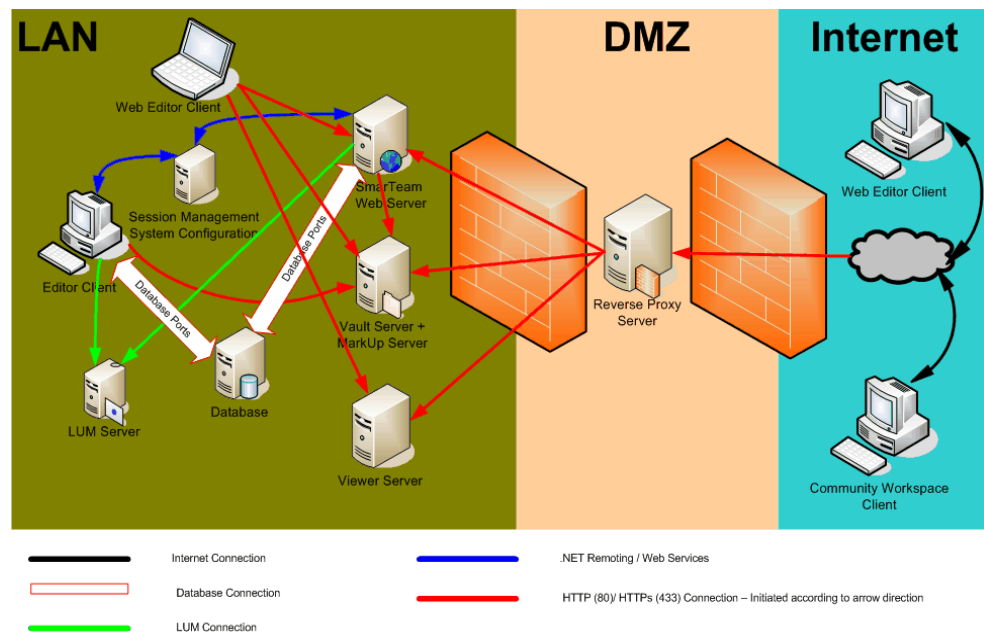
Deploy with Hardware and Software Recommendations

The SmarTeam system is tested on the production hardware as recommended in the SmarTeam Hardware and Software Guide. The system undergoes certification with the recommended software and operating systems. Adopting these recommendations during deployment enables rapid usage growth.

Sample Configurations

This section shows the possible configuration of SmarTeam components and the relationship between them.

The network configuration consists of an internal LAN and one DMZ network, which are separated by one firewall.



Chapter 4: SmarTeam – CATIA Web Integration

SmarTeam – CATIA Web Integration (CWI) is a new architecture of the SmarTeam CATIA Integration based on Web applications.

SmarTeam – Web Editor enables secure product lifecycle collaboration through the SmarTeam database from standard Internet browsers.

SmarTeam – Web Editor utilizes standard Web technologies to provide remote individuals and teams working on multi-platforms, with comprehensive access to the central SmarTeam database and managed files, enabling users to manipulate product data easily in a dynamic and secure environment from any location.

The main advantage of SmarTeam – CATIA Web Integration is that when using this product, SmarTeam does not need to be installed on the client.

There are several recommended scenarios for using SmarTeam – CATIA Web Integration in different environments of SmarTeam. The following sections describe the scenarios and the guidelines for using them.

Local Site Implementation

This scenario describes using CWI on a local site on which the SmarTeam Database, SmarTeam - Web Editor Server and the Vault server and files are located. In this case, all the components are connected on the same LAN.

Site (Local)

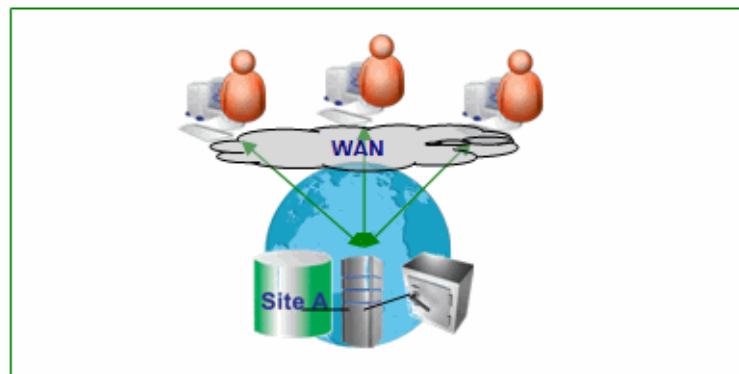


The main benefit of implementing CWI in this environment instead of the CAI (Windows-based CATIA Integration) is in the installation footprint. The SmarTeam installation on the client side will include only the client components, and the work of CATIA with SmarTeam will be done over the Web.

Off-Site Location

This scenario describes using CWI connected from an off-site location to a SmarTeam site which includes the SmarTeam Database, SmarTeam - Web Editor Server and the Vault server and files. In this case, the client machine is connected to SmarTeam components over the WAN.

Off-site location



The main benefit of implementing CWI in this environment is the use of the Web-based technology for remote connection – a common, lightweight and firewall-friendly methodology.

The remote connectivity will affect the performance of working with SmarTeam, mainly when files are copied to and from the client machine to the remote site over the WAN.

Conclusion

SmarTeam – CATIA Web Integration provides benefits and methods of implementation that extend the existing capability of the Windows-based SmarTeam – CATIA Integration.

The above guidelines are provided in order to optimize the capabilities of the new integration, and to avoid implementations that do not fit this architecture and will not provide the needed benefit.

Chapter 5: Capacity Planning, Sizing and Tuning

One of the keys for estimating enterprise-wide requirements for SmarTeam usage is to plan for future needs. Depending upon other configuration choices for multi-site and failover, there may be more than one network deployment configuration, each with its own load and capacity requirements. In this case, sharing of software components on the same hardware will be limited.

As an enterprise increases its SmarTeam usage by adding more users and activating more SmarTeam applications, we must ensure that the SmarTeam deployment will maintain the performance and capacity expectations of those applications.

The SmarTeam administrator can influence the capacity and performance of a given SmarTeam deployment in two phases:

- Planning phase: Take note of the requirements of all deployment constraints.
- Implementation phase: Monitor the system on a constant basis using Windows Performance Monitor tool, rearrange hardware as necessary, and install SmarTeam software components to meet the performance requirements.

Capacity Planning

Capacity planning is the process of determining performance and capacity requirements. The baseline should be the typical deployment synopsis of SmarTeam in the enterprise.

When trying to estimate the required capacity consider:

- The type of SmarTeam clients (SmarTeam - Editor, SmarTeam CAD integrations, SmarTeam - Web Editor)
- The number of users using those clients
- The nature of SmarTeam operations
- The Data Model design and number of objects in the database
- The number of concurrent users
- The peak rate at which operations must be performed by SmarTeam
- The average performance of operations required under peak load conditions

Sizing

After defining the fundamental capacity and performance requirements, the IT Manager translates these requirements into system sizing. The following issues should be considered:

- Database sizing in terms of number of CPUs and disk size
- The type and size of disk subsystems for the vault server computer
- The amount of RAM required for SmarTeam - Web Editor servers
- The number of SmarTeam - Web Editor servers
- If applicable, the number of locations in the multi site deployment

Tuning

After capacity planning is complete and all the necessary hardware is in place, it is necessary to ensure that the combined hardware and software are yielding the desired levels of performance. These are some guidelines for tuning SmarTeam:

- **CPU usage:** Determined, to a large extent, by the number of concurrent users. Consider adjusting these numbers to the appropriate levels based on available CPU resources and the expected peak load.
- **Memory usage:** The main consumer of memory in SmarTeam installation is the SmarTeam - Web Editor server. Tune the memory usage of the system so that all consumers of memory in the system utilize physical memory without needing to use paging.
- **Disk usage:** A large amount of data is passed through the SmarTeam application, primarily by the vault server. Special attention is needed to any tuning that can increase the I/O throughput.

Appendix A: Database Specific Details

Oracle

The Oracle Database server requires ports to be open for clients to be able to establish communication with the servers. By default, the port is 1521 (configurable at the server, listener.ora file).

If a firewall is present between the client and Oracle server, these ports should be opened either manually from the firewall administration or by using the Oracle Connectivity Module, which is available for many of the major firewalls.

Consult the Oracle support site for the following articles: Note:45226.1 and Note:131524.1.

MS SQL Server

The MS SQL Server requires TCP and UDP ports to be open for incoming connections. By default (and also assigned by IANA), the port's SQL Server listens to its TCP port 1433 (configurable).

For more information, consult Microsoft KB article:

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q287932&>

IBM DB2

IBM DB2 requires listener TCP ports to be open, by default, these ports are 523 and 50000 and an additional port for each instance.

For more information, consult the following document from IBM:

<http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245220.pdf>

Appendix B: System Specific Configuration Options

This section provides additional details on configuring specific components.

How to Enable Remote Copy Mode

To enable Remote Copy mode:

- 1 In SmarTeam - Editor, select Tools > Administrative Options > Life Cycle Options.
- 2 In the Life Cycle Options window, check "Remote copy to/from working directory".

SmarTeam Web Viewer Server Configuration

SmarTeam Web Viewer is a Java-based viewing solution that provides SmarTeam Web applications, such as SmarTeam – Web Editor or SmarTeam – Community Workspace, with the ability to view and apply markups to documents and drawings.

SmarTeam Web Viewer is composed of three components:

- 1 A Java-based server component (AutoVue for Java) that:
 - Processes client viewing requests
 - Streams the results in a compact format to the Java applet on the client station.
- 2 A Java applet download client embedded inside HTML page of the SmarTeam Web application client (such as SmarTeam – Web Editor or SmarTeam – Community Workspace).
- 3 A Markup Service that manages all markups (redline files) created or requested by Web users. The service copies these files to and from the vault and prepares them for display by the SmarTeam Web Viewer.

An additional component, the Servlet Engine, is deployed automatically by the SmarTeam Web Viewer installation. This component enables access to the AutoVue for Java server when it is deployed behind a firewall, which prevents non-HTTP (port 80) communication.

For more details on Viewer Server configuration, please consult the "SmarTeam - Web Viewer installation guide.pdf" that is included with the SmarTeam Web Viewer installation. It can be found on the SmarTeam – Web Editor CD or the SmarTeam – Community Workspace CD.

SmarTeam Session Management and System Configuration

SmarTeam Session Management Service and SmarTeam System Configuration Service communicate with SmarTeam Web applications and SmarTeam - Editor clients using .NET Remoting infrastructure. For general information on .NET Framework Remoting, please refer to:

<http://msdn.microsoft.com/library/default.asp?url=/library/enus/cpguide/html/cpconnetremoting-overview.asp>

.NET Remoting can be configured to use various network protocols (for example, TCP, HTTP). For more detailed information, see:

<http://msdn.microsoft.com/library/en-us/cpgenref/html/gnconremotingsettingsschema.asp>

Configuration Settings Path

The Configuration Settings path definition can be changed as follows:

- 1 On each Foundation server, open
<SmarTeam Home>\Bin\SmarTeam.Std.SystemConfiguration.Service.Host.exe.config
- 2 Change both the **SchemasPath** and **DataPath** keys to the new path (can be UNC on the network).

In this way, you can have several Foundation servers with the same configuration system files.

SmarTeam Online Help Configuration

To enable SmarTeam Online Help perform the following:

Using the System Configuration Editor, go to **Miscellaneous Configuration>Help Preferences>Virtual Root Path>** and add the following path:

`http://<computer_name>/SmarTeam/help`

If you are using the presented sample network configuration (using reverse proxy) the `<computer_name>` should be the web server published name.

Appendix C: High Availability and Failover

SmarTeam is designed to address the deployment needs of mission-critical applications requiring a high degree of system availability. To fulfill this need, the main components in the system must facilitate redundancy.

This section describes the availability and failover features of various components in SmarTeam, and provides guidelines for best utilizing them in a typical deployment that requires high availability and failover.

Load Sharing

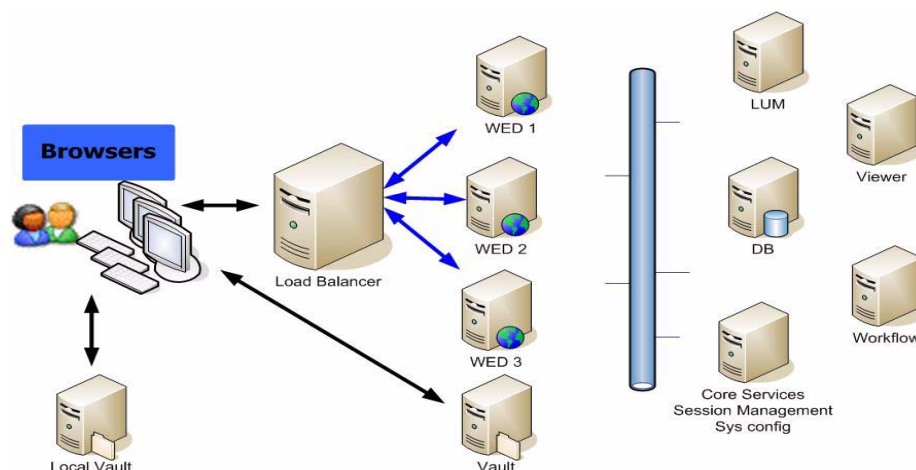
SmarTeam supports load-balancing architecture for its SmarTeam – Web Editor server, allowing scalable deployment of SmarTeam – Web Editor by adding more Web Application Servers. The load balancer intercepts all HTTP traffic, which is the transport layer of SmarTeam – Web Editor. When deploying a load balancer-based environment, the "sticky session" option should be activated so that all the requests of a certain user session will be directed to the same Web Application Server. The following is recommended:

- [Generic Deployment Sample](#)
- [Enterprise Deployment Samples \(Security\)](#)

Generic Deployment Sample

The diagram below describes the simplest scenario, in which no special security requirements exist. As indicated in the diagram, the load balancer receives all end-user requests and routes them to the Web Application Servers for further handling. The benefits of such a configuration include:

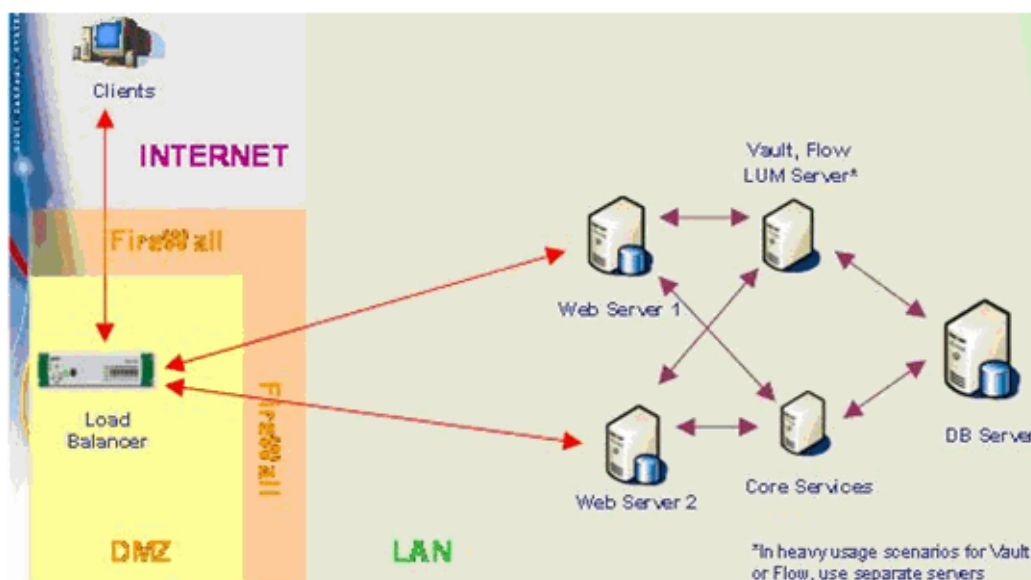
- Division of the load between several servers, allowing better response time for more users.
- Sharing of the load by other servers in the case of a failure by any particular Web Application Server, thus preventing system service interruption.
- The possibility for gradually increasing the sustained system load by adding more Web Application servers, while the system itself remains intact.



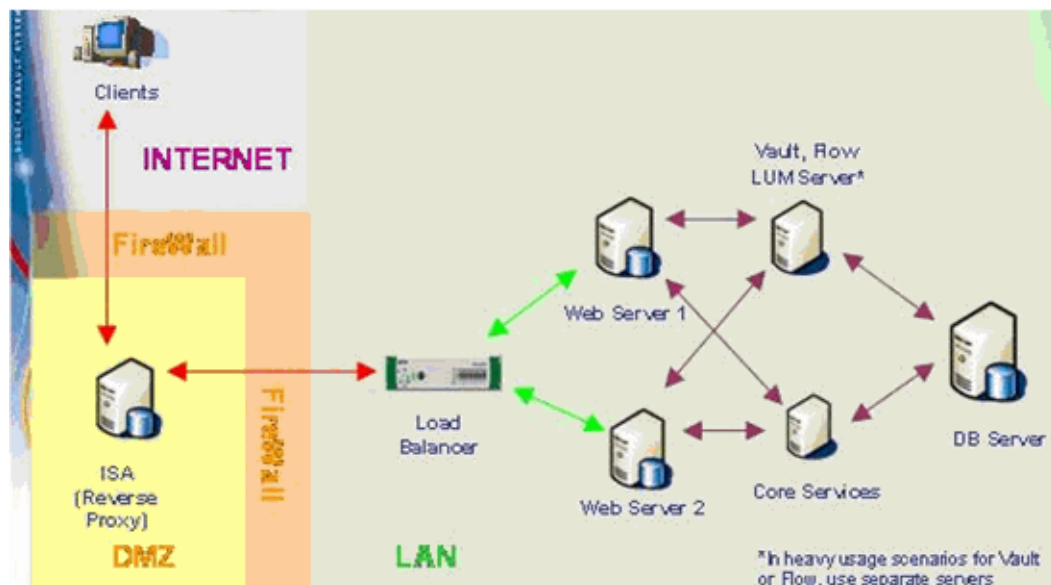
Enterprise Deployment Samples (Security)

There are two levels of network security in which SmarTeam can be deployed. Both configurations utilize the incumbent firewall to buffer between the end users (Web) and the back-end servers (including the Web Application Server). In the simpler case, the load balancer is located in the DMZ; in the second case, a reverse proxy is imposed in the DMZ and the load balancer is protected within the LAN from uninvited external access. The first diagram describes the simpler configuration, while the second one describes the configuration with reverse proxy:

Load balancer only



Reverse Proxy and Load Balancing



Note: For a specific scenario of LUM over Firewall, see [Appendix B: Implementing the LUM Server Over a Firewall](#).

Clustering

SmarTeam supports clusters that are implemented primarily for the purpose of improving the availability of services provided by the cluster. The clusters operate by having redundant nodes, which are then used to provide service when system components fail. The most common size for a High Availability (HA) cluster is two nodes, which is the minimum required to provide redundancy. High Availability cluster implementations attempt to manage the redundancy inherent in a cluster to eliminate single points of failure.

It is recommended to use Microsoft Cluster Server (MSCS) to provide failover and increased availability of SmarTeam applications.

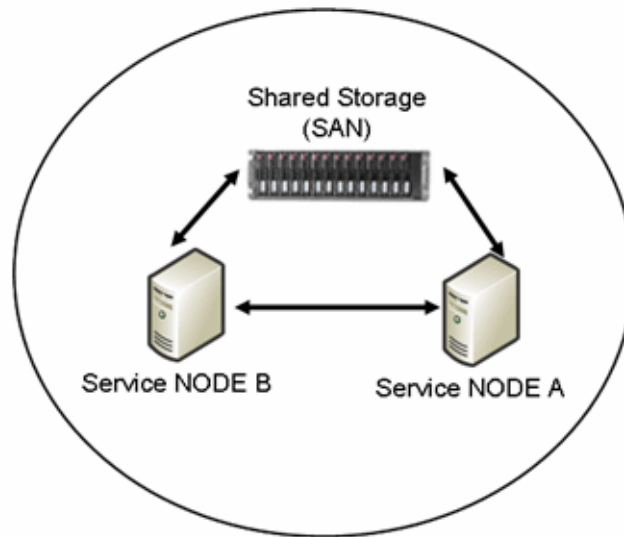
The following are the main components that were tested as a cluster:

- Vault Server (File Storage)
- Core services (System Configuration and Session Management)
- Workflow server
- Database Server (additional license is required from Database Provider)

Note: For a detailed explanation on clustering in a SmarTeam environment, refer to SmarTeam – Foundation Administration Guide, which is available on the SmarTeam Documentation CD.

Cluster Configuration

When deploying one of the above services in a cluster, SmarTeam Editor Clients and SmarTeam - Web Editor Server are connected to the cluster IP. Both nodes are configured to the same storage in order to have the same files. The following generic architecture is recommended:



Appendix D: Deployment Questionnaire

This questionnaire can be used to gather all the relevant information needed to prepare a successful SmarTeam deployment.

| Question | Answer | Comments |
|--|--------|--|
| General | | |
| How many SmarTeam - Web Editor users? | | Actual and planned number of licenses e.g. 100/500 |
| How many SmarTeam - Editor users? | | Actual and planned number of licenses e.g. 100/500 |
| How many CAD Integration Users? | | Actual and planned number of licenses e.g. 100/500 |
| How many Sites? | | Actual and planned number of sites e.g. 5/10 |
| Multi-site | | |
| Will you need Multi-site Database Replication? | | Yes or Not for all. If DB replication has constraints give details |
| Will you need Multi-site VAULT Replication? | | Yes, Partial or Special and give details |
| Per Site | | |
| Do you plan to use a Terminal Server? | | Yes or No. If Yes, name the type e.g. Win2003 |
| What is the Latency to Database? | | Perform simple "PING" for RTT (Round Trip Time) in milliseconds |
| What is the Bandwidth to Database? | | Mb/sec |
| What is the Latency to Core Services? | | Perform simple "PING" for RTT (Round Trip Time) in milliseconds |
| What is the Bandwidth to Core services? | | Mb/sec |
| How many LUM servers? | | Number of servers |

| Question | Answer | Comments |
|---|--------|--|
| What is the Latency to LUM servers? | | Perform simple "PING" for RTT (Round Trip Time) in milliseconds |
| What is the Latency to VAULT? | | Perform simple "PING" for RTT (Round Trip Time) in milliseconds |
| What is the Bandwidth to VAULT? | | Mb/sec - Recommended to have local vaults per site |
| How many users per site? | | Number of users |
| What types of user profiles do you use? (if applicable) | | If applicable indicate the kind of users e.g. Engineering, Viewers, SmarTeam - Editor, SmarTeam - Web Editor. If not applicable use NA |
| What languages are required | | List all possible languages |

Appendix E: Implementing the LUM Server over a Firewall

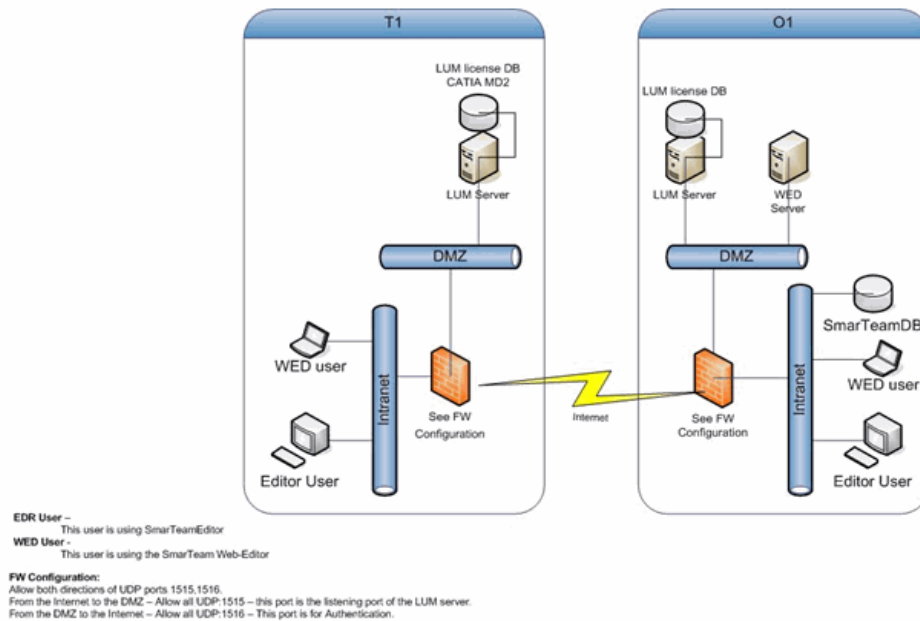
The purpose of this appendix is to describe the layout, conditions, and requirements to activate SmarTeam's License Use Management solution integrated in its product with the LUM server located in the organization's network, while a firewall machine is between them. This appendix outlines the recommended configuration for the solution to work. The suggested topology includes network rules, relevant machine layout, and configuration files.

SmarTeam – Editor, third party integration clients, as well as Web applications such as SmarTeam – Web Editor should interact with the SmarTeam core server from client machines over the Internet. Every computerized organization has a firewall that protects its data, and prevents unauthorized access to the company's internal network. SmarTeam integrated license solution is intended to overcome this boundary and allow clients from outside the firm and from its internal LAN to connect to the LUM server.

Network Configuration Requirements

- The Firewall redirects filtered traffic to three different networks - Intranet, DMZ and the Internet.
- Two kinds of users are to be available: SmarTeam - Web Editor and SmarTeam - Editor. Both types of users use the IBM LUM product which manages and validates licenses over the network.
- All the SmarTeam required components (including all LUM clients) are to be installed on machines located at the external side of the Firewall, outside of the organization, or on a different network (organization's LAN), other than the DMZ. Its' LUM client is to be configured to work with the LUM server placed in the organization's demilitarized zone (DMZ). For details, see the Network Topology diagram below.

Network Topology



- **SmartTeam – Web Editor (WED User)** - requires a SmartTeam – Web Editor license
- **SmartTeam – Editor User (Editor User)** - requires a SmartTeam – Editor license

Firewall Configurations

- From the organization's LAN or from the internet, **UDP** access should be allowed from any IP address and source, to the internal LUM Server only with **UDP** destination port number of **1515** (configurable).
- UDP responses are to be allowed from the LUM server out to the LAN and internet
- Make sure that on the same session that is allowed to get in to the DMZ (**1516**), responses with the source port of 1516 (authentication packets) will be allowed also.
- The actual rule:
 - Source: Any
 - Destination: LUM Server
 - Service: 1515, 1516
 - Action: Accept

LUM Server Configuration

- "On the server, set the following value in the configuration file I4LS.INI:
 - ipAuthPort=1516 (configurable)

Note: The ipAuthPort value must match the firewall configuration.

- "On the client, set the following value in the configuration file I4LS.INI:

- DirectBindServer1=ip:lum_server_ip [1515]

Additional license servers can be added, by changing the server number on the parameter to -2, 3, etc.