

ibm.com



e-business



# Powerful and secure infrastructures with WebSphere Application Server for z/OS

## WAS 5 Quickstart Hints & Tips



# Redbooks

International Technical  
Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

Holger Wunderlich / wunderl@us.ibm.com

## Trademarks

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

Affinity™  
AIX®  
CICS®  
DB2®  
@server™  
eServer™  
Everyplace™  
IBM®  
IMS™

IMS/ESA®  
MQSeries®  
MVS™  
MVS/ESA™  
Notes®  
OS/2®  
OS/390®  
Parallel Sysplex®  
Redbooks™

Redbooks(logo)™   
RACF®  
S/390®  
SecureWay®  
SOM®  
Tivoli®  
WebSphere®  
z/OS™  
zSeries™

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

Java and all Java-based trademarks and logos are trademarks or registered 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.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

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



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# Notices

This information was developed for products and services offered in the U.S.A.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:  
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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 and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

fff

# Objectives

## WebSphere Application Server on z/OS V5 - Quickstart

- Overview
- Install Base Server
- Enable Global Security
- Post Install
- RACF JOB Walkthrough
- Summary



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# Setup



Is it difficult?  
Will it work?  
Shall I go for it?  
**Yes!**



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## BASE or Network Deployment ?

	Base Application Server cell	Deployment manager cell
<b>Configuration</b>	<ul style="list-style-type: none"> <li>■ Each base application server node is installed using the ISPF customization dialog.</li> <li>■ Additional servers within the same node are created through the admin console.</li> </ul>	<ul style="list-style-type: none"> <li>■ Initial cell configuration through ISPF customization dialog.</li> <li>■ Add nodes through federating.</li> <li>■ Additional servers and clusters via admin console.</li> </ul>
<b>Address spaces</b>	<ul style="list-style-type: none"> <li>■ Min: 3 (daemon, controller, servant)</li> <li>■ Max: limited only by resources</li> </ul>	<ul style="list-style-type: none"> <li>■ Min: 6 (daemon, controller, servant, deployment manager controller and servant, node agent)</li> <li>■ Max: limited only by resources</li> </ul>
<b>Administrative isolation</b>	<ul style="list-style-type: none"> <li>■ Each base application server node has its own and separate administrative domain.</li> </ul>	<ul style="list-style-type: none"> <li>■ Each network deployment cell is an isolated domain. Nodes and servers within the ND cell are in the same administrative domain.</li> </ul>
<b>Administrative operation</b>	<ul style="list-style-type: none"> <li>■ Servers can only be started from the MVS console or SDSF.</li> <li>■ limited support for admin console.</li> </ul>	<ul style="list-style-type: none"> <li>■ Servers and clusters can be started from the admin console or from the MVS console or SDSF</li> </ul>
<b>Operational isolation</b>	<ul style="list-style-type: none"> <li>■ Servers can be started and stopped independently.</li> <li>■ No JNDI and application name conflicts with other servers.</li> </ul>	<ul style="list-style-type: none"> <li>■ Servers can be started and stopped independently.</li> <li>■ JNDI and Application name conflicts are possible within a cell.</li> </ul>
<b>Multiple server regions</b>	<ul style="list-style-type: none"> <li>■ Only if administrative application is not present. (additional servers has to be created)</li> </ul>	<ul style="list-style-type: none"> <li>■ Yes</li> </ul>
<b>Clustering</b>	<ul style="list-style-type: none"> <li>■ No</li> </ul>	<ul style="list-style-type: none"> <li>■ Yes</li> </ul>

## prepare installation

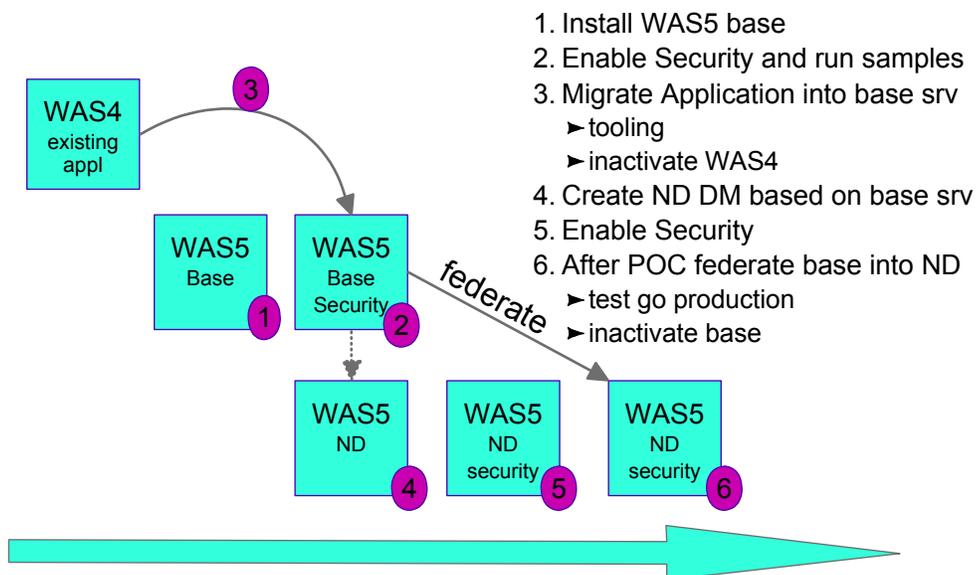
- ▶ Review for product status, APARS
  - ▶ Customers: [http://www.ibm.com/software/webervers/appserv/zos\\_os390/support.html](http://www.ibm.com/software/webervers/appserv/zos_os390/support.html)
  - ▶ IBMers <http://websphere.pok.ibm.com>
- ▶ Have the Infocenter always handy:
  - ▶ Customers: <http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp>
  - ▶ IBMers: <http://wasinfo.raleigh.ibm.com/help/index.jsp>
- ▶ For ND start with 5.01
- ▶ get WebSphere Application Server V5.0 for z/OS Operations and Administration, SA22-7912. Hardcopy
- ▶ see our application migration section later today



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Installation / Migration Roadmap



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# Setting Up a Base Server (1)

► SMP/E Apply is done, Naming Conventions understood, fixes applied

► Start of with defining some names and IP ports (see Chapter 1 of the Security Redbook)

► Keep track of names, userids and IP ports

- SOAP JMX Connector port.....: 38880
- DRS Client Address port.....: 37870
- ORB port.....: 32800
- HTTP port.....: 39080
- HTTP SSL port.....: 39440

► TSO ex 'hlq.SBBOCLIB(BBOWSTRT)'

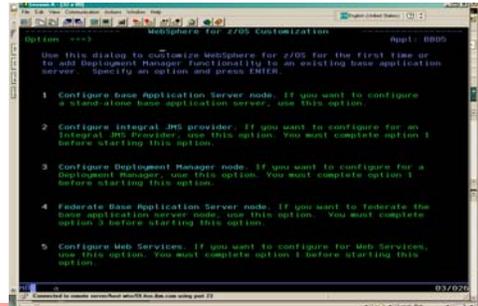
► Configure Base App server

► Load or/and Prime Variables

- (sample provided in the Security Redbook)

► Generate Customization Jobs

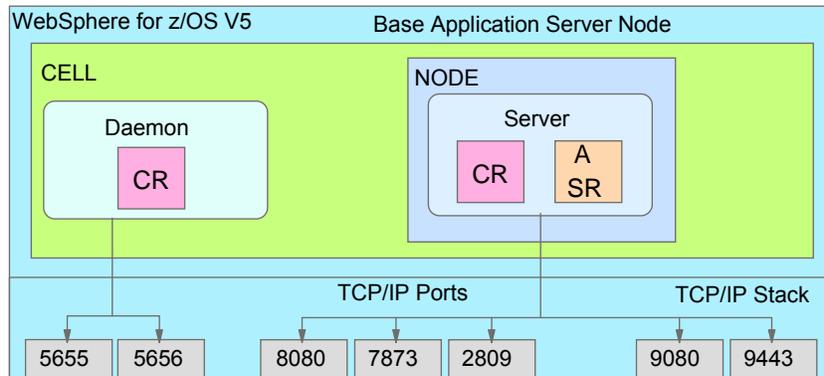
- about 70 Jobs generated...



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## (default) IP Ports



- **Daemon IP port 5655**  
daemon ip listener to resolve indirect IOR's.
- **SOAP JMX connector port 8080**  
JMX management uses the SOAP connector port.
- **DRS Client Address port 7873**  
used for data replication service.
- **ORB listener Port 2809**  
application server Object Request Broker listens for requests.
- **HTTP port 9080**  
internal HTTP port to access admin console and applications.



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Default Ports

TCP/IP Port Description	WAS V5 Base App Srv Port #	WAS V5 Depl.Mgr. Port #	WAS V5 Node Agent Port #	WAS V4.0.1 Port #	WAS V3.5 Port #
Daemon IP port	5655	5755	N/A	5555	N/A
Daemon SSL port	5656	5756	N/A	5556	N/A
Bootstrap port	2809	9809	2809	900	N/A
SOAP JMX Connector port	8080	8879	8878	N/A	N/A
CELL Discovery Address port	N/A	7277	N/A	N/A	N/A
NODE Discovery Address port	N/A	N/A	7272	N/A	N/A
DRS Client Address port	7873	7989	7888	N/A	N/A
ORB port	2809	9809	2809	N/A	N/A
ORB SSL port	0	0	0	N/A	N/A
HTTP port	9080	9090	N/A	no default	80
HTTP SSL port	9443	9043	N/A	no default	443

## Setting Up a Base Server (2)

pdf

- ▶ Then look at the generated instructions and run the jobs
  - ▶ only for the First server setup:
    - ▶ WLM ApplEnvs or use DAE on z/OS 1.2 and higher (IWMARIN0)
    - ▶ Update PARMLIB IPCS for dump analysis (BBOIPCSP)
    - ▶ Update PARMLIB PPT, mark DMN & CTRL nwsp, key2 (BBOSCHED)
    - ▶ Update PARMLIB PROG for APF libraries (BBOPROG)
    - ▶ Update PARMLIB SMFPRM for SMF120 recording
    - ▶ Update PARMLIB for PROG for LPA list updated
    - ▶ Update MSGENU/JPN for message xlat, optional (BBOMSGC)
    - ▶ Define the RRS logstream (BBORRSLs)

## Setting Up a Base Server (3)

IMPORTANT! BPX.SUPERUSER not honored. Use UID (0) to avoid corruption of other servers

- ▶ first and following servers (different RACF users)
  - ▶ make RACF user and STC definitions (errors for 2nd srv) (BBOCBRA\*)
  - ▶ Update OMVS segment (fileproc(1024))
  - ▶ RACF permit SRV & CTRL to TCPARM and PARMLIB
  - ▶ RACF permit daemon to PARMLIB
  - ▶ Update TCPARM for port reservations, optional (BBOTCPIP)
  - ▶ Define logstream structure (BBOERRLG)
    - ▶ PE V500.SC59.BS0F.LOG CLASS(LOGSTRM) ID(WUNDERL) ACC(ALTER)
  - ▶ Allocate CTRACE dataset (BBOWCTR)
  - ▶ Create mountpoint and HFS, do mount (BBOWCHFS)
  - ▶ Update PARMLIB BPXPRM to mount WAS config HFS
  - ▶ Populate HFS with WebSphere (BBOMCFG)
  - ▶ Populate HFS with WebServices and docu (BBOMCFGU)
  - ▶ Update SYS1.PROCLIB (BBOWCPY1)
  - ▶ Populate HFS with configuration data and scripting (BBOWCPY2)
  - ▶ Create was.env (BBOWC2N)
  - ▶ Create Admin Console and IVP (BBOWIAPP)
  - ▶ Finalize HFS install (BBOMCFG2)
  - ▶ Copy digital certificates into HFS (BBOCR2FA)



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Start Server and check

```
START WAS5DCF,JOBNAME=WASDF,ENV=CELDF.NODDF.WASDF
```

```
BBOO0222I WSVR0001I: Server SERVANT PROCESS wdfndfcdfsc59  
open for e-business
```

```
BBOO0020I INITIALIZATION COMPLETE FOR WEBSHERE FOR Z/OS  
SERVANT PROCESS WASDF
```

```
BBOO0019I INITIALIZATION COMPLETE FOR WEBSHERE FOR Z/OS  
CONTROL PROCESS WASDF.
```

### Run Installation Verification Test (BBOWIVT)

IVTL0015I: WebSphere Application Server wtsc59.itso.ibm.com is running on port: 39080

IVTL0050I: Servlet Engine Verification Status - Passed

IVTL0055I: JSP Verification Status - Passed

IVTL0060I: EJB Verification Status - Passed

IVTL0070I: IVT Verification Succeeded

IVTL0080I: Installation Verification is complete

### Install Samples now (BBODEFR, BBOINST), install SWIPE (RACF & deploy)

Try Admin Console: <http://yourhostname:yourport/admin/>

Try the samples gallery: <http://wtsc59.itso.ibm.com:39080/WSSamples/en/index.html>

Try out swipe: <http://wtsc59.itso.ibm.com:39080/IBMEBizWeb/EJBCaller>

You now have a base server without any security



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# Swipe Screenshot w/o security

## Servlet Security Info

Remote Userid	null
principalId	
Access to role: Worker	false

## EJB Security Info (Called by Servlet - no RunAS Specified)

id of caller	UNAUTHENTICATED
id this method running under	UNAUTHENTICATED

## EJB Role Access Report (No RunAs Specified)

Worker	false
--------	-------

## EJBSample Method --> runAsCaller <-- report

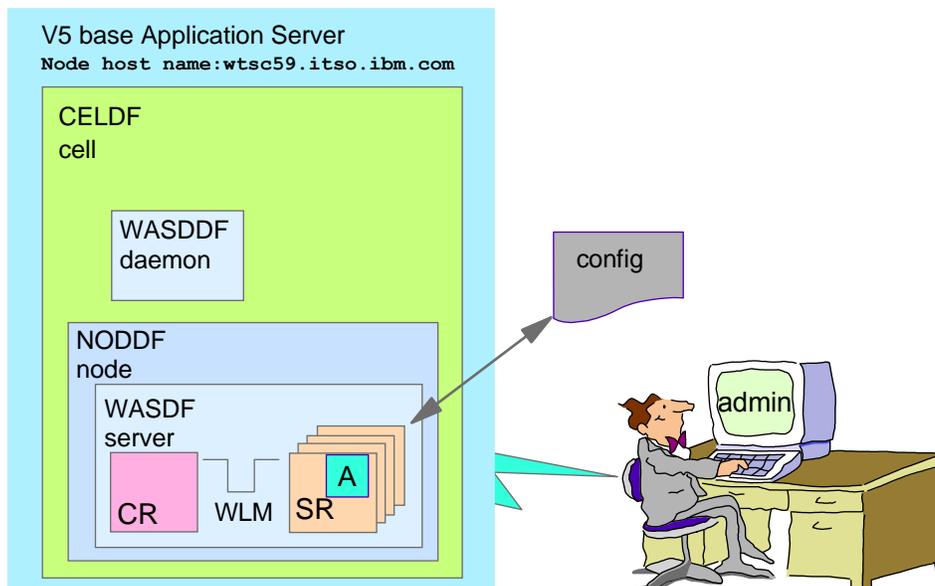
id of caller of this method	UNAUTHENTICATED
id this method running under	UNAUTHENTICATED
Permitted to role GrantPayRise	false



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

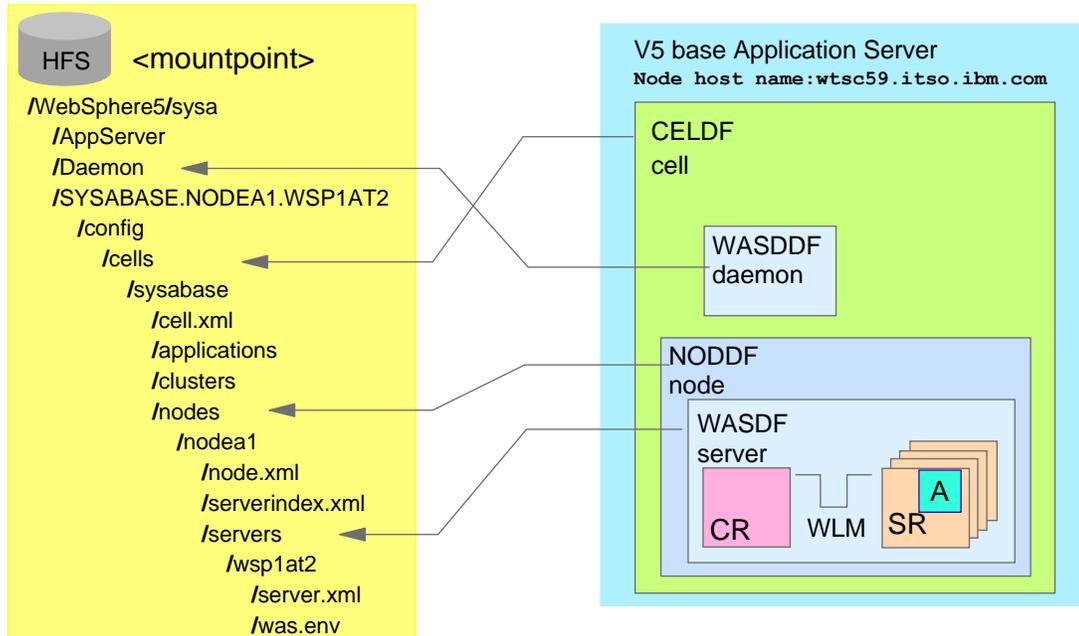
# Your Infrastructure Now: Base Server



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# HFS structure



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# enable Global security

## What is Global Security?

- Security configuration that effects entire security domain.
- Applies to all applications running on WebSphere Application Server.

## Why enabling Global Security ?

- To activate the settings which protect your server from unauthorized users.



	Enabled	Disabled
HTTP client authentication	Yes	Not configured
IIOP client authentication	Yes	Not configured
Admin console Security	Yes	No
Use of SSL Transport	Yes	No
Role based authorization checks of servlets, EJBs, and mbeans	Yes	No
RunAs settings	Yes	Ignored
CBIND check	Yes	No



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# enable Global security / Overview

08/07/2003

## Tools to Enable Global Security

- ISPF DIALOGs plus
- Administrative console or
- wsadmin scripting Tool
  - Interactively
  - JACL script

## Things to configure

- An active authentication mechanism **must** be specified (SWAM, LTPA, or ICSF)
- An active user registry **must** be specified (LocalOS, LDAP, or custom)
- Other options
  - Enforce Java 2 Security.
  - Use Domain Qualified User IDs
  - Cache Timeout
  - Issue Permission Warning
  - Active Protocol



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# enable Global security / RACF

```
Installation dependent WebSphere Security Customization definitions

SSL Customization

  WebSphere Certificate Authority Keylabel: WS for z/OS CA
  RACF Keyring Name.....: WASKEYRING EJBROLE

  Use RACF Authorization and Delegation.....: Y
  Support Passtickets for z/SAS authentication: Y
  Passticket Profile name.....: CBS390 PTKTDATA
  Passticket KEYMASK value.....: 1212121212121212

  Enable WebSphere Application Server to authenticate
  RACF users via WebSphere login tokens.....: Y

  Generate RACF commands for above.....: Y

Installation dependant z/OS Security Customization definitions

  Authorize Servers to APPL profile.....: n CBS390 APPL
  Sample OPERCMDS definitions for WebSphere Servers: n SDSF
```

1. Define variables / Security Customization
2. Generate customization jobs
3. Run ...CNTL(BBOCBRAJ) to generate commands
4. Check...DATA(BBOWBRAK) for generated commands
5. Run ...CNTL(BBOCBRAJ) to execute commands



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# Login to the Admin console

Login

User ID:

The User ID does not require a password, and does not need to be a User ID of a user in the local user registry. It is only used to track user-specific changes to configuration data. Security is NOT enabled

where is my password???



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# enable Global security

	General Properties	
check	Enabled	<input checked="" type="checkbox"/> <small>Enables security subsystem in this particular server.</small>
uncheck	Enforce Java 2 Security	<input type="checkbox"/> <small>Used to enable or disable Java 2 Security permission checking. When Java 2 Security is enabled and if the application policy file was not setup correctly, the application could potentially fail to run.</small>
	Use Domain Qualified User IDs	<input type="checkbox"/> <small>When true, user names returned by getUserPrincipal()-like calls, will be qualified with the security domain they reside within.</small>
	Cache Timeout	* <input type="text" value="600"/> <small>Timeout value for security cache in seconds.</small>
	Issue Permission Warning	<input checked="" type="checkbox"/> <small>When enabled, a warning will be issued during application installation, if an application requires a Java 2 Permission that normally should not be granted to an application.</small>
CSI & SAS	Active Protocol	<input type="text" value="CSI and SAS"/> <small>Specifies active security authentication protocol when security is enabled. Possible values are CSI (CSIv2), or CSI and SAS.</small>
LTPA	Active Authentication Mechanism	* <input type="text" value="LTPA (Light weight Third Party Authentication)"/> <small>Specifies the active authentication mechanism when security is enabled.</small>
Local	Active User Registry	<input type="text" value="Local OS"/> <small>Specifies the active user registry when security is enabled.</small>



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# enable Global security

## LTPA

Lightweight Third Party Authentication configuration settings. When security is enabled and any of these properties are changed, please go to the GlobalSecurity panel and click Apply or OK to validate the changes. The LTPA keys are automatically generated the first time security is enabled. After security is enabled, a new set of keys can be generated in two ways. If the password needs to be changed, change the password and press OK or Apply to generate the keys (no need to press the Generate Keys button). If password is the same, just press the Generate Keys button. The new set of keys will not be used until saved. [?]

Configuration		
General Properties		
Password	* [input field]	[?] The password to encrypt and decrypt the LTPA keys. This password should be used when importing these keys into other WebSphere Application Server administrative domain configurations (if any) and when configuring SSO for Domino Server. If the password is changed and OK or Apply is pressed, a new set of keys are automatically generated. This new set of keys will be used after saved.
Confirm Password	* [input field]	[?] Confirm the password to encrypt and decrypt the LTPA keys.
Timeout	* 120	[?] The time period in minutes at which an LTPA token will expire. This time period should be longer than cache timeout.

## Set LTPA Password



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

# enable Global security

[Global Security](#) > [Custom Properties](#) >

## EnableTrustedApplications

Specifies an arbitrary name/value pair of data, where the name is a property key and the value is an internal system configuration properties. [?]

Configuration	
General Properties	
Name	* EnableTrustedApplications
Value	* true
Description	[input field]

Apply OK Reset Cancel

- ▶ In User Registries-->Local OS, Custom Properties
- ▶ select com.ibm.security.SAF.authorization = true
- ▶ com.ibm.security.SAF.delegation = true
- ▶ enableTrustedApplications = true
- ▶ apply / save



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

## enable Global security

- ▶ restart your server
- ▶ checkout swipe <http://yourhost:yourport/IBMEBizWeb/secure/EJBCaller>
- ▶ Admin Console will be redirected to SSL port. Accept Server Certificate

### Servlet Security Info

Remote Userid	usremp
principalId	usremp
Access to role: Worker	false

### Client cookies

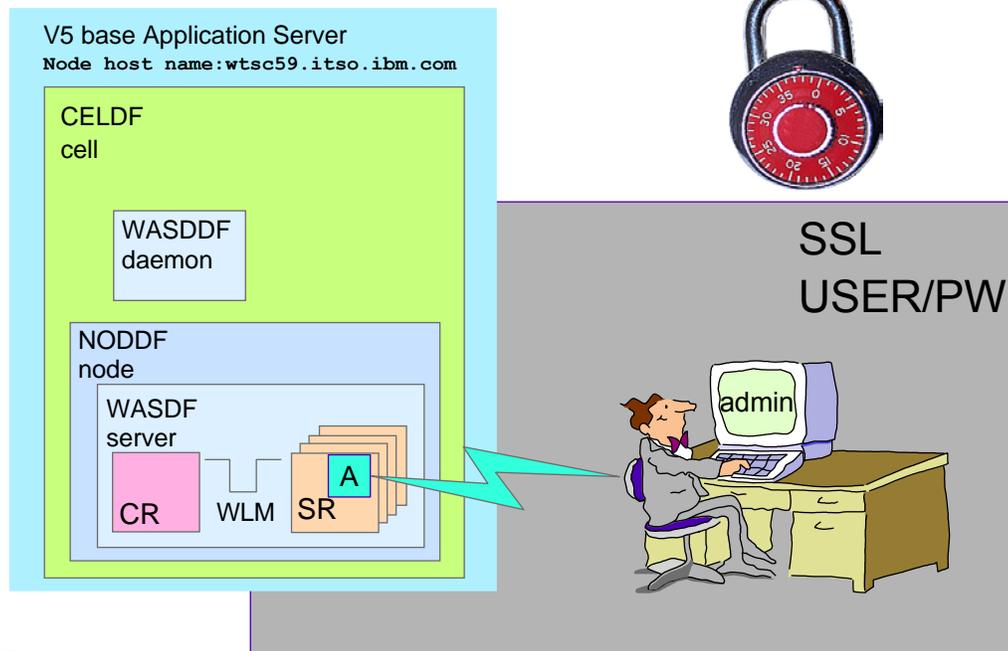
msp	2
w3ibmProfile	200109100906150150225929964 gAME 897 PLP en-us
IBMISP	6399613a6fc11d78fd7977cb121dd95-6399613a6fc11d78fd7977cb121dd95-c82cfdec28518653ffffe2074e8
LtpaToken	jQSp54ASG45dtzAjOThN+ni/2U7q06v60HzZyENr7jyFyO5ZL09CWBunp7oM1dqgrx1H916amhGTbF9Sf6Trj
LtpaToken	wxbUTcfV7vd78+gYDRmnDzyLGaRWWo5vDw5o6JKRIN+K3H6rXRJoQPdPinJfhFjtzjzMMN+wjiHB35imr
JSESSIONID	0000KV02HHORIEUZPKW15BXVAJLB9DA03359A8A1380000004540000007E090C0626



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Your Infrastructure Now: Base Server with security



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Cannot login to admin console?

Admin console uses form based login for authentication.

FBL does not know about expired passwords. Login to z/OS UNIX to check if user is ok.



[ibm.com/redbooks](http://ibm.com/redbooks)

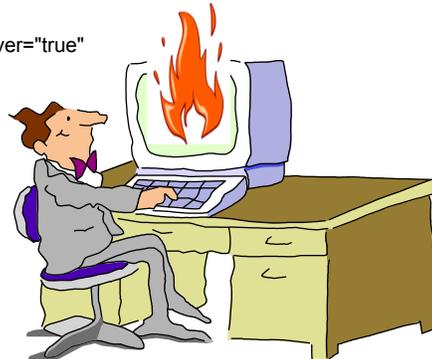
© Copyright IBM Corp. 2003. All rights reserved.

## If things are still not working as expected... in Base mode

- ▶ Edit <mountpoint>/AppServer/config/cells/<cell name>/ security.xml
- ▶ Change

```
<security:Security xmi:id="Security_1" useLocalSecurityServer="true"
useDomainQualifiedUserNames="false" enabled="true"
```
- ▶ to

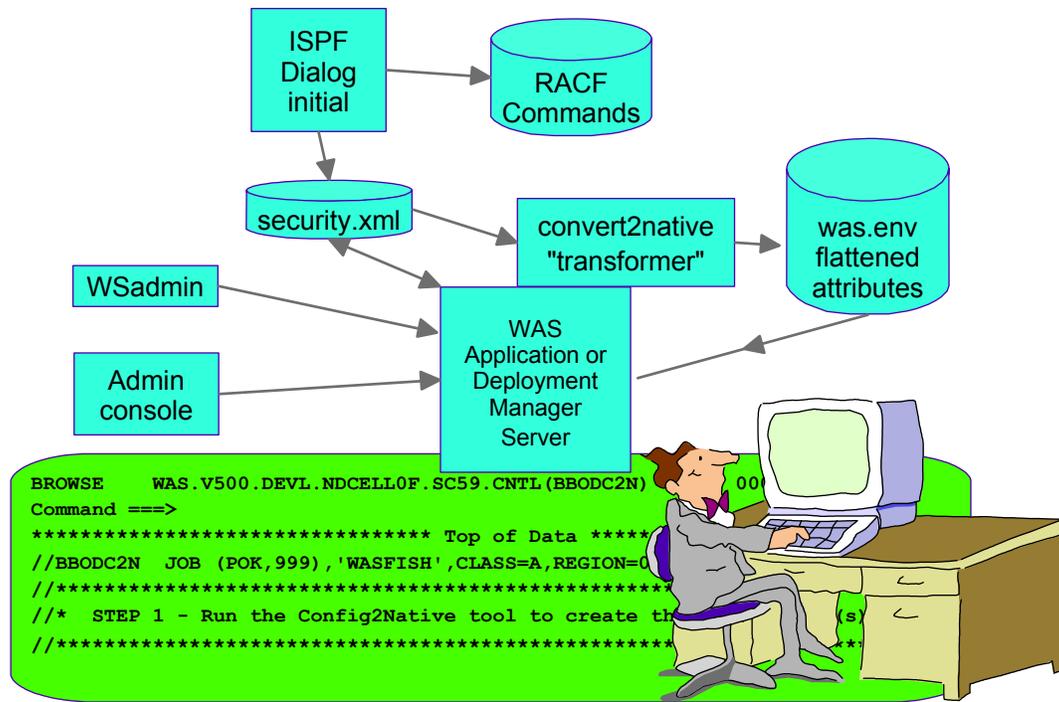
```
<security:Security xmi:id="Security_1" useLocalSecurityServer="true"
useDomainQualifiedUserNames="false" enabled="false"
```
- ▶ Restart your server and try again



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# If things are still not working as expected...in ND mode



```

BROWSE  WAS.V500.DEVL.NDCCELL0F.SC59.CNTL(BBODC2N)
Command ==>
***** Top of Data *****
//BBODC2N JOB (POK,999),'WASFISH',CLASS=A,REGION=0
//*****
//* STEP 1 - Run the Config2Native tool to create th
//*****
  
```

0Set	Address = 20248fa8	Length = 0023	EBCDIC	ASCII		
0000	E3D9C1C3	C5C4C5E3	C1C9D37E	4DF36BF4	TRACEDETAIL=(3,4	.....~M.k.
0010	6BC56BF0	6BF16BF3	6BF76BF9	6BC16BC6	,E,0,1,3,7,9,A,F	k.k.k.k.k.k.k.k.
0020	6BD15D				,J)	k."

- ▶ use SDSF kill to stop a single server region
- ▶ /f WASDF, tracedetail=(3,4,E) for sec
  - ▶ 0 RAS
  - ▶ 1 Common Utilities
  - ▶ 3 COMM
  - ▶ 4 ORB
  - ▶ 6 OTS
  - ▶ 7 Shasta
  - ▶ 9 OS/390 Wrappers
  - ▶ A Daemon
  - ▶ E Security
  - ▶ F Externalization
  - ▶ J JRAS
  - ▶ L J2EE
- ▶ F WASDF, tracejava='com.ibm.ws.security.\*=all=enabled'
- ▶ /F WASDF, TRACETOSYSPRINT=YES/NO
- ▶ /F WASDF, TRACENONE

0000	47455420	2F61646D	696E2048	5454502F	...../..>...&	GET /admin HTTP/
0010	312E310D	0A416363	6570743A	20696D61	...../	1.1..Accept: ima
0020	67652F67	69662C20	696D6167	652F782D	...../	ge/gif, image/x-
0030	78626974	6D61702C	20696D61	67652F6A	...../	xbitmap, image/j
0040	7065672C	20696D61	67652F70	6A706567	...../	peg, image/pjpeg
0050	2C206170	706C6963	6174696F	6E2F766E	...%../?>..>	, application/vn
0060	642E6D73	2D657863	656C2C20	6170706C	...%..%..%	d.ms-excel, appl
0070	69636174	696F6E2F	766E642E	6D732D70	.../?>..>..%	ication/vnd.ms-p
0080	65776573	706F696F	742C2061	70706C69	? > / %	support appli

## message hints

- Configuration & Trace Audit messages to [ras\\_default\\_msg\\_dd](#)
- WTOs to [ras\\_hardcopy\\_msg\\_dd](#)
- Trace Error, Service, and Fatal msgs to [ras\\_log\\_logstreamName](#)
  - Otherwise, they go to cerr (SYSOUT).
  - Early error messages go to stderr (SYSOUT) until logstream is active..
  - BBOO0153I is issued telling you how many messages went to stderr before connected to the logstream.
- Trace messages also routed to [ras\\_trace\\_outputLocation](#)
  - (BUFFER, SYSPRINT, or TRCFILE DD)
- System.out.println, Tr.Sysout, & stdout (cout) to SYSPRINT.
- System.out.printerr, Tr.Syserr, & stderr (cerr) to SYSOUT.

### Set in the adminconsole via:

- ▶ At the server level: Under Servers, select Application Servers > server\_name > Process Definition > Control > Custom Properties > New . . .
- ▶ At the cell level: Environment > Manage WebSphere Variables > New . . .



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Some useful commands

### **F WASDF, DISPLAY, SERVERS**

```
BBOO0182I SERVER          ASID  SYSTEM  LEVEL
BBOO0183I CELDF    /WASDDF    4Fx   SC59   W501000
BBOO0183I CLUDF    /WASDF     271x  SC59   W501000
BBOO0188I END OF OUTPUT FOR COMMAND DISPLAY,SERVERS
```

### **F WASDF, DISPLAY, SERVANTS**

```
BBOO0185I SERVER CLUDF/WASDF HAS 1 SERVANT PROCESS (ASID: 0268x)
BBOO0188I END OF OUTPUT FOR COMMAND DISPLAY,SERVANT
```

### **FWASDF, DISPLAY, JVMHEAP, ALL**

```
BBOO0201I JVM HEAP INFORMATION FOR SERVER CLUDF/WASDF/STC30346
BBOO0202I (STC30346) HEAP(MIDDLEWARE), COUNT(00000004),
FREE STORAGE(199B7D88), TOTAL STORAGE( 2FFFA00)
BBOO0204I JVM HEAP INFORMATION FOR SERVER CLUDF/WASDF/STC30346 200 COMPLETE
+BBOO0201I JVM HEAP INFORMATION FOR SERVER CLUDF/WASDF/STC30347
+BBOO0202I (STC30347) HEAP(MIDDLEWARE), COUNT(00000002),
FREE STORAGE(20267C1E68), TOTAL STORAGE( FFEFA00)
+BBOO0204I JVM HEAP INFORMATION FOR SERVER CLUDF/WASDF/STC30347 203 COMPLETE
```



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Hints and Tips

08/07/2003

- Admin console is redirected to SSL port after global security is enabled
- In Network Deployment environment, configuration is stored temporarily in the Deployment Manager until it is synchronized with all of the node agents
- Configuration is at cell level, but can be customized to some extent at application server level
  - Cannot configure a different authentication mechanism or user registry on a per server basis
- Individual server security can be disabled if global security is enabled. But naming and admin security is still enabled
- Individual server security can NOT be enabled if global security is disabled
- File security.xml - edit it to disable global security if global security fails to work properly `<security:Security ...enabled="true" ---> "false"..>`
  - In base configuration, `/mount_point/appserver/config/cells/cellname/security.xml`
  - In ND configuration, `/mount_point/DeplMgr/config/cells/cellname/security.xml`



TIP: use anFTP  
client for editing  
ascii files  
(FILEZILLA)

[ibm.com/redbooks](http://ibm.com/redbooks)

ts reserved.

## Federation Hints

m

For BBOWADDN add the following in `/usr/lpp/java/IBM/J1.3/lib/security/` java.security:

```
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.security.cert.IBMCertPath
```



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# upgrading BASE to 5.01

- ▶ install PTF
- ▶ shutdown server
- ▶ login as WSADMIN
  - ▶ run /usr/lpp/zWebSphere/V5R0M0/bin/postinstall.sh)
  - ▶ Enter absolute path to a configured root :
    - ▶ /WebSphere/BS0F/appserver/ (terminating slash needed)
- ▶ Start ISPF DIALOG (ex 'BBO5S59.SBBOCLIB(BBOWSTRT)')
  - ▶ configure base appserver node, load vars, generate jobs
  - ▶ run BBOWCPY1 (updates PROCLIB)
- ▶ edit wsadmin.properties change
  - ▶ com.ibm.ws.scripting.tmpdir to
  - ▶ /mywashomedirectory/temp
- ▶ copy BBOWIAPP to BBOWUADM and BBOWIADM
  - ▶ edit BBOWUADM, delete STEP2, update step 1&3 (holddoc), save
  - ▶ edit BBOWIADM, delete STEP2, save
  - ▶ submit BBOWUADM, BBOWIADM (uninstall/install admin console)
  - ▶ ==> Application adminconsole uninstalled / installed successfully.
- ▶ Start Server



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

## Post Install delete IVT etc

too much real?

```

SDSF DA IBM2 SC59 PAG 0 SIO 0 CPU 27/ 23 LINE 19
COMMAND INPUT ==>
NP JOBNAME StepName ProcStep JobID Owner C Pos DP Real F
WASDD2 WASDD2 BBODAEMN STC26590 WDD2STU NS FE 105
WASDDF WASDDF BBODAEMN STC26167 WDDFSTU NS FE 110
WASDD0 WASDD0 BBODAEMN STC25563 WDD0STU NS FE 104
WASDF WASDF BBOCTL STC26680 WDCFSTU NS FE 31T
WASD0 WASD0 BBOCTL STC26172 WDC0STU NS FE 729
WASDFS WASDFS BBOSR STC26681 WDSFSTU IN C2 68T
WASD2S WASD2S BBOSR STC26591 WDS2STU IN C1 35T
WASD02 WASD02 BBOCTL STC26589 WDC2STU NS FE 18T
    
```

too many apps!

A list of installed applications. A single application can be deployed onto multiple servers.

Total 5

Filter

Preferences

Start Stop Install Uninstall Update Export Export DDL

<input type="checkbox"/>	Name	Status
<input type="checkbox"/>	SWPEVS	➔
<input type="checkbox"/>	SamplesGallery	➔
<input type="checkbox"/>	TechnologySamples	✖
<input type="checkbox"/>	adminconsole	➔
<input type="checkbox"/>	ivtApp	➔



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

## enabling SMF

Click on

Servers > Application Servers > server\_name  
> Process Definition > Control > Custom Properties

and enter the appropriate variables where the value of '1' is to enable, and '0' is to disable:

Server\_SMF\_server\_activity\_enabled  
server\_SMF\_server\_interval\_enabled  
server\_SMF\_container\_activity\_enabled  
server\_SMF\_container\_interval\_enabled  
server\_SMF\_web\_container\_activity\_enabled  
server\_SMF\_web\_container\_interval\_enabled  
server\_SMF\_interval\_length <-- '0' selects the default interval



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## SMF Viewer

WSC SMF 120 Performance Summary V500 Date: Tue Oct 21 12:07:45 EDT 2003 SysID: SYSC

- record subtypes: 1:Svr\_Act. 3:Svr\_Int. 5:EJB\_Act. 6:EJB\_Int. 7:Web\_Act. 8:Web\_Int.

SMF Numbr	-Record Type	Time	Server	Bean/WebAppName	Bytes	Bytes	# of	El.Time (mSec)	WLM_Enclave_CPU_Time (uSec)			
		hh:mm:ss	Instance	Method/Servlet	toSvr	fromSvr	Call	Avg	Max	Tot/Av	Max	Min
42	120.1	12:07:45	X5SRV1C		669	266				12954		
43	120.7	12:07:45	X5SRV1C									
45	120.1	12:07:55	X5SRV1C							3391		
46	120.7	12:07:55	X5SRV1C	SimpleFileServlet				3		1271		
				My_IVT_Application#MyIVTWebApp.war								
47	120.1	12:07:55	X5SRV1C		569	25179				8677		
48	120.7	12:07:55	X5SRV1C	SimpleFileServlet				38		6461		
				My_IVT_Application#MyIVTWebApp.war								
96	120.1	12:15:55	X5SRV1C		733	657				6107		
97	120.7	12:15:55	X5SRV1C	JSP 1.2 Processor				13		3522		
				/ivtDate.jsp				1		1090		
				My_IVT_Application#MyIVTWebApp.war								
98	120.1	12:15:55	X5SRV1C							2389		
					701	212						
99	120.7	12:15:55	X5SRV1C	SimpleFileServlet				1		1038		
				My_IVT_Application#MyIVTWebApp.war								
100	120.1	12:15:55	X5SRV1C									

This chart might not be in your handouts



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# defining the log stream

## After allocating the VSAM cluster during server setup

[WebSphere Variables](#) >

ras\_log\_logstreamName

Substitution variables allow specifying a level of indirection for values defined in the system, such as filesystem roots. Variables can be defined at the server, node, or cell level. When variables in different scopes have the same name, the order of resolution is server variables, then node variables, then cell variables. [i]

**Configuration**

General Properties		
Name	<input type="text" value="ras_log_logstreamName"/>	[i] Specifies the symbolic name representing a physical path or URL root.
Value	<input type="text" value="V500.SC59.BS0F.LOG"/>	[i] Specifies the absolute path that the symbolic name represents.
Description	<input type="text" value="Logstream"/>	[i] Provides an optional description for your administrative records.

Apply OK Reset Cancel

+BBOO0222I WSVR0001I: Server SERVANT PROCESS wdfndfcdsc59 open for e-business  
+BBOO024I ERRORS WILL BE WRITTEN TO V500.SC59.BS0F.LOG LOG STREAM FOR JOB WASDFS.



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## controlling and browsing Useful operator command:

```
D LOGGER, LOGSTREAM
IXG601I 16.58.43  LOGGER DISPLAY 108
INVENTORY INFORMATION BY LOGSTREAM
LOGSTREAM          STRUCTURE          #CONN  STATUS
-----
ATBAPPC.LU.LOGNAMES  *DASDONLY*          000001  IN USE
  SYSNAME: SC59
  DUPLEXING: STAGING DATA SET
V500.SC59.BS0F.LOG  *DASDONLY*          000001  IN USE
  SYSNAME: SC59
  DUPLEXING: STAGING DATA SET
V500.SC59.BS00.LOG  *DASDONLY*          000000  AVAILABLE
```

## Browsing the logstream (profile nopref):

ex 'BBO5S59.SBBOEXEC(BBORBLOG)' 'V500.SC59.BS0F.LOG'

```
BROWSE V500.SC59.BS0F.LOG Line 00000023 Col 001 08
Command ==> Scroll ==> CSR
/bborjtr.cpp+812 ... BB000222I SRVE0180I: Yadminconsole" Y/admin"
YServlet.LOG": /secure/layouts/tabsLayout.jsp: init
2003/10/09 20:57:39.564 01 SYSTEM=SC59 SERVER=WASDF JobName=WASDFS
ASID=0X0052 PID=0X03000367 TID=0X1FF82B00 0X000017 c=3.4
/bborjtr.cpp+812 ... BB000222I SRVE0180I: Yadminconsole" Y/admin"
YServlet.LOG": /secure/layouts/detailTitleLayout.jsp: init
2003/10/09 20:57:39.186 01 SYSTEM=SC59 SERVER=WASDF JobName=WASDFS
ASID=0X0052 PID=0X03000367 TID=0X1FF82B00 0X000017 c=3.4
/bborjtr.cpp+812 ... BB000222I SRVE0180I: Yadminconsole" Y/admin"
YServlet.LOG": /secure/layouts/configboxLayout.jsp: init
2003/10/09 20:57:39.160 01 SYSTEM=SC59 SERVER=WASDF JobName=WASDFS
ASID=0X0052 PID=0X03000367 TID=0X1FF82B00 0X000017 c=3.4
/bborjtr.cpp+812 ... BB000222I SRVE0180I: Yadminconsole" Y/admin"
YServlet.LOG": action: VariableSubstitutionEntryDetailForm was
null.Creating new form bean and storing in session
```



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# enabling Tivoli Performance Viewer

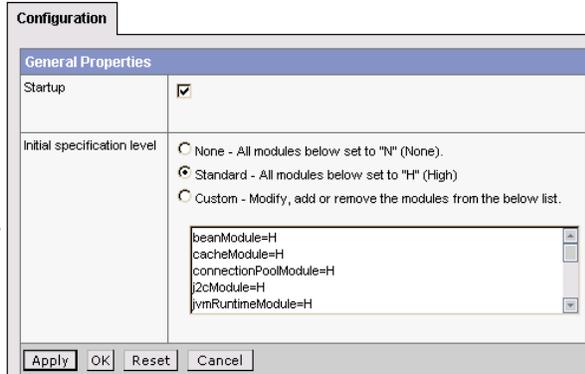
- ▶ **Uninstall AAT and client development kit**
- ▶ **Install "IBM WebSphere Client Development Kit for z/OS" on your workstation**  
(/usr/lpp/zWebSphere/V5R0M0/lib/setup.exe)
- ▶ **Enable Performance Monitoring**
- ▶ **Restart your Server**
- ▶ **From Start > Programs > IBM WebSphere Client Development Kit for z/OS > Tivoli Performance Viewer**
- ▶ **Edit host & port or**
- ▶ **c:\Programs\IBM\WebSphereClientDevelopment KitforzOS\bin\tperfviewer wtsc59.itso.ibm.com 38880 soap**



Application Servers > wdfndcdfs59 >

## Performance Monitoring Service

Configuration and Runtime Settings for Performance Monitoring Infrastructure (PMI) ⓘ



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## Doesn't work? Your security is enabled :-) This is how it should work

### Server Edit:

/WebSphere/BS0F/appse...ties/

### soap.client.props:

```
# JMX SOAP connector  
com.ibm.SOAP.securityEnabled=true  
com.ibm.SOAP.loginPassword=holcur  
com.ibm.SOAP.loginUserId=WSADMIN
```

### sas.client.props:

```
# JMX SOAP connector identity  
com.ibm.SOAP.loginPassword=holcur  
com.ibm.SOAP.loginUserId=WSADMIN
```

### Client Edit

```
C:\Programs\IBM\WebSphereClientDevelopmentKitforzOS\bin\setupCmdline.bat  
SET CLIENTSAS=-Dcom.ibm.CORBA.ConfigURL=file:%WDK_HOME%/properties/sas.client.props  
SET CLIENTSOAP=-Dcom.ibm.SOAP.ConfigURL=file:%WDK_HOME%/properties/soap.client.props  
Run setupCmdline.bat
```

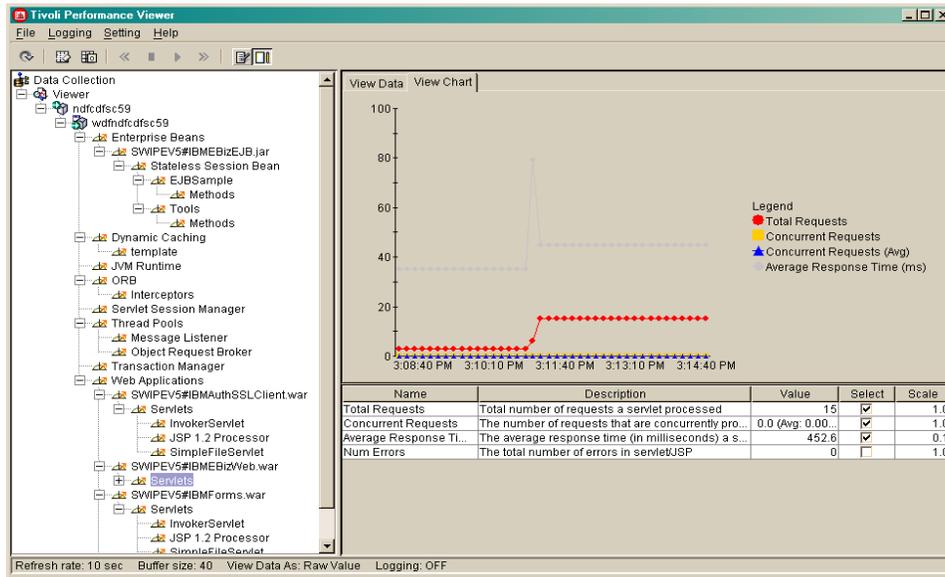
Run client



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

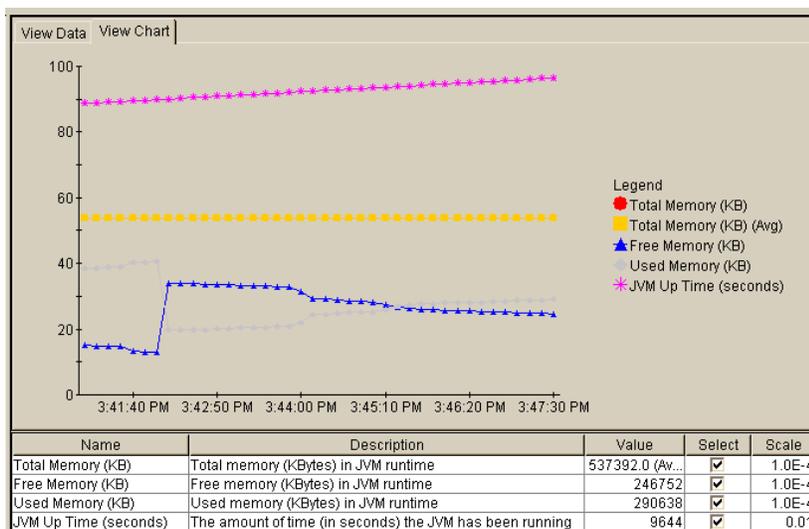
# Sample Screenshot



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# looking at the JVM



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## more tools

- get a good telnet client (Tera Term)
  - ▶ <ftp://riksun.riken.go.jp/pub/pc/misc/terminal/teraterm/>
- learn vi
  - ▶ get a "cheat-sheet" for the 20 common commands
  - ▶ viascii - <http://www.ibm.com/servers/eserver/zseries/zos/unix/bpxa1toy.html>
- Other Tools:
  - ▶ jad (decompile java class files) <http://kpdus.tripod.com/jad.html>
  - ▶ Programmers File Editor: <http://www.lancs.ac.uk/people/cpaap/pfe>
  - ▶ vedit, ascii/ebcdic [http://www.vedit.com/quick\\_update.htm](http://www.vedit.com/quick_update.htm)
  - ▶ ultra edit, ascii/ebcdic <http://www.idmcomp.com/downloads/index.html>
  - ▶ WS\_FTP: <http://www.ipswitch.com>
  - ▶ filezilla: <http://www.sourceforge.net/projects/filezilla>
  - ▶ MXI - "MVS sysprog browser": <http://www.secltd.co.uk>, TASID/QCB like
  - ▶ NEDIT: <http://www.nedit.org>, xwindows editor
  - ▶ Jinsight profiling: <http://www.alphaworks.ibm.com>
  - ▶ MS Web Application Stress Tool: <http://webtool.rte.microsoft.com/>
  - ▶ http sniffer, Page Detailler: <http://www.alphaworks.ibm.com>
- Sample Apps - Snoop, StatelessSessionBean, MemoryLeak, swipe



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## more stuff, maybe not in your handout wsadmin, also to verify your setup

### connect to wsadmin command line interface

- ▶ Windows (WSAS needs to be installed)
  - ▶ `C:\IBM\WASV5\WebSphere\AppServer\bin>wsadmin conntype -host wtsc59 -port 38880 -user wsadmin -password secret`
- ▶ z/OS
  - ▶ `wunderl@SC59:/WebSphere/BS0F/appserver/bin/wsadmin.sh conntype -host wtsc59 -port 38880 -user wsadmin -password secret`



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## more stuff, maybe not in your handout well hidden keystore definitions

### Message(s)

- ⚠ Changes have been made to your local configuration. Click [Save](#) to apply changes to the master configuration.
- ℹ The server may need to be restarted for these changes to take effect.

[Application Servers](#) > [wdfndfsc59](#) > [Administration Services](#) > [JMX Connectors](#) > [SOAPConnector](#) > [Custom Properties](#) >

### sslConfig

Specifies arbitrary name/value pairs of data, where the name is a property key and the value is a string value which can be used to set internal system configuration properties. ⓘ

#### Configuration

##### General Properties

Name	* sslConfig	ⓘ Specifies the name (or key) for the property.
Value	* ndfcdesc59/DefaultSOAPSSLSettings ndfcdesc59/DefaultSSLSettings ndfcdesc59/RACFJSSESettings ndfcdesc59/DefaultSOAPSSLSettings	ⓘ Specifies the value paired with the specified name.
Description		ⓘ Provides information about the name-value pair.

Apply OK Reset Cancel



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com



e-business



## RACF JOBS walkthrough



# Redbooks

International Technical  
Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

## RACF Customization Job Walk through

```
/* Class activation.
SETROPTS CLASSACT(CBIND)
SETROPTS RACLIST(CBIND) GENERIC(CBIND)
SETROPTS CLASSACT(SERVER)
SETROPTS RACLIST(SERVER) GENERIC(SERVER)
SETROPTS CLASSACT(STARTED)
SETROPTS RACLIST(STARTED) GENERIC(STARTED)
SETROPTS CLASSACT(FACILITY)
SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)
SETROPTS GRPLIST
/* Create WAS configuration group.
ADDGROUP WASADM OMVS(GID(20000))
ADDGROUP WASSRV OMVS(GID(20001))
/* Creating group for default WAS userid.
ADDGROUP MISC OMVS(GID(2502))
/* Adding Protected users for WAS Controller / Servants Regions.
ADDUSER WDDFSTU DFLTGRP(WASADM) OMVS(UID(2710) HOME(/tmp) PROGRAM(/bin/sh))
NAME('WAS DAEMON CR') NOPASSWORD NOIDCARD
ADDUSER WDCFSTU DFLTGRP(WASADM) OMVS(UID(2530) HOME(/tmp) PROGRAM(/bin/sh))
NAME('WAS APPSVR Controller') NOPASSWORD NOIDCARD
ADDUSER WDSFSTU DFLTGRP(WASSRV) OMVS(UID(2630) HOME(/tmp) PROGRAM(/bin/sh))
NAME('WAS APPSVR Servant') NOPASSWORD NOIDCARD
ADDUSER CTCSTU DFLTGRP(STG) NAME('WAS TRACE WRITER') NOPASSWORD NOIDCARD
```

enable classes

no logon  
no revoke

USS GIDs



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## RACF Customization Job Walk through

```
/* Adding WAS admin userid.
ADDUSER WSADMIN DFLTGRP(WASADM) OMVS(UID(2403) HOME(/tmp) PROGRAM(/bin/sh))
NAME('WAS ADMINISTRATOR')
PW USER(WADMIN) NOINTERVAL
ALU WSADMIN PASSWORD(WADMIN) NOEXPIRED
/* Adding default WAS userid for base servers.
ADDUSER WASDFTU RESTRICTED DFLTGRP(MISC) OMVS(UID(2402) HOME(/tmp)
PROGRAM(/bin/sh)) NAME('WAS DEFAULT USER')
/* Connecting administrator to the WebSphere configuration group.
CONNECT WSADMIN group(WASADM)
/* Connecting STC users to the WebSphere configuration group.
CONNECT WDDFSTU group(WASADM)
CONNECT WDCFSTU group(WASADM)
CONNECT WDSFSTU group(WASADM)
/* CF of DASD logstream
RDEFINE LOGSTRM V500.SC59.BS0F.LOG UACC(READ)
PERMIT V500.SC59.BS0F.LOG CLASS(LOGSTRM) ID(WASADMIN) ACCESS(UPDATE)
SETROPTS CLASSACT(LOGSTRM)
/* Defining CBIND CB.BIND.cluster_name.
RDEFINE CBIND CB.BIND.* UACC(NONE)
RDEFINE CBIND CB.BIND.BBO* UACC(READ)
PERMIT CB.BIND.BBO* CLASS(CBIND) ID(WASADM) ACCESS(CONTROL)
RDEFINE CBIND CB.BIND.CLUDF UACC(READ)
PERMIT CB.BIND.CLUDF CLASS(CBIND) ID(WASADM) ACCESS(CONTROL)
/* Defining CBIND CB.cluster.
RDEFINE CBIND CB.* UACC(NONE)
```

default admin (get rid off later)

not good!

who can connect



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# RACF Customization Job Walk through

```
/* Defining CBIND CB.cluster access for WAS systems servers */
RDEFINE CBIND CB.CLUDF UACC(READ)
RDEFINE CBIND CB.BBO* UACC(READ)
SETROPTS RACLIST(CBIND) GENERIC(CBIND) REFRESH
/* Defining SERVER CB.cluster.generic_server. */
RDEFINE SERVER CB.* UACC(NONE)
RDEFINE SERVER CB.*.BBO* UACC(NONE)
RDEFINE SERVER CB.*.BBO*. * UACC(NONE)
RDEFINE SERVER CB.*.CLUDF UACC(NONE)
/* Permitting SERVER class access. */
PERMIT CB.*.CLUDF CLASS(SERVER) ID(WDSFSTU) ACC(READ)
RDEFINE SERVER CB.*.CLUDF.* UACC(NONE)
/* Permitting SERVER class access. */
PERMIT CB.*.CLUDF.* CLASS(SERVER) ID(WDSFSTU) ACC(READ)
SETROPTS RACLIST(SERVER) GENERIC(SERVER) REFRESH
/* Assigning userids to started tasks. */
RDEFINE STARTED WAS5DDF.* STDATA(USER(WDDFSTU) GROUP(WASADM) TRACE(YES))
RDEFINE STARTED WAS5DCF.* STDATA(USER(WDCFSTU) GROUP(WASADM) TRACE(YES))
RDEFINE STARTED WASDFS.* STDATA(USER(WDSFSTU) GROUP(WASADM) TRACE(YES))
RDEFINE STARTED BBO*. * STDATA(USER(WDSFSTU) GROUP(WASADM) TRACE(YES))
RDEFINE STARTED CTRBS0F.* STDATA(USER(CTRCSTU) GROUP(STG) TRACE(YES))
SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH
```



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# RACF Customization Job Walk through

```
/* APPL class setup. */
RDEFINE APPL CBS390 UACC(NONE)
PERMIT CBS390 CLASS(APPL) ID(WASADM) ACCESS(READ)
PERMIT CBS390 CLASS(APPL) ID(WASDFTU) ACCESS(READ)
SETROPTS CLASSACT(APPL)
/* OPERCMDS: These are really Samples, DO NOT USE AS IS */
RDEFINE OPERCMDS MVS.START.STC.** UACC(NONE)
RDEFINE OPERCMDS MVS.STOP.STC.** UACC(NONE)
RDEFINE OPERCMDS MVS.MODIFY.STC.** UACC(NONE)
RDEFINE OPERCMDS MVS.CANCEL.STC.** UACC(NONE)
RDEFINE OPERCMDS MVS.FORCE.STC.** UACC(NONE)
/* Permitting WAS Daemon and AppServer to Operator Cmds */
PERMIT MVS.START.STC.** CLASS(OPERCMDS) ID(WDDFSTU WDCFSTU WDSFSTU)
ACC(UPDATE)
PERMIT MVS.STOP.STC.** CLASS(OPERCMDS) ID(WDDFSTU WDCFSTU WDSFSTU)
ACC(UPDATE)
PERMIT MVS.MODIFY.STC.** CLASS(OPERCMDS) ID(WDDFSTU WDCFSTU WDSFSTU)
ACC(UPDATE)
PERMIT MVS.CANCEL.STC.** CLASS(OPERCMDS) ID(WDDFSTU WDCFSTU WDSFSTU)
ACC(UPDATE)
PERMIT MVS.FORCE.STC.** CLASS(OPERCMDS) ID(WDDFSTU WDCFSTU WDSFSTU)
ACC(CONTROL)
SETROPTS CLASSACT(OPERCMDS)
SETROPTS RACLIST(OPERCMDS) GENERIC(OPERCMDS)
```



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# RACF Customization Job Walk through

```
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
/* Create SSL CA Certificate for WebSphere CA
/* EXPIRE DATE BEFORE CONVERTING OVER 20100810
/* FORMAT_DATE IS 2010/08/10
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('WAS CertAuth') C('US')) WITHLABEL('WS
for z/OS CA') TRUST NOTAFTER(2010/08/10)
/* Creating SSL keyrings for WebSphere servers
RACDCERT ADDRING(WASKEYRING) ID( WDCFSTU )
/* Generating certificates for WebSphere servers
RACDCERT ID (WDCFSTU) GENCERT SUBJECTSDN(CN('WAS z/OS AppServer.CLUDF') O('IBM'))
WITHLABEL('CLUDF') SIGNWITH(CERTAUTH LABEL('WS for z/OS CA'))
/* Connecting Server Certificates to their keyrings
RACDCERT ID(WDCFSTU) CONNECT (LABEL('CLUDF') RING(WASKEYRING ) DEFAULT)
/* Connect WAS CA Certificates to Servers keyring
RACDCERT ID(WDCFSTU) CONNECT (RING(WASKEYRING) LABEL('WS for z/OS CA') CERTAUTH)
/* Connect Commercial CAs to Servers keyring
RACDCERT ID(WDCFSTU) CONNECT (RING(WASKEYRING) CERTAUTH label('Verisign Class 3
Primary CA') USAGE(CERTAUTH))
RACDCERT ID(WDCFSTU) CONNECT (RING(WASKEYRING) CERTAUTH label('Verisign Class 1
Primary CA') USAGE(CERTAUTH)).....
/* Grant access to LISTRING
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(WASADM) ACC(READ)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(WASADM) ACC(READ)
/* Facility class refresh
SETROPTS CLASSACT(FACILITY) REFRESH
```

ICSF

create CA cert

create cert



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# RACF Customization Job Walk through

```
/* Setting up the passticket.
*
SETROPTS CLASSACT(PTKTDATA)
RDEFINE PTKTDATA CBS390
SSIGNON(KEYMASKED(1212121212121212)) UACC(NONE)
PERMIT CBS390 CLASS(PTKTDATA) ID(WASADM MISC) ACC(READ)
SETROPTS RACLIST(PTKTDATA)
```

no



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

# RACF Customization Job Walk through

```
/* Setting up EJBRoles Profiles for admin roles
SETROPTS CLASSACT(EJBROLE)
/* Defining roles for SAF access
RDEFINE EJBROLE administrator UACC(NONE)
RDEFINE EJBROLE monitor UACC(NONE)
RDEFINE EJBROLE configurator UACC(NONE)
RDEFINE EJBROLE operator UACC(NONE)
/* Setting up EJBRoles access for administrator and CR
PERMIT administrator CLASS(EJBROLE) ID(WASADM) ACCESS(READ)
PERMIT administrator CLASS(EJBROLE) ID(WSADMIN) ACCESS(READ)
PERMIT monitor CLASS(EJBROLE) ID(WASADM) ACCESS(READ)
PERMIT monitor CLASS(EJBROLE) ID(WSADMIN) ACCESS(READ)
PERMIT configurator CLASS(EJBROLE) ID(WASADM) ACCESS(READ)
PERMIT configurator CLASS(EJBROLE) ID(WSADMIN) ACCESS(READ)
PERMIT operator CLASS(EJBROLE) ID(WASADM) ACCESS(READ)
PERMIT operator CLASS(EJBROLE) ID(WSADMIN) ACCESS(READ)
/* Setting up EJBRoles Profiles for Naming roles
RDEFINE EJBROLE CosNamingRead UACC(READ)
PERMIT CosNamingRead CLASS(EJBROLE) ID(WASDFTU) ACCESS(READ)
RDEFINE EJBROLE CosNamingWrite UACC(READ)
RDEFINE EJBROLE CosNamingCreate UACC(READ)
RDEFINE EJBROLE CosNamingDelete UACC(READ)
RDEFINE EJBROLE operator UACC(NONE)
SETROPTS RACLIST(EJBROLE) REFRESH
```

ADMIN  
roles

user 2  
role

?

naming  
roles

?



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.

## RACF backout tool

This exec reads the generated RACF commands from the BROWBRK member of the target .DATA partitioned data set, and creates RACF DELUSER, DELGROUP, RDELETE, etc. commands (in reverse order). Before running the resultant RACF commands, you should review the output and delete any commands that would delete users, groups or profiles used by other servers that you want to retain.

Be very careful not to delete users & generic profiles used by others!

<http://www.ibm.com/support/techdocs/atmastr.nsf/WebIndex/TD101128>



[ibm.com/redbooks](http://ibm.com/redbooks)

© Copyright IBM Corp. 2003. All rights reserved.