Welcome to the CEF eDelivery Webinar on Domibus 4.0

Start 10:30 (CET)

Ground Rules for the Live Webinar

Please mute your microphone before the webinar starts

To chat with other participants and submit questions, please use the Chat function to the right of your screen

To connect your audio go to the Quick Start tab and connect your audio (dial-in, dial-out or connect via computer)

Today's speakers

Cosmin Baciu

Cosmin Baciu is the technical leader of Domibus. He is an experienced Technical Expert/Java Architect with more than 10 years of experience actively involved in software requirement analysis, design and development phases of every project ensuring that the development adheres to the required standards. He has a strong educational background and he is passionate about software architecture and Java related technologies.

Content

Domibus 4.0

1   New features, improvements & fixed bugs

2   Upgrading to Domibus 4.0 step by step

New features, improvements & fixed bugs

New features & improvements

- Java 8 support only

- Support for multiple domains(multi-tenancy)

- Configurable alerts and notifications

- Ping remote access points

- History of the PMode changes

- Management of parties using the Administration Console

- Export UI tables metadata as CSV files

- Support for WildFly 12

- Audit support

- Certificates expiration warnings included in the logs

- Configurable Domibus Admin Console browser title

- Editable text area for Pmode

- Messages page: performance increase with millions of messages

European Commission

New features & improvements
Support for multiple domains(multi-tenancy)

- Domibus supports multiple domains (configurations) configured in one Domibus instance.

- This means that each domain has its own configuration (database schema, PMode, keystore, truststore and Domibus properties, etc).

- These multiple configurations allow one Domibus instance to process messages from multiple domains simultaneously

- Domibus uses **Schema per tenant strategy** to implement multi-tenancy, meaning that the data associated to a domain will be saved in a database schema dedicated to the domain

New features & improvements
Multi-tenancy
Domain segregation

- Store messages metadata and payloads in a dedicated database **schema** per domain

- Segregates the log statements per domain, each domain has its own set of the log files: domibus.log, domibus-business.log and domibus-security.log

- Each domain has its own set of configuration files: Keystore, Truststore, PMode, Domain properties

New features & improvements
Multi-tenancy
Configuration

- By default, multi-tenancy is not activated.

- In order to activate multi-tenancy, the following property that defines the database general schema needs to be configured in *domibus.properties*:

  domibus.database.general_schema=general_schema

    where **general_schema** is the database schema in which the association between users and domains is stored.

- The **general_schema** is not associated to any domain.

New features & improvements
Multi-tenancy
The default domain

- Once multi-tenancy is activated, Domibus starts with a domain named **default**

- The domain default is configured in **domibus.properties**

- Default domain is used when Domibus C2 receives messages and no domain is specified

- Default domain makes the migration to multi-tenancy easier

New features & improvements
Multi-tenancy
Creating new domains

- New domains can be created by adding domain configuration files under **cef_edelivery_path/conf/domibus** directory.

- The domain configuration file must be configured according to the domain name, which means that the domain schema, keystore, truststore, PMode etc., must be configured.

- The domain configuration file must respect the following convention:

    domain_name-domibus.properties

    where **domain_name** is the name of the domain.

New features & improvements
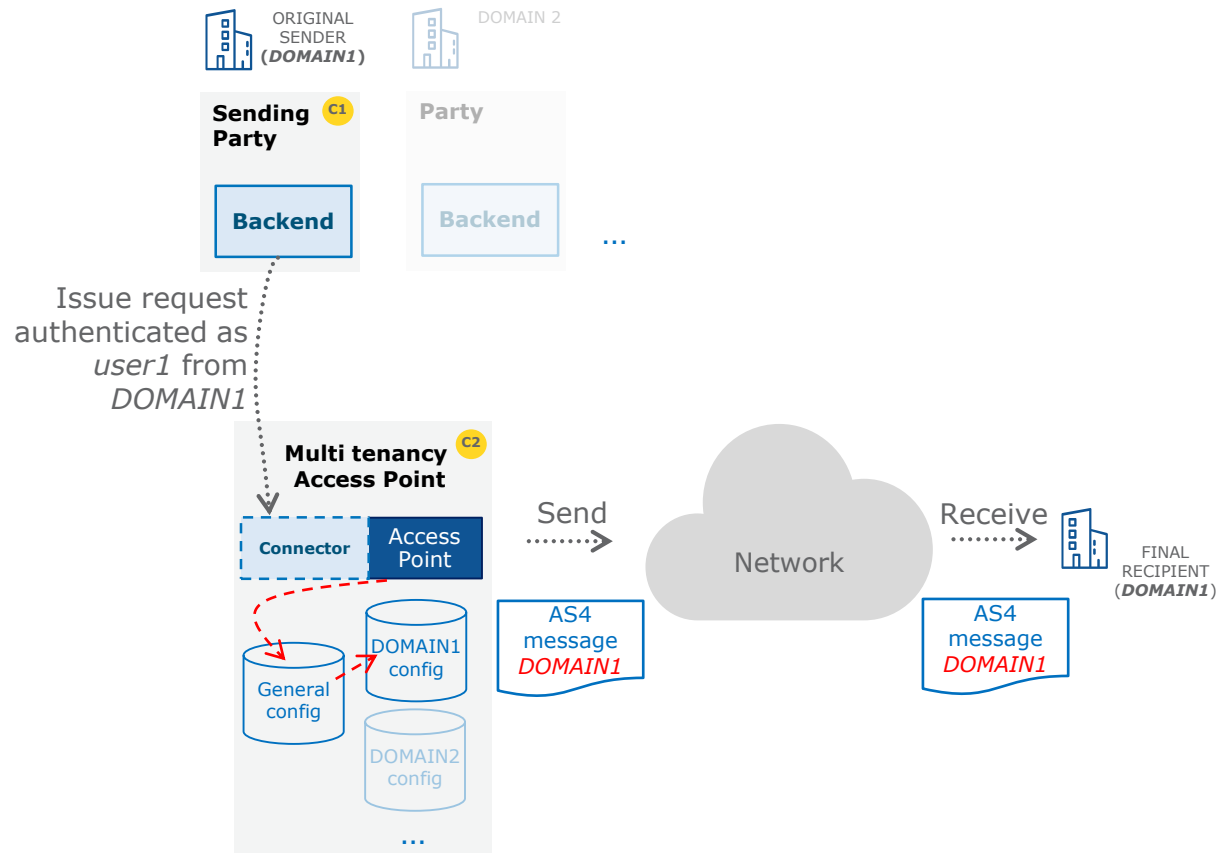**Multi-tenancy**
Outgoing messages

- For outgoing messages, sent by C2 to C3, the plugins security becomes mandatory overriding the value configured using the following property:

- *domibus.auth.unsecureLoginAllowed=false*

- The association to a specific domain is performed based on the Spring Security info available after the authentication has been done in the plugins

New features & improvements
Multi-tenancy
Outgoing messages

ORIGINAL SENDER (**DOMAIN1**)

DOMAIN 2

Sending Party C1

Backend

Party

Backend

...

Issue request authenticated as *user1* from *DOMAIN1*

Multi tenancy Access Point C2

Connector | Access Point

General config

DOMAIN1 config

DOMAIN2 config

...

Send

Network

Receive

AS4 message *DOMAIN1*

AS4 message *DOMAIN1*

FINAL RECIPIENT (**DOMAIN1**)

New features & improvements
Multi-tenancy
Incoming messages

- When C2 wants to send messages to a **C3 running in multi-tenancy mode**, the endpoint URL of C3 configured in the C2 PMode can contain the domain name at the end, configured as an HTTP parameter to indicate the domain that will receive the message.

- **Example**:

  Let us suppose that C3 exposes the MSH endpoint under the URL: http://localhost:8080/domibus/service/msh. If C2 wants to send messages to C3 to the domain DIGIT, it will call the following MSH C3 endpoint URL:

  http://localhost:8080/domibus/service/msh?domain=DIGIT

  In case C2 does not specify the domain in the endpoint URL, the message will be sent to the C3 **default** domain.

New features & improvements
Multi-tenancy
Incoming messages
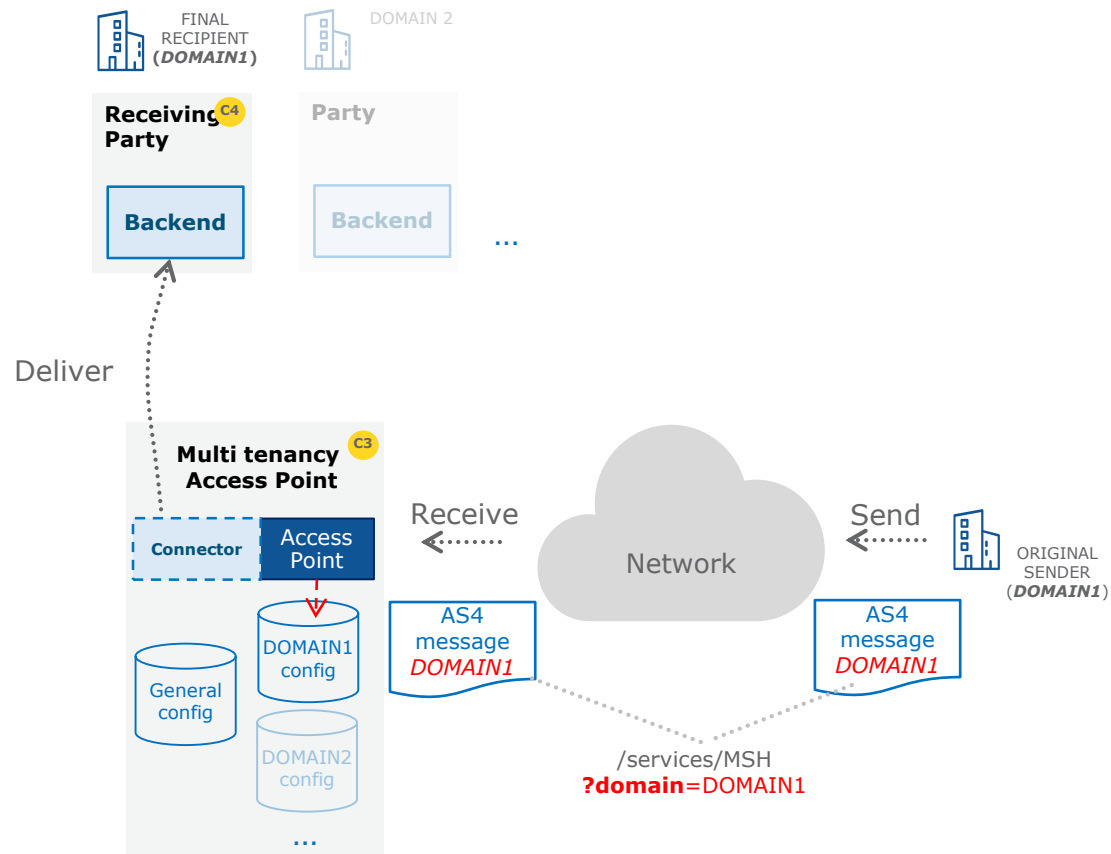
New features & improvements

Multi-tenancy
Domain properties

- A domain uses a dedicated configuration file named **domain_name-domibus.properties,** where **domain_name** is the name of the domain

- A sample domain configuration file **domain_name-domibus.properties** is present in the Domibus distribution

- Some properties are defaulting to the properties defined in **domibus.properties** if they are not defined in the domain properties file. The full list of properties that can be configured per domain can be found in the **Domain Administration Guide**

16

New features & improvements

Multi-tenancy
Logging

- The Domibus log configuration file **logback.xml** has to be modified in order to include the log configuration for each domain.

- This is necessary to segregate the log statements per domain, each domain having its own set of the 3 logs files: **domain_name-domibus.log**, **domain_name-business.log** and **domain_name-security.log**

  where **domain_name** is the name of the domain

- A sample domain logback configuration file named **default-logback.xml** is present in the Domibus distribution

New features & improvements
Multi-tenancy
Users

- In multi-tenancy mode there is a new user named **super** with role **ROLE_AP_ADMIN** which has the privileges to access all the available domains.

- The default password for the super user is **123456**.

- The first time a new domain is created, the super user creates a new user in the **Domibus Administration Console** with role ROLE_ADMIN associated to the newly created domain

- All normal users (ROLE_ADMIN, ROLE_USER) can be associated to only and only one domain

- A username must be **unique across domains**

New features & improvements
Multi-tenancy
Plugins

- In multi-tenancy mode the plugins security is activated by default, no matter if value configured in domibus.properties for the **domibus.auth.unsecureLoginAllowed** property

- This is needed in order to identify the request performed by the user and associate it to a specific domain. As a result, every request sent to Domibus needs to be authenticated

- Plugin Users: a plugin must use a configured plugin user associated to a specific domain in order to authenticate every request sent to Domibus. The management of the plugin users is implemented in the Plugin Users page

New features & improvements

Multi-tenancy
More details

- The **Domibus Administration Guide** contains detailed instructions on how to configure multi-tenancy in Domibus

- The **Software Architecture Document** contains more details on the technical aspects of multi-tenancy and how it is implemented in Domibus

New features & improvements
Configurable alerts and notifications

- A Domibus alert is created when certain events occur in Domibus

- By default an email is sent in order to notify the user. The email sending can be disabled per each type of alert in domibus.properties

- The alerts can be inspected in the **Alerts** page

- The alerts can be configured in domibus.properties and some parameters can be tweaked like: the frequency of alerts, the alert level, email subject, etc

New features & improvements
Configurable alerts and notifications

- The following alerts are implemented in Domibus:

  - **MSG_STATUS_CHANGED**

  Occurs when a message changes status, for instance a message failed to be sent and it changes the status to SEND_FAILURE

  - **CERT_IMMINENT_EXPIRATION**

  A job runs periodically and triggers an alert if a certificate from the keystore/truststore is about to expire(default value is 2 months)

  - **CERT_EXPIRED**

  A job runs periodically and triggers an alert if a certificate from the keystore/truststore is already expired.

  - **USER_LOGIN_FAILURE**

  Occurs each time a user fails to login in by using wrong credentials

  - **USER_ACCOUNT_DISABLED**

  Occurs when:

    - the first time the user account gets disabled due to too many invalid login attempts

    - a user tries to login in to a disabled account

New features & improvements
Ping remote access points

- Allows a party to "Ping" a communication partner

- This feature allows communication partners to perform a basic test of the communication configuration (**including security at network, transport and message layer, and reliability**) in any environment, including the **production** environment.

- This feature requires additional configuration in the Pmode. The service **eb:UserMessage/eb:CollaborationInfo/eb:Service** and action **eb:UserMessage/eb:CollaborationInfo/eb:Action** have to be declared in the PMode

- Ping messages are not delivered to any Consumer business application

New features & improvements
History of the PMode changes

- The PMode history page in the **Domibus Admin Console** displays the history of the PMode changes

- Domibus keeps a snapshot of the Pmode each time the PMode is modified

- The user can restore a particular version and make it as the current PMode

New features & improvements
Management of parties using the Administration Console

- A new page in the **Domibus Admin Console** allows the management of the parties in the PMode

- Parties can be search using filter criteria, added, updated or deleted

- The PMode and the truststore is automatically updated in one action when adding, updating or deleting parties

- A PMode snapshot is created when parties are added, updated or deleted

New features & improvements
Messages page: performance increase with millions of messages

- This feature has been introduced in order to ensure a faster search on Admin Console Messages page when the database contains more than 100k messages and the time to perform a search is longer

- The mechanism uses a flat table which is populated asynchronously(almost in real time) based on master data

- By default the UI replication mechanism is disabled but it can be activated in domibus.properties

- During the night a job checks if there are differences between the replicated data and master data

New features & improvements
Miscellaneous

- Export Export UI tables metadata as CSV files

- Support for WildFly 12

- Editable text area for Pmode

- Audit support: Domibus keeps track of changes performed in the PMode, Parties, Message Filter and Users pages

Fixed bugs

- Incorrect Domibus behaviour for missing eb3:MessageProperties or eb3:PartProperties in the message

- LDAP support for CRL

- Proxy configuration in Dynamic discovery Dynamic discovery in a mixed configuration

- The notifications events sent to the plugins should be configurable

- Not existing folder handling for domibus.attachment.storage.location

- Default WS Plugin:

  - domibus-backend.xsd violates Unique Particle Attribution

  - With secure login enabled, receiver is not authorized to get the status of his message.

  - Fixed schema validation

Known issues & limitations

- The Admin Console cannot be used in IE (not EDGE)

- UI admin console: user is logged out when logging-in in another tab

- Max retry limit may be exceeded on Wildfly 9

- Issue starting Tomcat/WildFly cluster the first time with an empty MySQL schema

- Messages page: performance decrease when certain filters are applied on millions of messages

Administration console

New features
Multi-tenancy
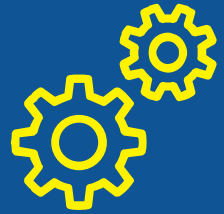
Upgrading to Domibus 4.0 step by step

Upgrading to Domibus 4.0 step by step(Tomcat)
Prerequisites

- Un-deploy the current **war** installation of Domibus

- Upgrade to 3.3.4 if an older version of Domibus is installed. Detailed instructions can be found as usual in the **upgrade-info.txt**

Upgrading to Domibus 4.0 step by step
Database migration

- Execute the database migration script
    a) **mysql5innoDb-3.3.4-to-4.0-migration.dd**l for MySQL
    b) **oracle10g-3.3.4-to-4.0-migration.dd**l for Oracle

Upgrading to Domibus 4.0 step by step
Update the activemq.xml configuration

1. Copy the **activemq.xml** file from the Domibus 4.0 distribution and override the existing one

2. Reproduce the changes in the **activemq.xml** file in case it was modified in 3.3.4 installation

Upgrading to Domibus 4.0 step by step
Configure the domibus properties

- Adapt several properties in the **domibus.properties** configuration file

- Full instructions which properties must be adapted can be found in the distributed **upgrade-info.txt** file

Upgrading to Domibus 4.0 step by step
Install the Domibus 4.0 war

- Install the new Domibus war file and the default plugins

- For WebLogic and WildFly the procedure is similar

3

Q&A

All

Find out more on CEF Digital

ec.europa.eu/cefdigital

#BIG
REUSE

Contact us

✉ CEF-BUILDING-BLOCKS@ec.europa.eu