



| IBM Software Group

WAS V7 Security Features



@business on demand.

© 2008 IBM Corporation
Updated September 28, 2009

Agenda

- X-Force
- Multiple security domains
- Fine-grained administrative security
- Security auditing
- Certificate management enhancements
- Kerberos

X-Force WebSphere Vulnerability Search

- <http://webapp.iss.net/Search.do?searchType=vuln>

Search

- Keyword Search
- Vulnerability Search
- Malware Search

Home »

X-Force Vulnerability Search

Search for:

 [Search Tips](#)

Sort by date / [Sort by relevance](#)

Results 1 to 10 of 159 total results for **websphere**

ISS X-Force Database:
websphere-console-session-hijacking(49499) ...
... IBM **WebSphere** Application Server administrative console forced logout session hijacking.
websphere-console-session-hijacking (49499), Medium Risk. Description:
...
2009-03-30

ISS X-Force Database: websphere-jax-rpc-username-token(49532):
IBM ...
... IBM **WebSphere** Application Server JAX-RPC WS-Security UsernameToken unspecified.
websphere-jax-rpc-username-token (49532), Low Risk. Description: ...
2009-03-26

Section

Multiple Security Domains

Security domains

- In previous WAS releases:
 - ▶ Most security attributes can be configured at the cell level only.
 - ▶ Individual servers can override only a few specific configurations.

- WAS V7 supports multiple security domains
 - ▶ Allow different security settings in the same cell
 - ▶ More flexible

WebSphere security domains

- Separate security configurations for administrative applications and user applications
- Administrative applications continue to use the data from global security
- Global security domain represents the default configuration for user applications
- Configuration data stored in domains overrides the data from the global security configuration

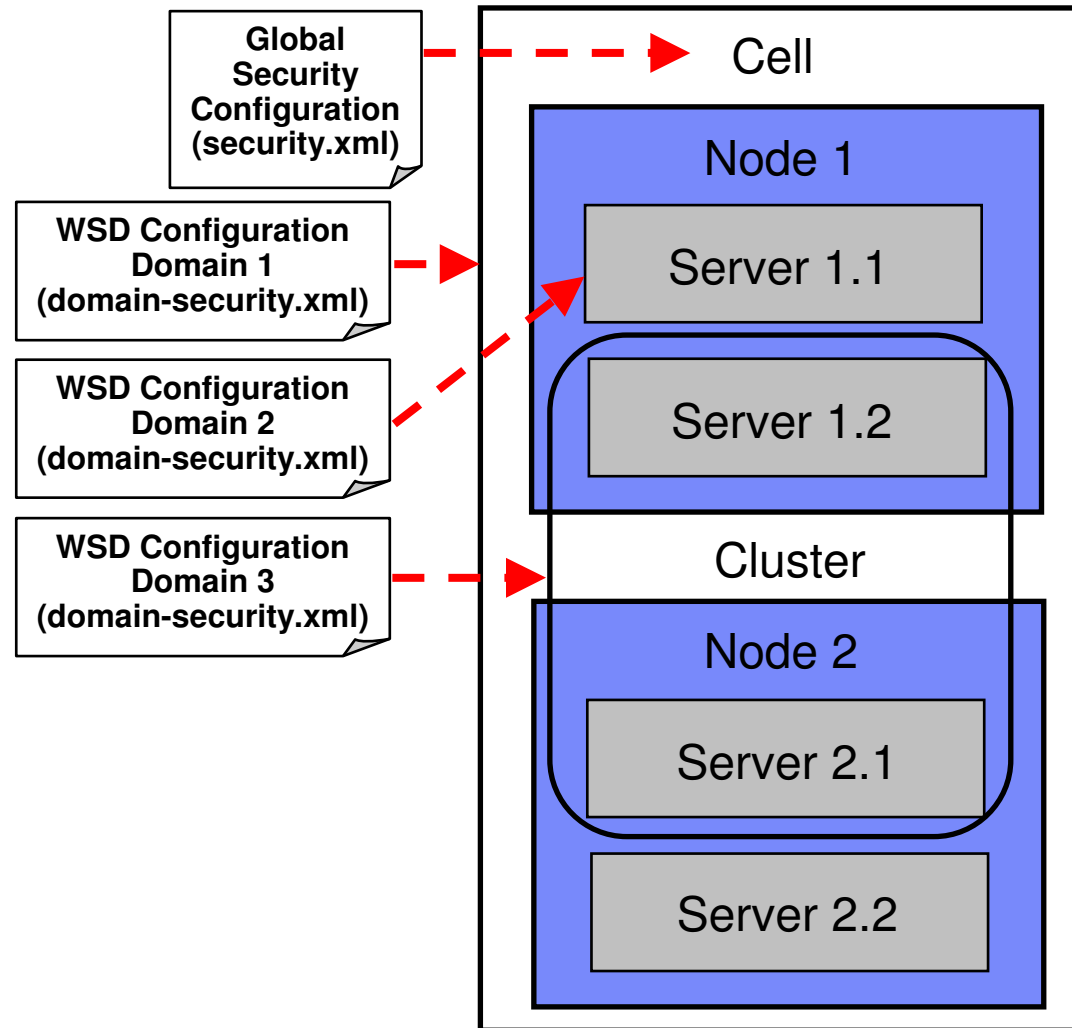
WebSphere security domains: configuration

Global security

- ▶ User registry
- ▶ Trust Association Interceptor (TAI)
- ▶ SPNEGO
- ▶ Authorization
- ▶ Login configurations
- ▶ Application security enablement
- ▶ Java™ 2 security
- ▶ RMI/IIOP (CSlv2 protocol)
- ▶ Custom Properties
- ▶ Authentication mechanisms
- ▶ SSL
- ▶ Web attributes (SSO)
- ▶ Audit

Server security

- ▶ User registry
- ▶ Trust Association Interceptor (TAI)
- ▶ SPNEGO
- ▶ Authorization
- ▶ Login configurations
- ▶ Application security enablement
- ▶ Java 2 security
- ▶ RMI/IIOP (CSlv2 protocol)
- ▶ Custom Properties
- ▶ LTPA Timeout (Lightweight Third party Authentication)



Admin console: Security domains

View: All tasks

- Welcome
- ⊕ Guided Activities
- ⊕ Servers
- ⊕ Applications
- ⊕ Services
- ⊕ Resources
- ⊖ Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus Security
- ⊕ Environment
- ⊕ System administration
- ⊕ Users and Groups
- ⊕ Monitoring and Tuning
- ⊕ Troubleshooting
- ⊕ Service integration
- ⊕ UDDI





- List the configured security domains
- Create and manage security domains

Security domains

Security domains provide a mechanism to use different security settings for administrative applications and user applications. They also provide the ability to support multiple security settings so different applications can use different security attributes like user registry or login configurations.

⊕ Preferences

New Delete Copy Selected Domain... Copy Global Security...

Select	Name	Description
You can administer the following resources:		
<input type="checkbox"/>	Domain1	A test security domain
<input type="checkbox"/>	Domain2	A second test security domain
Total 2		

Security domain attributes

- Configure the scope for a security domain
 - ▶ Entire cell
 - ▶ Specific servers, clusters or service integration buses
- Attribute sections can be expanded to show the security settings used by the domain
- Attributes can be customized and saved

The screenshot displays the 'Security domains' configuration page for 'Domain1'. It includes a description, 'Assigned Scopes' section with a 'Show:' dropdown set to 'All scopes' and a 'Cell' checkbox, and a 'Security Attributes' section listing various security settings such as Application Security (Enabled), Java 2 Security (Disabled), User Realm (Administrative realm), Trust Association (Disabled), SPNEGO Web Authentication (Disabled), RMI/IIOP Security (Global security settings), JAAS Application Logins (6 login configurations), JAAS System Logins (41 login configurations), JAAS J2C Authentication Data (0 entries), Authentication Mechanism Attributes (120 minute LTPA timeout), and Authorization Provider (Built-in authorization). A 'Web Service Bindings' section is partially visible on the right with a link to 'Default policy set bindings'. At the bottom are 'Apply', 'OK', 'Reset', and 'Cancel' buttons.

Restrictions in WebSphere Security Domains

- Federated Repositories
 - ▶ Can be only one configuration or instance of a federated repository in a cell
 - ▶ Multiple security domains can use federated repositories but need to share the same instance

- Tivoli Access Manager
 - ▶ There can be only one Tivoli Access Manager or Java Authorization Contract for Containers (JACC) configured at the global level
 - ▶ Cannot be configured at the domain level

Section

Fine-grained Administrative Security

Fine-grained administrative security

- WebSphere Application Server provides fine-grained administrative capability
- Users can be defined with administrative roles on a specific set of resources:
 - ▶ Cells, Node Groups, Nodes, Clusters, Servers and Applications
 - ▶ Not SI bus resources
- New in WAS V7:
 - ▶ Supported through the administrative console and a wsadmin scripting interface
 - ▶ Cell wide monitor role is minimally required to effectively use the administrative console.

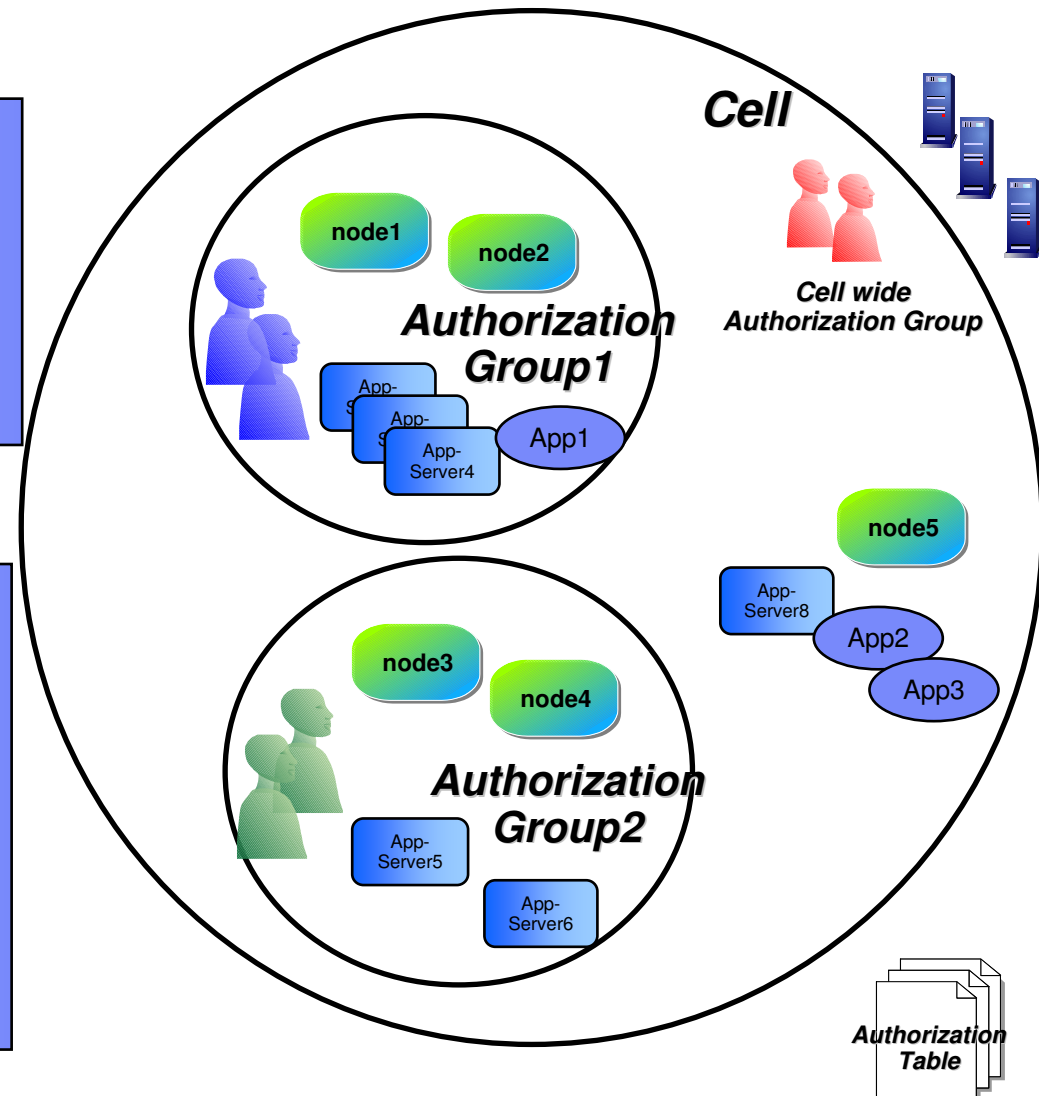
Administrative authorization group

Administrative authorization group

- Resources that require the same privileges are placed in the authorization group
- Users with specific administrative roles can be added to an authorization group

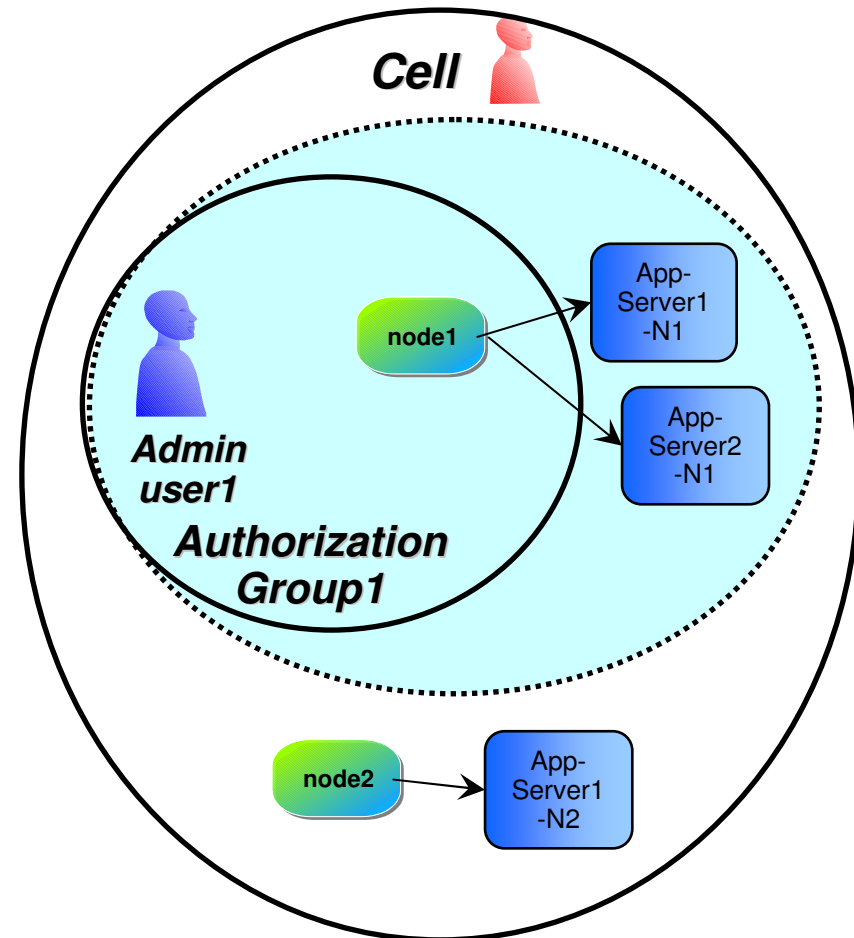
Cell wide authorization group

- By default there is a cell wide authorization group
- Resources that are not assigned to any other authorization group belong to this group
- Users assigned to administrator roles in the cell wide authorization group have access to all the resources within the cell



Resource relationships

- In this example:
 - ▶ User1 is granted access to Node1 which is within Authorization Group1
 - ▶ Application Servers are not explicitly defined under any authorization group
 - ▶ Because servers are child resource of nodes, user1 can access Server1-N1 and Server2-N1



Example: Create an Authorization Group

Integrated Solutions Console Welcome wsadm

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
 - JAX-WS and JAX-RPC security runtime

Administrative authorization groups

Administrative authorization groups > MyCluster

Use this page to set up an administrative authorization group and to specify the associated administrative resources.

Configuration

General Properties

* Name:

Resources

Show: All scopes

- Clusters
 - MyCluster
- Business-level applications
- Assets
- Applications
 - query
 - ivtApp
 - WebApp
 - DefaultApplication
- Nodes
- Node groups

Additional Properties

- [Administrative group roles](#)
- [Administrative user roles](#)

Administrative authorization groups > MyCluster > Administrative user roles

Use this page to add, update or to remove administrative roles to users. Assign administrative application servers through the administrative console or through wsadm.

Logout Add... Remove

Select	User	Role(s)	Logi
None			
Total 0			

Assign Users/Roles to Authorization Group

- Assign Operator role to John

Administrative authorization groups

[Administrative authorization groups](#) > [MyCluster](#) > [Administrative user roles](#) > [User](#)

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to administer application servers through the administrative console or through wsadmin scripting.

* Role(s)

Configurator
Deployer
Monitor
Operator

Search and Select Users

Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string
* Search

Maximum results to display 20

Available
michael

Mapped to role
john

Select All Deselect All Select All Deselect All

OK Reset Cancel

Example: Fine-grained administrative security

- John has the Operator role
- John can start/stop MyCluster and ivtApp
- John cannot change the configuration e.g. create a new cluster

The screenshot shows the administrative console interface for a resource named 'MyCluster'. At the top, there are four buttons: 'Start', 'Stop', 'Ripplestart', and 'ImmediateStop'. The 'Start' and 'Stop' buttons are highlighted with a red rectangular box. Below the buttons are several icons for actions like refresh, copy, and delete. A table below shows the resource details:

Select	Name	Status
<input type="checkbox"/>	MyCluster	✘

Total 1

The screenshot shows the administrative console interface for a resource named 'ivtApp'. At the top, there are three buttons: 'Start', 'Stop', and 'Rollout Update'. Below the buttons are several icons for actions like refresh, copy, and delete. A table below shows the resource details:

Select	Name	Application Status
<input checked="" type="checkbox"/>	ivtApp	✘
You can monitor the following resources:		
	DefaultApplication	▶
	WebApp	▶
	query	▶

Total 4

Section

Security Auditing

Security auditing overview

- Designed to provide audit records which may be used to ensure the integrity of a secured computing environment
- Captures security events into logged audit event records
 - ▶ Authentication
 - ▶ Authorization
 - ▶ system management, and other
- Audit trail for accountability
 - ▶ Vulnerability analysis
 - ▶ Adherence to regulatory compliance

Auditor role

- New auditor role
 - ▶ Separate auditing security role from the administrative security role
 - ▶ During installation the administrator will be included in the auditor role
 - ▶ Not supported in fine-grained administration
- Enable/disable auditing, configure the auditing feature, define the security events to be captured
- Used to grant additional users the same role

Securing the Audit data

- The audit data collected can be protected against tampering
 - ▶ Mechanisms to encrypt and sign the data are available
- Encryption is managed by the auditor
 - ▶ The certificate used to encrypt the data records is managed within the audit subsystem, in audit.xml
- Signing is managed by WebSphere Application Server
 - ▶ The certificate used to sign the data records is managed with WebSphere Application Server, in security.xml

Secure auditing feature

- Generate reports based on different events
 - ▶ Authentication, authorization, resource access etc
 - ▶ Filters can be used to capture a subset of events
- Minimal Overhead of audit event collection

The screenshot displays the IBM WebSphere Administration Console interface. On the left, a navigation tree under 'Security' has 'Security auditing' highlighted with a red box. The main content area, titled 'Security auditing', contains the following information:

- Security auditing**
Security auditing provides a means to gather and store auditable event records to help assure the integrity of the business computing environment.
- General Properties**
 - Enable security auditing
 - Audit subsystem failure action:
 - Primary auditor user name:
 - Enable verbose auditing
- Related Items**
 - [Event type filters](#)
 - [Audit service provider](#)
 - [Audit event factory configuration](#)
 - [Audit encryption key stores and certificates](#)
 - [Audit record encryption configuration](#)
 - [Audit record signing configuration](#)
 - [Audit monitor](#)

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

Audit reader report

Audit Records		
Hostname CHEYENNE . ReportTime Sep 27, 2007, 11:12:53		
Record Number	Event Type	Outcome
2	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:33 CDT 2007	Action=authz	ProgName=NameServer.bind_new_corba_context
RegistryType=WIMUserRegistry	Domain=global	Realm=defaultWIMFileBasedRealm
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=NameServer	ResourceType=WAS	ResourceUniqueld=0
3	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:33 CDT 2007	Action=authz	ProgName=NameServer.rebind_java_object
RegistryType=WIMUserRegistry	Domain=global	Realm=defaultWIMFileBasedRealm
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=NameServer	ResourceType=WAS	ResourceUniqueld=0
4	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:34 CDT 2007	Action=authz	ProgName=NameServer.bind_new_corba_context
RegistryType=WIMUserRegistry	Domain=global	Realm=defaultWIMFileBasedRealm
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=NameServer	ResourceType=WAS	ResourceUniqueld=0
5	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:34 CDT 2007	Action=authz	ProgName=NameServer.rebind_java_object

Section

Certificate Management Enhancements

Certificate management enhancements

- Certificate decisions at profile creation time
- Generate personal certificates by connecting directly to internal Certificate Authority (CA)
- Writable SAF Keyring support
 - ▶ Certificate write operations can be performed via the administrative console or scripting as with file based keystores
- Added a keystore to hold default trusted and deleted certificates
- Option to create chained personal certificates
 - ▶ More scalable solution for flexible certificate management

Certificates during Profile Creation

Profile Management Tool 7.0

Security Certificate (Part 1)

Choose whether to create a default personal certificate and root signing certificate, or import them from keystores. To create new certificates, proceed to Part 2 and provide the certificate information. To import existing certificates from keystores, locate the certificates then proceed to Part 2 and verify the certificate information.

Create a new default personal certificate.
 Import an existing default personal certificate.

Default personal certificate

Path: Browse...

Password:

Keystore type:

Keystore alias:

Create a new root signing certificate.
 Import an existing root signing certificate.

Root signing certificate

Path: Browse...

Password:

Keystore type:

Keystore alias:

Profile Management Tool 7.0

Security Certificate (Part 2)

Modify the certificate information to create new certificates during profile creation. If you are importing existing certificates from keystores, use the information to verify whether the selected certificates contain the appropriate information. If the selected certificates do not, click **Back** to import different certificates.

Default personal certificate (a personal certificate for this profile, public and private key):

Issued to distinguished name:

Issued by distinguished name:

Expiration period in years:

Root signing certificate (personal certificate for signing other certificates, public and private key):

Expiration period in years:

Default keystore password:

Confirm the default keystore password:

Note: The default value for the keystore is well documented in the Information Center and should be changed to protect the security of the keystore files and SSL configuration.

Chained personal certificates

- A chained certificate is a personal certificate signed with another certificate known as a root certificate
- The public key of the root certificate will be added to the NodeDefaultTrustStore (trust.p12 in the node directory)
 - ▶ This should provide all the trust necessary for all servers to communicate with each other
 - ▶ These root certificates have a longer lifespan (15 years by default) to avoid the need to replace signers in the trust stores
- The personal certificates signed by these root certificates root-key.p12 have a shorter lifetime (1 year) and unique private keys, thus the communications remain secure
 - ▶ Personal certificates signed by a root certificate can be replaced without any impact to communication if the client has the signer from the root certificate

Default key stores and trust stores

SSL certificate and key management > **Key stores and certificates**

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

Keystore usages

Preferences

New Delete Change password... Exchange signers...

Select	Name	Description	Management Scope	Path
You can administer the following resources:				
<input type="checkbox"/>	NodeDefaultDeletedStore	Key store containing deleted certificates for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/deleted.p12
<input type="checkbox"/>	NodeDefaultKeyStore	Default key store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/key.p12
<input type="checkbox"/>	NodeDefaultRootStore	Root certificate key store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/root-key.p12
<input type="checkbox"/>	NodeDefaultSignersStore	Key store containing default signers for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/default-signers.p12
<input type="checkbox"/>	NodeDefaultTrustStore	Default trust store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	LTPA key store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/ltpa.jceks
<input type="checkbox"/>	NodeRSATokenKeyStore	RSAToken key store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/rsatoken-key.p12
<input type="checkbox"/>	NodeRSATokenRootStore	RSAToken root certificate key store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/rsatoken-root-key.p12
<input type="checkbox"/>	NodeRSATokenTrustStore	RSAToken key store for localhostNode01	(cell):localhostNode01Cell; (node):localhostNode01	\${CONFIG_ROOT}/cells/localhostNode01Cell/nodes/localhostNode01/rsatoken-trust.p12
Total 9				

Section

Kerberos

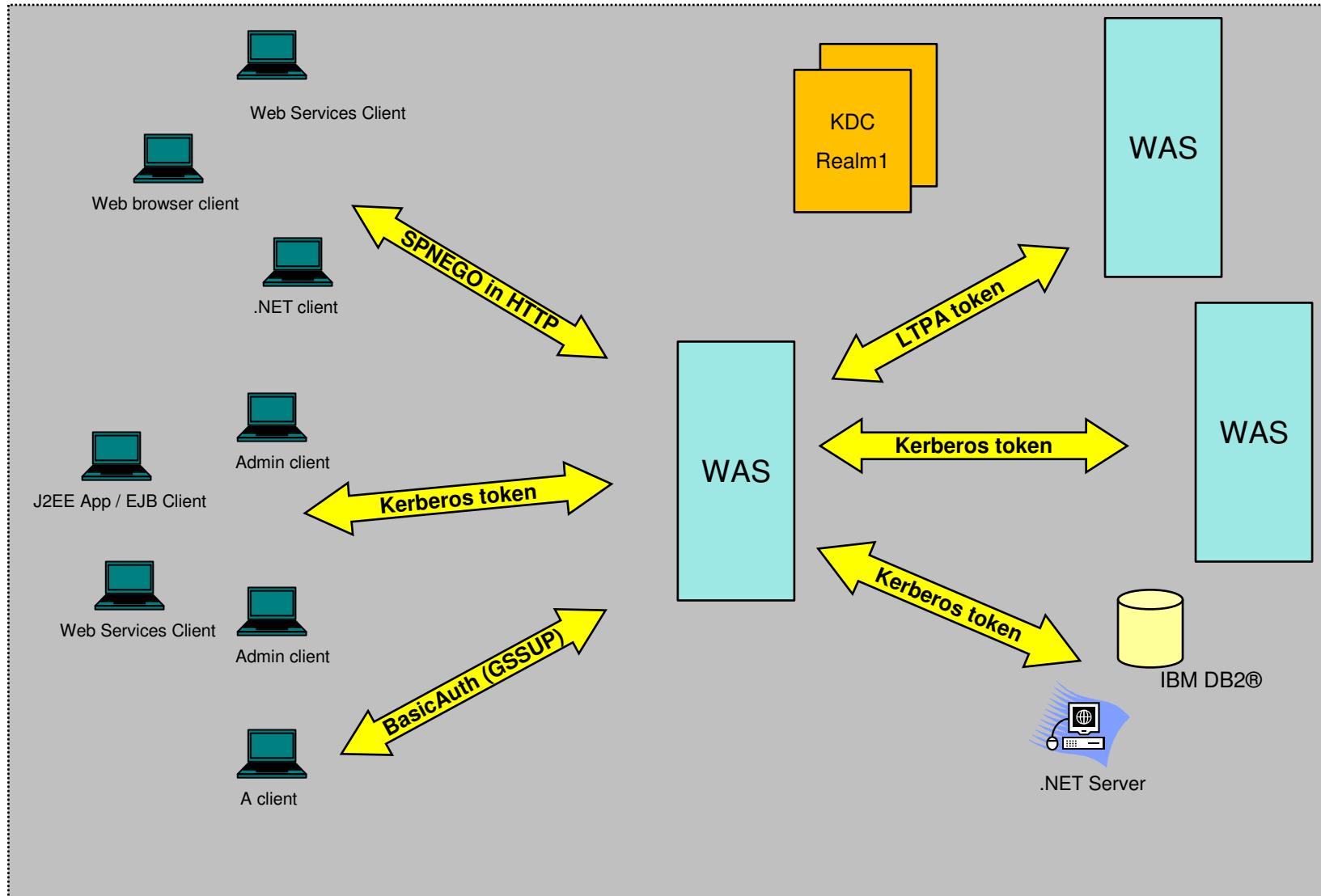
Kerberos authentication

- SSO application authentication mechanisms
 - ▶ LTPA
 - ▶ Kerberos (KRB5)
- Resource adapter to support Kerberos
 - ▶ Use a client Kerberos credential to authenticate to back end resource
- Cannot be configured for multiple security domains
- All WebSphere Application Servers have to use the same Kerberos realm

Kerberos web authentication enhancements

- SPNEGO HTTP web authentication
 - ▶ SPNEGO - Simple and Protected GSSAPI Negotiation Mechanism
 - ▶ Simplified configuration via admin console
 - ▶ Allow to fall back from SPNEGO to application login method
 - ▶ SPNEGO trust association interceptor (TAI) is deprecated
- Web Services Security Kerberos Token Profile 1.1
 - ▶ Provides Kerberos token in the SOAP header

SPNEGO Web and Kerberos authentication and Java Client support Kerberos



Section

Summary

Summary

- Multiple security domains provides better flexibility for security configurations
- Flexible fine-grained administrative security
- Security auditing feature allows users to capture and maintain audit controls over their environments
- Improvements to certificate management
- Robust support for Kerberos authentication

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكراً
Arabic

Merci
French

Obrigado
Brazilian Portuguese

Grazie
Italian

多谢
Simplified Chinese

Danke
German

நன்றி
Tamil

ありがとうございました
Japanese

감사합니다
Korean

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.