IBM Lotus Domino Admin to IBM WebSphere Application Admin

- With Special Mention of ST85

Gabriella Davis
The Turtle Partnership
gabriella@turtlepartnership.com

Agenda

- Who Are You?
- Let’s Talk Websphere!
- WAS And Friends - How It All Fits Together
- I Know How To Do This In Domino But.....
- Other WAS Stuff Worth Knowing About
  - Network Deployment
  - Clustering and DR
  - Upgrading
- Summary

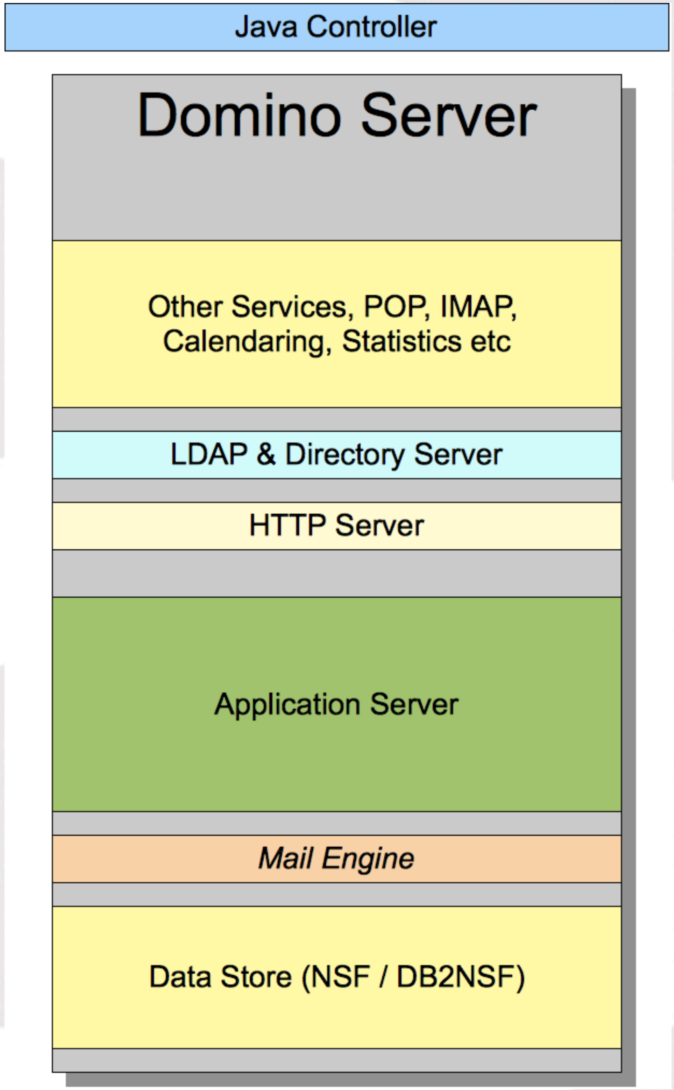
Who Are You?

- You’re a Domino Admin with experience (or not) of Sametime and little to no experience of WAS
- We’re going to talk to you like you’ve never seen WAS before in your life
- Apologies to anyone for whom this is too basic, we hope you’ll get some useful tips too

Why Talk Websphere

- Websphere has become the underlying infrastructure behind all the advanced collaboration tools coming out of Lotus.
- If you want to run those tools you need to be able to install and support WAS. They include:
  - Lotus Connections
  - Quickr for Portal
  - and of course
    - Sametime Proxy
    - Sametime Advanced
    - Sametime Meeting Server
    - Sametime Media Server
    - Sametime Gateway ...+++++

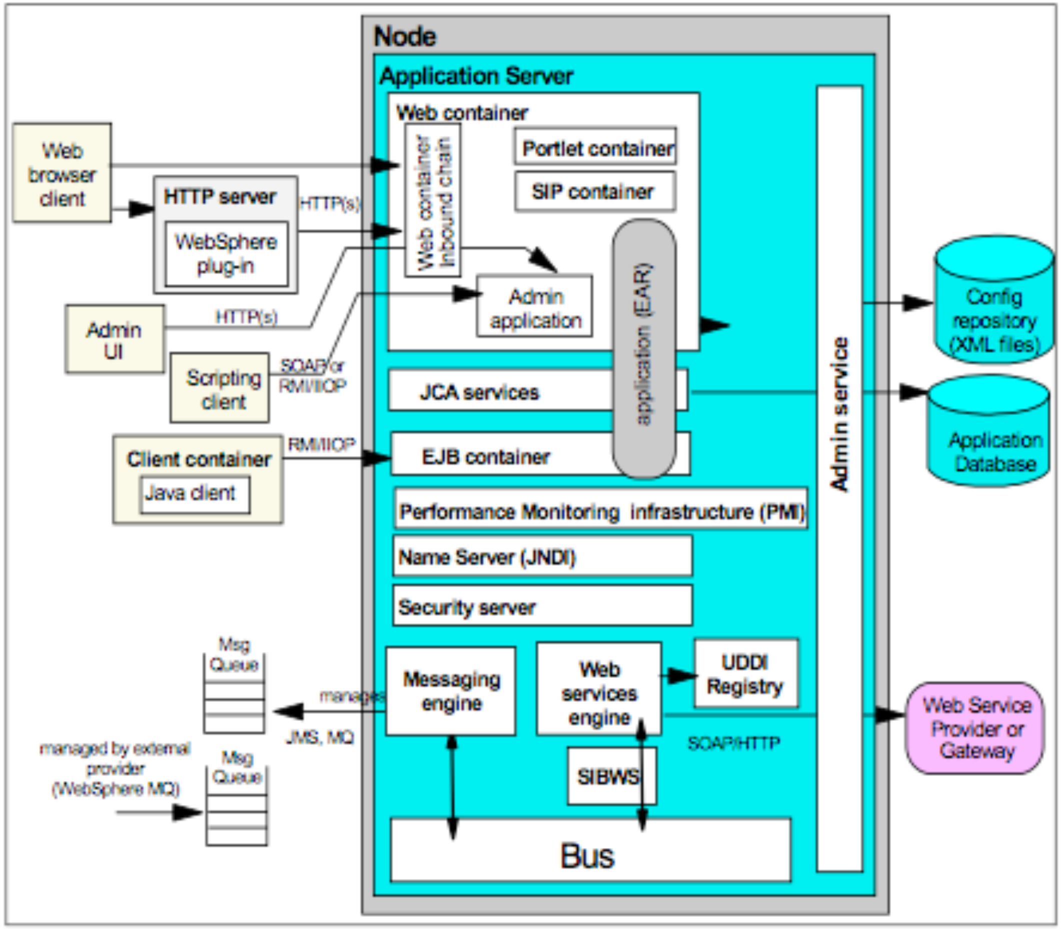
Domino Infrastructure



- Each component and service running on a single server as individual tasks that talk to each other

- Multiple Domino Servers run as separate instances on separate computers (or separate partitions)

WAS Infastructure

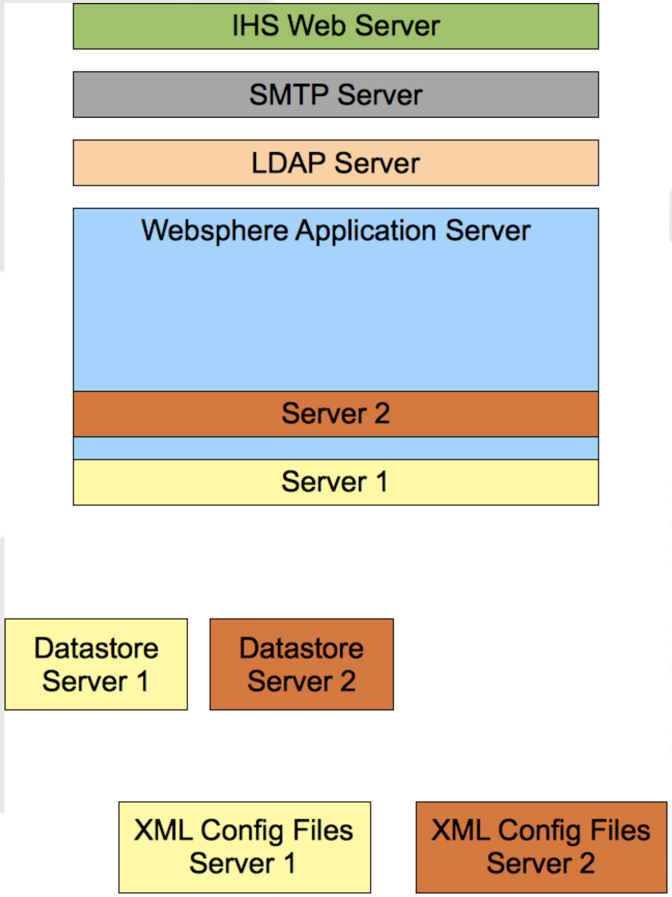


Let’s Take a Step Back

- Each Websphere Server is installed in a Node
- Each Node must exist within a Cell
- A single Cell can contain multiple separate WAS servers in different Nodes
- Each server is isolated from the other within the Cell
- Clustering is done at a Node level
  - Clustering for Sametime 8.5 is not for load balancing but for failover

BLUG
Belux Lotus User Group

WAS Infastructure - The Simple Version



- Each application server managed by Websphere
- Uses an external database source that can also be managed externally
  - DB2 for Sametime 8.5
- Services do not talk to each other by default
- All configuration information is held in disk based XML files

Using Sametime 8.5 As Our Example

Sametime Servers - Nodes & Cells

- All Servers are installed under the main Websphere directory (“AppServer”)
- In that directory there is a ‘profiles’ directory which lists all the Cells
- On Sametime 8.5 install (where everything except Community Services is on one box) all profiles are contained in the directory
  - C:\ibm\webspherebeta\appserver\profiles
    - I chose not to install under program files to keep the path name short
- Each server is installed under its own Cell

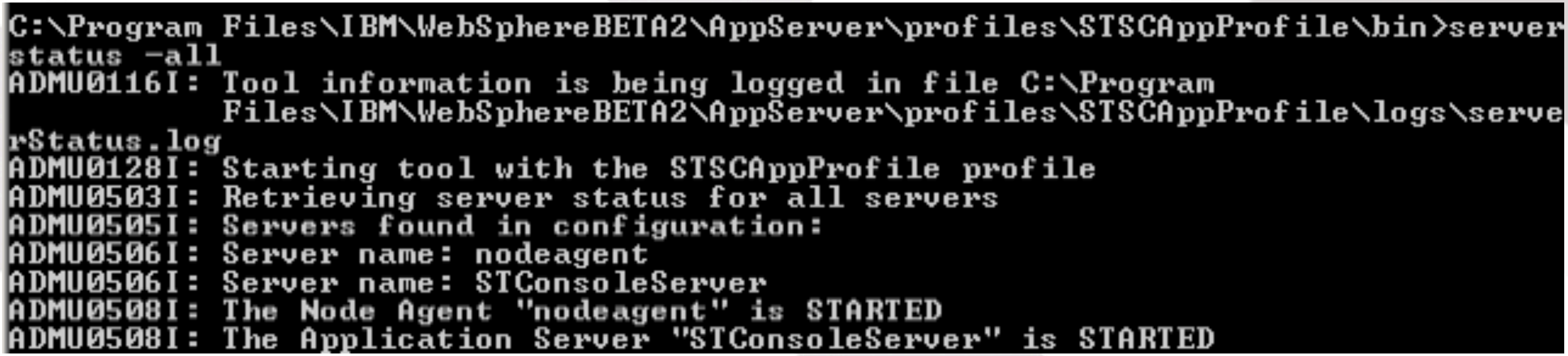
Sametime Server Profiles

- The *DMProfile cell contains the deployment manager node for that server so <servername>MeetingDMProfile1 is the cell for the deployment manager of the Meeting Server
  - <servername>ProxyDMProfile is for Proxy Server
    - STSCDMmgrProfile is for Systems Console
- The *PNProfile is the cell that contains the nodes for the specific servers. Each cell contains the nodeagent and the server component itself, eg:
  - <servername>ProxyPNProfile1 contains
    - nodeagent and STProxyServer
  - <servername>MeetingPNProfile1 contains
    - Nodeagent , STMeetingServer, STMeetingHttpProxy

BLUG
Belux Lotus User Group

Tip!

- If you don’t know what Cells you have then look in the profiles directory under ‘Appserver’
- If you don’t know what Nodes are installed under those cells then navigate to the Cell directory itself and its ‘bin’ subdirectory and type
  - serverstatus -all
  - you will be prompted for the WAS credentials you chose during installation and then told what servers are enabled in that Cell and if they are running
    - You can pass the credentials on the command line using the parameters –username xxx –password xxx



```
C:\Program Files\IBM\WebSphereBETA2\AppServer\profiles\STSCAppProfile\bin>server
status -all
ADMU0116I: Tool information is being logged in file C:\Program
           Files\IBM\WebSphereBETA2\AppServer\profiles\STSCAppProfile\logs\serve
rStatus.log
ADMU0128I: Starting tool with the STSCAppProfile profile
ADMU0503I: Retrieving server status for all servers
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: nodeagent
ADMU0506I: Server name: STConsoleServer
ADMU0508I: The Node Agent "nodeagent" is STARTED
ADMU0508I: The Application Server "STConsoleServer" is STARTED
```

Domino Server & what it does

- Mail Services
- Web Server
- LDAP Server
- Application Server

WAS Server & what it does

- Application Server for Java applications
- Manages and Secures the application
- Provides an environment in which to run multiple applications in isolation from each other

- Configuration details held in XML files on the file system (the "Configuration Repository")

What might you expect to find that's not immediately apparent

- Mail services or routing
  - You define an SMTP server to send mail to
  - POP3 and IMAP can be configured
- A local directory for authentication or security
  - There are various options for user repositories and registries but Websphere doens't have a user directory built in
  - You use an external LDAP server for authentication in most Lotus implementations and in Sametime 8.5
- An HTTP server
  - Although it comes with IBM HTTP Server to be installed on top as a web interface
- The Lotus Sametime Community Server

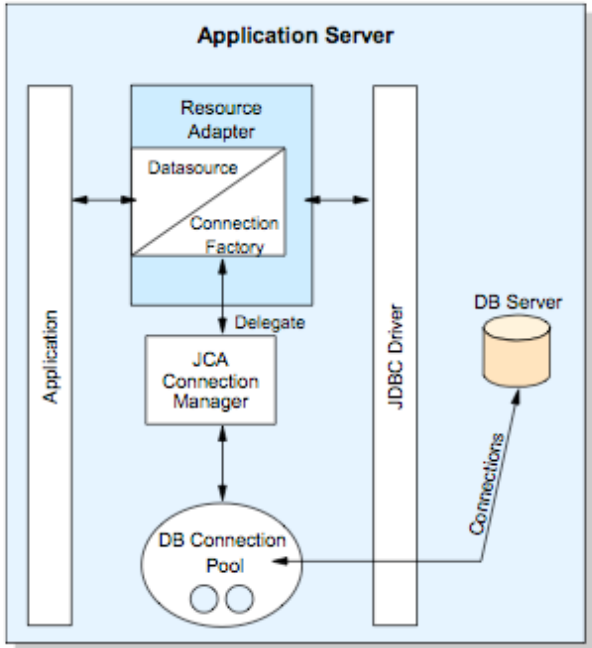
What you might expect that’s not there at all

- A live console
- A list of servers with their running status
- A single place to ‘start’ everything

Domino DB component

- NSF
- ~~DB2NSF~~

WAS DB component



- DB2 for most Lotus applications and for Sametime 8.5
- although in general it can use Oracle, SQL or countless other DB application servers using JDBC drivers

Sametime 8.5 DB Component

- Sametime 8.5 requires DB2 to be installed to store the databases used by the different individual servers
- The Sametime Systems Console and the Meeting Server both require databases but although they can use the same DB2 server they cannot use the same DB2 database
  - You must create separate DB2 databases for each server
- DB2 has its own management console and runs as a service outside of Websphere
- If you want to check your databases you have to go into the DB2 Administration interface
- If you want to know if DB2 is running you can see if it's listening on port 50000

Domino Authentication component

- Internal Directory NSF always
- Surfaced as LDAP
- External LDAP Directories

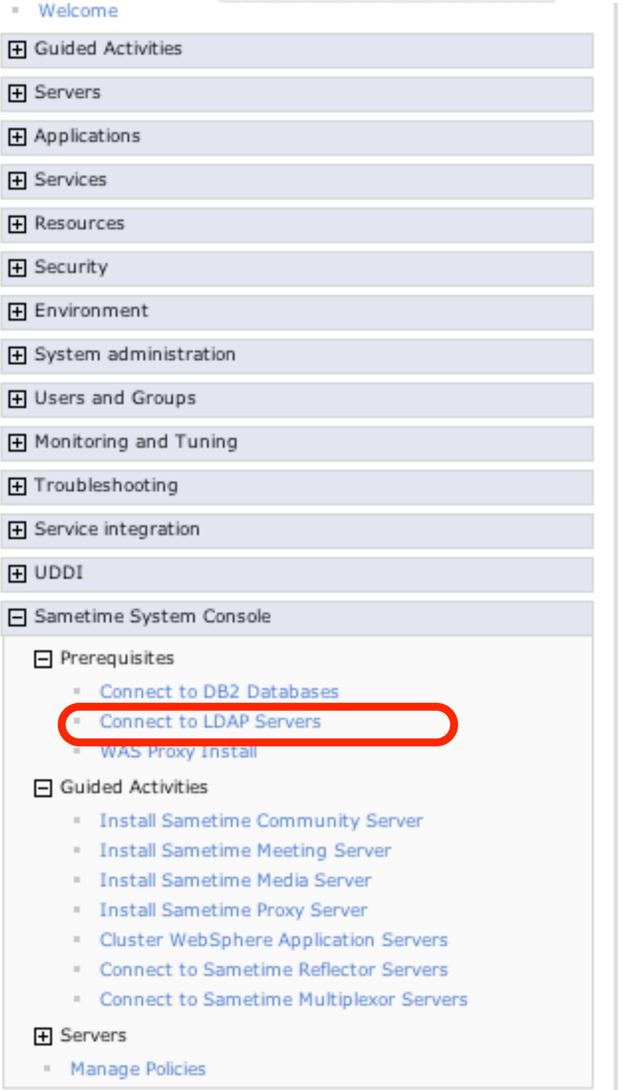
WAS Authentication component

- Local Operating System Repository
- LDAP Server
- Federated Repositories
- Custom Repository
- Only one authentication type can be used
  - Federated repositories allow you to have multiple types configured
  - Each repository must use different credentials to bind with since credentials must be unique across the consolidation of all repositories

Sametime Authentication Component

- Sametime 8.5 uses LDAP for authentication
- However the LDAP configuration is done outside of the standard Websphere server menu
- The configuration is done via the Sametime Server menu option in the ISC which represents the SSC
- You could use your Domino IM server as your LDAP server for Sametime by configuring it for LDAP and pointing Websphere at it
  - Then you are still using your Domino Directory for all Sametime authentication

Sametime Authentication



- Welcome
- ⊞ Guided Activities
- ⊞ Servers
- ⊞ Applications
- ⊞ Services
- ⊞ Resources
- ⊞ Security
- ⊞ Environment
- ⊞ System administration
- ⊞ Users and Groups
- ⊞ Monitoring and Tuning
- ⊞ Troubleshooting
- ⊞ Service integration
- ⊞ UDDI
- ⊟ Sametime System Console
  - ⊟ Prerequisites
    - Connect to DB2 Databases
    - Connect to LDAP Servers
    - WAS Proxy Install
  - ⊟ Guided Activities
    - Install Sametime Community Server
    - Install Sametime Meeting Server
    - Install Sametime Media Server
    - Install Sametime Proxy Server
    - Cluster WebSphere Application Servers
    - Connect to Sametime Reflector Servers
    - Connect to Sametime Multiplexor Servers
  - ⊞ Servers
  - Manage Policies

Domino HTTP component

- HTTP Server
- IIS in front of Domino HTTP Server

WAS HTTP component

- Installs various admin and server components on specific ports
- Uses IBM HTTP Server as a web server interface for many applications
- Installed and configured separately but managed from within the WAS Integrated Solutions Console
  - Other HTTP servers can be used as a web server interface but don’t offer the same levels of administrative integration

Sametime HTTP Components

- Installed as part of each individual server
- Each one listening on its own port eg SSC=8701

I Know How To Do This In Domino But......

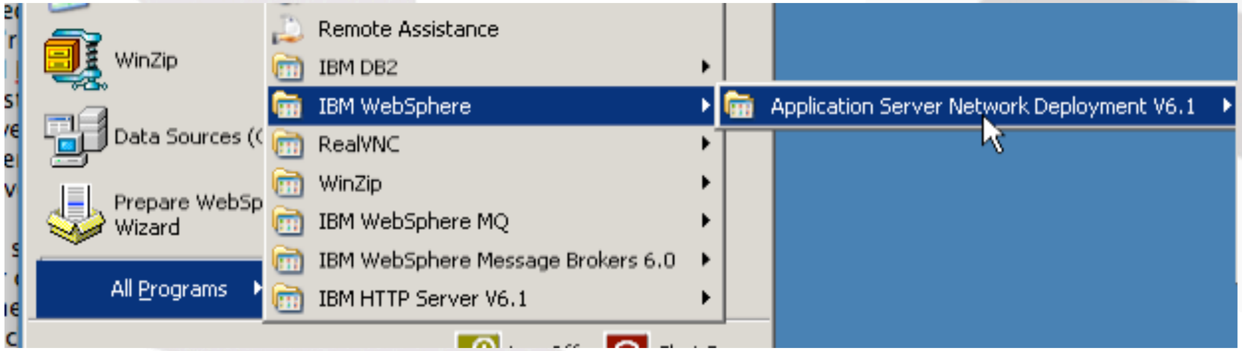
- Starting and Stopping Servers
- Administration Interface
- Configuring LDAP For Authentication
- Configuring SSO
- Troubleshooting
- HTTP Server and Virtual Hosts
- Upgrading

Domino Starting & Stopping Servers

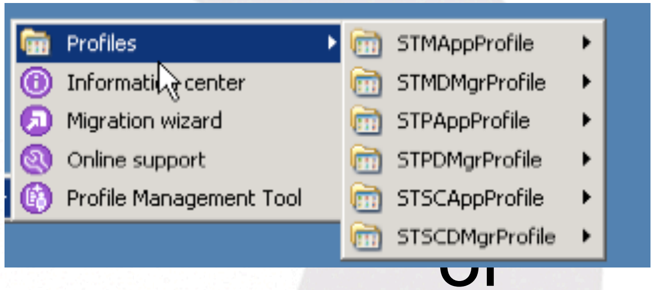
- OS-specific start command ‘server’ or ‘nserver’
  - Ensure server starts using a system or background account so it isn’t stopped when you log out
  - If you’re using linux or aix, use Daniel Nashed’s (free) script files for start, stop , monitoring and cleanup
    - http://www.nashcom.de/nshweb/pages/startscript.htm
- When server is running restart using “Restart Server” on the server console (some server document settings are cached in earlier Domino versions)
- Use “Exit” server on the console to stop the server completely
- If using the java console to start the server (-jc) you can connect to it even when the server isn’t running to restart it

WAS Starting & Stopping Servers

- Drill down

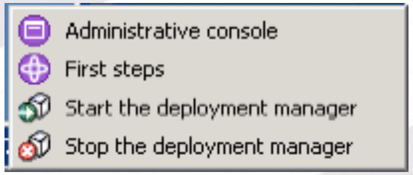


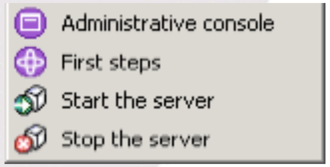
- and drill down



- and finally .....

or



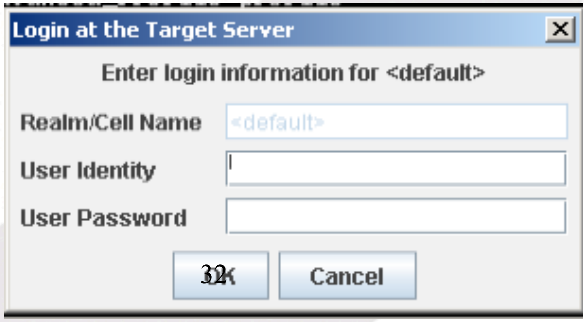


WAS Starting & Stopping Servers - the OTHER way

- <websphereprogramdirectory>\appserver\profiles\<profile>\bin
  - location of files to perform automated start and stop tasks
- Since WAS can and does run several different server applications each defined in their own isolated space you have to specify which instance you want to start or stop
- startserver <servername>
  - startserver dmgr - starts the deployment manager server in the profile you are ‘sat’ in
  - stopserver nodeagent
  - stopserver STConsoleServer will only work from within the STSCAMgrProfile\bin directory as this is where the server resides

WAS Starting & Stopping Servers - the OTHER way

- Use -all to issue a command for all server profiles to start or stop
  - startserver -all
- ServerStatus -all shows the status for all servers
  - You will need to pass the command a username and password for the server you want to report status on
    - serverstatus server -username wasadmin -password waspassword
    - if you don’t pass those parameters on the command line or you are doing -all you will be prompted to supply the credentials when the command runs
- Stopserver also requires -username and -password to stop the server with no interaction, otherwise you will receive this prompt



Login at the Target Server

Enter login information for <default>

Realm/Cell Name <default>

User Identity

User Password

Belux Lotus User Group

Domino Administration Interface

- Directly on the server - access a live running console
- Domino Administrator client
- webadmin.nsf web interface
  - requires HTTP to be running on the server

WAS Administration Interface

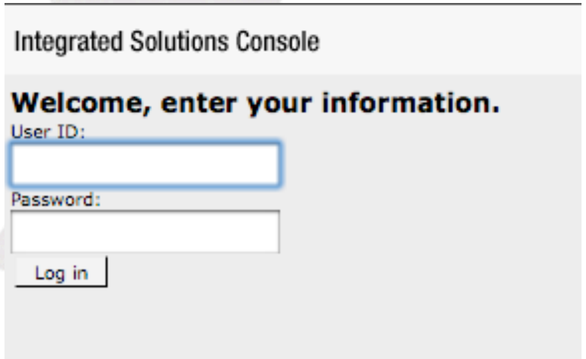
- Integrated Solutions Console
- Runs securely on 9043 by default
- virtual host redirection for /ibm/console
  - http://stadv.turtleweb.com:9060/ibm/console
  - secure: https://stadv.turtleweb.com:9043/ibm/console
- The default credentials for administration are those configured when you first install the server
  - Don’t lose these!

The Sametime Interface

- The Sametime System Console is on port 8701
- It uses the WAS Integrated Solutions Console UI but with an additional menu for Sametime specific configuration
- http://<systemconsolehostname>:8701/ibm/console/logon.jsp
- If all you are installing is Sametime then you won’t have the WAS ISC itself on 9043 or 9060

WAS Administration Interface

- Login



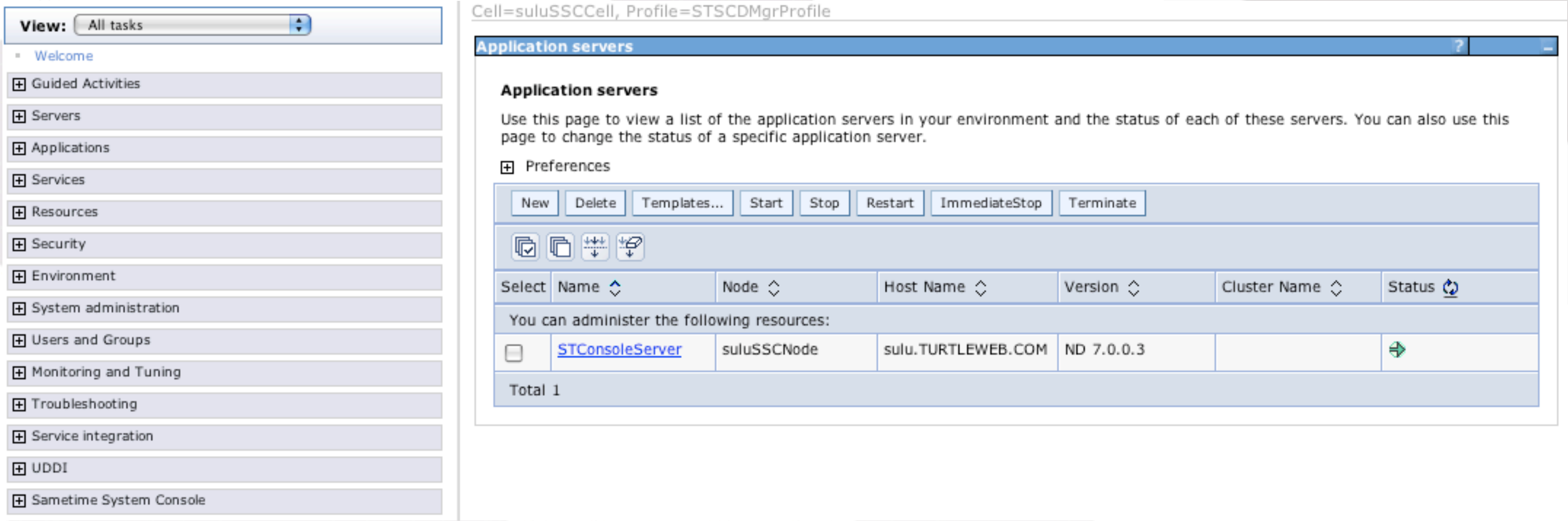
Integrated Solutions Console

Welcome, enter your information.

User ID:

Password:

WAS Administration Interface



Cell=suluSSCCell, Profile=STSCDMgrProfile

Application servers

Application servers

Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.

⊞ Preferences

Select	Name	Node	Host Name	Version	Cluster Name	Status
You can administer the following resources:						
□	STConsoleServer	suluSSCNode	sulu.TURTLEWEB.COM	ND 7.0.0.3		➔
Total 1						

Doh! I've locked myself out!

- Modify Security.XML file
- <websphereprogramdir>\appserver\profiles \<serverprofile>\config\cells\<yourcellname> \security.xml
  - useLocalSecurityServer="true" useDomainQualifiedUserNames="false" enabled="false" cacheTimeout="600" issuePermissionWarning="true"
- Will let you into the Integrated Solutions Console without supplying credentials in an emergency but won't let your servers run

Working within the ISC

- Changes you make are saved locally but need to be applied to the 'Master Repository' before taking effect
- For modifications you therefore have an 'apply' which makes the change locally and then 'save to master repository' which writes out the configuration to the relevant XML files
  - Next page tells you where to find those
- When you have modified the Master repository you will want to stop and start the Websphere server you changed

Sametime Server Configuration

- If you change the configuration of the Sametime server you will want to stop both the server itself and the nodeagent in the same directory
- Only use the ‘Sametime System Console” menu of the ISC to modify other servers
  - If you can’t see the Sametime System Console when logged into the ISC make sure that all 3 servers (dmgr, nodeagent, STConsoleServer) are started

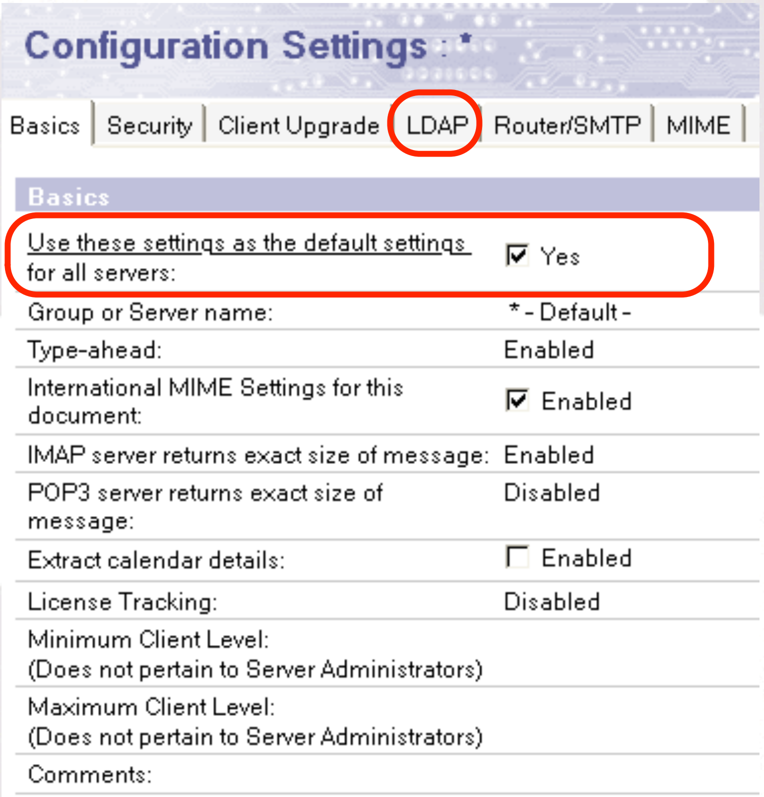
Some XML Files Worth Knowing About

- It’s worthing knowing this stuff is there but don’t worry too much about understanding the hierarchy at this point
- Under the Websphere install directory (Appserver) each of your profiles is listed
  - find ‘profiles’ and then the directory for your profile and in there is a config directory
  - if my profile is “STSCDMgrProfile” (the deployment manager for SSC)
  - and my cellnode ‘sulu’ then
    - <websphereprogramdir>\profiles\STSCDMgrProfile\config\cells\suluSSCCell
- In there you will find a folder for the cell you are working on named by the cellname you will also find a nodes directory containing documents for the node
  - The cellname will take the servername by default so name your server 8 chars or less
  - if XML documents in both the cell and node directories have the same name, the node documents take precedence. The most specific folder name wins!
    - server.xml
    - resources.xml
    - security.xml
    - variables.xml

So..

- My server is called ‘sulu’ & my SSC Cell suluSSCell
- The configuration files for my SSC server are in:
  - c:\ibm\webspherebeta\appserver\profiles \STSCDMgrProfile\config\cells\suluSSCCell\nodes
  - In there I have 2 directories, one for each node in the cells
  - Dmgrnode contains the deployment manager configuration
  - SuluSSCNode contains the Systems Console configuration

Domino - Configuring LDAP for Authentication



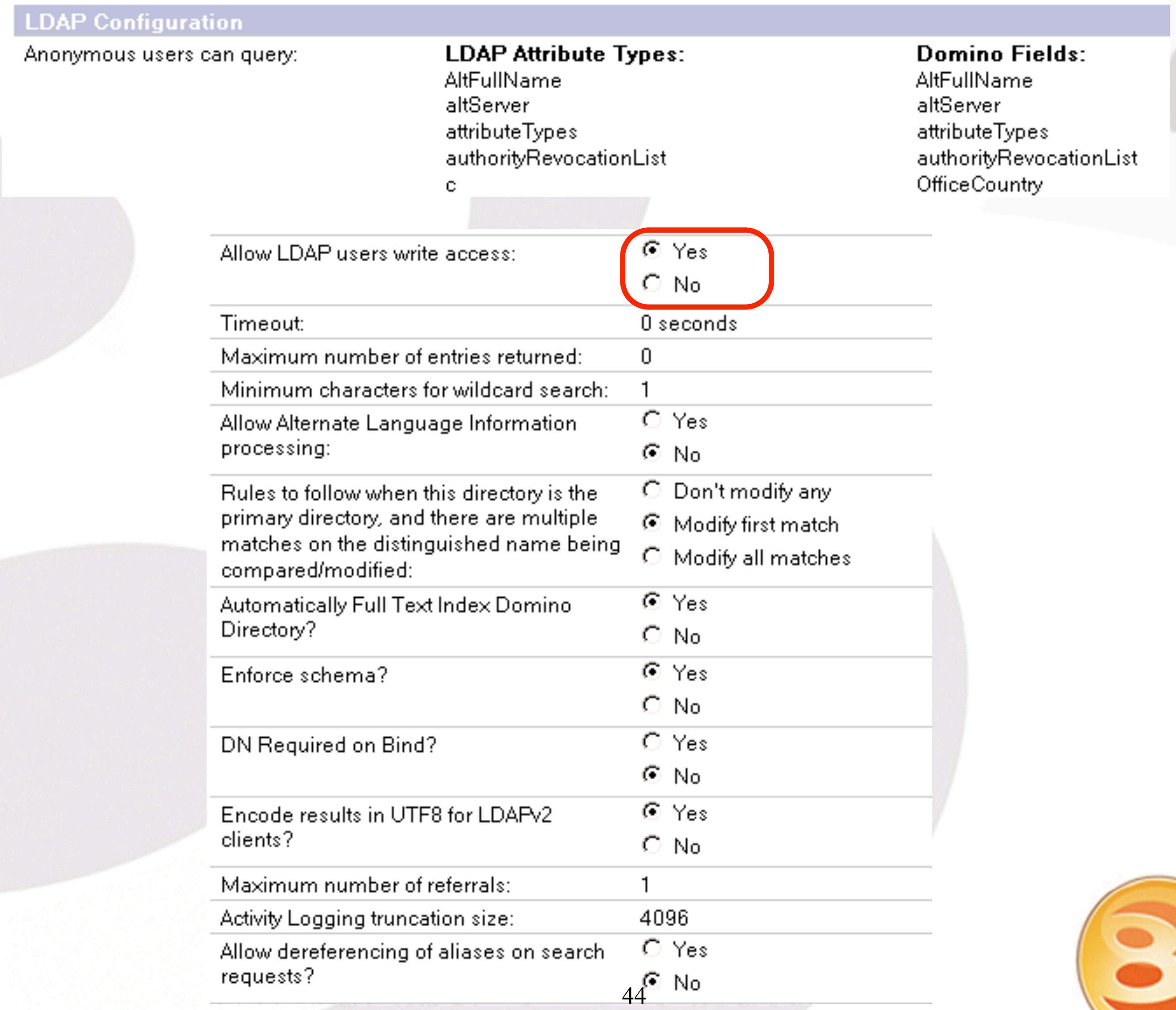
Configuration Settings : *

Basics

Use these settings as the default settings for all servers:	☑ Yes
Group or Server name:	* - Default -
Type-ahead:	Enabled
International MIME Settings for this document:	☑ Enabled
IMAP server returns exact size of message:	Enabled
POP3 server returns exact size of message:	Disabled
Extract calendar details:	☐ Enabled
License Tracking:	Disabled
Minimum Client Level: (Does not pertain to Server Administrators)	
Maximum Client Level: (Does not pertain to Server Administrators)	
Comments:	

- Global Server Configuration Document
  - The one marked with an ‘asterisk’
  - It’s the only one that will have an LDAP tab

Domino - Configuring LDAP for Authentication



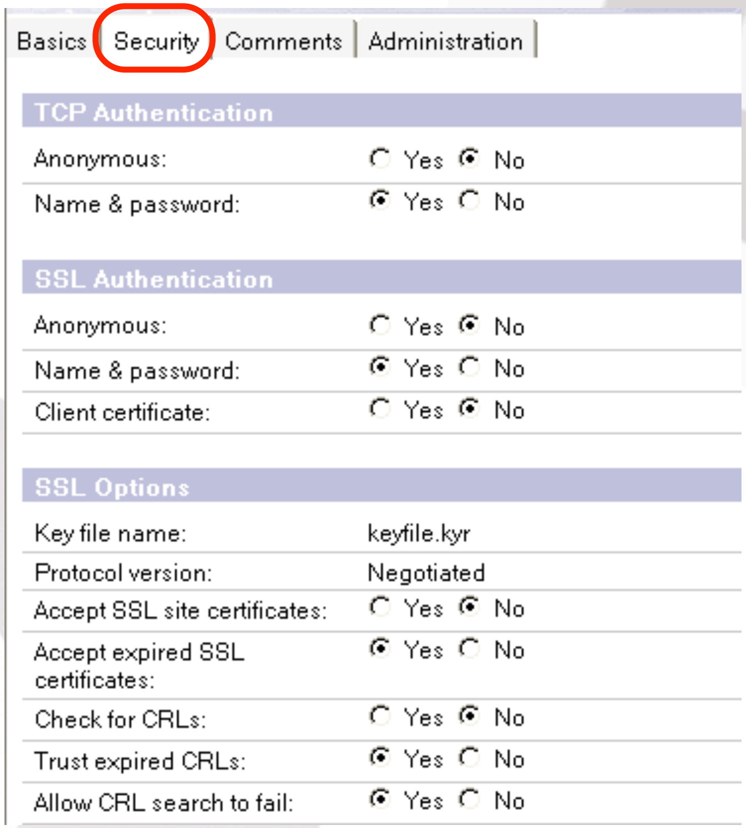
LDAP Configuration

Anonymous users can query:	**LDAP Attribute Types:**	**Domino Fields:**
	AltFullName	AltFullName
	altServer	altServer
	attributeTypes	attributeTypes
	authorityRevocationList	authorityRevocationList
	c	OfficeCountry

Allow LDAP users write access:	● Yes ○ No
Timeout:	0 seconds
Maximum number of entries returned:	0
Minimum characters for wildcard search:	1
Allow Alternate Language Information processing:	○ Yes ● No
Rules to follow when this directory is the primary directory, and there are multiple matches on the distinguished name being compared/modified:	○ Don't modify any ● Modify first match ○ Modify all matches
Automatically Full Text Index Domino Directory?	● Yes ○ No
Enforce schema?	● Yes ○ No
DN Required on Bind?	○ Yes ● No
Encode results in UTF8 for LDAPv2 clients?	● Yes ○ No
Maximum number of referrals:	1
Activity Logging truncation size:	4096
Allow dereferencing of aliases on search requests?	○ Yes ● No

Domino - Enabling LDAP

- Server Document
  - Internet Protocols



TCP Authentication

Anonymous:	○ Yes ● No
Name & password:	● Yes ○ No

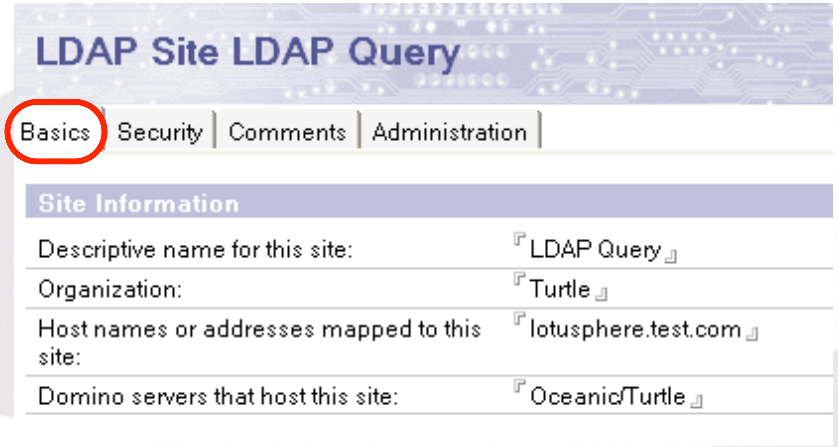
SSL Authentication

Anonymous:	○ Yes ● No
Name & password:	● Yes ○ No
Client certificate:	○ Yes ● No

SSL Options

Key file name:	keyfile.kyr
Protocol version:	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No
Check for CRLs:	○ Yes ● No
Trust expired CRLs:	● Yes ○ No
Allow CRL search to fail:	● Yes ○ No

- Internet Site Document



LDAP Site LDAP Query

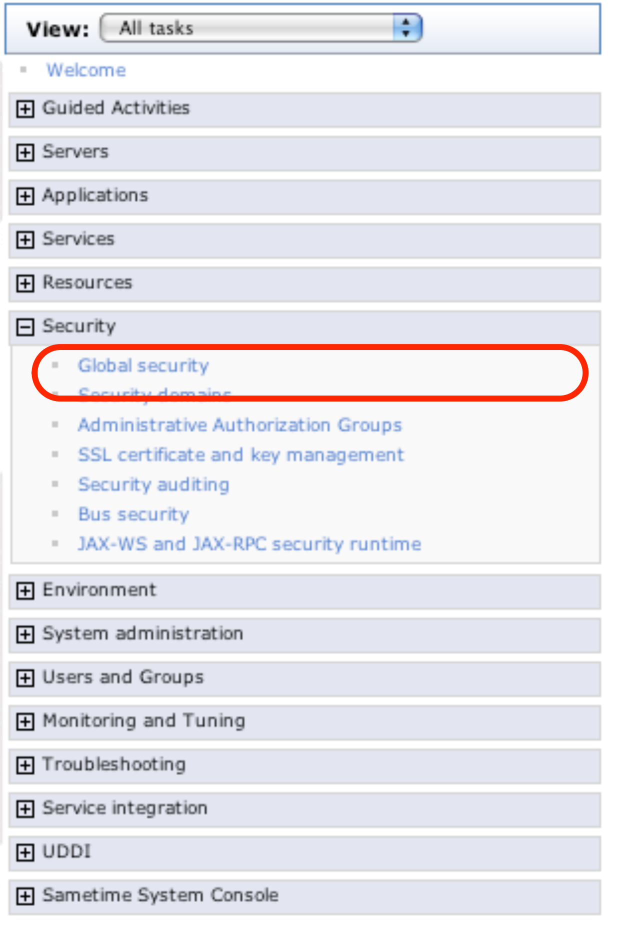
Site Information

Descriptive name for this site:	LDAP Query
Organization:	Turtle
Host names or addresses mapped to this site:	lotusphere.test.com
Domino servers that host this site:	Oceanic/Turtle

- Load LDAP

WAS - Configuring LDAP for Authentication

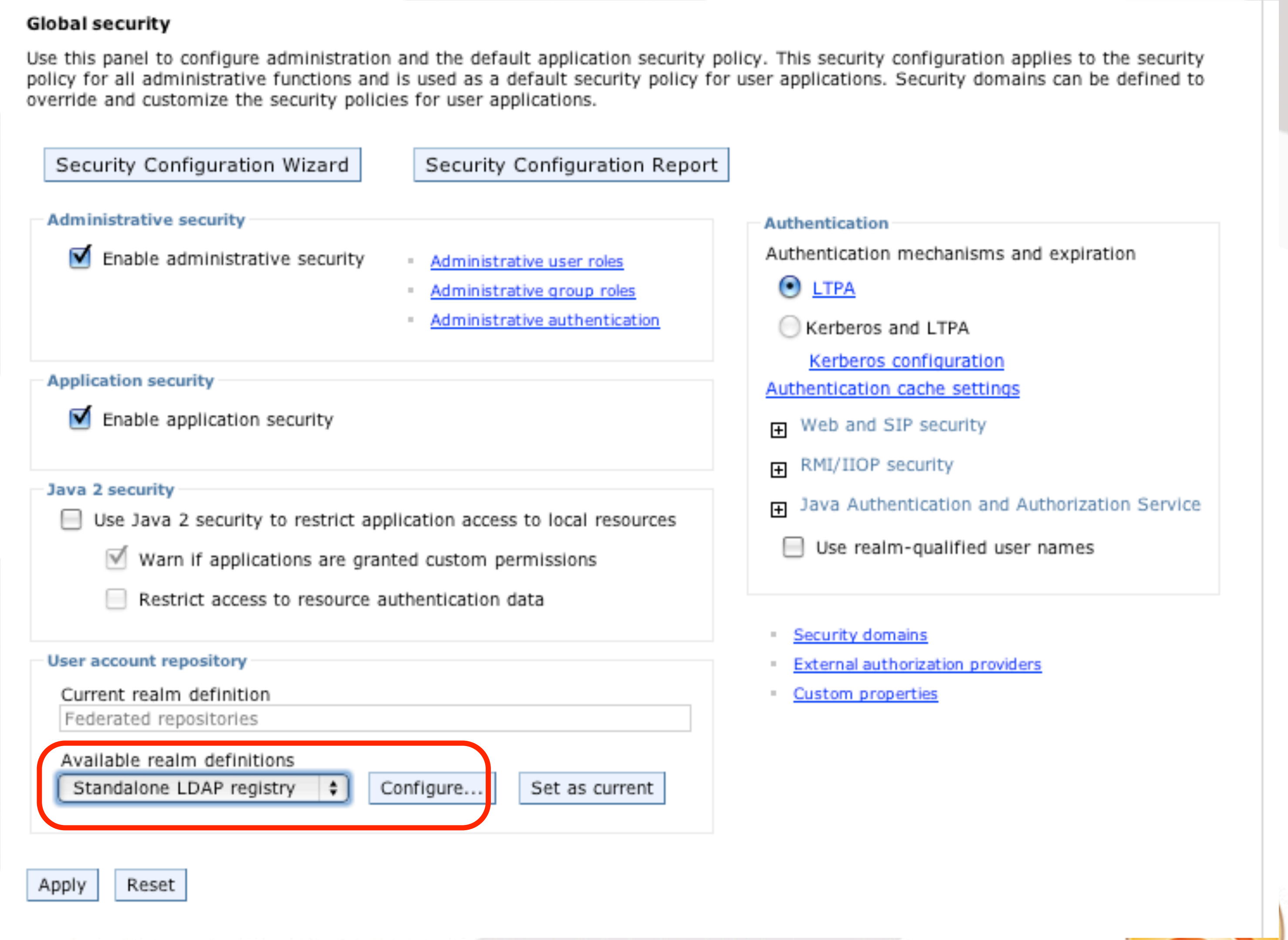
- Security - Global Security



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
- ⊞ Environment
- ⊞ System administration
- ⊞ Users and Groups
- ⊞ Monitoring and Tuning
- ⊞ Troubleshooting
- ⊞ Service integration
- ⊞ UDDI
- ⊞ Sametime System Console

WAS Configuring LDAP For Authentication



Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Current realm definition: Federated repositories

Available realm definitions: Standalone LDAP registry

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

Authentication cache settings

⊞ Web and SIP security

⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

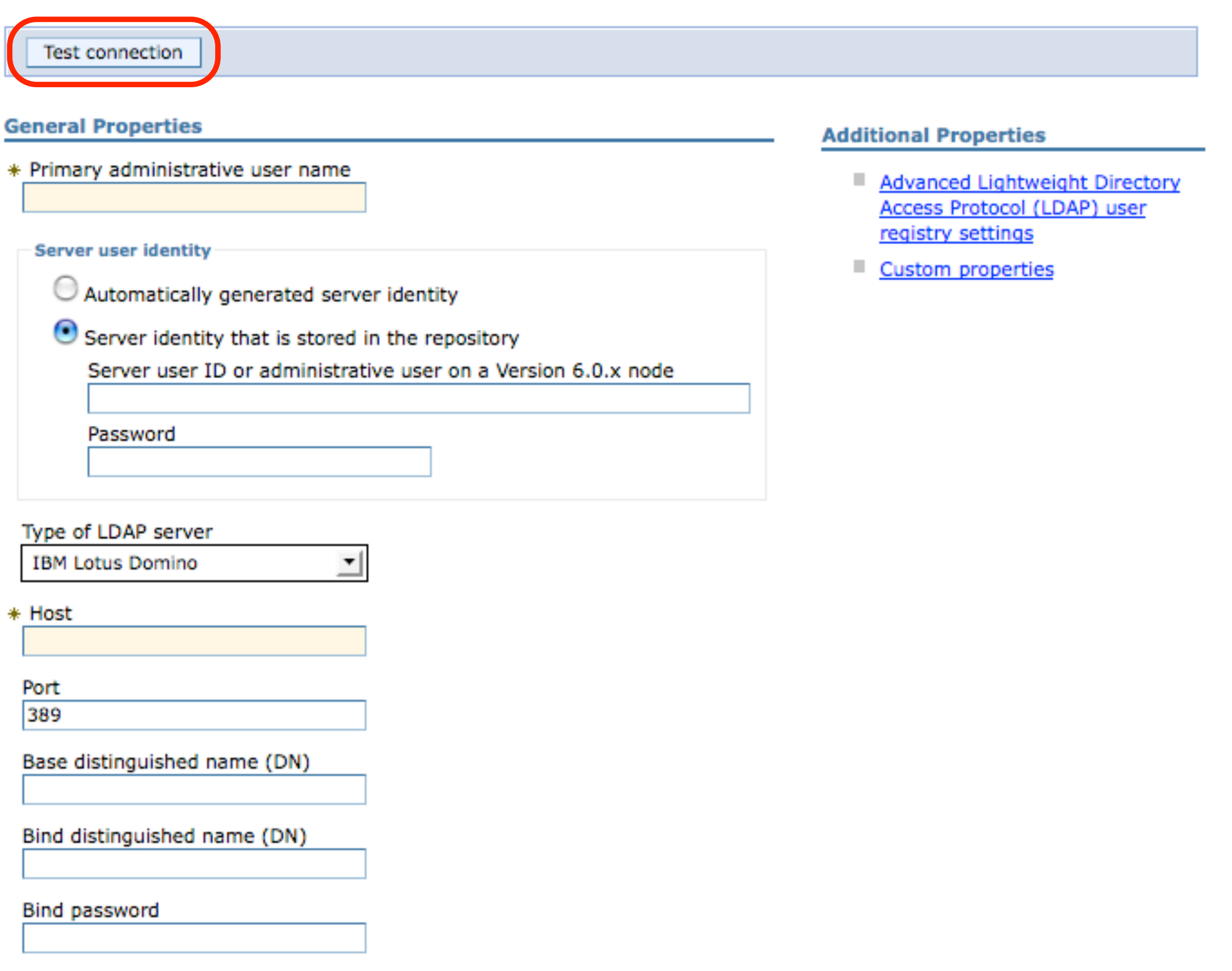
□ Use realm-qualified user names

- Security domains
- External authorization providers
- Custom properties

WAS Configuring LDAP for Authentication

- Configure LDAP server parameters
  - including bind identity
  - base dn
  - port
  - administrative account
  - type of LDAP server
    - IBM Tivoli Directory Server
    - IBM Secureway Directory Server
    - IBM Lotus Domino
    - Microsoft Active Directory
    - Sun One
    - Novell eDirectory
    - Custom

WAS Configuring LDAP for Authentication



General Properties

* Primary administrative user name

Server user identity

○ Automatically generated server identity

● Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

Type of LDAP server

IBM Lotus Domino

* Host

Port

389

Base distinguished name (DN)

Bind distinguished name (DN)

Bind password

Additional Properties

- Advanced Lightweight Directory Access Protocol (LDAP) user registry settings
- Custom properties

Federated Repositories vs LDAP

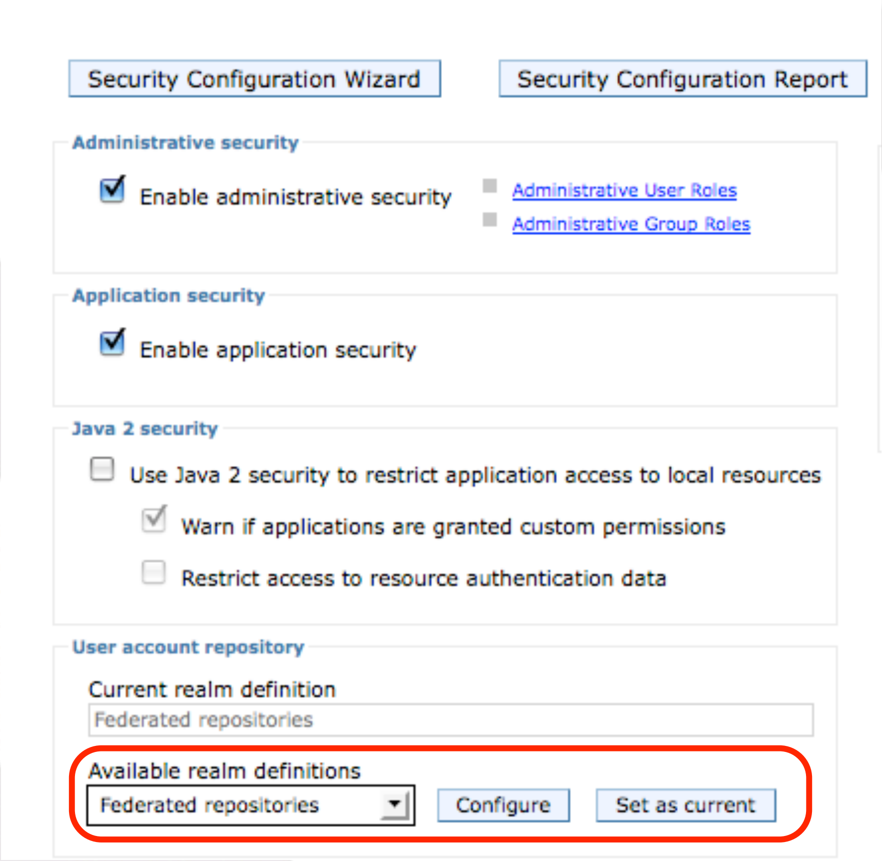
- Allows the use of multiple repositories
  - the file-based user repository
  - external directory repositories
  - a combination of both
- Whichever method you choose for authentication, there can only be one and it runs for all servers
- If you use LDAP you can only have one LDAP directory and can't use the file repository or OS user directory
- Using Federated Repositories is similar to using Directory Assistance, you can have multiple directories that all load as a consolidated user list.

Sametime 8.5

- The configuration of Sametime 8.5 you perform in the Sametime Systems Console section creates a Federated Repository configuration for your LDAP connection here

WAS Using Federated Repositories for Authentication

- Security - Global Security
- Under 'user account repository' choose 'Federated repositories'
  - then 'configure'



Security Configuration Wizard
Security Configuration Report

Administrative security

☑ Enable administrative security

Administrative User Roles
Administrative Group Roles

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

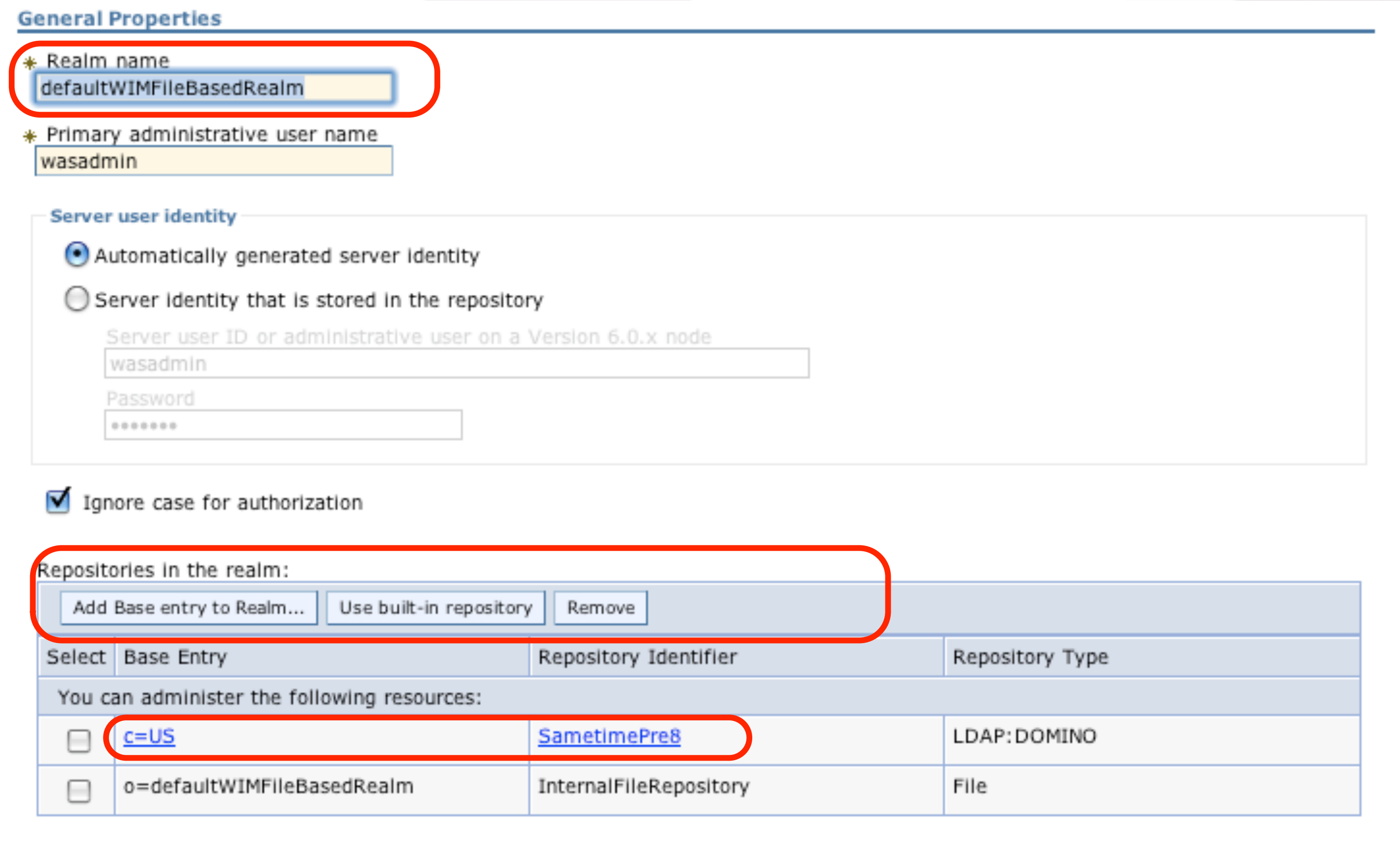
□ Restrict access to resource authentication data

User account repository

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

WAS Using Federated Repositories for Authentication



General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
wasadmin

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node
wasadmin

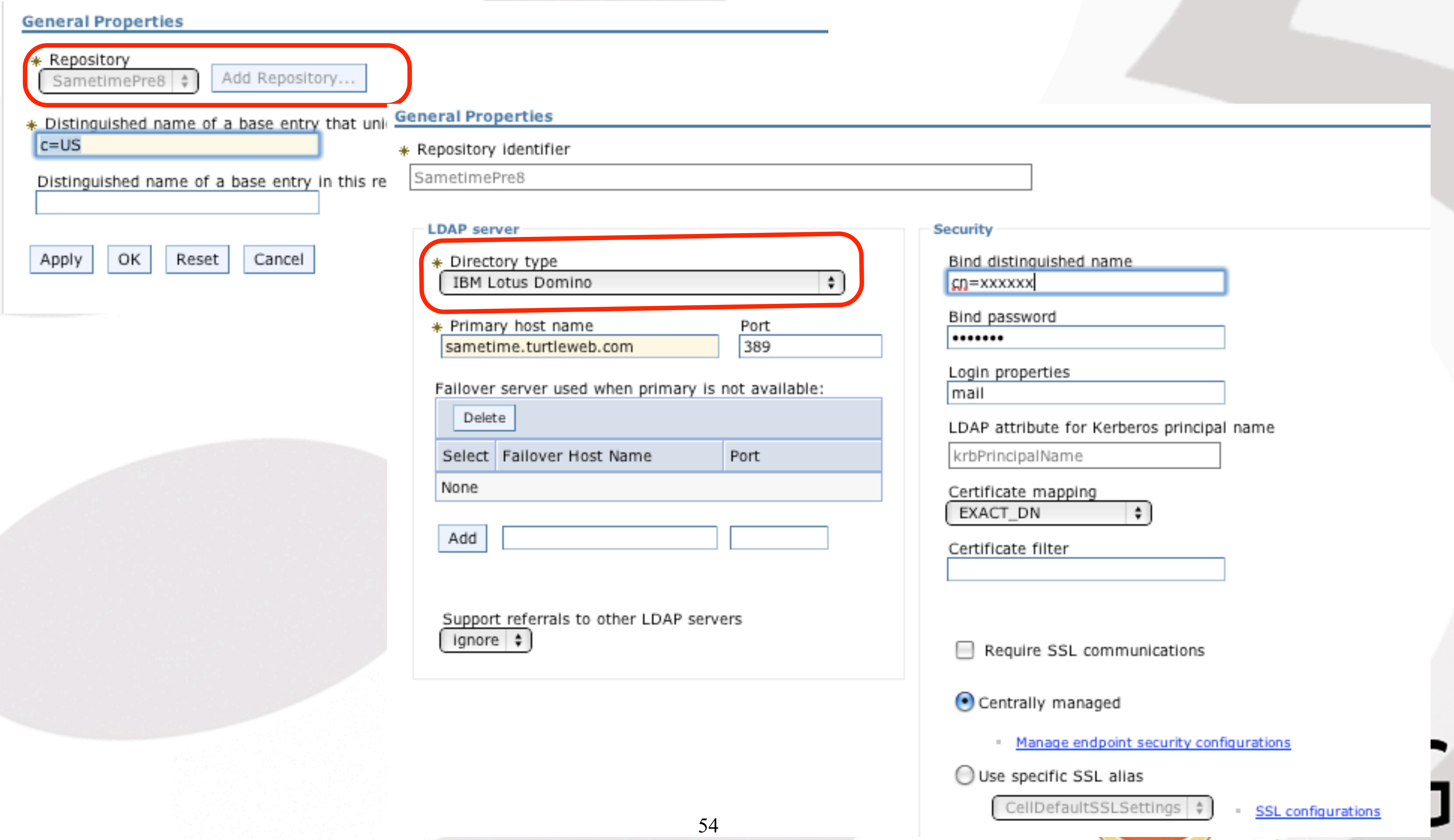
Password
•••••••

☑ Ignore case for authorization

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	c=US	SametimePre8	LDAP:DOMINO
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File

WAS Using Federated Repositories for Authentication



General Properties

* Repository
SametimePre8

* Distinguished name of a base entry that uni
c=US

Distinguished name of a base entry in this re

General Properties

* Repository identifier
SametimePre8

LDAP server

* Directory type
IBM Lotus Domino

* Primary host name
sametime.turtleweb.com

Port
389

Failover server used when primary is not available:

Select	Failover Host Name	Port
None		

Support referrals to other LDAP servers
ignore

Security

Bind distinguished name
cn=xxxxxx

Bind password
•••••••

Login properties
mail

LDAP attribute for Kerberos principal name
krbPrincipalName

Certificate mapping
EXACT_DN

Certificate filter

□ Require SSL communications

● Centrally managed

- Manage endpoint security configurations

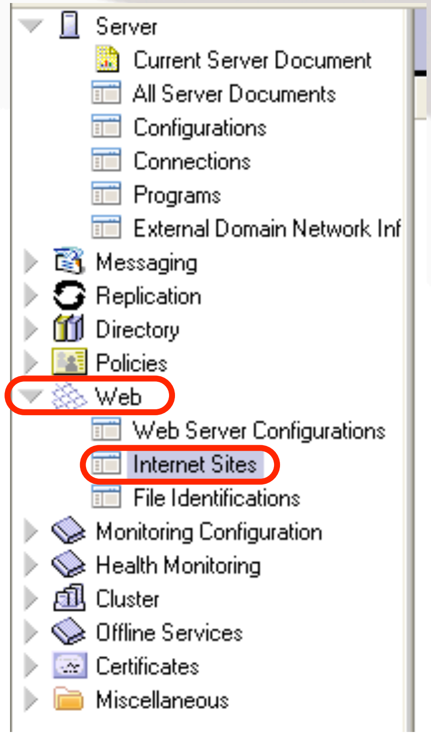
○ Use specific SSL alias

CellDefaultSSLSettings

- SSL configurations

Domino Configuring SSO

- Launch Domino Administrator
  - Click on the Configuration tab
  - Choose “Internet Sites” under “Web”
    - even if you’re not using ‘Internet Site Documents’ in your server configuration

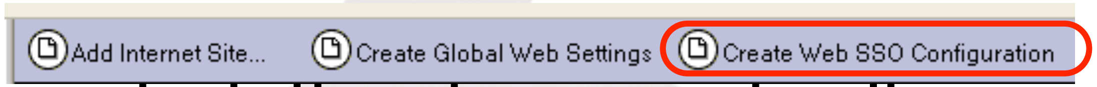


- Server
  - Current Server Document
  - All Server Documents
  - Configurations
  - Connections
  - Programs
  - External Domain Network Inf
- Messaging
- Replication
- Directory
- Policies
- Web
  - Web Server Configurations
  - Internet Sites
  - File Identifications
- Monitoring Configuration
- Health Monitoring
- Cluster
- Offline Services
- Certificates
- Miscellaneous

BLUG
Belux Lotus User Group

Domino Configuring SSO

- Select “Create Web SSO Configuration” from Action tab

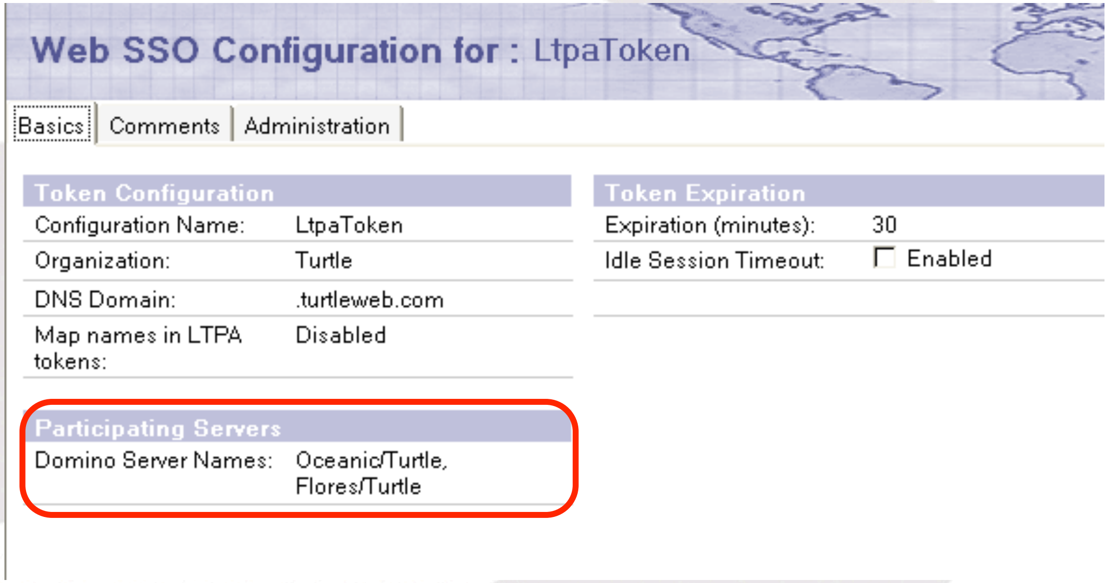


- Once created, the document will appear in the view as
  - Web SSO Configuration: <TokenName>

- DNS domain must be the same for all servers involved in SSO

Domino Configuring SSO

- Default configuration name is LTPAToken
  - leave this name in place if you can
- The document is encrypted for use only by certain servers and users
  - with the public keys of the servers listed under Domino server names
  - with the public keys of the Administrators listed on the Administration tab
- When saving the SSO configuration, the server documents for servers you have chosen must be present in the directory you're working in



Web SSO Configuration for : LtpaToken

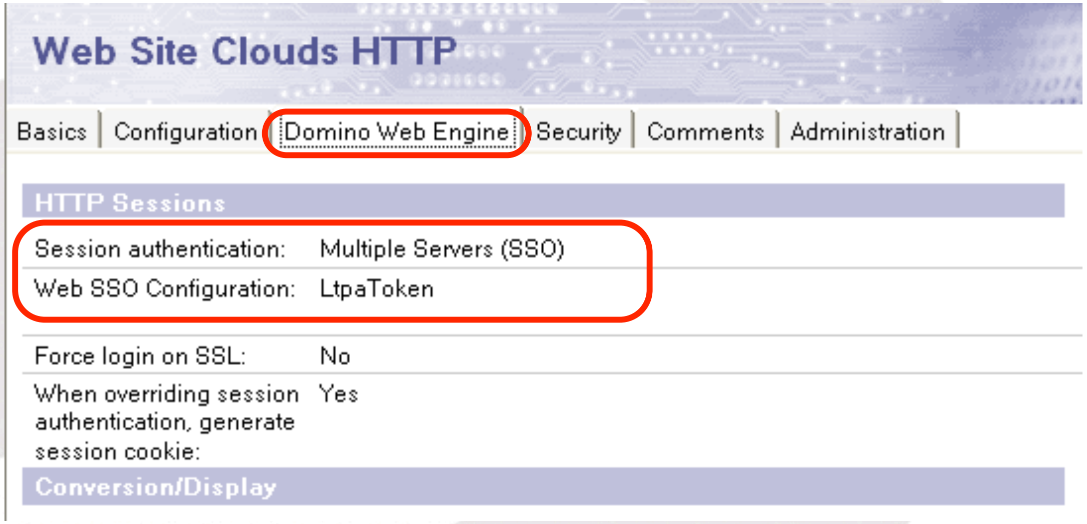
Token Configuration	
Configuration Name:	LtpaToken
Organization:	Turtle
DNS Domain:	.turtleweb.com
Map names in LTPA tokens:	Disabled

Token Expiration	
Expiration (minutes):	30
Idle Session Timeout:	□ Enabled

Participating Servers	
Domino Server Names:	Oceanic/Turtle, Flores/Turtle

Domino Configuring SSO

- Edit the Server Document, OR...
- Edit the Web Site document (if using Internet Site documents)
- Choose ‘Multiple Servers (SSO)’ under Domino Web Engine
- Choose the SSO token name under Web SSO Configuration
  - If yours isn’t available to select then ensure it is created in this directory and that it is encrypted for the server you are assigning it to



Session authentication: Multiple Servers (SSO)

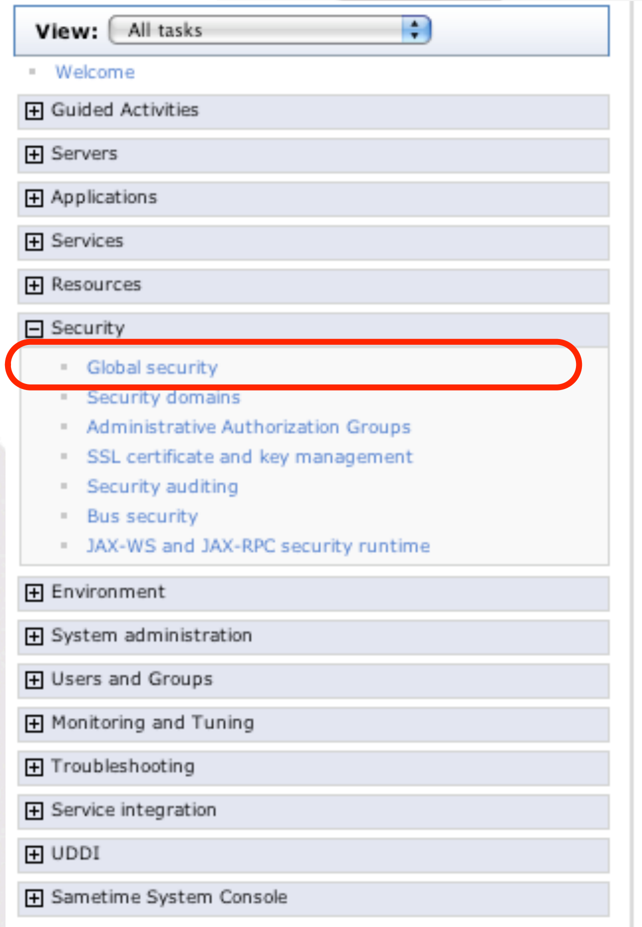
Web SSO Configuration: LtpaToken

Force login on SSL: No

When overriding session authentication, generate session cookie: Yes

Websphere Configuring SSO

- The token is usually originated and exported from Websphere for sharing with Domino
- When SSO is enabled, a cookie is created and passed in the HTTP header to other servers that share the same domain
- Security - Global Security

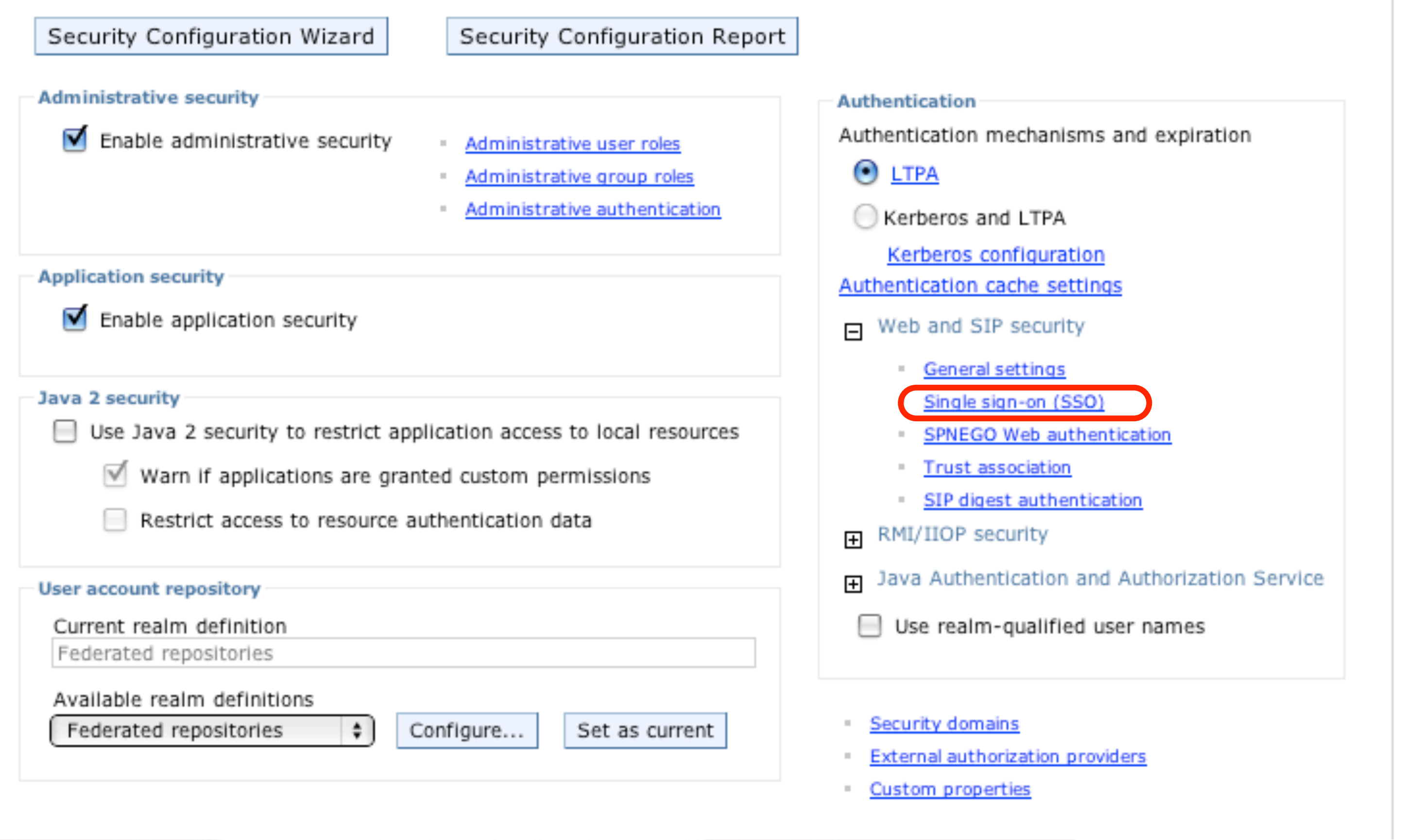


View: All tasks

- 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
- ⊞ Environment
- ⊞ System administration
- ⊞ Users and Groups
- ⊞ Monitoring and Tuning
- ⊞ Troubleshooting
- ⊞ Service integration
- ⊞ UDDI
- ⊞ Sametime System Console

Websphere Configuring SSO

- Single sign-on (SSO) under 'Web Security'



Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

Authentication cache settings

⊟ Web and SIP security

- General settings
- Single sign-on (SSO)
- SPNEGO Web authentication
- Trust association
- SIP digest authentication

⊞ RMI/IIOP security

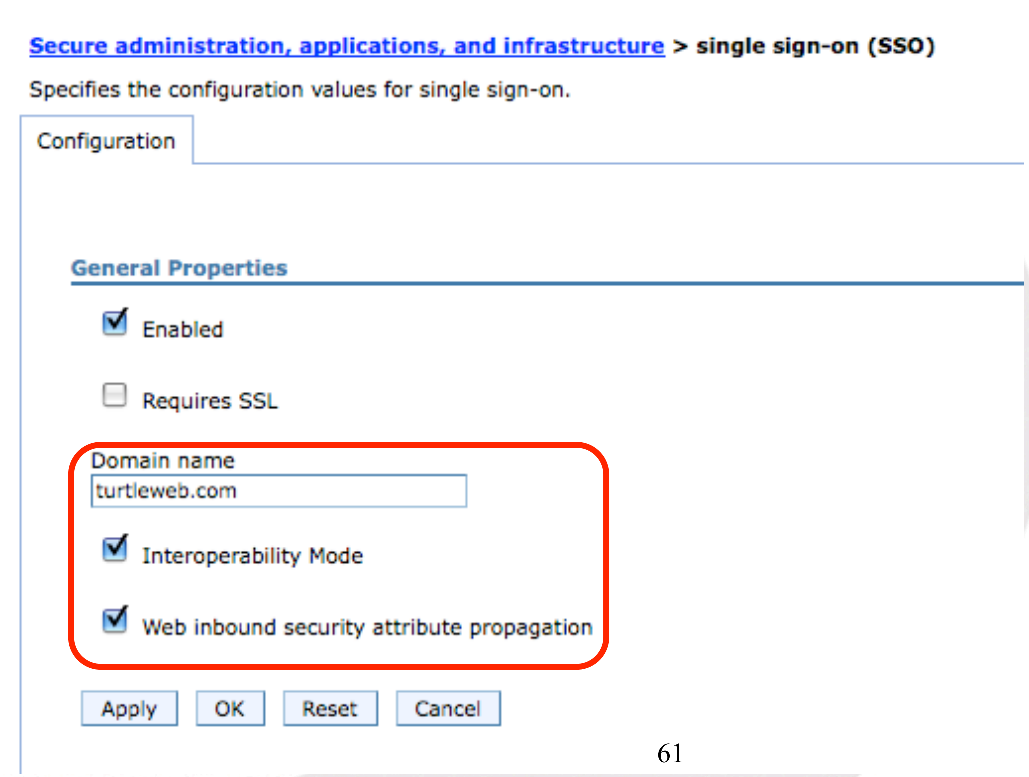
⊞ Java Authentication and Authorization Service

□ Use realm-qualified user names

- Security domains
- External authorization providers
- Custom properties

Websphere Configuring SSO

- Interoperability mode issues LTPAToken
- Web inbound security attribute propagation issues LTPAToken2
  - LTPAToken is for working with pre 5.1 versions of Websphere



Secure administration, applications, and infrastructure > **single sign-on (SSO)**

Specifies the configuration values for single sign-on.

Configuration

General Properties

☑ Enabled

□ Requires SSL

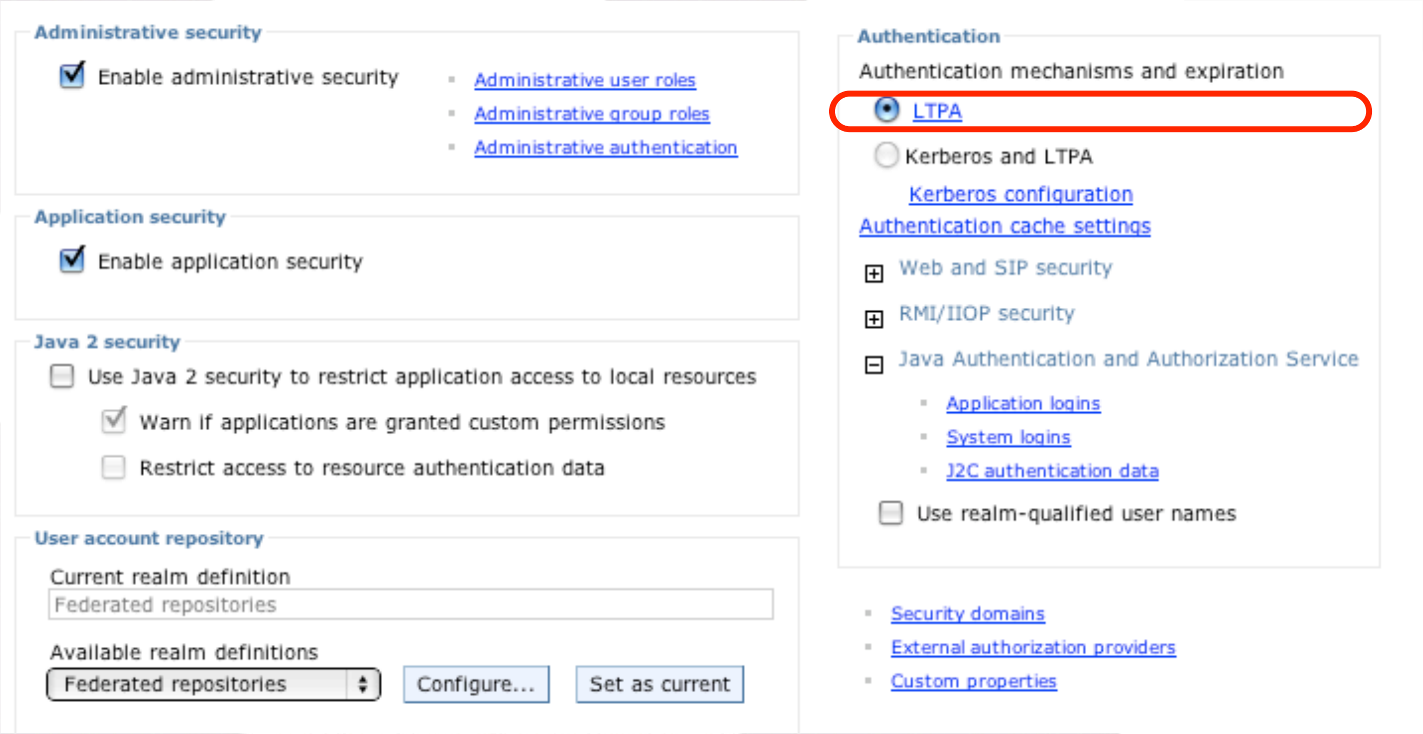
Domain name
turtleweb.com

☑ Interoperability Mode

☑ Web inbound security attribute propagation

Websphere Exporting a SSO Key

- If you want to enable SSO with another server such as Domino, you'll need to generate then export a key to share
  - LTPA



Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

Authentication cache settings

⊞ Web and SIP security

⊞ RMI/IIOP security

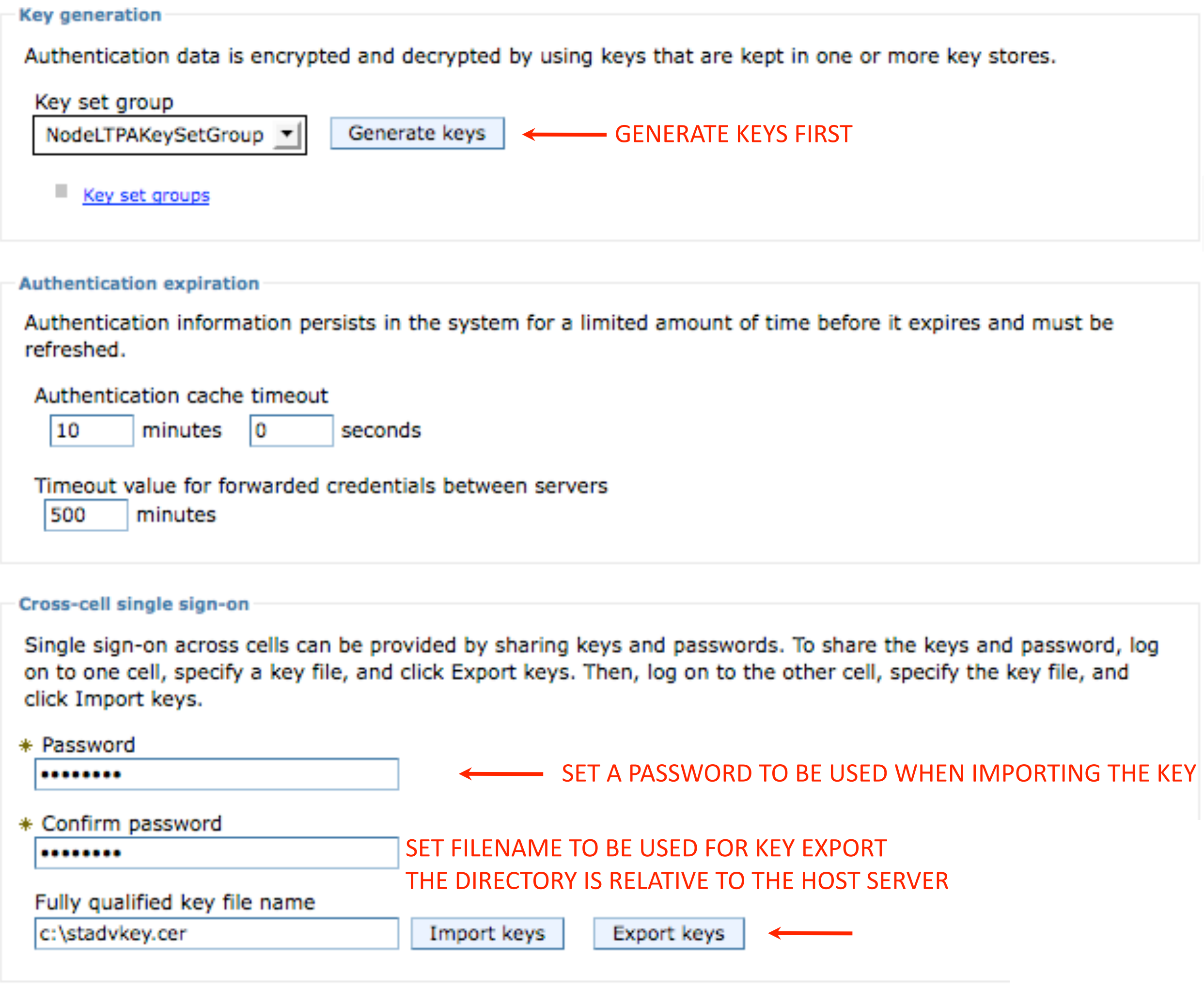
⊟ Java Authentication and Authorization Service

- Application logins
- System logins
- J2C authentication data

□ Use realm-qualified user names

- Security domains
- External authorization providers
- Custom properties

Websphere Generating a SSO Key



Key generation

Authentication data is encrypted and decrypted by using keys that are kept in one or more key stores.

Key set group

NodeLTPAKeySetGroup ▼ Generate keys

GENERATE KEYS FIRST

- Key set groups

Authentication expiration

Authentication information persists in the system for a limited amount of time before it expires and must be refreshed.

Authentication cache timeout

10 minutes 0 seconds

Timeout value for forwarded credentials between servers

500 minutes

Cross-cell single sign-on

Single sign-on across cells can be provided by sharing keys and passwords. To share the keys and password, log on to one cell, specify a key file, and click Export keys. Then, log on to the other cell, specify the key file, and click Import keys.

* Password

••••••••

SET A PASSWORD TO BE USED WHEN IMPORTING THE KEY

* Confirm password

••••••••

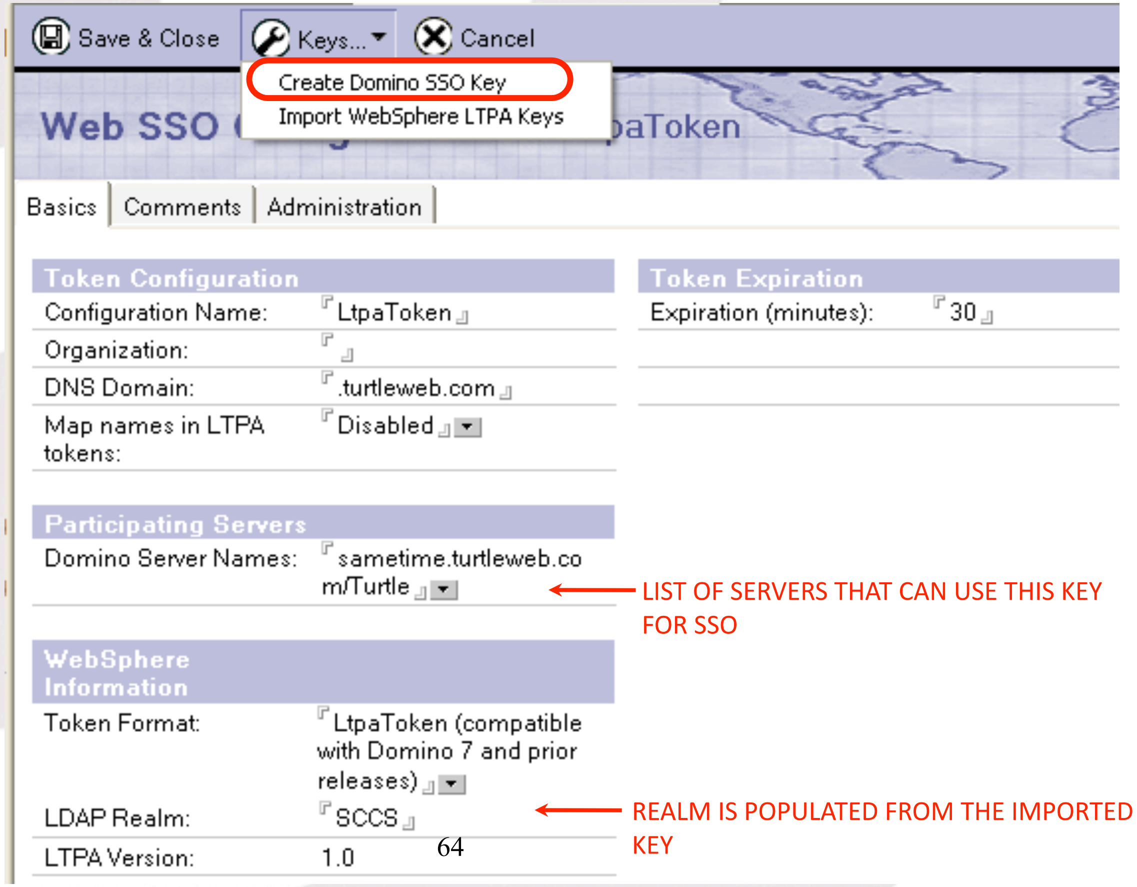
SET FILENAME TO BE USED FOR KEY EXPORT
THE DIRECTORY IS RELATIVE TO THE HOST SERVER

Fully qualified key file name

c:\stadvkey.cer Import keys Export keys

Domino & Websphere SSO

- Create the Domino Web SSO Configuration
  - Don't modify an existing Domino-only one, delete that and create a new one
- Keys - Import Websphere LTPA Key
  - Use the file you have exported



Token Configuration

Configuration Name: LtpaToken

Organization:

DNS Domain: .turtleweb.com

Map names in LTPA tokens: Disabled

Token Expiration

Expiration (minutes): 30

Participating Servers

Domino Server Names: sametime.turtleweb.com/Turtle

WebSphere Information

Token Format: LtpaToken (compatible with Domino 7 and prior releases)

LDAP Realm: SCCS

LTPA Version: 1.0

LIST OF SERVERS THAT CAN USE THIS KEY FOR SSO

REALM IS POPULATED FROM THE IMPORTED KEY

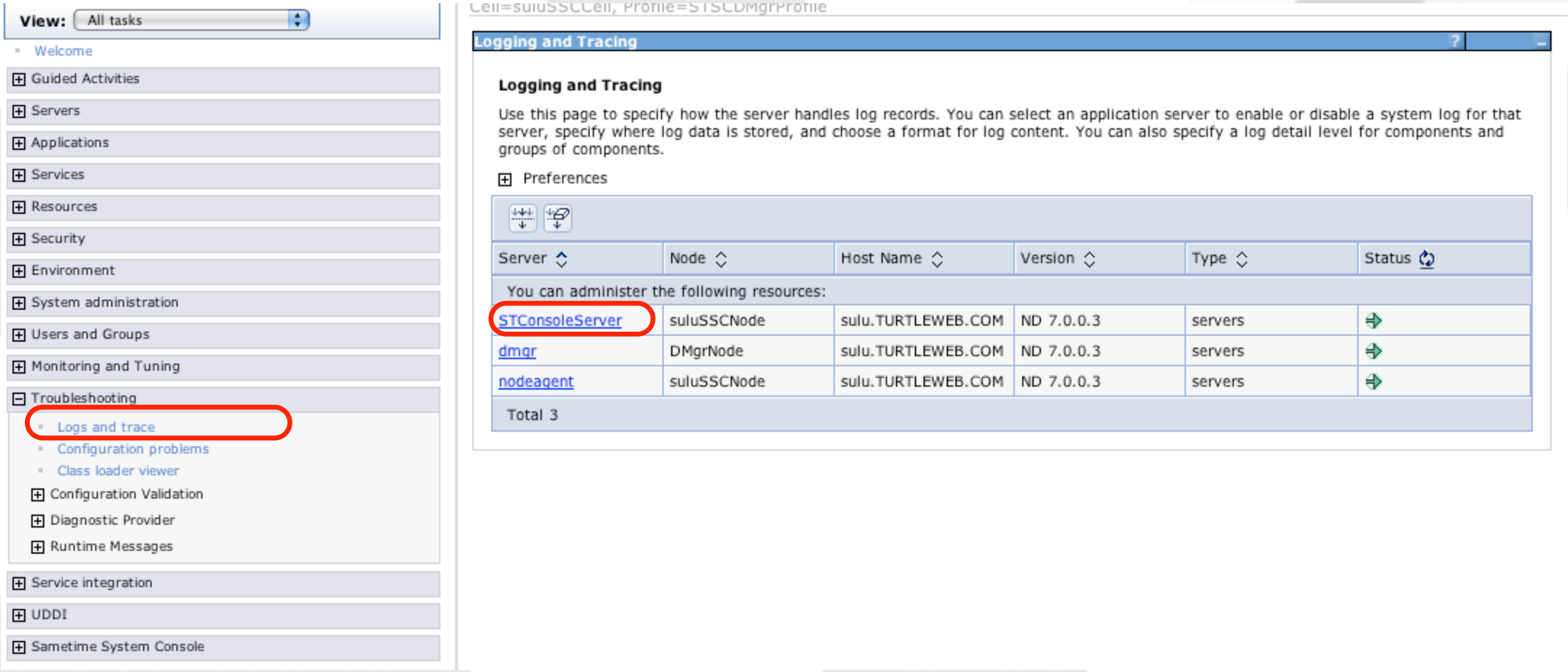
Domino Troubleshooting

- Where do you look if the server:
  - Won’t start
  - Suddenly stops
  - Is behaving oddly / slowly
- Log.nsf
- Console.log
- NSDs
- Domino Domain Monitoring
- Domino Configuration Tuner

Websphere Troubleshooting

- Log files created on file system for each server instance
- <websphereprogramdir>\profiles\<yourprofile>\logs \<serverinstance>
  - startserver.log
  - stopserver.log
  - systemout.log
  - systemerr.log
  - The logs for the Meeting Server itself are in
    - c:\ibm\webspherebeta\appserver\profiles \<servername>MeetingPNProfile1\logs\STMeetingServer
- Configuring additional trace output can be done via Integrated Solutions Console

Websphere Troubleshooting



Cell=suluSSCCell, Profile=STSCDMgrProfile

Logging and Tracing

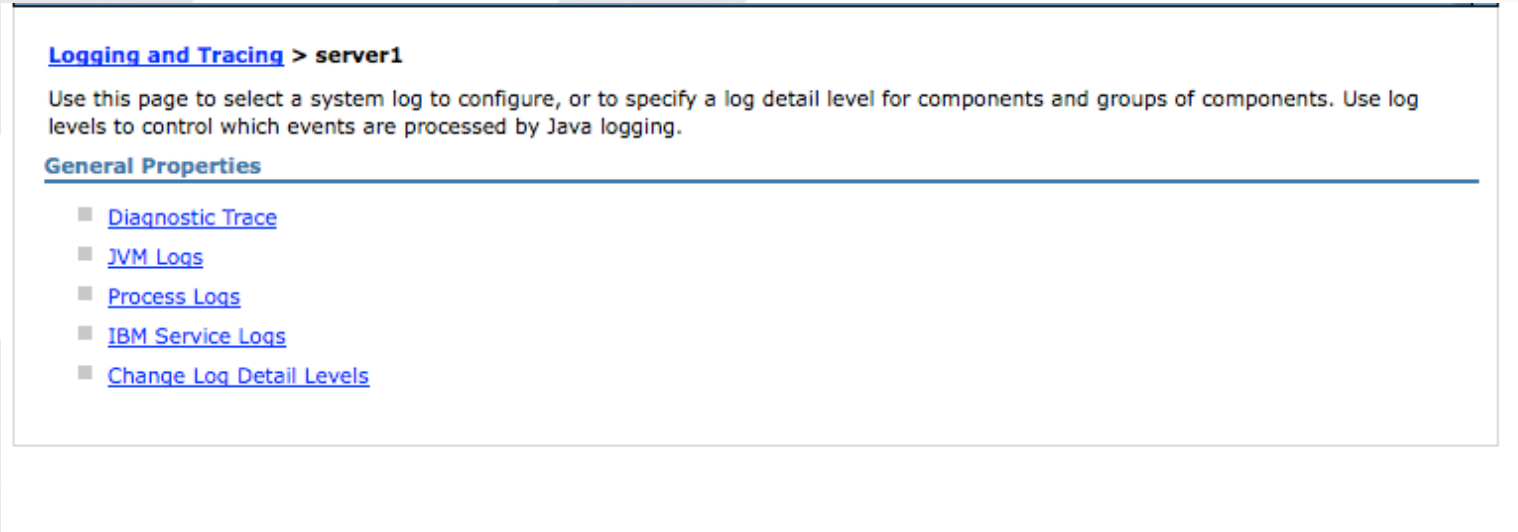
Logging and Tracing

Use this page to specify how the server handles log records. You can select an application server to enable or disable a system log for that server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Server	Node	Host Name	Version	Type	Status
You can administer the following resources:					
STConsoleServer	suluSSCNode	sulu.TURTLEWEB.COM	ND 7.0.0.3	servers	➜
dmgr	DMgrNode	sulu.TURTLEWEB.COM	ND 7.0.0.3	servers	➜
nodeagent	suluSSCNode	sulu.TURTLEWEB.COM	ND 7.0.0.3	servers	➜
Total 3					

Websphere Troubleshooting

- Select the server whose logs you want to view
- Select the type of log to configure or view



Logging and Tracing > server1

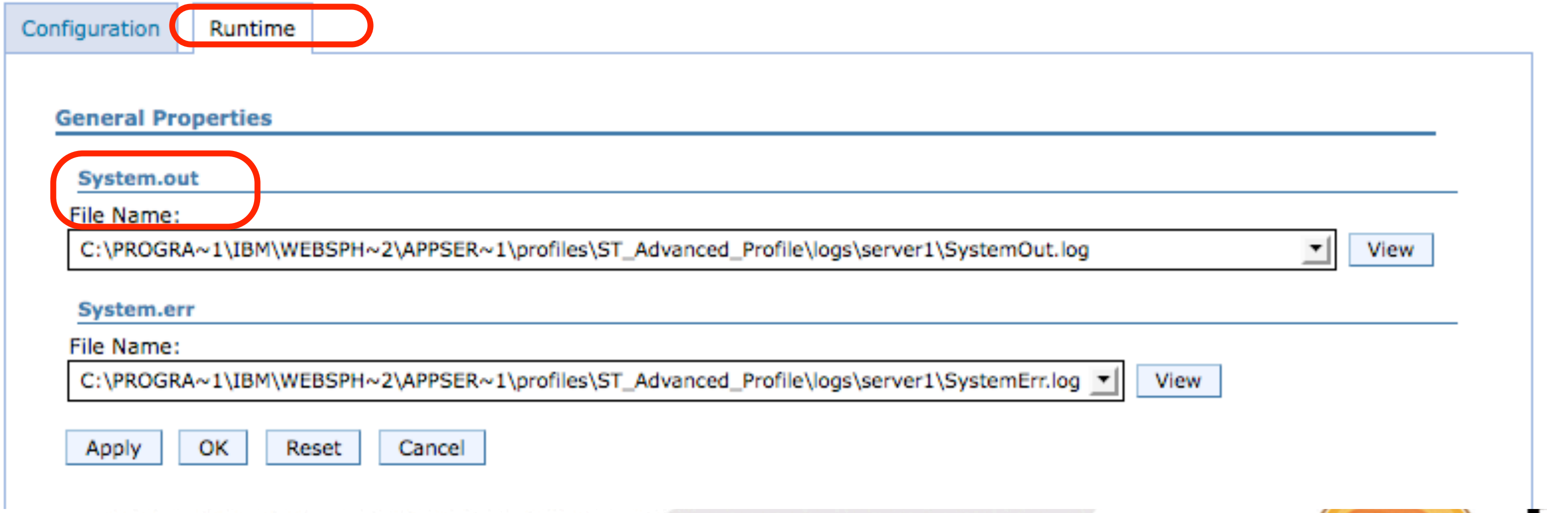
Use this page to select a system log to configure, or to specify a log detail level for components and groups of components. Use log levels to control which events are processed by Java logging.

General Properties

- Diagnostic Trace
- JVM Logs
- Process Logs
- IBM Service Logs
- Change Log Detail Levels

Websphere Troubleshooting

- Each log configuration screen also shows you where the relevant logs are located
- Changes to ‘Configuration’ requires a server restart
- Changes to ‘Runtime’ happen live
  - JVM Logs

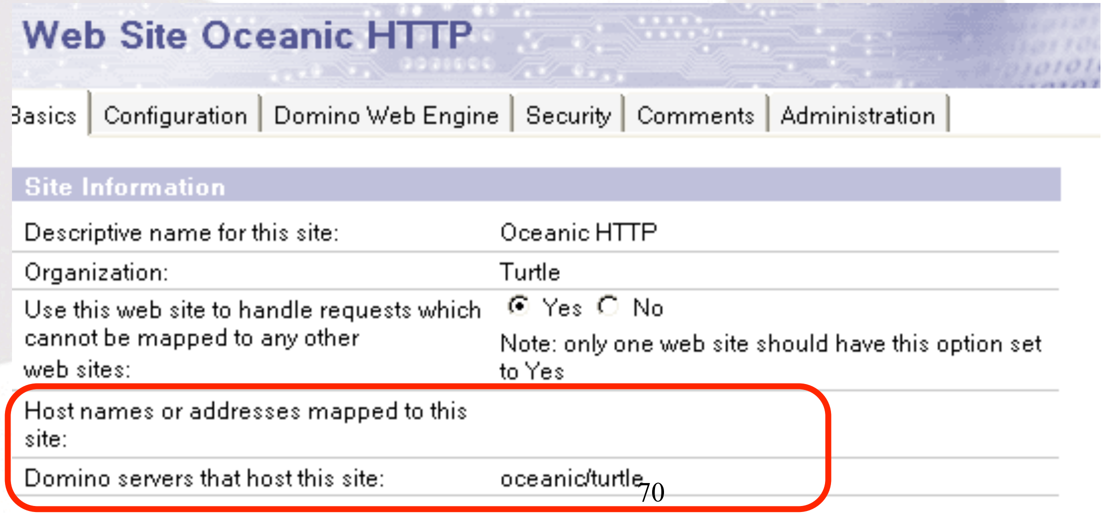


File Name: C:\PROGRA~1\IBM\WEBSPH~2\APPSER~1\profiles\ST_Advanced_Profile\logs\server1\SystemOut.log

File Name: C:\PROGRA~1\IBM\WEBSPH~2\APPSER~1\profiles\ST_Advanced_Profile\logs\server1\SystemErr.log

Domino HTTP & Virtual Hosts

- If using Internet Site Documents
  - HTTP Internet Site Documents
    - applies to which hostnames or ips
    - security access
    - port configuration
    - SSO configuration



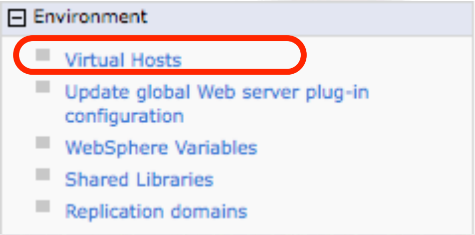
Web Site Oceanic HTTP

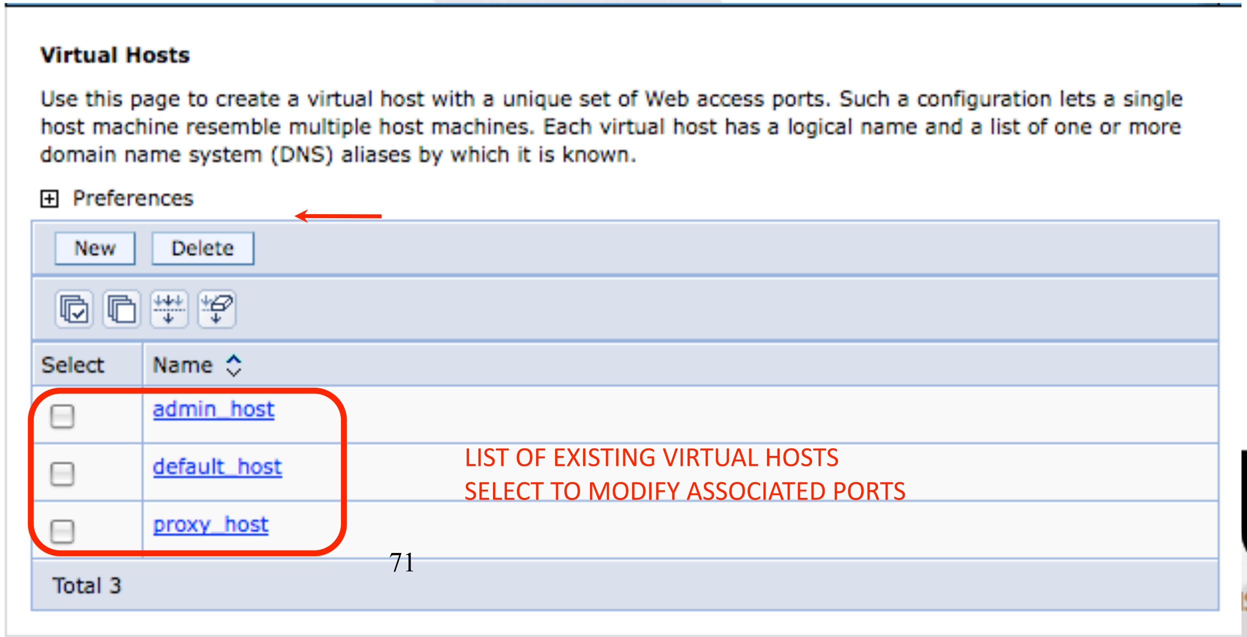
Site Information

Descriptive name for this site:	Oceanic HTTP
Organization:	Turtle
Use this web site to handle requests which cannot be mapped to any other web sites:	● Yes ○ No Note: only one web site should have this option set to Yes
Host names or addresses mapped to this site:	
Domino servers that host this site:	oceanic/turtle

Websphere HTTP & Virtual Hosts

- HTTP Configured through IBM HTTP Server (IHS)
  - Or other front end web server
- Virtual hosts configured in Integrated Solutions Console
  - For the Application Server it allows different ports to be isolated for different sites
  - Environment - Virtual Hosts





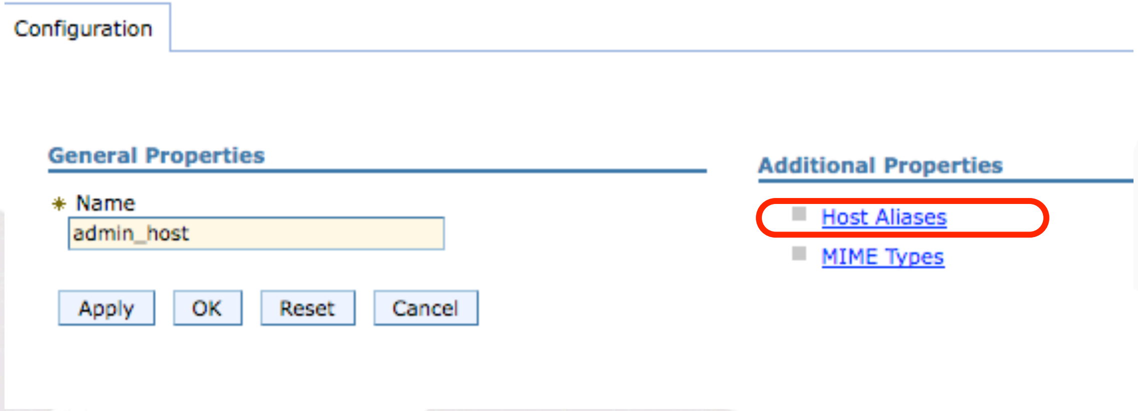
Virtual Hosts

Use this page to create a virtual host with a unique set of Web access ports. Such a configuration lets a single host machine resemble multiple host machines. Each virtual host has a logical name and a list of one or more domain name system (DNS) aliases by which it is known.

Select	Name ⇕
□	admin_host
□	default_host
□	proxy_host
Total 3	

LIST OF EXISTING VIRTUAL HOSTS
SELECT TO MODIFY ASSOCIATED PORTS

Websphere HTTP & Virtual Hosts



Configuration

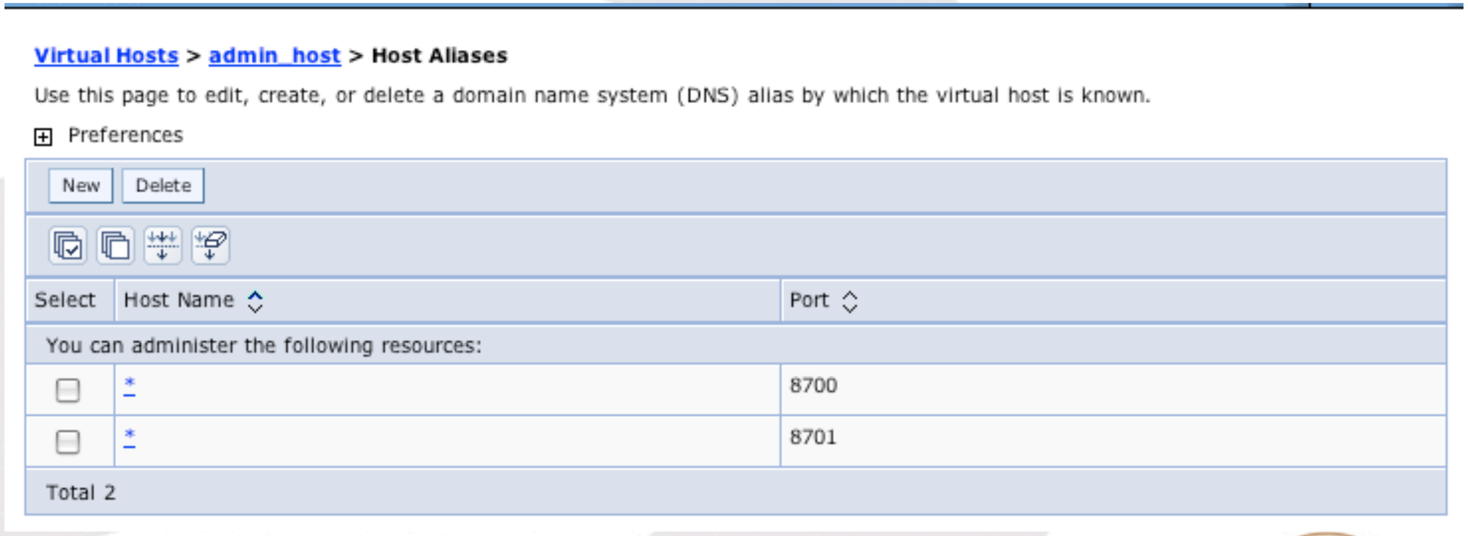
General Properties

* Name

admin_host

Additional Properties

- Host Aliases
- MIME Types



Virtual Hosts > admin_host > Host Aliases

Use this page to edit, create, or delete a domain name system (DNS) alias by which the virtual host is known.

⊞ Preferences

Select	Host Name	Port
You can administer the following resources:		
□	*	8700
□	*	8701
Total 2		

Websphere HTTP & Virtual Hosts

- Can be configured at several levels
  - Environment applies to the entire WAS server
  - Servers - Web Servers applies to all applications managed by that web server
  - Enterprise Applications applies just to that application

Other Websphere stuff worth knowing about

- Network Deployment
  - Websphere can be deployed via Network Deployment whereby a central Websphere server handles the configuration of multiple nodes and distributes them to different hardware
  - This is only useful is all your nodes are using the same version of Websphere
  - This can’t be used for managing the infrastructure of several Lotus products if each currently uses a different version of Websphere
- Clustering and Disaster Recovery
- Upgrading - and when not to!

Contact Details

- Gabriella Davis
- gabriella@turtlepartnership.com
- http://blog.turtleweb.com
- Gabriella Davis on Skype, LotusLive etc
- Nerd Girl Community on LinkedIn