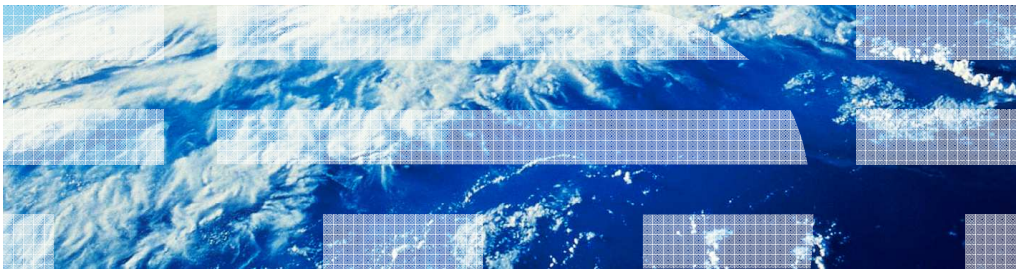
IBM WebSphere Application Server V8

Federated repository support for multiple security domains



WebSphere software

This presentation describes federated repository support for multiple security domains in IBM WebSphere Application Server V8. The “federated repository” feature is also known as “virtual member manager” or VMM.

Table of contents

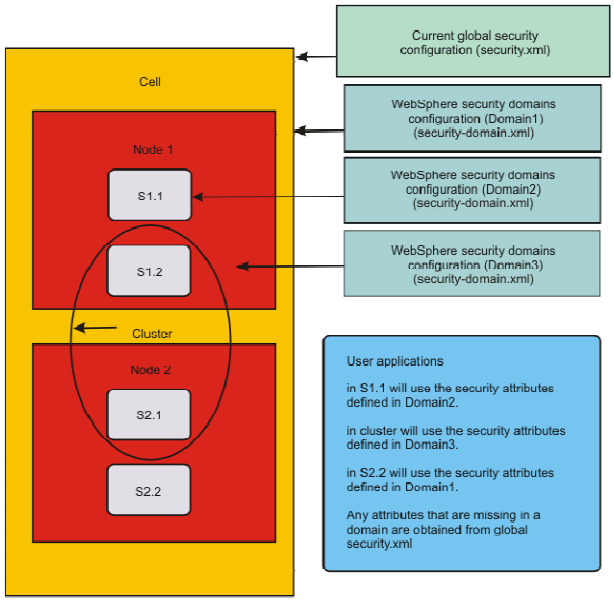
This presentation describes Virtual Member Manager (VMM) enhancements to support Multiple Security Domains in IBM WebSphere Application Server V8.

It describes how VMM was modified to support multiple instances within a server. The presentation will discuss how the VMM configuration, data model, and EJBs look like in this environment, and how it works in a flexible management environment.

It also describes the new management rights added to allow a non-WebSphere Administrator access the VMM APIs.

The new “change password” wsadmin command and enhancements to property extension, entry mapping and database repositories setup and configuration will also be described.

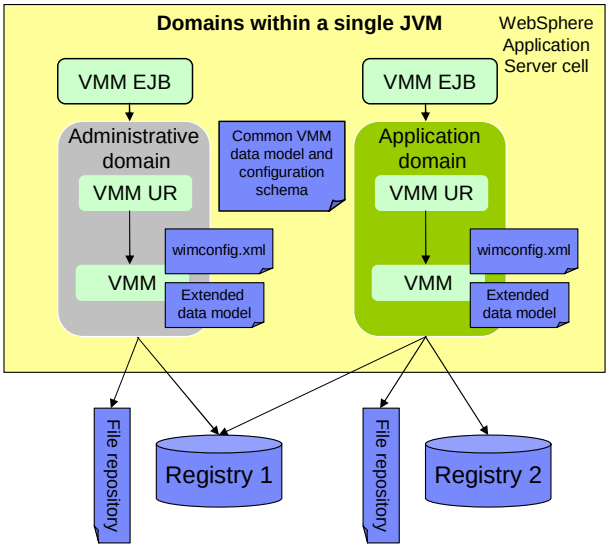
Multiple security domains overview



Federated repository support for multiple security domains

Support for multiple security domains was introduced in WebSphere Application Server V7, and allows for greater flexibility in configuring security. It separates the security configuration for administration from the security configurations for applications. Login modules, authorization engines, and trust association interceptors can be configured at scopes rather than the cell scope, including servers, clusters, or service integration buses. A global security configuration must still be defined, and any attributes not defined in a security domain are inherited from global security.

Security domain support in VMM 8.0



Federated repository support for multiple security domains

This diagram shows an example of multiple virtual member manager instances with a server: there is one instance per security domain.

Each instance has its own file repository, its own configuration, and can extend the data model for domain-specific schema.

The configuration schema and default data model schema are the same for all instances.

A VMM EJB is required for each domain (if remote access is needed).

User and group management

Federated repository support for multiple security domains

Users and groups can now be managed on a per-domain basis. An optional parameter, “securityDomainName” has been added to management command-line interfaces. The “Manage users” and “Manage groups” links on the left panel will continue to be used to manage profile data for global security. New links have been added to the domain panel in the administrative console to manage profile data for domains.

Section

VMM changes for multiple security domains

This section covers changes in VMM to support multiple security domain.

Overview

- Singletons, schema, configuration, file repository
- New VMM instance per domain
- Admin applications use the default global security of VMM
- Application can use VMM as user registry if defined in corresponding domain
- Domain can be configured to use global security settings

A VMM runtime instance is represented by a set of its internal singleton objects, VMM schema and configuration files, and a default file repository.

In a multi-domain environment, WebSphere Application Server will load a new instance of VMM for each domain if the user registry security attribute is defined as “Federated Repository”. Administrative applications in WebSphere Application Server will continue to use the default global security instance of VMM.

If VMM is not selected as the active user registry, applications can still use VMM as their user registry in that domain.

Usage (1 of 2)

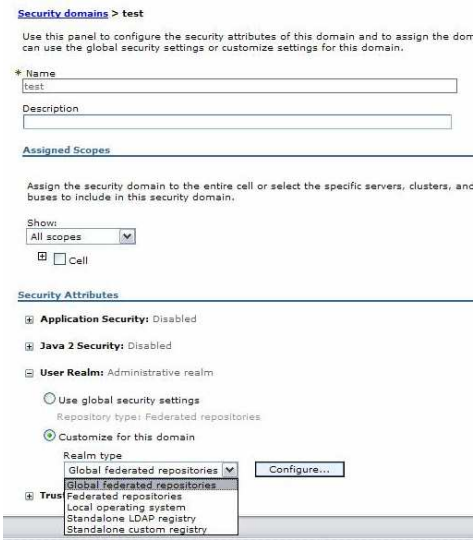
- VMM configuration files created on the fly
  - Whether VMM is configured as active user registry or not
- Unique realm name required for a VMM instance
- Use existing commands with new parameter “securityDomainName ”
- Administrative console can also be used to configure domain specific configuration

During domain creation, all VMM configuration files are created on the fly, whether VMM is configured as active user registry or not. Realm names must be unique.

A VMM instance for an application domain can be configured using existing commands by specifying the “securityDomainName” parameter.

The administrative console can also be used to configure domain-specific configurations.

Usage (2 of 2)



Federated repository support for multiple security domains

You can choose to use the global VMM instance for an application domain by selecting the option “Global Federated Repositories” when customizing the user realm of a security domain.

When the global federated repository option is enabled for a domain, user and group management tasks are performed at administrative domain level only. This means that on the command line, the “securityDomainName” parameter is ignored; and in the administrative console, no separate links are available for managing users and groups from the domain panel.

Highlights

- No interface change
- Singleton domain model
- No change in default data model
- Domain-specific extended profile schema, configuration data and file registry

There are no changes to VMM interfaces. There are VMM singleton objects for a specific security domain. At present, VMM supports the default schema, extended schema, configuration data, and file registry at the cell level. The default data model has not changed. All VMM instances share the same default data model.

With multiple security domain capability, VMM supports configuration data, extended schema and file registry at the domain level.

Migration

- Global security settings are used by default when migrating from a version that does not support multiple security domains

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.migration.nd.doc/info/ae/ae/tmig_migrate_cells_commandline.html

When installations that do not use multiple security domains are migrated to WebSphere Application Server V8, they will use global security settings by default.

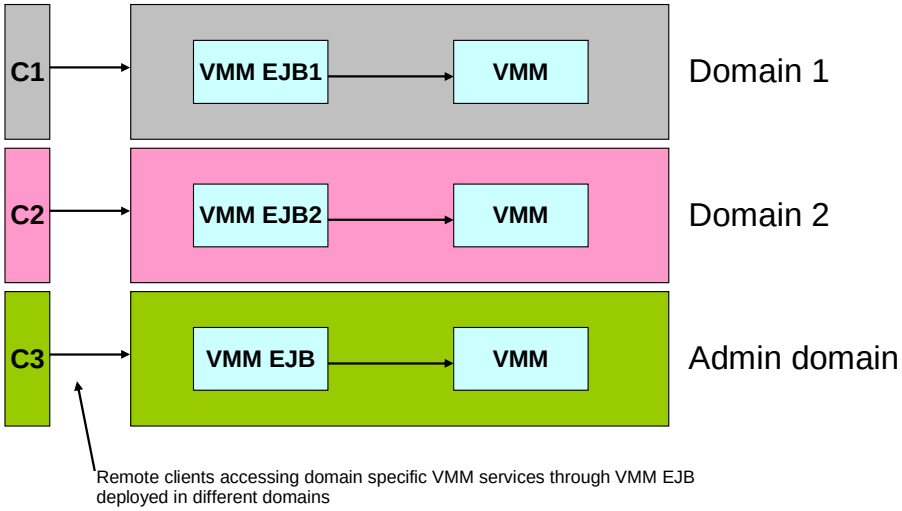
More information on migration is provided in the information center.

Section

EJB support for multiple security domains

This section covers EJB support for multiple security domains.

VMM EJB support



Federated repository support for multiple security domains

VMM can be remotely accessed through the VMM EJB interface. VMM EJB is an administrative application that is a stateless bean that supports all public APIs provided by VMM core service interface APIs. With the support of separate VMM instances in multiple domains, this EJB will not be sufficient to serve multiple domain specific VMM services. In addition to existing system application wim.ear a new wimperdomain.ear is created as a standard application so that the same EJB can be deployed on multiple servers for each domain.

Deploying WIM EJB for a domain

- wimperdomain.ear application deployed on server scoped to domain
- Unique JNDI URL required for the EJB
- Sample command to install WIM as user application:

```
AdminApp.install('C:/wasx/installableApps/wimperdomain.ear', '[-appname
wimperdomain -BindJndiForEJBNonMessageBinding [[ wim.ejb WIMService
wimejb.jar,META-INF/ejb-jar.xml
ejbd2/com/ibm/websphere/wim/ejb/WIMServiceHome]] -MapModulesToServers [[
wim.ejb wimejb.jar,META-INF/ejb-jar.xml WebSphere:cell=IBM-
19D40CACAF4Cell01,node=IBM-19D40CACAF4Node01,server=server1 ]]]')
```


The wimperdomain.ear application is available in the “installableApps” directory. A unique JNDI URL for the EJB must also be provided during deployment.

This section talks about federated repository management rights.

Feature overview

- New roles to allow non-administrators to access VMM APIs
- Configure authorization for the specific domain/admin domain
- Users and groups/Special Subject (ALLAUTHENTICATED) mapped to VMM roles to perform required operations
- Role-permissions mapping hardcoded

Role name	Method permissions
IdMgrAdmin (same authority as WebSphere Administrator)	create/update/delete/search/get/createSchema/getSchema
IdMgrWriter	create/update/delete/search/get
IdMgrReader	search/get

Previously, VMM had limited roles: namely, administrators who were allowed full functionality, while other users were limited to changing their password and searching on themselves.

With VMM's multiple security domain support, there is a need for other users (non WebSphere Application Server administrators) to access VMM APIs.

New VMM roles with specific permissions are pre-defined, and users and groups can be mapped to these roles.

The role names are IdMgrAdmin, IdMgrWriter, and IdMgrReader.

IdMgrAdmin has the same permissions as WebSphere Administrator and can perform many operations.

IdMgrWriter has permissions to call read and write profile management API.

IdMgrReader has permissions to call read APIs.

The special subject “ALLAUTHENTICATED” can also be mapped to VMM roles to map all authenticated users to a role.

Users with VMM configured for domains can use this feature to configure authorization for the specific domain or administrative domain.

However, since role-permissions are hardcoded, this cannot be customized and attribute-group level access checks cannot be enforced.

High level design

- VMM commands to map user or group to role
- Only one role per user or group during configuration
- Multiple roles possible at runtime through group membership
- Cumulative effect in case of multiple roles
- Backward compatibility with existing roles

VMM commands can be used to map users and groups to roles. A user or group can be mapped to only one role during configuration. However, multiple roles can be associated with a user at run-time through the groups they belong to.

In such a scenario the user will have permissions corresponding to all the roles they are assigned/inherit.

Here's an example: user1 has the IdMgrReader role. user1 is member of group1, group2. group1 has the IdMgrReader role and group2 has the IdMgrWriter role.

Now if user1 attempts a write operation, then access will be granted.

Compatibility with older roles, namely WebSphere Application Server administrator and ACCOUNT_OWNER_ROLE is ensured.

Usage

- Command line interfaces (CLIs) to map users/groups to VMM roles
  - mapIdMgrUserToRole
  - mapIdMgrGroupToRole
  - removeIdMgrUsersFromRole
  - removeIdMgrGroupsFromRole
  - listIdMgrUsersForRoles
  - listIdMgrGroupsForRoles
- Only in server mode
- No server restart required
- No administrative console support

Command line interfaces are provided to map users and groups to VMM roles.

These commands can be used only in server mode and not in local mode.

All the commands update the runtime policy and hence there is no server restart needed for the role changes to be applicable.

There is no support for these commands through administrative console. Refer to the information center for command syntax and usage.

Section

Support for flexible administrative configurations

This section talks about multiple security domain support for flexible administrative configurations.

Overview

- Administrative agents and servers can have different VMM configurations and schemas
- Manage configurations of registered subsystem
- Does not support domains, rather manages domains for base profiles
- Custom repository of subsystems can be managed with a limitation of in memory data
- VMM instance per domain in subsystem created and managed by administrative agent

Federated repository support for multiple security domains

In a flexible administration environment, the administrative agents and base servers can have different VMM configurations and schemas.

Administrative agents can now manage global and domain level VMM configurations of registered subsystems.

Administrative agents manage the registered base profiles and their domain specific configuration. The administrative agent does not directly use domains; rather it will manage domains for base profiles.

Custom repositories can be managed by administrative agents, provided they don’t have the memory data to represent the repository.

Based on Context UUID and Domain ID, multiple VMM instances can be created per domain.

Unique identifiers for file repositories of different domains of subsystems are managed and identified by concatenating the context UUID, domain ID, and file ID.

References

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.nd.iseries.doc/info/iseriesnd/ae/tagt_adminagent.html

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.nd.iseries.doc/info/iseriesnd/ae/tagt_jobmgr.html

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/txml_7managejobs.html

Additional information on this topic is available in the information center.

Section

Change password command

This section covers the change password command.

Feature overview

- New command “changeMyPassword” enables self password update for logged-in user
- No administrative console support
- Command example

```
$AdminTask changeMyPassword {-oldPassword pwd1 –newPassword pwd2 –
 confirmNewPassword pwd2}
```


A new command, “changeMyPassword”, has been added to the WIMManagement command group for the AdminTask object.

This command enables self-password-updates for logged-in users.

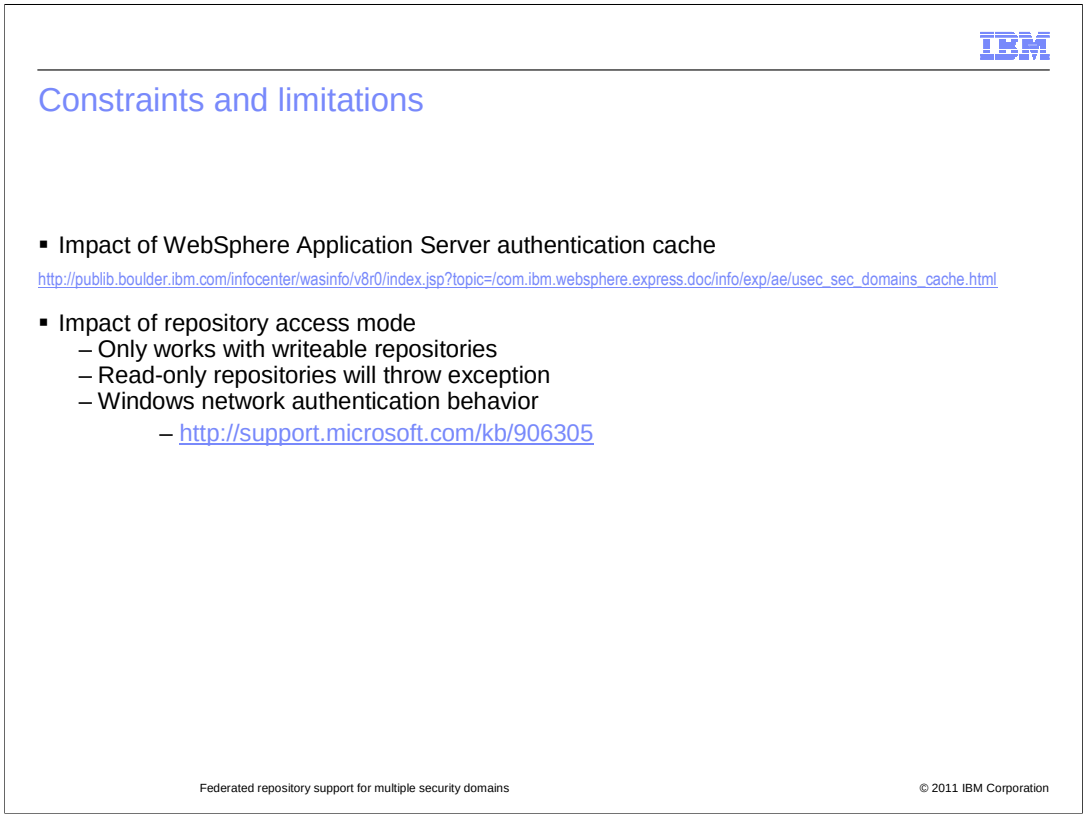
Messages and exceptions

- On successful update “Command completed successfully” message seen.
- Exception on mismatch of new password and confirm new password
  - The value for new password and confirm new password do not match.
- Exception on mismatch of old and new passwords
  - Example, for File and DB Adapters following exception is displayed:

    CWWIM4513E The password match failed for the '<principalname>' principal name.
  - Example, for LDAP adapter following exception is displayed: CWWIM4529E The password verification for the '<principalname>' principal name failed. Root cause 'exception message string'.

Upon a successful password change, you will see a “Command completed successfully” message.

Exceptions are thrown if the old password is incorrect, or if the value of new password and confirm new password do not match.



After you change your password, your old password may remain in effect, allowing you to login using your old password. This happens if both the authentication cache and basic authentication cache keys are enabled, causing the old password to remain valid according to the value specified for cache timeout or cache size. More information can be found in the information center.

The changeMyPassword command will only work for repository types that can be written to by VMM. It will not work for read-only repositories or the VMM user repository bridge adapter configured with LocalOS or a custom user registry. If you are using active directory as an LDAP repository, then by default the old password of a user is valid for 60 minutes.

This value can be changed in the active directory configuration.

Section

Buffer pool parameters on z/OS

This section covers buffer pool parameters on z/OS.

Feature overview

- All VMM tables were created in same pre-defined buffer pool.
- Buffer pools can now be specified or customized for each database object type.
  - For Simple/Default table – **tablesBufferPool**
  - For LOB table – **LOBTablesBufferPool**
  - For unique index - **indexTablesBufferPool**

On z/OS, the schema DDLs had a predefined buffer pool value “BP0”, resulting in all tables being created in the same buffer pool.

In V8, you can specify the buffer pool to be used while creating tables/objects by using three new parameters in commands or scripts.

Usage

- Configure buffer pool using existing commands
- Commands updated with new parameters
- Configure buffer pool values while using DDL.
  - export DEFAULT_TABLE=<buffer pool value for default tables>
  - export LOB_TABLE= <buffer pool value for LOB tables>
  - export INDEX_TABLE=<buffer pool value for unique index tables>
- If not specified, default buffer pool is BP0 as earlier

Example:

```
wsadmin>$AdminTask setupIdMgrEntryMappingRepositoryTables {-schemaLocation
   /WebSphere/Base/AppServer/etc/wim/setup -databaseType db2zos -dbURL
   jdbc:db2://9.42.87.57:8070/WAS00D01 -dbAdminId user203 -dbAdminPassword passw0rd -dbDriver
   com.ibm.db2.jcc.DB2Driver -reportSqlError true -dbSchema user1 -tabspacePrefix em3 -tablesBufferPool BP3}
```


Buffer pools can be configured by using existing VMM database setup commands, which are updated with new parameters in V8.

Three new parameters are introduced as part of the database setup commands.

If any of the parameters are not specified, the default value of “BP0” is assumed.

Troubleshooting

- Buffer pools must already exist
- DB2 exception if buffer pool is not valid

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/twim_fedmap_wsadmin.html

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/twim_manpropextrepos_db2.html

A DB2 exception is thrown if a buffer pool value that is not valid is passed to the commands as a parameter or when incorrect values are passed using a DDL.

Section

Ability to specify schema names for VMM tables

This section covers ability to specify schema names for VMM tables.

Feature overview

- Default schema same as user namespace
- Allows table storage and data retrieval from specified schema
- Limitation: manual setup mandates specifying schema even if default has to be used

VMM by default creates and looks up tables in the default schema, which is the namespace of currently logged in database user.

In V8 you can create VMM tables in a schema of your choice.

While compatibility with earlier versions is available for using commands without specifying the “dbSchema” parameter, for manual DB creation using DDLs, “dbSchema” needs to be set to at least an empty string.

Usage (1 of 2)

DB Setup CLIs
- setupIdMgrDBTables
- deleteIdMgrDBTables
- setupIdMgrPropertyExtensionRepositoryTables
- deleteIdMgrPropertyExtensionRepositoryTables
- setupIdMgrEntryMappingRepositoryTables
- deleteIdMgrEntryMappingRepositoryTables

DB Configuration CLIs
- createIdMgrDBRepository
- updateIdMgrDBRepository
- setIdMgrEntryMappingRepository
- setIdMgrPropertyExtensionRepository

Example:

```
$AdminTask setupIdMgrDBTables {-schemaLocation /WebSphere/Base/AppServer/etc/wim/setup -
dbPropXML /WebSphere/Base/AppServer/etc/wim/setup/wimdbproperties.xml -databaseType db2 -
dbURL jdbc:db2://localhost:8070/WIMDB -dbAdminId user62 -dbDriver com.ibm.db2.jcc.DB2Driver -
dbAdminPassword passw0rd -reportSqlError true -dbSchema user1 }
```


This slide shows command usage, including the new “dbSchema” parameter.

Usage (2 of 2)

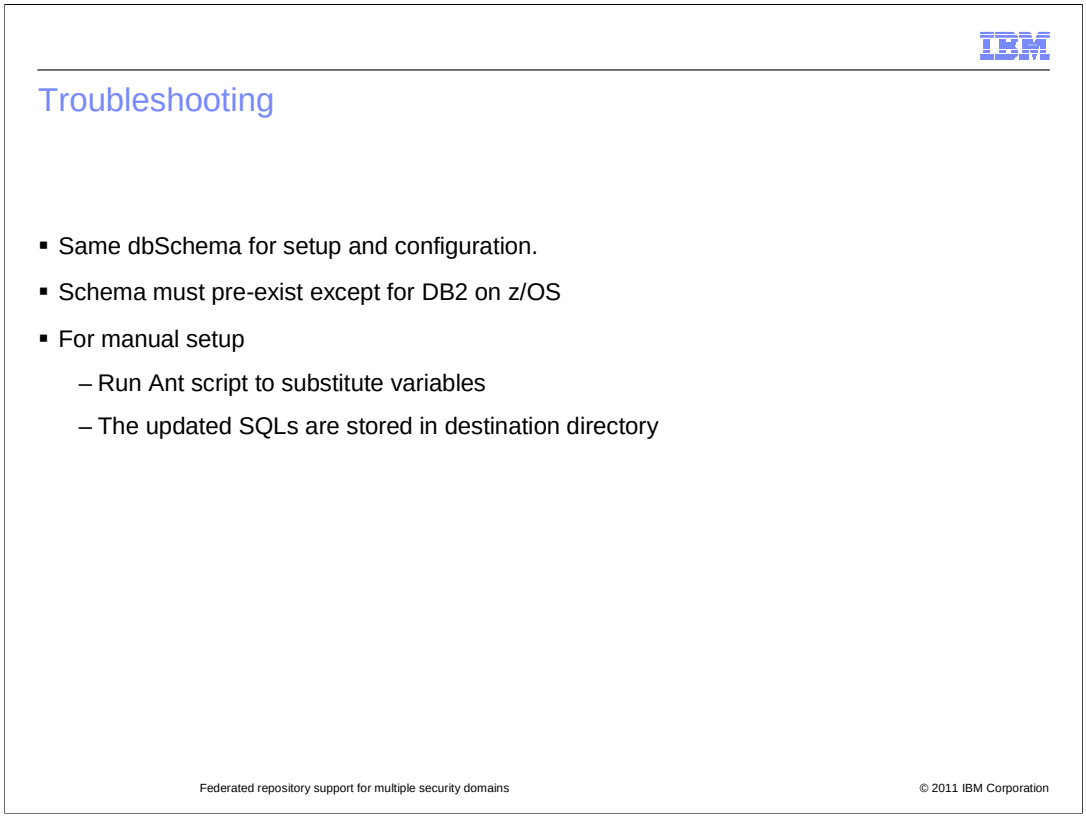
- Specify schema during manual setup of property extension repository through DDL.
- Additional steps required:

  export SCHEMA_LOCATION=app_server_root/etc/wim/setup/lookaside
  export DBTYPE=<db_type>
  where the value of <db_type> is db2, derby, informix, oracle, or sqlserver

  export DBSCHEMA=dbschemaname
  export SCHEMA_DEST_LOCATION=<location where the updated SQL files with replaced variables should be copied>
  ws_ant.sh -f app_server_root/etc/wim/setup/filterbuild.xml

You can also specify the database schema while manually setting up the property extension repository using a DDL.

Additional steps vary by operating system, and can be found in the information center.



The schema specified for database setup and repository configuration should be the same.

For all databases other than DB2 on z/OS, the schema must exist in the database before it can be used for VMM setup.

While manually setting up VMM repository using DDLs or scripts, an Ant script to substitute variables in SQL scripts needs to be run. If tables need to be created in default schema or namespace, skip setting the DBSCHEMA environment variable while running the ant script.

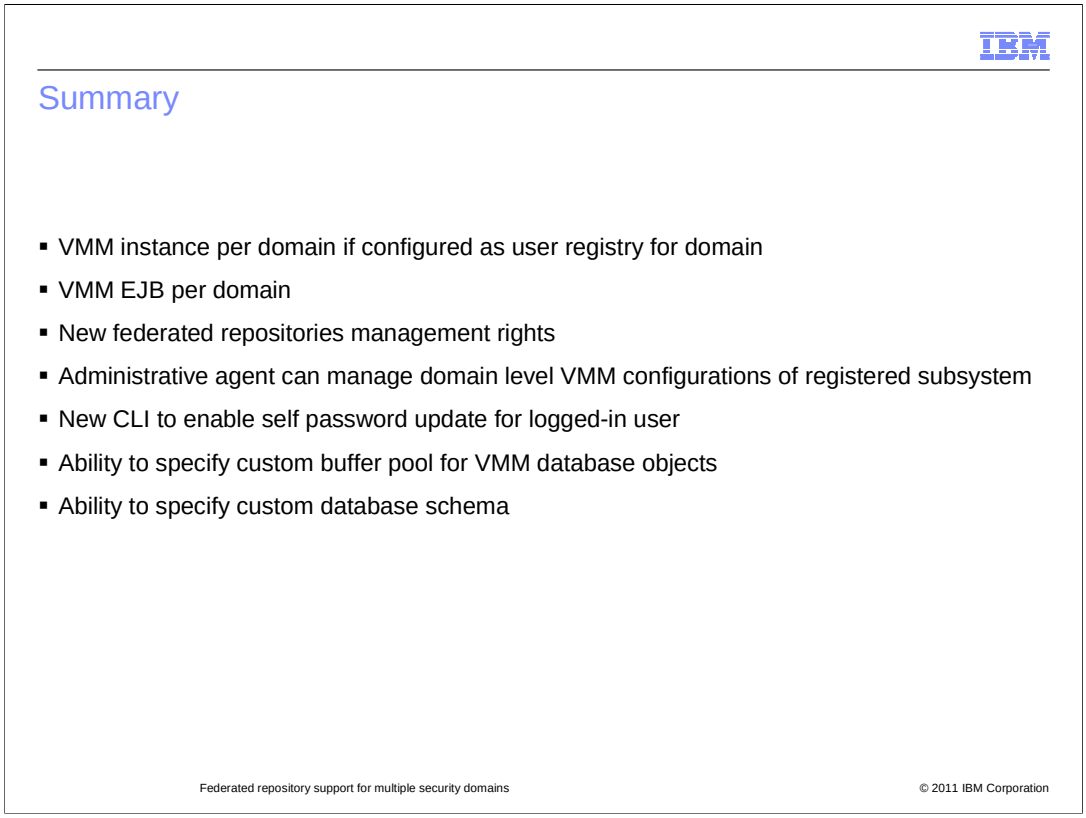
The updated SQL commands with substituted values are located in the directory specified by SCHEMA_DEST_LOCATION and further invocation of scripts to run DDLs should be made from this.

Reference materials

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/twim_manpropextrepos_db2.html

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/twim_manpropextrepos_db2.html

Additional information on this topic is available in the Information Center.



In a multiple security domain environment, WebSphere Application Server security will load a new instance of VMM per domain if the User Registry security attribute is defined as Federated Repositories.

The administrative application wim.ear has been re-packaged as wimperdomain.ear so that the same EJB can be deployed on multiple servers for each domain.

New VMM management rights with specific permissions can be used to configure authorization for particular domains.

Administrative agents can now manage global and domain VMM configurations of registered subsystem.

The new command “changeMyPassword” enables logged-in administrative users to update their passwords.

Custom Buffer pools can be specified explicitly while creating tables or objects in a database.

Custom database schema names can now be specified, allowing you to create and use VMM database tables in a chosen schema.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv8_VMM.ppt

This module is also available in PDF format at: ../WASv8_VMM.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information