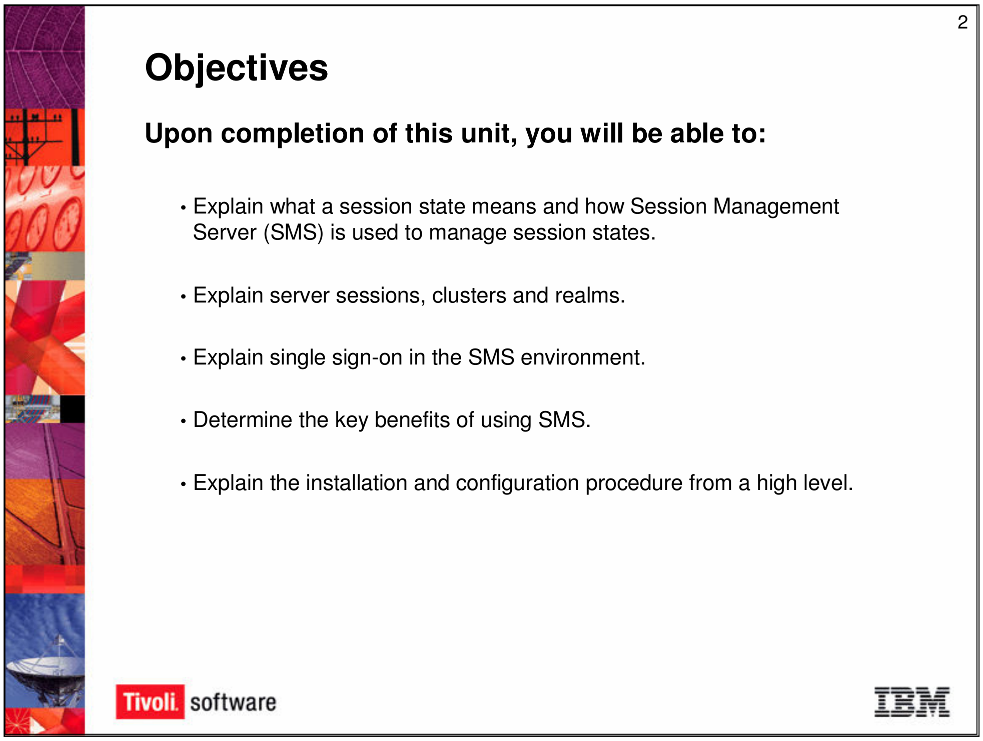
Tivoli software

IBM

Session Management Server for IBM Tivoli Access Manager

e business software

IBM Software Group

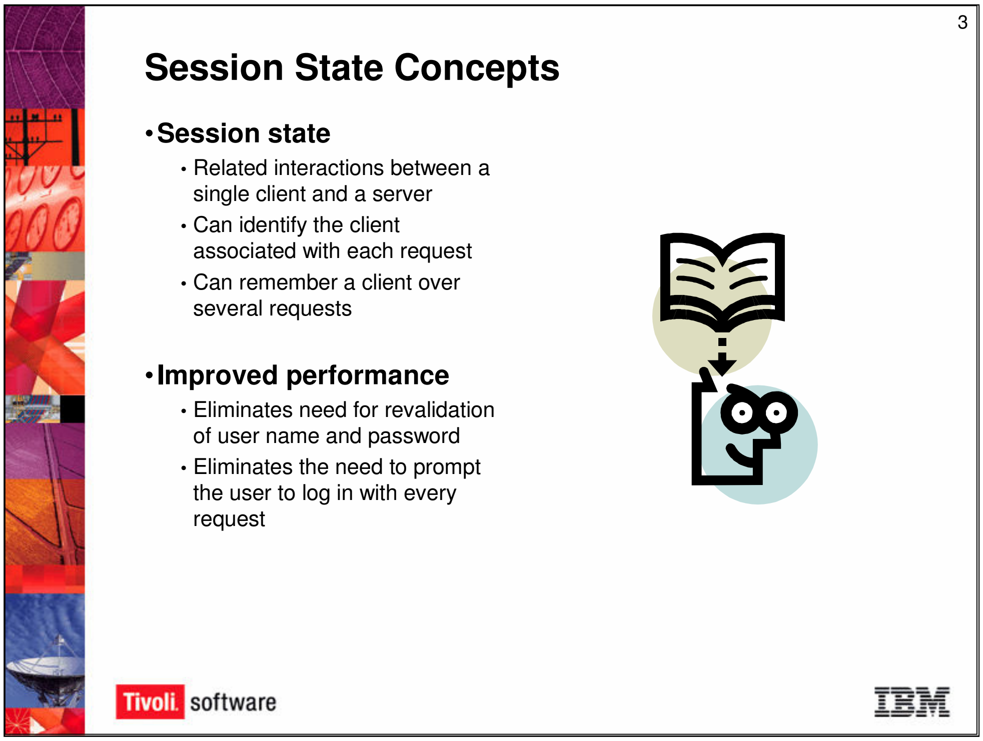


Objectives

Upon completion of this unit, you will be able to:

- Explain what a session state means and how Session Management Server (SMS) is used to manage session states.
- Explain server sessions, clusters and realms.
- Explain single sign-on in the SMS environment.
- Determine the key benefits of using SMS.
- Explain the installation and configuration procedure from a high level.

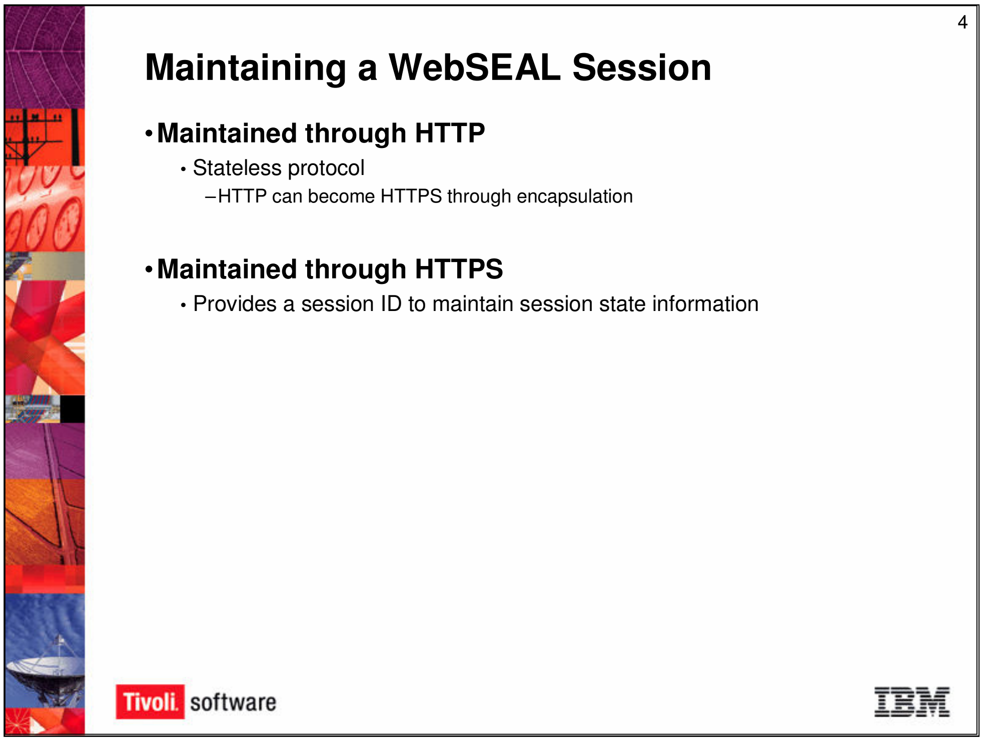
Tivoli. software



Session State Concepts

- **Session state**
  - Related interactions between a single client and a server
  - Can identify the client associated with each request
  - Can remember a client over several requests

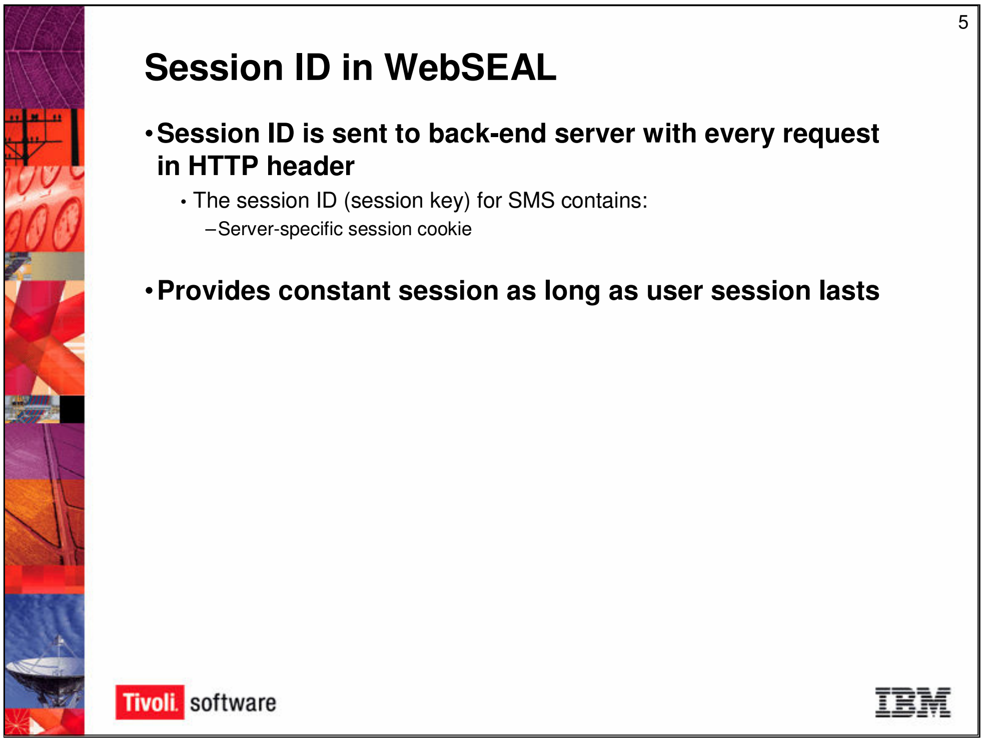
- **Improved performance**
  - Eliminates need for revalidation of user name and password
  - Eliminates the need to prompt the user to log in with every request



Maintaining a WebSEAL Session

- **Maintained through HTTP**
  - Stateless protocol
    - –HTTP can become HTTPS through encapsulation

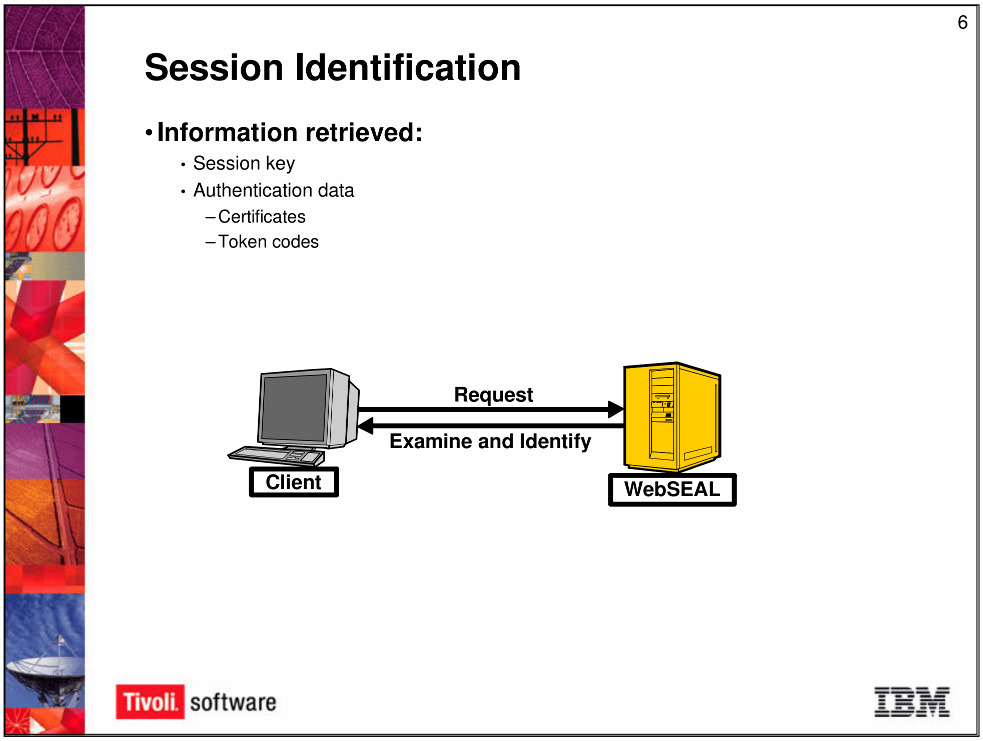
- **Maintained through HTTPS**
  - Provides a session ID to maintain session state information



Session ID in WebSEAL

- **Session ID is sent to back-end server with every request in HTTP header**
  - The session ID (session key) for SMS contains:
    - Server-specific session cookie

- **Provides constant session as long as user session lasts**



Session Identification

- **Information retrieved:**
  - Session key
  - Authentication data
    - Certificates
    - Token codes

Request

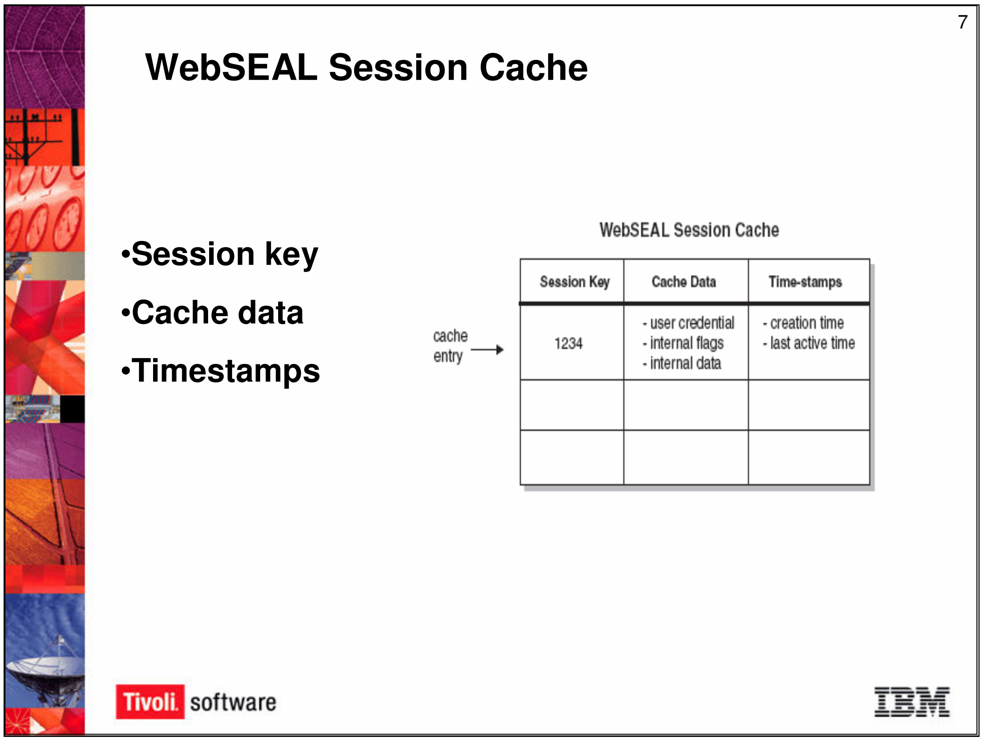
Examine and Identify

Client

WebSEAL

Tivoli. software

IBM



WebSEAL Session Cache

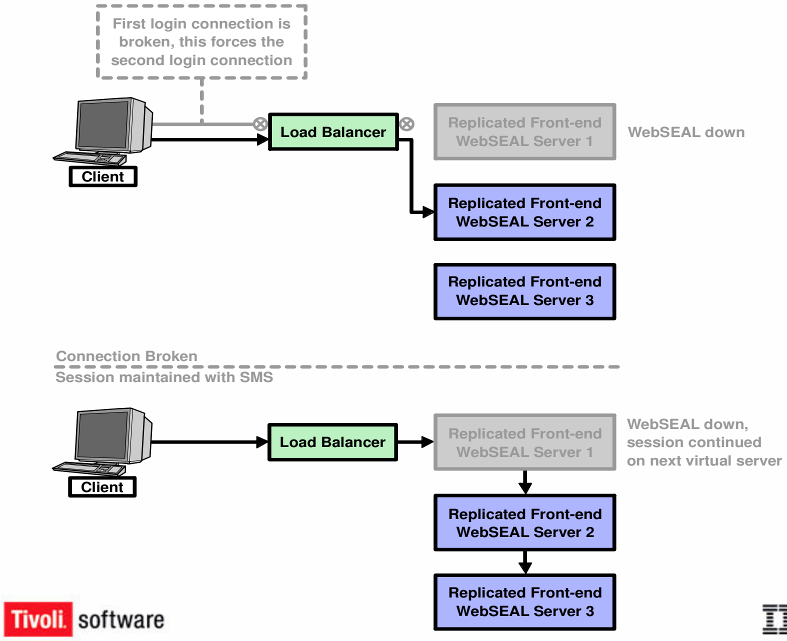
- •Session key
- •Cache data
- •Timestamps

WebSEAL Session Cache

cache entry →

Session Key	Cache Data	Time-stamps
1234	- user credential - internal flags - internal data	- creation time - last active time

Failover Scenario



First login connection is broken, this forces the second login connection

Client

Load Balancer

Replicated Front-end WebSEAL Server 1

WebSEAL down

Replicated Front-end WebSEAL Server 2

Replicated Front-end WebSEAL Server 3

Connection Broken

Session maintained with SMS

Client

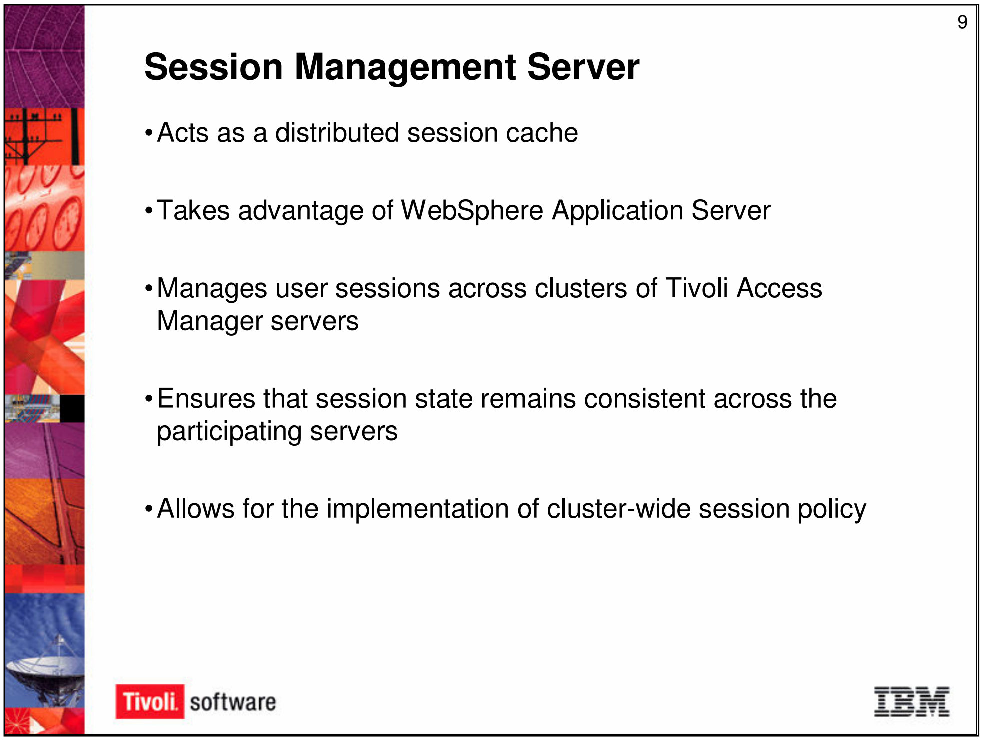
Load Balancer

Replicated Front-end WebSEAL Server 1

WebSEAL down, session continued on next virtual server

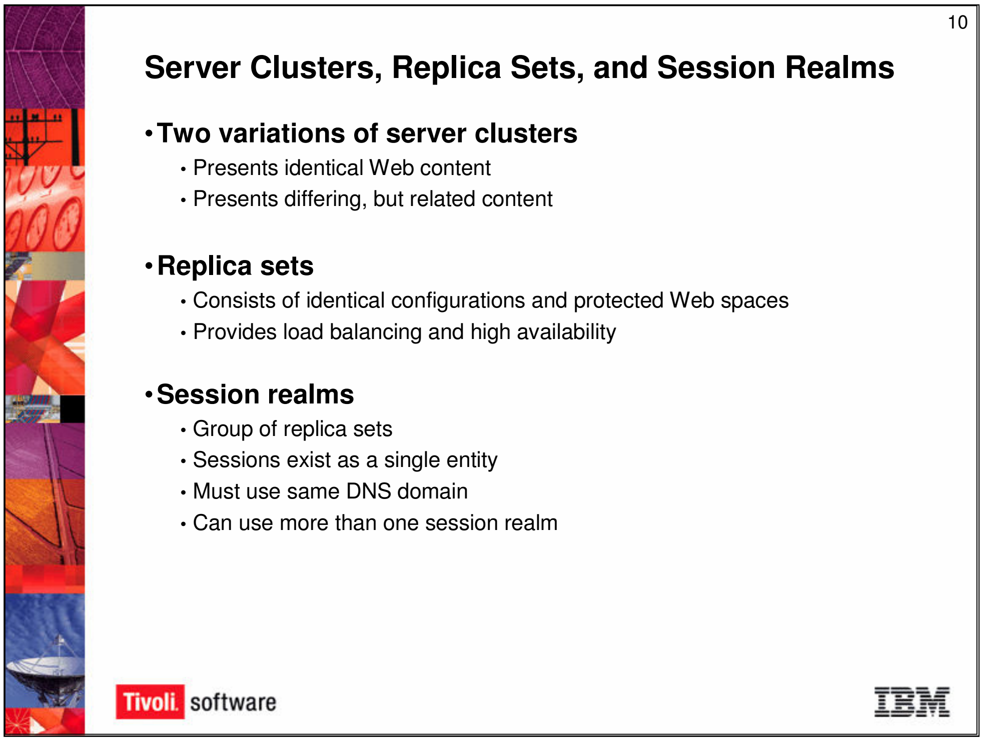
Replicated Front-end WebSEAL Server 2

Replicated Front-end WebSEAL Server 3



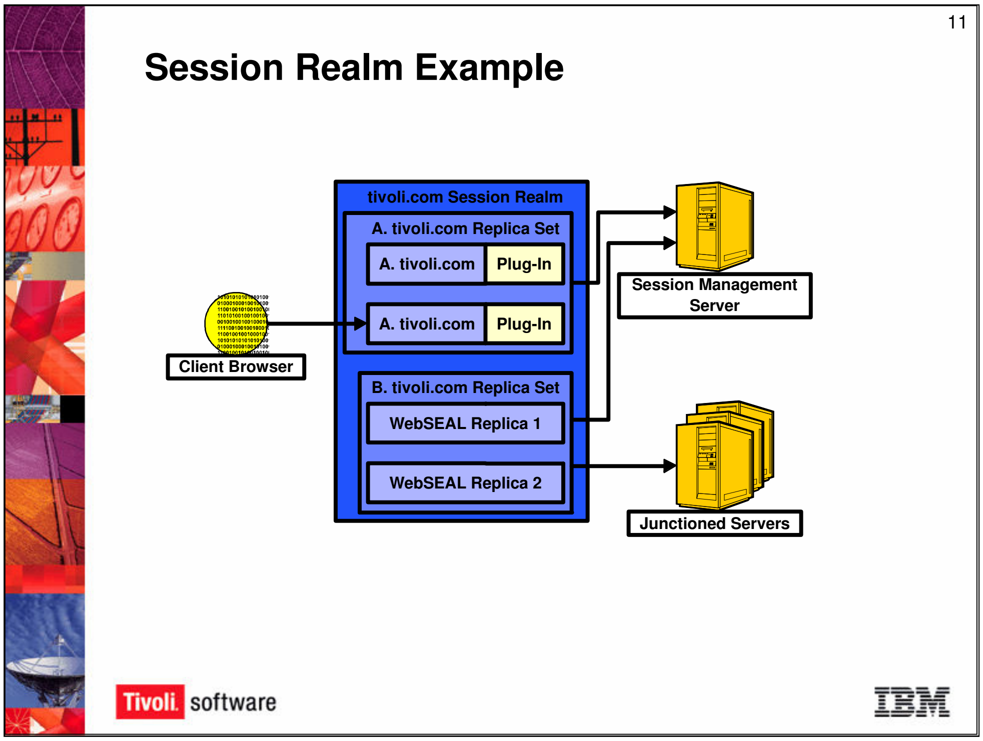
Session Management Server

- Acts as a distributed session cache
- Takes advantage of WebSphere Application Server
- Manages user sessions across clusters of Tivoli Access Manager servers
- Ensures that session state remains consistent across the participating servers
- Allows for the implementation of cluster-wide session policy



Server Clusters, Replica Sets, and Session Realms

- **Two variations of server clusters**
  - Presents identical Web content
  - Presents differing, but related content
- **Replica sets**
  - Consists of identical configurations and protected Web spaces
  - Provides load balancing and high availability
- **Session realms**
  - Group of replica sets
  - Sessions exist as a single entity
  - Must use same DNS domain
  - Can use more than one session realm



Session Realm Example

tivoli.com Session Realm

A. tivoli.com Replica Set

A. tivoli.com | Plug-In

A. tivoli.com | Plug-In

B. tivoli.com Replica Set

WebSEAL Replica 1

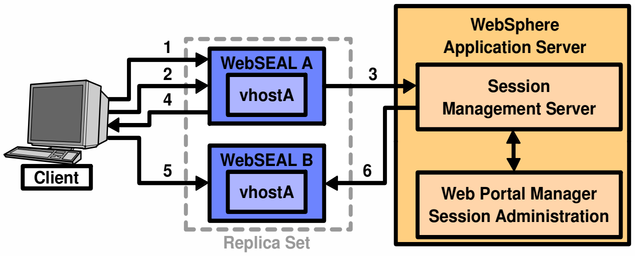
WebSEAL Replica 2

Client Browser

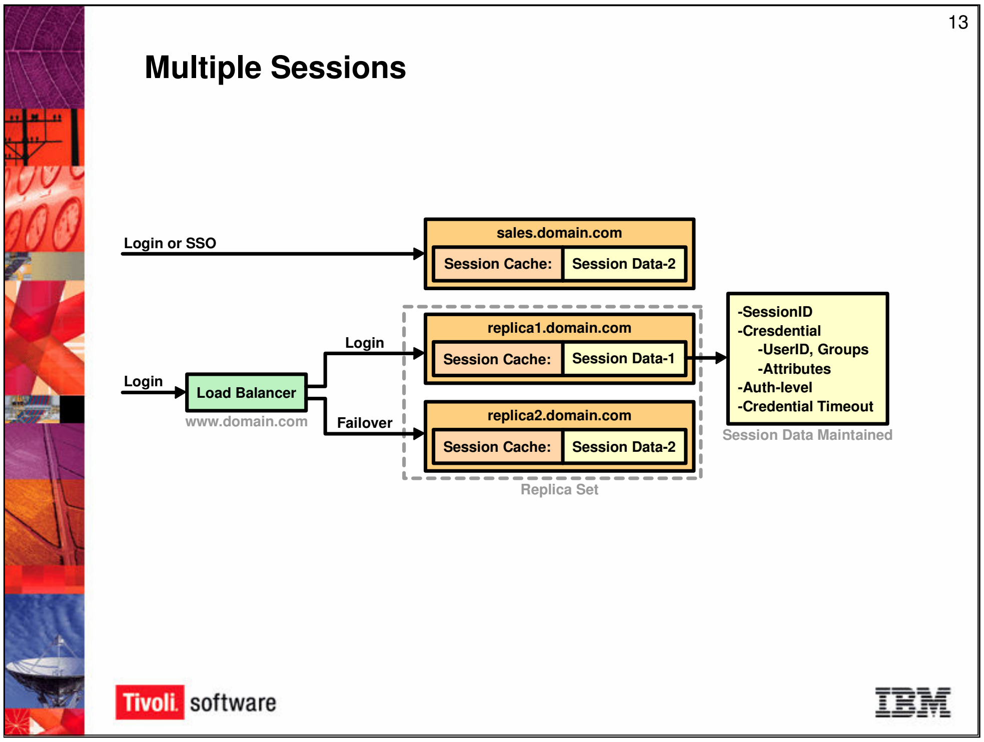
Session Management Server

Junctioned Servers

SMS Process Flow


WebSphere Application Server
Session Management Server
Web Portal Manager Session Administration
WebSEAL A
vhostA
WebSEAL B
vhostA
Replica Set
Client
1
2
3
4
5
6

Multiple Sessions



Login or SSO

sales.domain.com

Session Cache: | Session Data-2

Login

Load Balancer

www.domain.com

Login

Failover

replica1.domain.com

Session Cache: | Session Data-1

replica2.domain.com

Session Cache: | Session Data-2

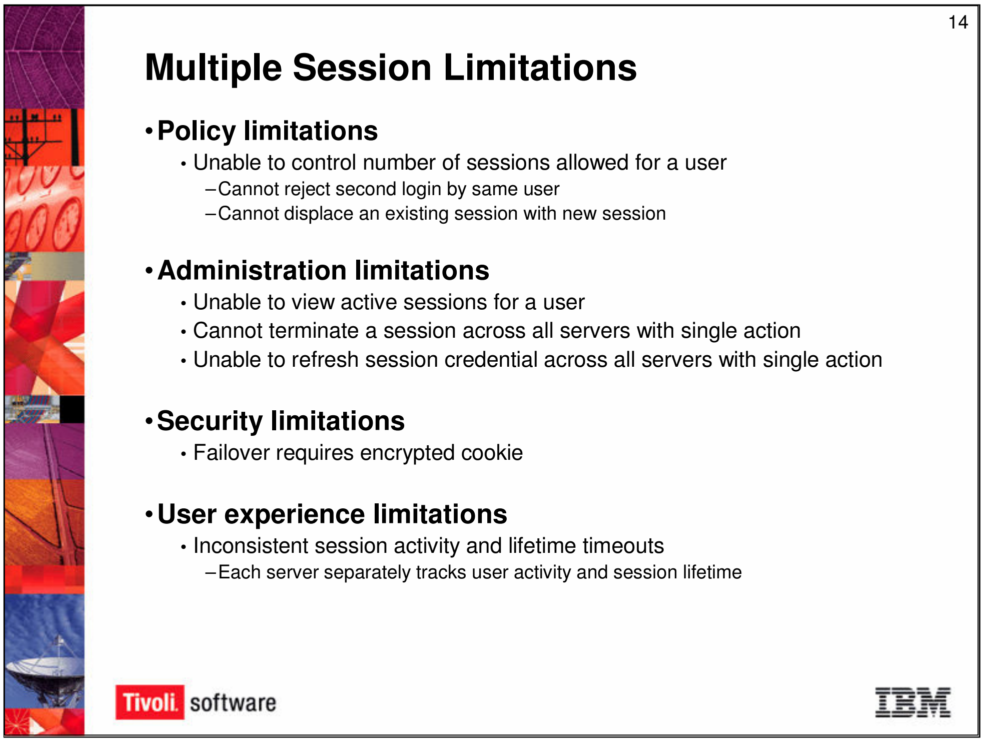
Replica Set

-SessionID
-Cresdential
  -UserID, Groups
  -Attributes
-Auth-level
-Credential Timeout

Session Data Maintained

Tivoli. software

IBM



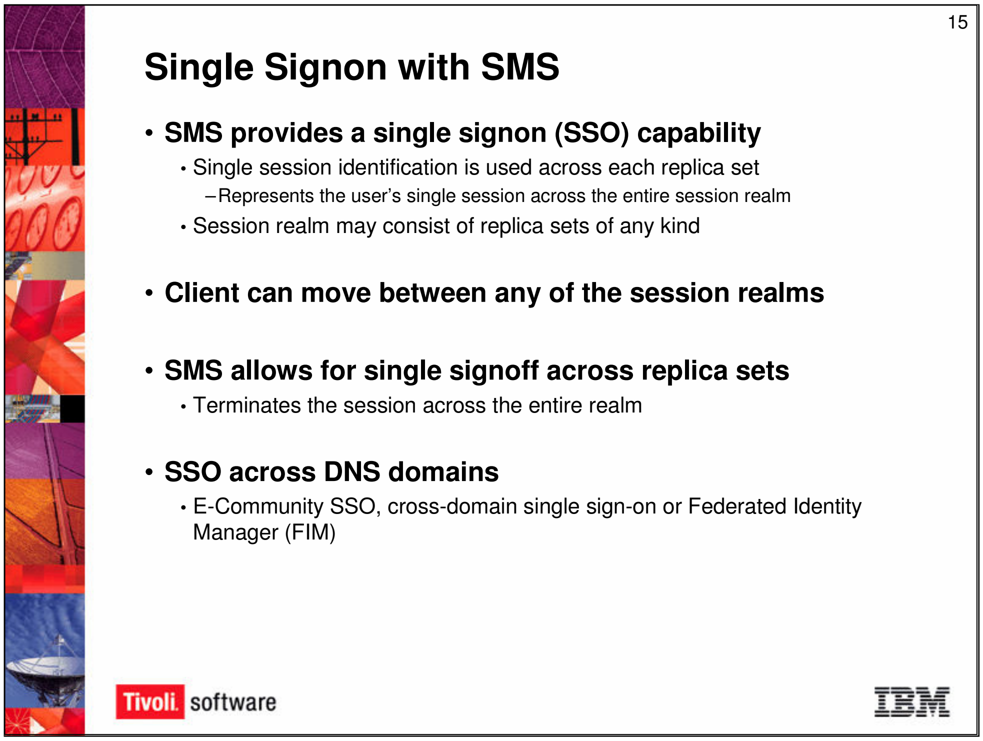
Multiple Session Limitations

- **Policy limitations**
  - Unable to control number of sessions allowed for a user
    - Cannot reject second login by same user
    - Cannot displace an existing session with new session

- **Administration limitations**
  - Unable to view active sessions for a user
  - Cannot terminate a session across all servers with single action
  - Unable to refresh session credential across all servers with single action

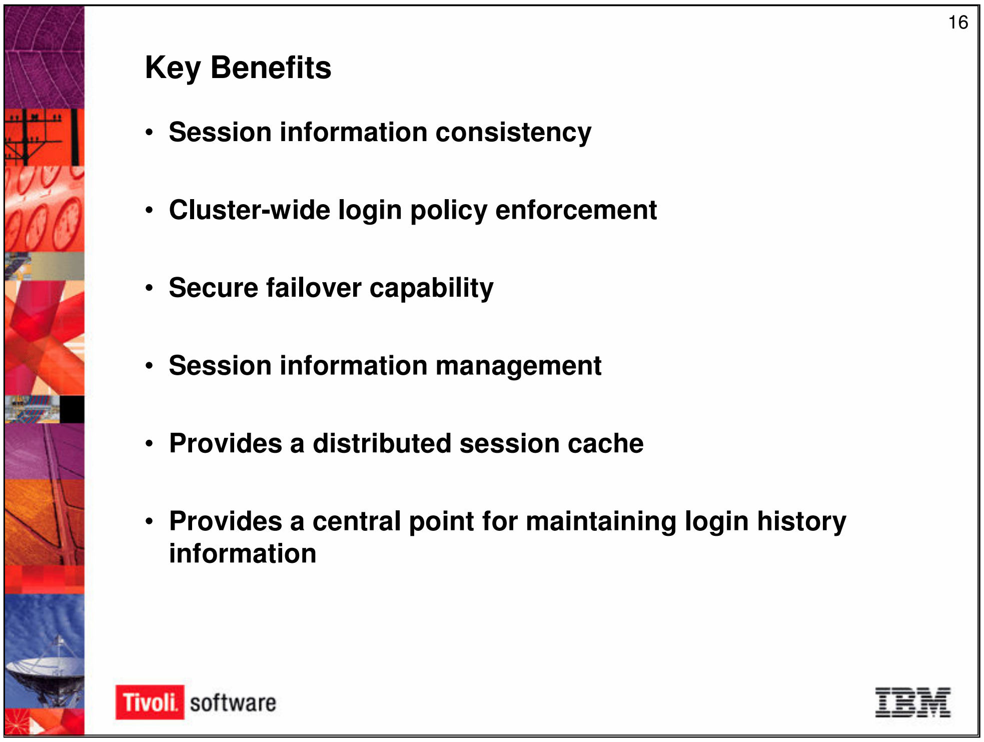
- **Security limitations**
  - Failover requires encrypted cookie

- **User experience limitations**
  - Inconsistent session activity and lifetime timeouts
    - Each server separately tracks user activity and session lifetime



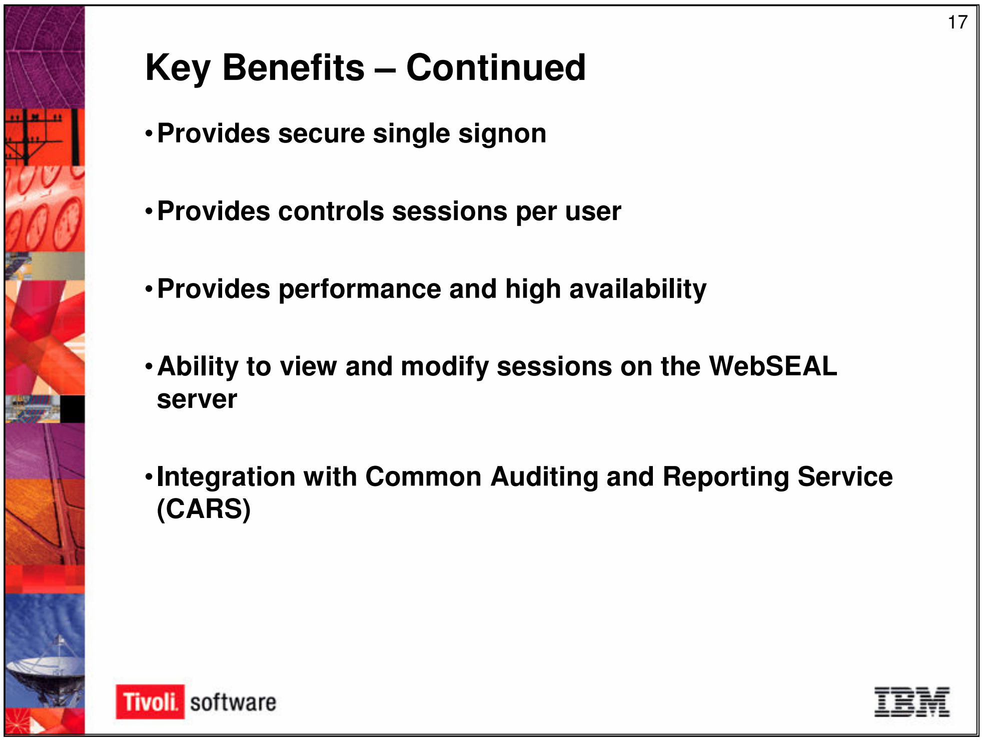
Single Signon with SMS

- **SMS provides a single signon (SSO) capability**
  - Single session identification is used across each replica set
    - Represents the user’s single session across the entire session realm
  - Session realm may consist of replica sets of any kind
- **Client can move between any of the session realms**
- **SMS allows for single signoff across replica sets**
  - Terminates the session across the entire realm
- **SSO across DNS domains**
  - E-Community SSO, cross-domain single sign-on or Federated Identity Manager (FIM)



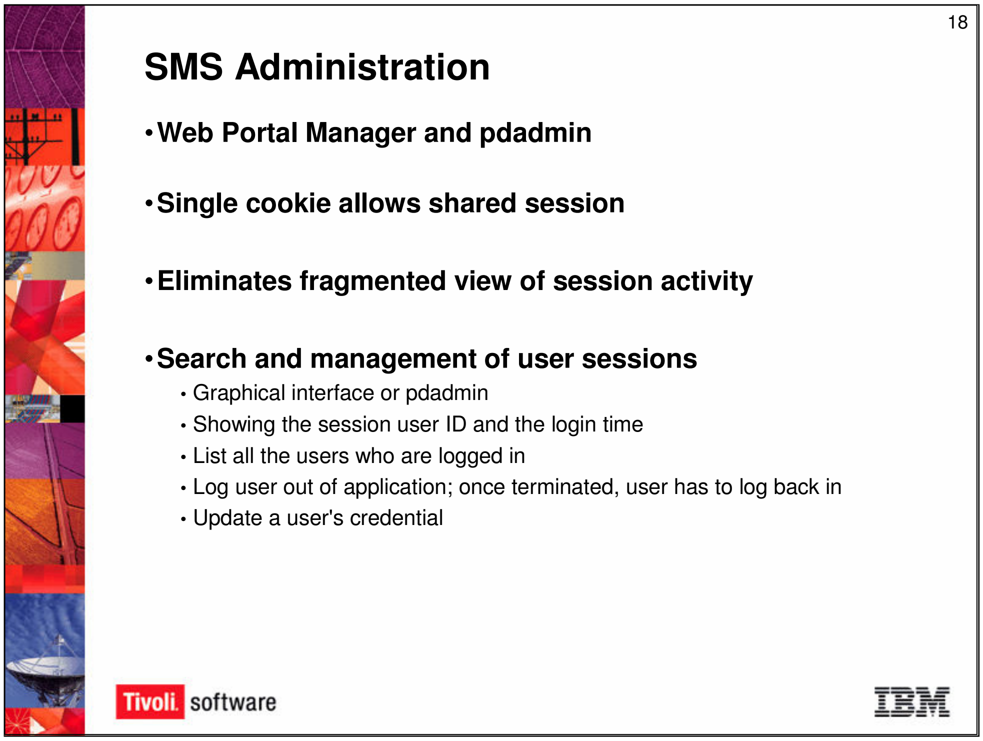
Key Benefits

- Session information consistency
- Cluster-wide login policy enforcement
- Secure failover capability
- Session information management
- Provides a distributed session cache
- Provides a central point for maintaining login history information



Key Benefits – Continued

- Provides secure single signon
- Provides controls sessions per user
- Provides performance and high availability
- Ability to view and modify sessions on the WebSEAL server
- Integration with Common Auditing and Reporting Service (CARS)



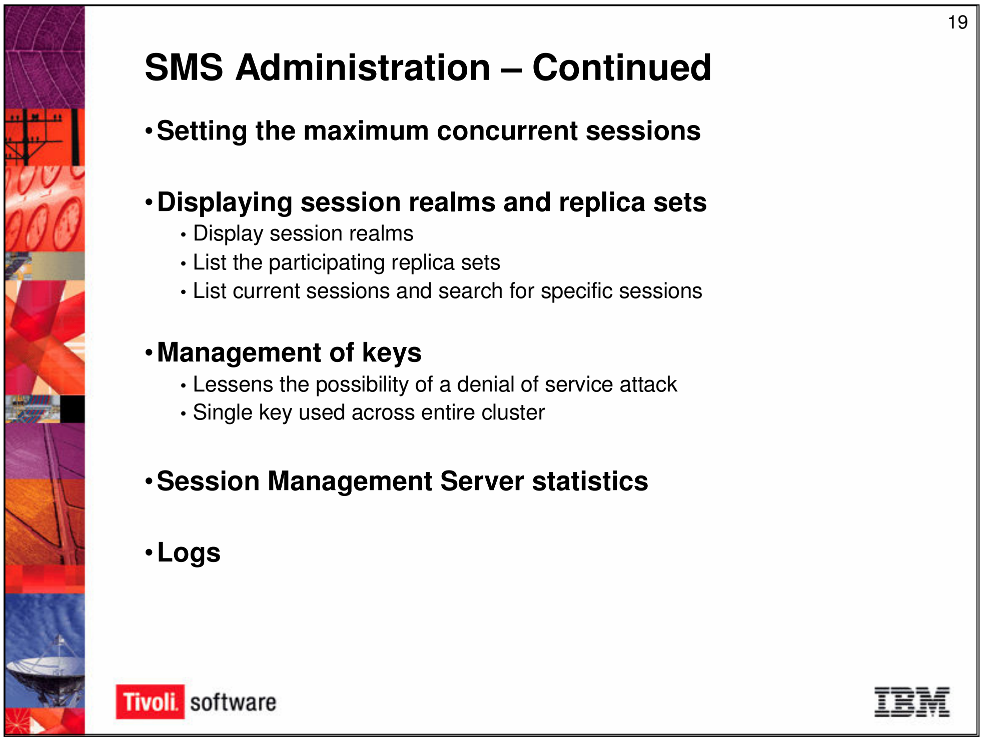
SMS Administration

- Web Portal Manager and pdadmin

- Single cookie allows shared session

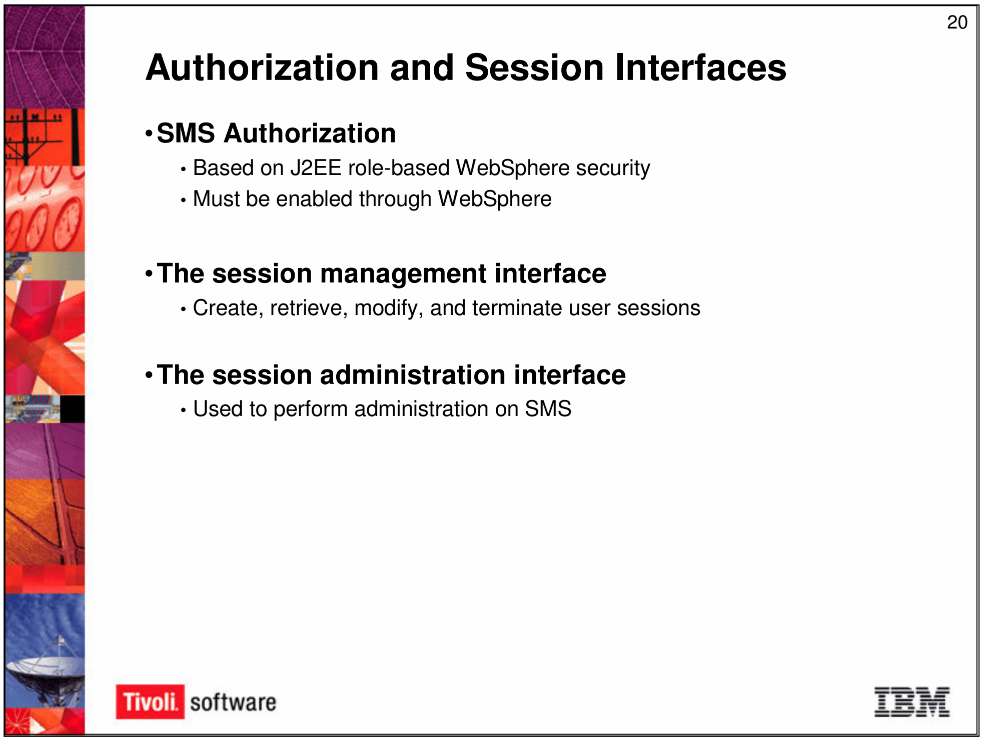
- Eliminates fragmented view of session activity

- Search and management of user sessions
  - Graphical interface or pdadmin
  - Showing the session user ID and the login time
  - List all the users who are logged in
  - Log user out of application; once terminated, user has to log back in
  - Update a user's credential



SMS Administration – Continued

- **Setting the maximum concurrent sessions**
- **Displaying session realms and replica sets**
  - Display session realms
  - List the participating replica sets
  - List current sessions and search for specific sessions
- **Management of keys**
  - Lessens the possibility of a denial of service attack
  - Single key used across entire cluster
- **Session Management Server statistics**
- **Logs**



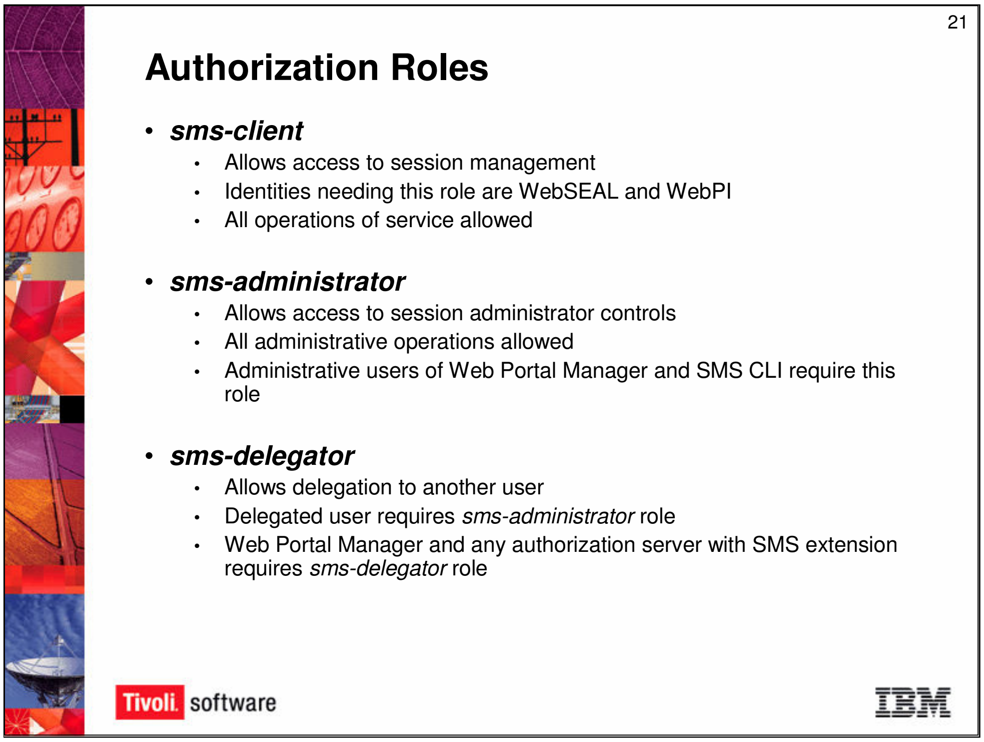
Authorization and Session Interfaces

- **SMS Authorization**
  - Based on J2EE role-based WebSphere security
  - Must be enabled through WebSphere

- **The session management interface**
  - Create, retrieve, modify, and terminate user sessions

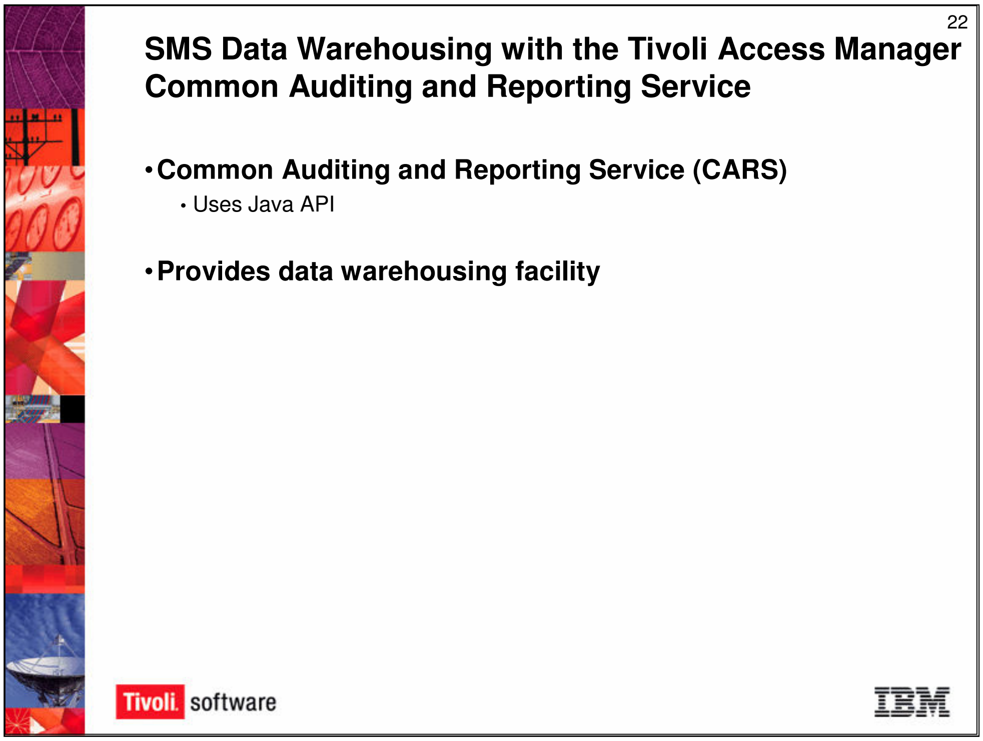
- **The session administration interface**
  - Used to perform administration on SMS

Tivoli. software
IBM



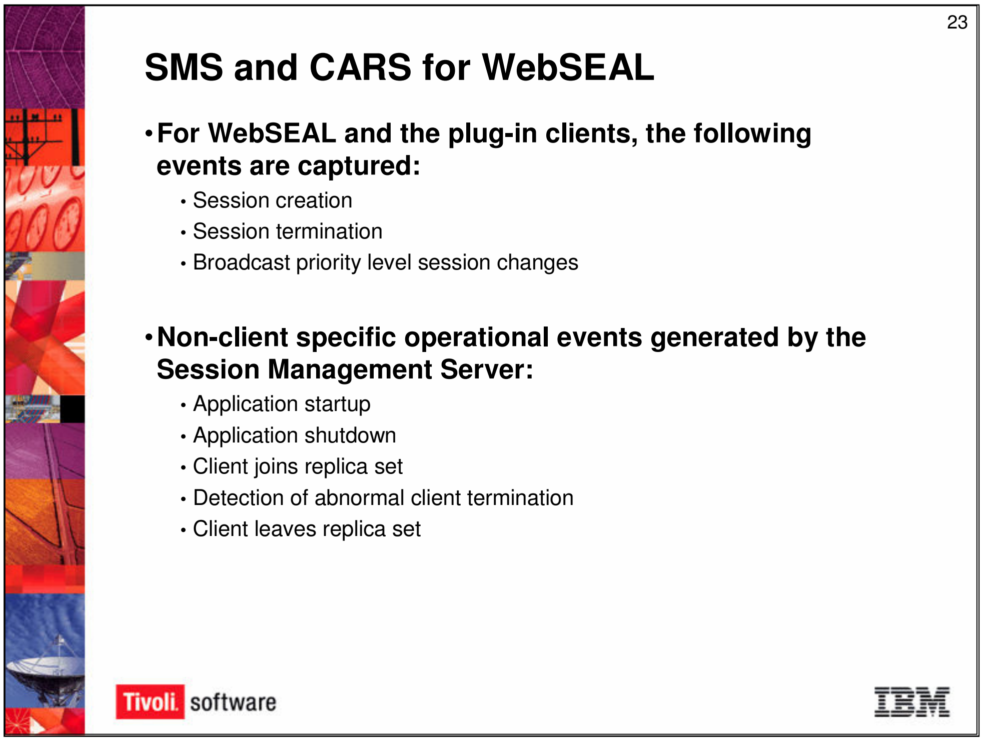
Authorization Roles

- ***sms-client***
  - Allows access to session management
  - Identities needing this role are WebSEAL and WebPI
  - All operations of service allowed
- ***sms-administrator***
  - Allows access to session administrator controls
  - All administrative operations allowed
  - Administrative users of Web Portal Manager and SMS CLI require this role
- ***sms-delegator***
  - Allows delegation to another user
  - Delegated user requires *sms-administrator* role
  - Web Portal Manager and any authorization server with SMS extension requires *sms-delegator* role



SMS Data Warehousing with the Tivoli Access Manager Common Auditing and Reporting Service

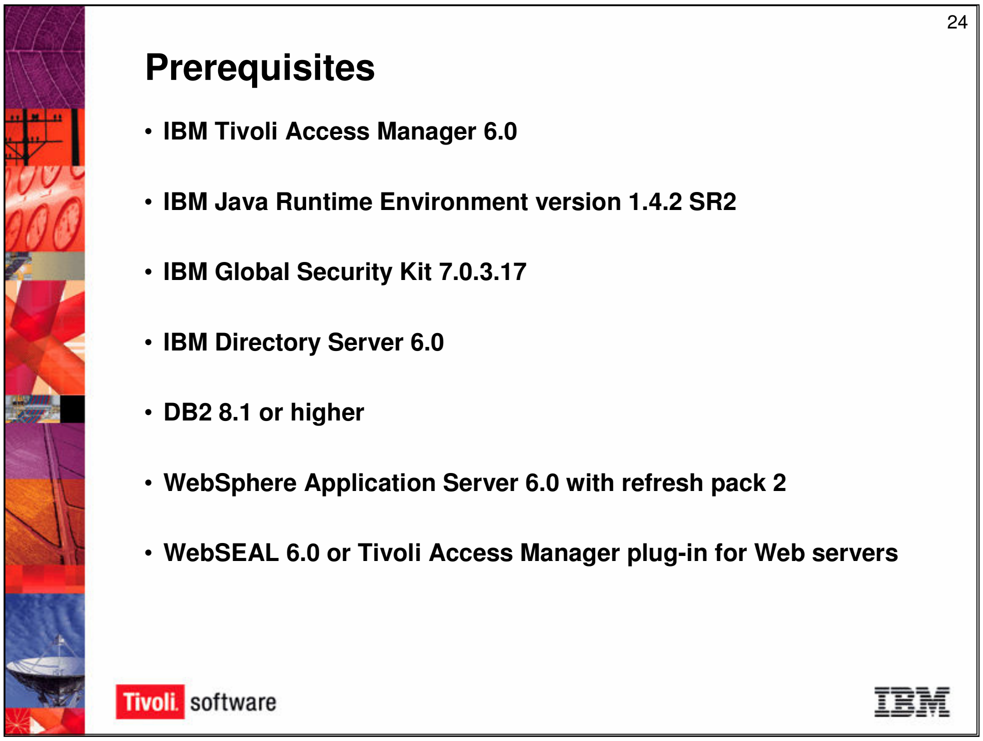
- **Common Auditing and Reporting Service (CARS)**
  - Uses Java API
- **Provides data warehousing facility**



SMS and CARS for WebSEAL

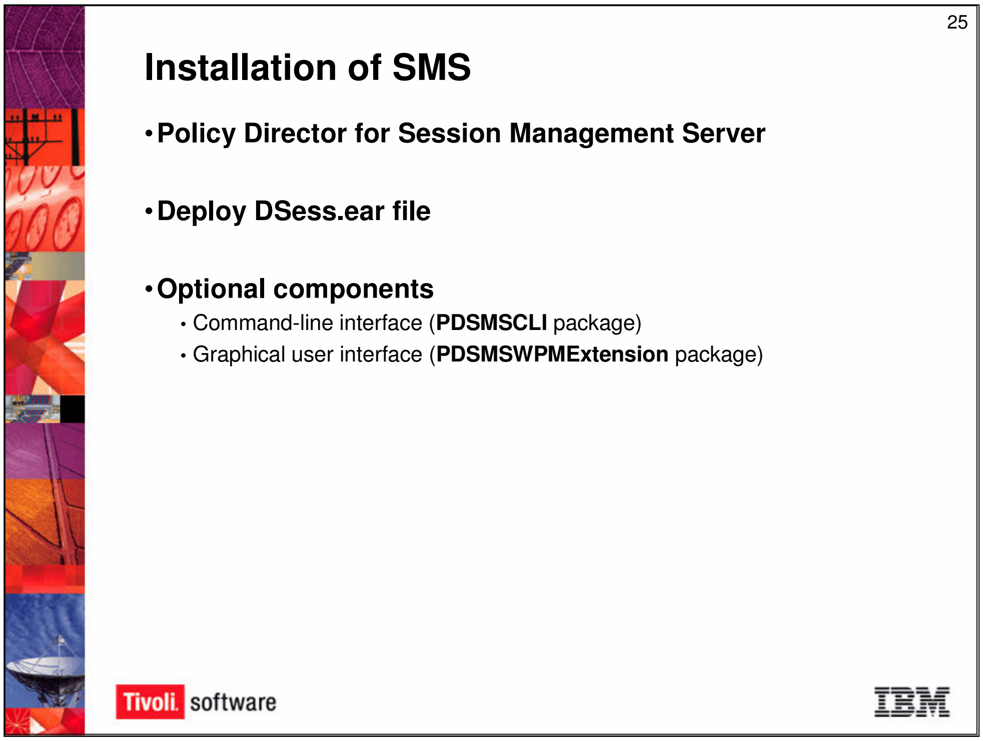
- **For WebSEAL and the plug-in clients, the following events are captured:**
  - Session creation
  - Session termination
  - Broadcast priority level session changes

- **Non-client specific operational events generated by the Session Management Server:**
  - Application startup
  - Application shutdown
  - Client joins replica set
  - Detection of abnormal client termination
  - Client leaves replica set



Prerequisites

- IBM Tivoli Access Manager 6.0
- IBM Java Runtime Environment version 1.4.2 SR2
- IBM Global Security Kit 7.0.3.17
- IBM Directory Server 6.0
- DB2 8.1 or higher
- WebSphere Application Server 6.0 with refresh pack 2
- WebSEAL 6.0 or Tivoli Access Manager plug-in for Web servers

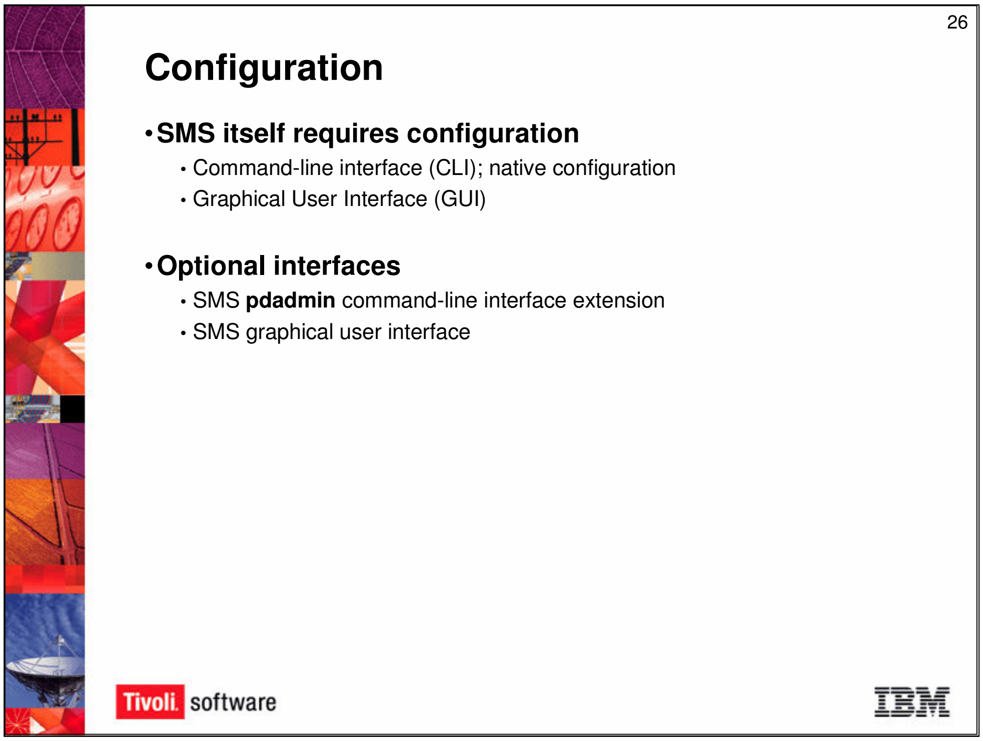


Installation of SMS

- **Policy Director for Session Management Server**

- **Deploy DSess.ear file**

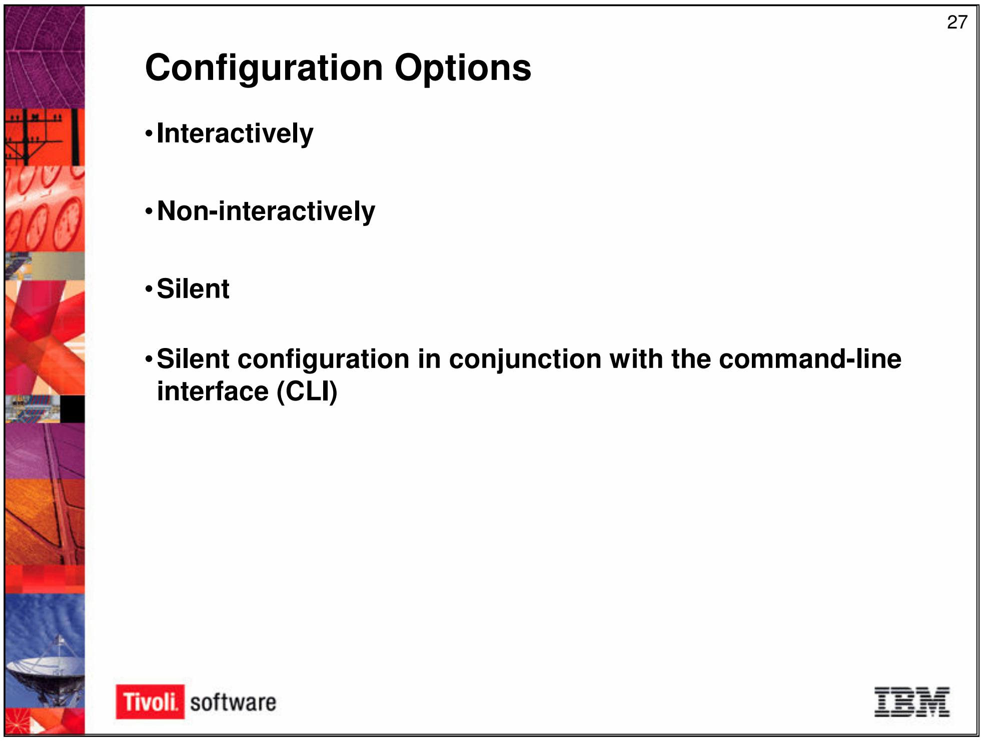
- **Optional components**
  - Command-line interface (**PDSMSCLI** package)
  - Graphical user interface (**PDSMSWPMExtension** package)



Configuration

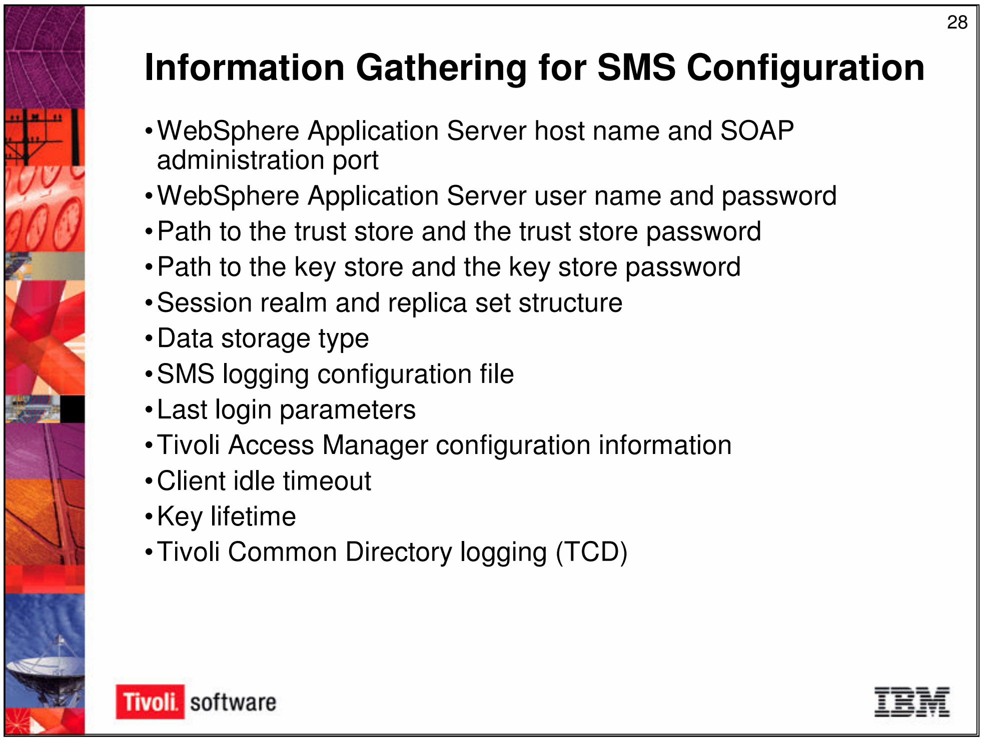
- **SMS itself requires configuration**
  - Command-line interface (CLI); native configuration
  - Graphical User Interface (GUI)

- **Optional interfaces**
  - SMS **pdadmin** command-line interface extension
  - SMS graphical user interface



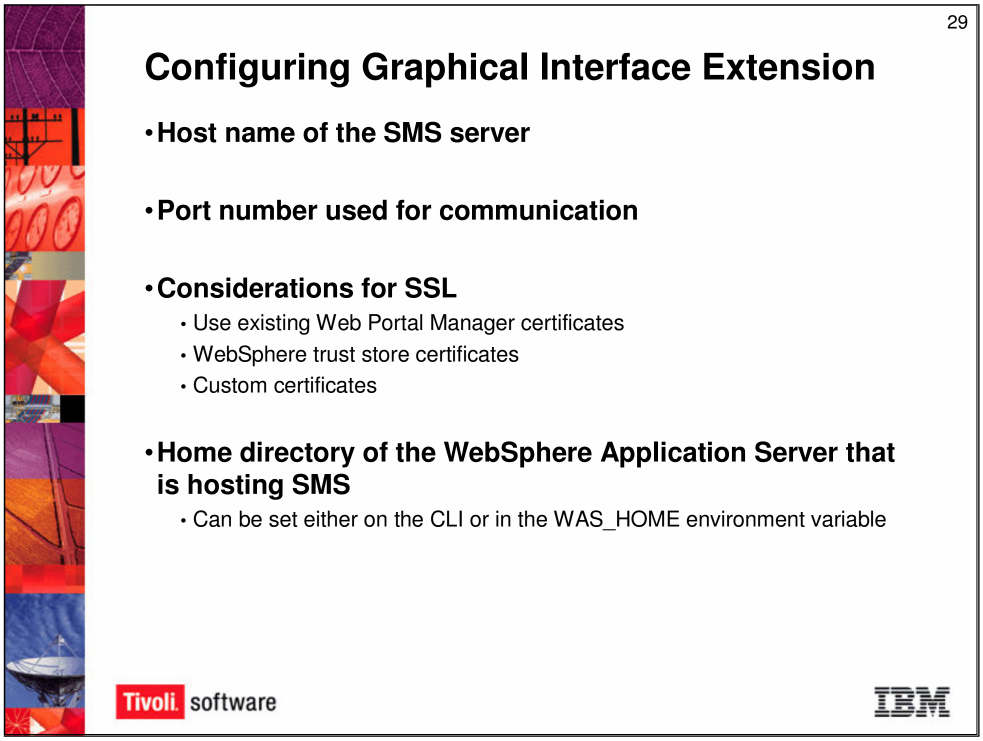
Configuration Options

- Interactively
- Non-interactively
- Silent
- Silent configuration in conjunction with the command-line interface (CLI)



Information Gathering for SMS Configuration

- WebSphere Application Server host name and SOAP administration port
- WebSphere Application Server user name and password
- Path to the trust store and the trust store password
- Path to the key store and the key store password
- Session realm and replica set structure
- Data storage type
- SMS logging configuration file
- Last login parameters
- Tivoli Access Manager configuration information
- Client idle timeout
- Key lifetime
- Tivoli Common Directory logging (TCD)



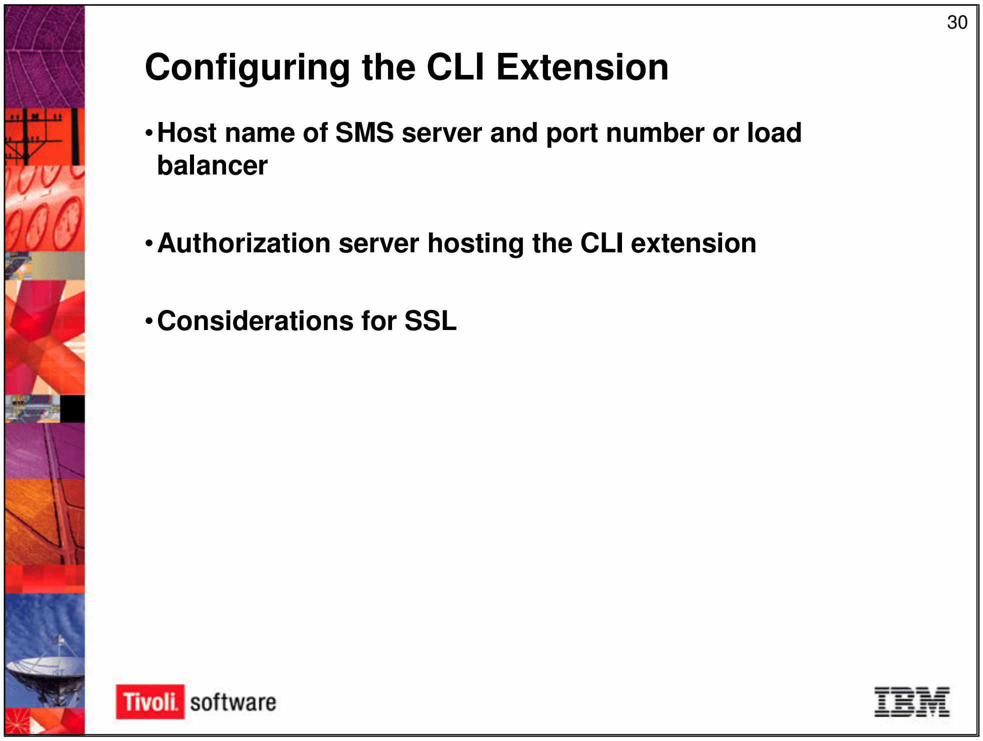
Configuring Graphical Interface Extension

- **Host name of the SMS server**

- **Port number used for communication**

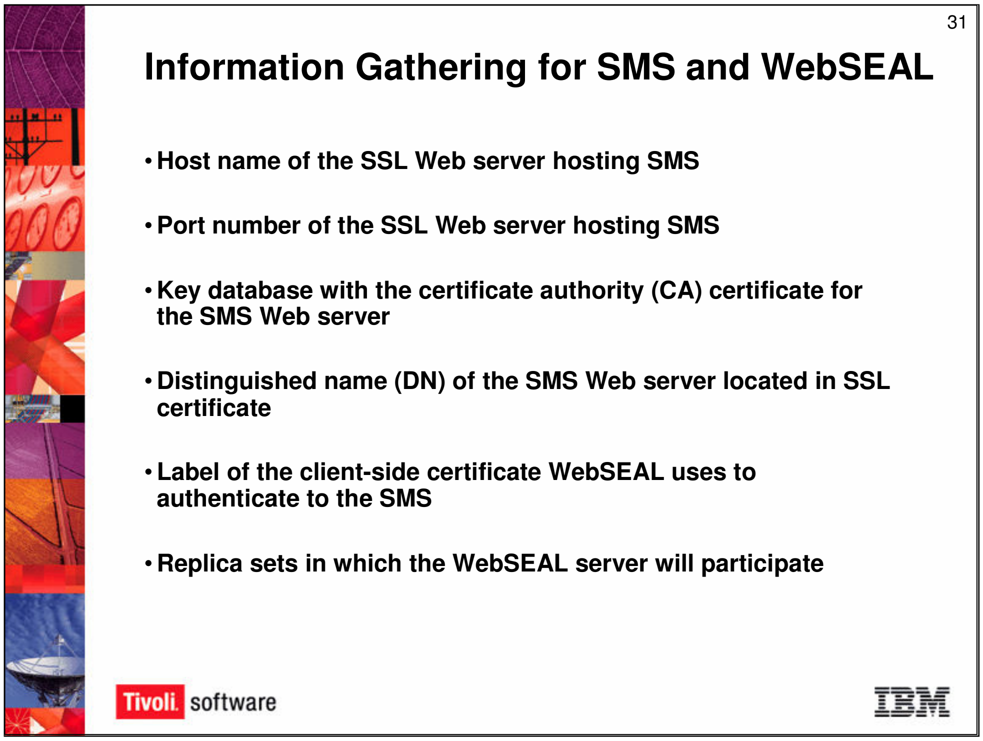
- **Considerations for SSL**
  - Use existing Web Portal Manager certificates
  - WebSphere trust store certificates
  - Custom certificates

- **Home directory of the WebSphere Application Server that is hosting SMS**
  - Can be set either on the CLI or in the WAS_HOME environment variable



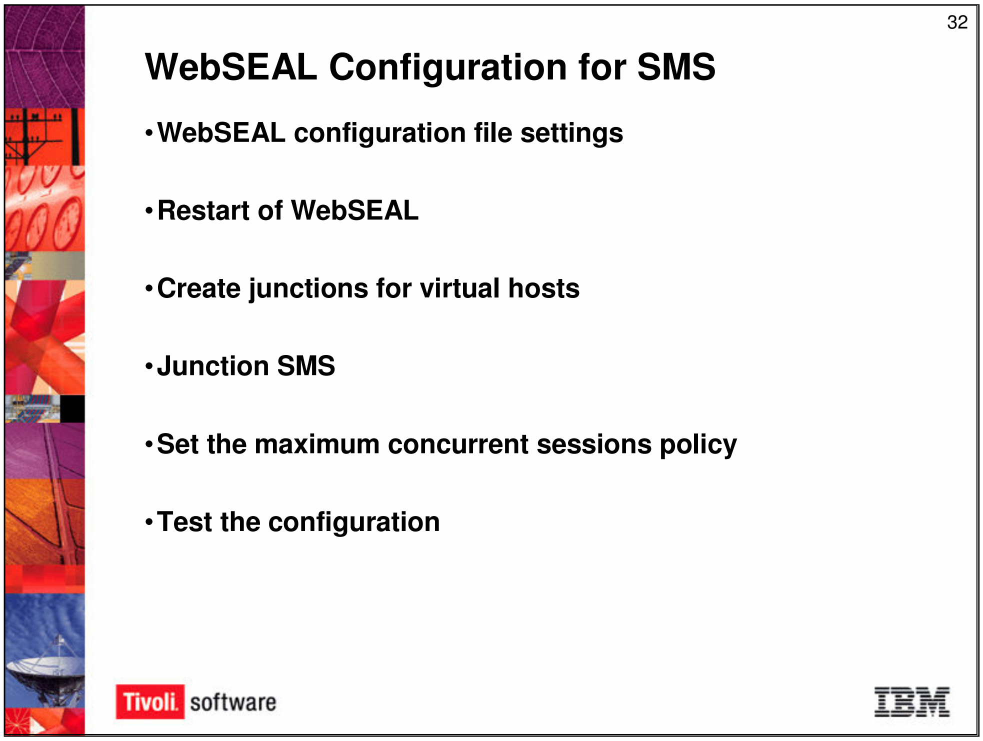
Configuring the CLI Extension

- Host name of SMS server and port number or load balancer
- Authorization server hosting the CLI extension
- Considerations for SSL



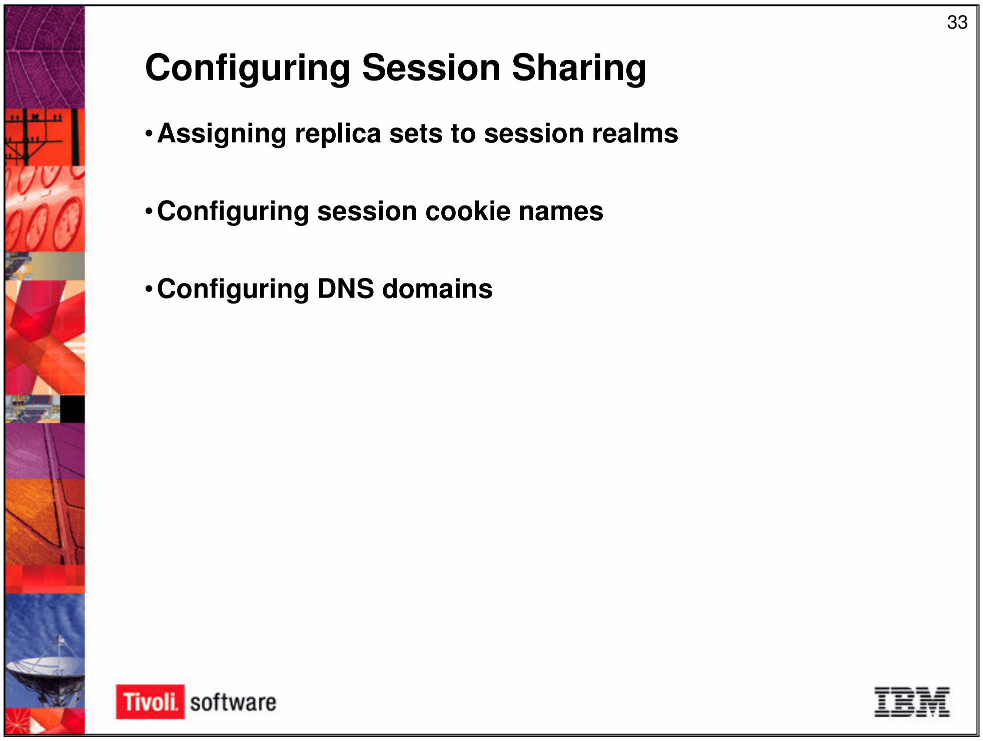
Information Gathering for SMS and WebSEAL

- Host name of the SSL Web server hosting SMS
- Port number of the SSL Web server hosting SMS
- Key database with the certificate authority (CA) certificate for the SMS Web server
- Distinguished name (DN) of the SMS Web server located in SSL certificate
- Label of the client-side certificate WebSEAL uses to authenticate to the SMS
- Replica sets in which the WebSEAL server will participate



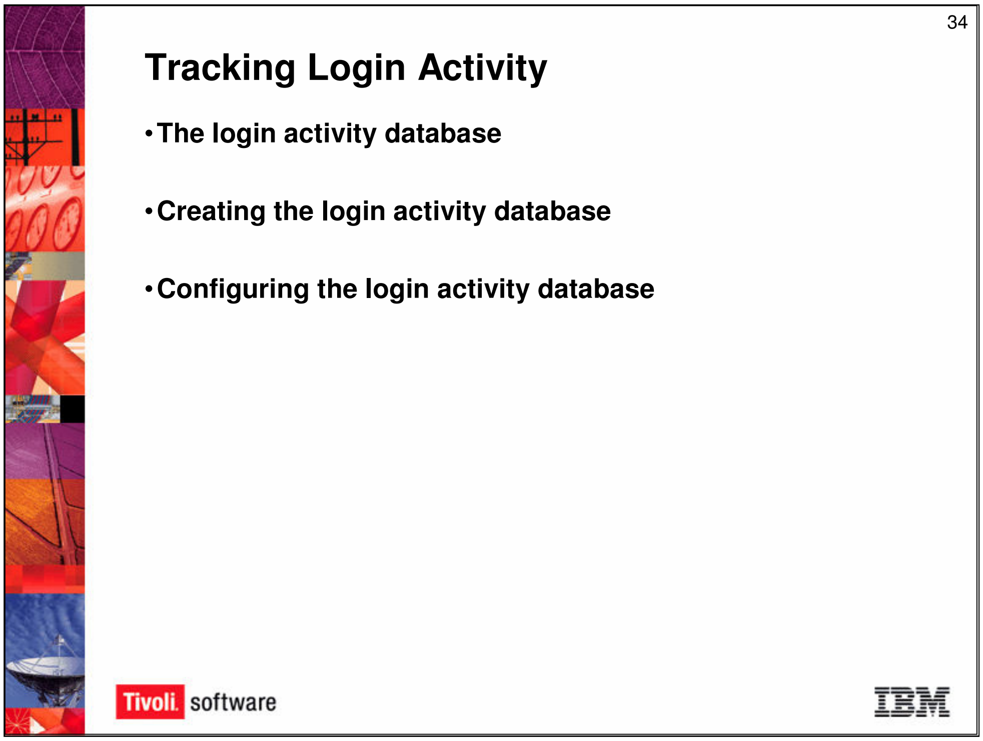
WebSEAL Configuration for SMS

- WebSEAL configuration file settings
- Restart of WebSEAL
- Create junctions for virtual hosts
- Junction SMS
- Set the maximum concurrent sessions policy
- Test the configuration



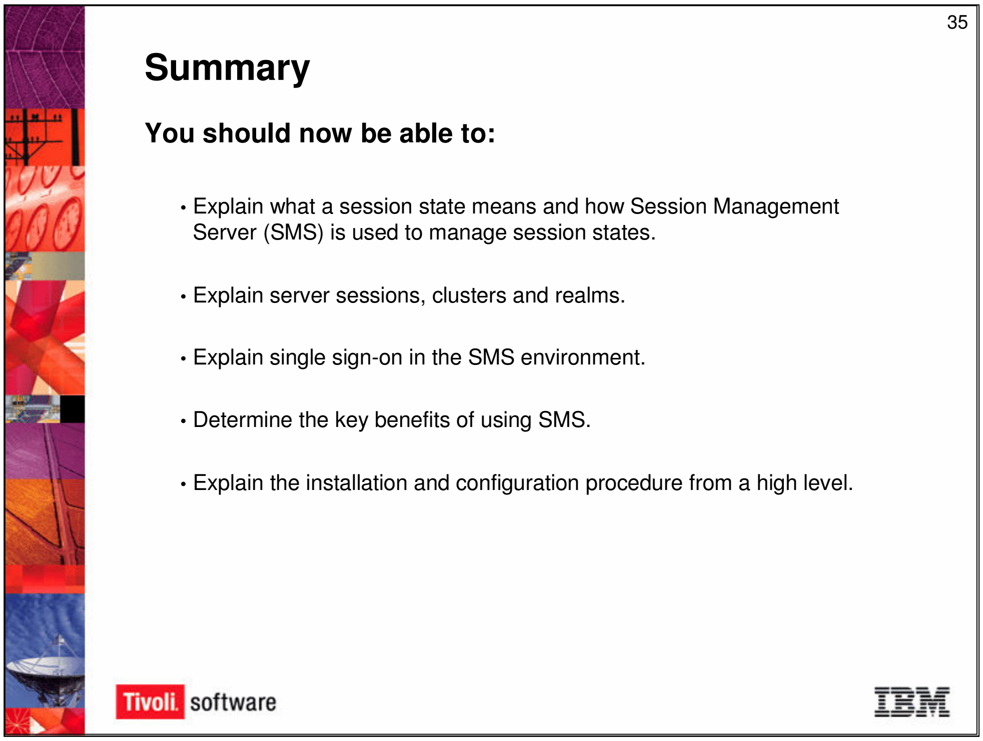
Configuring Session Sharing

- Assigning replica sets to session realms
- Configuring session cookie names
- Configuring DNS domains



Tracking Login Activity

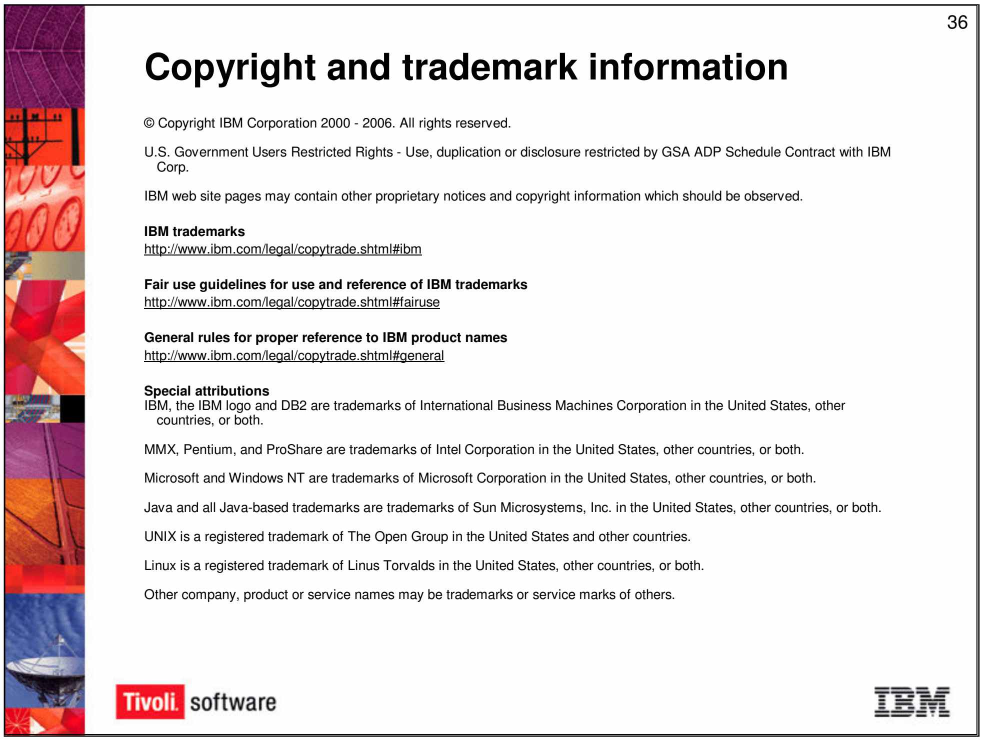
- The login activity database
- Creating the login activity database
- Configuring the login activity database



Summary

You should now be able to:

- Explain what a session state means and how Session Management Server (SMS) is used to manage session states.
- Explain server sessions, clusters and realms.
- Explain single sign-on in the SMS environment.
- Determine the key benefits of using SMS.
- Explain the installation and configuration procedure from a high level.



Copyright and trademark information

IBM trademarks
http://www.ibm.com/legal/copytrade.shtml#ibm

Fair use guidelines for use and reference of IBM trademarks
http://www.ibm.com/legal/copytrade.shtml#fairuse

General rules for proper reference to IBM product names
http://www.ibm.com/legal/copytrade.shtml#general

Special attributions
IBM, the IBM logo and DB2 are trademarks of International Business Machines Corporation in the United States, other countries, or both.

MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.