IBM Enterprise Content Management System Monitor Version 5.2

Installation Guide



IBM Enterprise Content Management System Monitor Version 5.2

Installation Guide



Before using this information and the product it supports, read the information in "Notices" at the end of this document.

This edition applies to version 5, release 2, modification 0 of IBM Enterprise Content Management System Monitor (product number 5724R91) and to all subsequent releases and modifications until otherwise indicated in new editions.

Table of Contents

Preface	6
About this document.	
ECM SM identification of Servers and Agents	Q
Agent ID the unique identifier for Servers and Agents	0
Agent ID - the unique identifier for Servers and Agents	0
ECM SM Server functionality	9
Distributed Installation of ECM SM Server components	9
ECM SM Agent functionality	
ECM SM Agent functionality	
Installation Requirements and Server Proparation	1.1
Installation Requirements and Server Preparation	
IBM Collocation Support Information	
Detabase system	10 10
HP-IIX	
Redhat Linux	
Solaris	
SuSE Linux	
Windows	
Preliminary Considerations	30
Enhanced exercity EIDS 140.2 compliant paceword energy tion	
SSL authentication in CALA, PEX	
Integrating FCM SM into an existing authentication system	48
	40
Installing ECW SW Server.	
Installation Prerequisites	
Server Installation process.	
CALA PEX and Tack execution logging on the Server and Agente	
Troublesbooting	
Troubleshouting	
Event formula in to an EOM Overteen viel onfile	400
Event forwarding to an ESW System via Logfile	
Event integration to an ESM System via SNMP	
ECM SM SNMPv1 traps and variable settings	
ECM SM SNMPv2c or SNMPv2c Inform traps and variable settings	140
Prepared MIB files	
Prepared trap definition files	
Event forwarding to HP OpenView Operations (OVO)	144
Over termining the FOM ON Web Over a bi	4.40

Changing Fonts and Colors Icon Sets	146 147
How to Configure and Use the UnifiedDatabaseClient (UDC).	148
General	. 148
Requirements	149
Usage	150
Agent Installation Requirements	.157
AIX	. 157
HP-UX	159
Redhat Linux	160
Solaris	161
SuSE Linux.	. 163
Windows	164
Configuring and installing ECM SM clients	. 165
CALA_REX Installation	. 165
Preparation.	188
Starting the ECM SM agent Installer	
Configuring ECM SM clients for IBM FileNet Image Manager	202
Configuring ECM SM clients for IBM FileNet P8	270
Configuring FileNet Capture	
Configuring a FileNet Listener	303
Configuring ECM SM clients for IBM FileNet Content Services	. 306
Configuring ECM SM clients for IBM FileNet P8 4.x/5.x	314
Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)	371
Installing ECM SM clients	408
Additional Configuration Tasks	412
Additional ECM SM specific Configuration Tasks	434
ECM SM Mobile app installation and configuration	. 451
Installation Prerequisites	451
IBM Enterprise Content Management System Monitor Mobile Installation and config routine	uration 452
FCM SM UA and DD aumnart	450
	.433
General ECM SM HA and DR support	453
ECM SM Agent HA and DR support	404
ECM SM Agent multi agent / multi destination CALA_REX and CALA installation	457
CALA configuration settings	458
Configuration variables for ECM SM Client Unix	458
Configuration variables for ECM SM Client Windows	. 475
Appendix A. Further CALA REX installation and configuration options	. 495
Installing CALA REX to run as non-root	. 495
Adjusting CALA_REX configuration settings	498
Starting and Stopping CALA_REX daemons manually	512

Appendix B. How To	513
Adding a new monitor command table to a configuration archive	513
Adding a new logfile to a configuration archive	514
Change hostname or IP address of ECM SM server	515
Start a Unix-like shell on Microsoft Windows	517
Deinstall the ECM SM agent software	518
Deinstall the ECM SM server software	519
Reinstall CALA_REX agent or server	520
Move a ECM SM agent to another server	521
How to install ECM SM on a Windows Cluster	522
JVM Properties for an IBM WebSphere Based Installation	
Creation of a datasource on IBM WebSphere	
The deployment of the ECM_SM on IBM WebSphere	539
Appendix C. Ap example charget alias file	543
An example ///er/lib/charget alias file for Solaris 9	
All example /usi/lib/charset.allas file for Solaris o	
Appendix D. Constal Configuration of ECM SM Server	544
Appendix D. General Configuration of ECIVI SIVI Server	
Introduction	
Appendix E. FIR configuration	547
FIR configuration	547
Transfer CALA -> ECM SM 5.2.0 configuration	550
Architecture Model	554
Event Processing	558
User Management	
How to Reset the Admin Account?	
Annendix E. Longing Configuration	574
Appendix F. Logging Configuration	
Introduction	
How to Configure Logging	572
Annual Resonant and the second s	570
Appendix G. InstallAnywhere Installer variables	
Documentation of the InstallAnywhere installer variables	576
Annendiv II. Denvired detekses normissions	500
Appendix n. Required database permissions	
DB2.	
MSSQL	
Generic monitors	
Configuration scripts	
Appendix L Ungrade Explanation	60F
IDM FOM ON Converting and Dath Funder store	
IBIVI ECIVI SIVI Server Opgrade Path Explanation	605
Annendia I. Commint the tion	000
Appendix J. Copyright notice.	
IBM Enterprise Content Management System Monitor (December 2016)	606

Preface

About this document

Who should read this guide?

The target audience for this guide are those who install or maintain ECM SM environments.

Every effort has been made to provide you with complete installation instructions. If information becomes available after the creation of the installation media from which you accessed this guide, we will provide an updated version of the guide on the IBM/FileNet Customer Service and Support web site (http://www.ibm.com/support). As a general rule, you should refer to the IBM web site to obtain the current version of this guide.

This guide provides instructions for installing and/or upgrading IBM Enterprise Content Management System Monitor, and identifies the IBM/FileNet and 3rd Party products that are certified for the current release. Be aware that each release of IBM Enterprise Content Management System Monitor may have multiple Interim Fixes, or Fix Packs available for installation, each with potentially different dependencies and installation requirements. Therefore, before you attempt to install or upgrade IBM Enterprise Content Management System Monitor, review the list of releases and their associated dependencies on the IBM Support web site (http://www.ibm.com/support).

Before you start

Users of the guide should have knowledge about Unix and/or Microsoft Windows® operating system, web servers, database systems and middleware platforms. The configuration of managed systems (clients) requires advanced knowledge of all IBM ECM systems that should be monitored.

If you lack the requisite skill sets it is strongly recommended to have IBM Lab Services or a certified ValueNet Partner in order to install this product.

Where you find this guide

You can find this documentation on the ECM SM installation media in the following folder:

UNIX: <Mount point>/INSTALL/docs

Windows: <Drive letter>:\INSTALL\docs

Feedback on documentation

Send your comments by e-mail to <u>comments@us.ibm.com</u>. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a chapter and section title, a table number, a page number, or a help topic title).

ECM SM identification of Servers and Agents

Agent ID - the unique identifier for Servers and Agents

While ECM SM Server used the IP address and full qualified IP name to identify agents this no longer identifies an agent, because changed domain names and IP addresses can occur. In addition to the above scenario ECM SM supports multi-agent installation on a single server. To be able to identify the correct agent it was necessary to add a unique identifier.

Since version 4.5 the Agent Postfix exists. The Agent Postfix allows users to add an identifier in the case more than one agent need to be installed. This identifier was only added to the Windows Service Name and the UNIX/Linux Daemon control scripts to be able to start an specific instance of the agent. With the multi-agent support the enhanced server required an unique identifier for each agent, to so called 'Agent ID'.

The new 'Agent ID' is build from 2 parts, the hostname and the Postfix the user specifies during agent installation, combined with an underscore: <lower case hostname>_<lower case postfix>, example: The Agent ID for server 'MyServer1' with Postfix 'Serv1_DB' will be 'myserver1_Servdb', since all underscores and blanks will be removed.

Starting with version 5.2.0 the Agent ID will be used within the ECM SM CALA Agent Installer, the Task Execution Manager and the Monitoring Manager. In the case no Postfix is specified (older agents from version 4.5x and 5.1x) the default postfix 'agent' will be used.

Note: Version 4.5 and 5.1 didn't allow multi-agent installation connected to one ECM SM server, the agents had to use different servers.

9

ECM SM Server functionality

Distributed Installation of ECM SM Server components

This chapter describes the distributed installation and configuration of ECM SM Server components, describes customer scenarios where the distributed installation adds significant additional value.

Distributed Server installation scenarios

There are two major scenarios for the distributed Server component scenario:

- High availability
- Scaling (Performance)

Server components

The following server components are available

- Database initialization Required once in a ECM SM to generate the database tables and content
- CALA_REX Server Used to install and control agents, communication to the Java WebStart tools
- GUI Server

At least one GUI Server or one GUI EAR package deployed on a WebSphere Application Server is required in a ECM SM environment. Several GUI Server components can be active at one time. The GUI Server serves the GUI, in non-WAS based ECM SM environment the GUI Server additionally servers all Download functionality and internal links of the product.

Event Server

The Event Server component is used to processes Events, generates Reports and forwards Events to other systems (email, SNMP forwarding, etc). With this release only one Event Server can be active at a time, but more than one Event Server can be installed for High Availability purposes.

- Download Server Only available in distributed environments without a GUI Server on the Primary Server or in the case of WAS based environments.
- Embedded CALA_REX Agent

Since this release the ECM SM server installer can install an embedded CALA_REX agent with the server installation. Together with an installed CALA Monitoring agent on the embedded CALA_REX Agent (Agent name <lower case hostname>_srvagnt) the installed Server components can be monitored and controlled. It is strongly recommended to install the embedded CALA_REX Agent to the server, since otherwise the new 'ServerPomponentStatus' monitor that monitors and controls the server components cannot be used.

© Copyright Cenit AG 2000, 2016, © Copyright IBM Corp. 2005, 2016

Three different ECM SM Server installation types

Starting with version 5.2.0 ECM SM supports three different ECM SM installation types.

Complete installation of the ECM SM Server

The installation type 'Complete installation' is similar to the installation of previous releases. All required server components will be installed.

Note: Only one 'Complete Server' or 'Primary Server' installation can be part of a ECM SM environment.

	Jetty based installation	IBM WAS based installa- tion	Function	
Database initialization	✓	٧	Provides the database initialization and content	
CALA_REX Server	\checkmark	✓	Used to install and con- trol agents, communica- tion to the Java WebStart tools	
Download Server	-	✓	Background Download Service for JRE pack- ages (CALA_REX Up- grade task and download links provided through GUI Service), UNIX-like shell archive (Windows agent installation only) and CALA_REX Installer Images (access provided through GUI Service)	
GUI Server	✓	-	Serves the GUI, Back- ground Download Ser- vice for JRE packages (CALA_REX Upgrade task and download links provided through GUI Service), UNIX-like shell archive (Windows agent installation only) and CALA_REX Installer Images (access provided through GUI Service)	
Event Server	<i>√</i>	-	Processes and forwards events, provides Report- ing functionality	
WAS EAR Package GUI Server	-	<i>√</i>	Serves the GUI	

	Jetty based installation	IBM WAS based installa- tion	Function
WAS EAR Package Event Server	-	\checkmark	Processes and forwards events, provides Report- ing functionality
Optional CALA_REX Agent	\checkmark	✓	Used as control agent for all above listed services (except WAS based ser- vices)

The optional CALA_REX Agent is required on all installed servers in the case the new 'Server Component Monitor' is planned to monitor the installed ECM SM server components.

Note: Upgrading from 5.1.0 to the current release is similar to a Complete installation, since the previous release only contained the full installation functionality. Once a 5.1.0 ECM SM server is upgraded to 5.2.0 as many 'Secondary Server installations' as required can be connected to the upgraded server, which is in fact a 'Complete Installation'.

Primary Server installation of ECM SM Server

The installation type 'Primary Server installation' contains the minimum required components to implement a ECM SM environment.

Note: Only one 'Complete Server' or 'Primary Server' installation can be part of a ECM SM environment.

	Jetty based installation	IBM WAS based installa- tion	Function
Database initialization	✓	✓	Provides the database initialization and content
CALA_REX Server	✓	 Image: A second s	Used to install and con- trol agents, communica- tion to the Java WebStart tools
Download Server	✓ Optional, can be re- placed by GUI Server or the WAS EAR Package GUI Server	/	Background Download Service for JRE pack- ages (CALA_REX Up- grade task and down- load links provided through GUI Service) and CALA_REX Installer Images (access provided through GUI Service)
GUI Server	✓ Optional, can be re- placed by Download Server (default)	-	Serves the GUI
WAS EAR Package GUI Server	-	✓ Optional, can be re- placed by Download Server (default)	Serves the GUI

	Jetty based installation	IBM WAS based installa- tion	Function
Optional CALA_REX Agent	1	✓ 	Used as control agent for all above listed services (except WAS based ser- vices)

The optional CALA_REX Agent is required on all installed servers in the case the new 'Server Component Monitor' is planned to monitor the installed ECM SM server components.

Secondary Server installation of ECM SM Server component

The installation type 'Secondary Server installation' contains the components that can be installed more than one time in a ECM SM environment.

Note: As many 'Secondary Servers installations' as required can be added to a 'Complete Server' or 'Primary Server' installation.

During the 'Secondary Server installation' the installation process requires access (network communication to the CALA_REX server component) of the 'Primary Server / Complete Server Installation'.

The 'Secondary Server installation' can be done on a different platform than the 'Primary Server / Complete Server installation' (mixed OS support).

	Jetty based installation	IBM WAS based installa- tion	Function	
GUI Server	✓ Optional	-	Serves the GUI	
Event Server 🗸 Optional		-	Processes and forwards events, provides Report- ing functionality	
WAS EAR Package GUI Server	-	✓ Optional	Serves the GUI	
WAS EAR Package Event Server	-	✓ Optional	Processes and forwards events, provides Report- ing functionality	
Optional CALA_REX Agent	\checkmark	\checkmark	Used as control agent for all above listed services (except WAS based ser- vices)	

The optional CALA_REX Agent is required on all installed servers in the case the new 'Server Component Monitor' is planned to monitor the installed ECM SM server components.

ECM SM Agent functionality

ECM SM Agent functionality

ECM SM contains 2 agents: the 'ECM SM CALA_REX agent' and the 'ECM SM CALA Agent'. Both agents exist on ECM SM Servers (managing servers) and managed systems (FileNet, Database, Web Application Servers or other servers).

ECM SM CALA_REX Agent

 The ECM SM CALA_REX Agent (Windows service or UNIX daemon) is used for the communication between the ECM SM Server and the clients. The installation of the ECM SM CALA agent (described below) is realized with the ECM SM CALA_REX Agent, too. The communication between the graphical tools like ECM SM Monitoring Manager or the ECM SM Task Execution Manager is handled by the ECM SM CALA_REX agent, too.

ECM SM CALA Agent

 The ECM SM CALA Agent (known as CALA or Cenit Advanced Logfile Adapter) is the monitoring component of ECM SM. The ECM SM CALA agent (Windows service or UNIX daemon) checks thresholds (configured with the graphical tools like ECM SM Monitoring Manager) and analyzes logfiles and Windows Eventlogs for errors.

Installation Requirements and Server Preparation

IBM Collocation Support Information

The ECM SM Server cannot be collocated on servers running IBM FileNet, IBM Content Manager OnDemand or IBM CM8 software or any other IBM ECM software, that will be monitored by an ECM SM Agent.

Requirements of all Server platforms

ECM SM server hardware requirements

ECM SM server components require the following minimum system configuration:

- 2 Core/CPU hardware platforms (recommended 4 Core/CPU)
- 2 GByte RAM (4 GByte recommended). If running a WebSphere-based installation this value can be higher
- see system os specified section for disk space requirements

Static IP address for ECM SM server

The ECM SM server must have a static IP address. It is not possible to use a machine that has a DHCP address only.

For network performance reasons, the server and all clients should be added to the DNS.

Web Application Server

During installation of the ECM SM server component the user can decide to use either the embedded Jetty Web Application Server shipped with the product or a pre-installed IBM WebSphere Application Server.

Embedded Jetty Web Application Server

If the Embedded Jetty Web Application Server is selected during installation there is no need to install or configure any additional Web Server component before or after the ECM SM server installation.

IBM WebSphere Application server

If IBM WebSphere Application Server is selected during installation this requires an installed and configured IBM WebSphere Application server environment. See Hardware and Software Guide for details about supported IBM WAS versions.

IBM WebSphere Application server requirements

If ECM SM should be installed based on IBM WebSphere Application Server the following installation and configuration steps are required:

Software requirements:

 IBM WebSphere Server (see the Hardware and Software Guide of ECM SM for details about the supported/required versions)

The following section describes the installation steps of a IBM WebSphere based ECM SM server installation:

- IBM WebSphere Server Base installation (see WAS documentation)
- IBM WebSphere Server Fixpack installation with IBM UpdateInstaller for WebSphere (see WAS documentation)
- IBM WebSphere Software Development Kit update with IBM UpdateInstaller for WebSphere (see documentation)
- Import of the existing WAS installation into the IBM Installation Managers
- Installation of the ECM SM (InstallAnywhere installation, see later chapter)
- Create a new WAS profile (from default profile 'aries') or edit an existing profile by using the IBM WebSphere Profile Management Tool.
- Deploy the two ECM SM ear packages (applications) in the adjusted profile.
- Create or adjust the WAS datasource, custom properties according to the Database settings of the ECM SM installation.

user <db-user>

password

<db-password>

- Extend the JVM custom properties of the WAS server as documented in JVM Properties for an IBM WebSphere Based Installation.
- Restart the WAS profile.
- Starting of the two ECM SM WAS applications

Perl 5

ECM SM expects Perl 5 to be installed on the client and server systems.

For Microsoft Windows systems, Perl 5 is included in the ECM SM server and client installation packages.

On Linux and Unix systems, Perl 5 should be installed using the system depend package management system.

Java JRE

ECM SM requires a Java runtime environment (JRE) greater than or equal to 7 to be installed in the ECM SM server. ECM SM server and client installation packages contain a bundled Java JRE version 7 package. This JRE is automatically installed in the directory jre in both the ECM SM server and the client installation directory. Previous versions of the ECM SM CALA_REX client can be upgraded using the appropriate CALA_REX upgrade task. See Migration Tasks guide for further details.

Database

ECM SM supports the following database management systems as ECM SM database. Check the latest ECM SM Hardware and Software requirements guide for supported databases and JDBC driver and versions.

- IBM DB2
- Microsoft SQL Server
- Oracle
- PostGreSQL (only supported for Demo and testing purposes)

ECM SM uses one technical user for installation and runtime connection to the database. The user name can be adjusted during installation.

JDBC Driver

The ECM SM CALA_REX and ECM SM CALA server agents are using JDBC to connect to the database. Therefor a jdbc driver has to be present on the ECM SM server system.

Database system

Database installation requirements

Database

ECM SM supports local and remote database access. The access is based on JDBC. This no longer requires the database vendor specific Database client tools installed on the ECM SM server. Only the supported database JDBC driver needs to be installed on the ECM SM server. See ECM SM Hardware and software guide for detailed information about supported database systems and JDBC drivers.

IBM DB2

General installation parameters

- Create a ECM SM database (use codeset UTF-8 and database Page size 32k). Smaller Page size settings are not supported and cause installation errors.
- Create the ECM SM technical DB user on your operating system (select a name, e.g. webadmin).
- Create the ECM SM technical DB user on your previously created ECM SM database with at least the rights "Connect to database", "Create tables" and "Create schema implicitly".

W2K3DB291 - DB2 - FSMDB
Database Schema Table Index View Table Space Function Procedure Method Package
Specifiu a user name. You can select a user name from the list or tupe one in
Choose the appropriate authorities to grant to the selected user.
Connect to database
Create tables
Create packages
Register routines to execute in database manager's process
Database administrator authority
Create schemas implicitly
Access to the load utility
Create external routines
Connect to guiesced database
J Security administrator authority
OK Cancel Apply <u>R</u> eset Show SQL Help

IBM DB2: Example to create user WEBADMIN.

Oracle

General installation parameters

Use the Oracle database configuration assistant (dbca) to create the ECM SM database.

 Create a ECM SM database. Use character set AL32UTF8 and minimum database Block size of 8192 (parameter db_block_size). Smaller Block size settings are not supported and cause runtime errors.

Select 'Shared Server mode' for the ECM SM database.

Set or create the following parameters for the ECM SM database: shared_servers = 10 and max_shared_servers = 20 (in the case these parameters are configured with smaller values or do not exist). In the case these parameters are already assigned with bigger values leave them unchanged.

 Create the ECM SM technical DB user on your previously created ECM SM database with the following roles: "CONNECT" and "RESOURCE".

MS SQL Server

General installation parameters

The MS SQL Server must be configured for SQL Server Authentication, Mixed Mode Authentication or Windows Authentication (only for Windows-based ECM SM Servers). To change the authentication mode from Windows Authentication mode to SQL Server and Windows Authentication mode, see MS SQL Server documentation.

- Create a database to use with ECM SM Server. Assign the Latin1_General_CI_AS collation to the database.
- Create a database user. Assign the just created ECM SM Server database as Default database and assign the db_datareader, db_datawriter, db_owner and public roles within the database role membership.
 - **NOTE** Make sure, the database schema, that you will use, is the **Default Schema** of your specified database user, which will be used to connect to your ECM SM Server database and for database initialization and import, otherwise database initialization for instance will fail.

🚪 Login Properties - webadmi	in	
Select a page	🔄 Script 👻 📑 Help	
General Server Roles Suser Mapping	Login <u>n</u> ame:	webadmin Sgarch
Securables	$old C$ \underline{W} indows authentication	
	SQL Server authentication	
	Password:	
	<u>C</u> onfirm password:	•••••
Connection	Enforce password policy Enforce password expiration User must change password Mapped to certificate Certificate name: Mapped to asymmetric key Key name:	at next login
Server: W2K3SERV\W2K3SQL2005	Default <u>d</u> atabase:	FSMDB
Connection: W2K3SERV\Administrator	Default l <u>a</u> nguage:	English
View connection properties		
Progress		
Ready		
		OK Cancel

Example: MS SQL Server configured as remote database using SQL Server authentication (General Properties)

🚪 Login Properties - webadmi	in	
Select a page	🛒 Script 👻 📑 Help	
General Server Roles User Mapping	Server role is used to grant server-wide security privileges to a user.	
Securables		
Status	Server roles: bulkadmin dbcreator diskadmin processadmin securityadmin setupadmin setupadmin sysadmin	
Connection		
Server: W2K3SERV\W2K3SQL2005 Connection: W2K3SERV\Administrator		
View connection properties		
Ready		
	ОК Са	ancel

Example: MS SQL Server configured as remote database using SQL Server authentication (Server Roles Properties)

🚪 Login Properties - webadmii	n				<u>_ ×</u>
Select a page	<u>S</u> Script 👻	📑 Help			
Server Roles	Users map	ope <u>d</u> to this login:			
Securables	Мар	Database	User	Default Schema	
Status		FSMDB	fsmwebadmin	dbo	
		master			
		model			
		msdb			
		tempdb			
	☐ Guest	account enabled for; FSMD role membership for; FSMDI	B 3		
Connection	db_ac	cessadmin			
Server:	∐ db_ba II db_da	ickupoperator itareader			
W2K3SERV\W2K3SQL2005	v db_da	itawriter			
Connection: W2K3SEBV\Administrator	db_dd	lladmin			
	l ⊡ db_de	nydatareader Invdatawriter			
	✓ db_ov	vner			
Progress	db_se	curityadmin			
Deck	Public				
Heady					
.db.					
				ОК	Cancel //

Example: MS SQL Server configured as remote database using SQL Server authentication (User Mapping Properties)

🚦 Login Properties - webadmir	1			
. Select a page	🔄 Script 👻 📑 Help			
General				
Server Holes	Login <u>n</u> ame: webadn	nin		
Securables	<u>S</u> ecurables:			
📑 Status	Name			Туре
	Effective Perm	issions	<u>A</u> dd	<u>R</u> emove
	Explicit permissions:			
Connection	Permission	Grantor	Grant	With Grant Deny
Server: W2K3SEBV\W2K3SDL2005				
Connection:				
W2K3SERV\Administrator				
View connection properties				
Progress				
Ready				
The start of the s				
				OK Cancel
				///

Example: MS SQL Server configured as remote database using SQL Server authentication (Securables Properties)



Example: MS SQL Server configured as remote database using SQL Server authentication (Status Properties)

JDBC driver

• It is recommended to download the JDBC driver from the website of the database vendor.

AIX

Required Perl version ECM SM server

ECM SM server requires the following software to be installed on the server system:

• perl 5 required but NOT installed during ECM SM server install

Creating filesystems

Please use **smitty** to create the following AIX filesystems for ECM SM server installation:

Filesystem mount point	Filesystem minimum size (in GB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: /tmp)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is /opt/IBM/ECMSM</path></pre>	10.0

If the system temporary filesystem (/tmp) is not big enough to hold the temporarily extracted InstallAnywhere installer files it is possible to set the UNIX environment variable IATEMPDIR to a directory that has enough free space, which then is used as extraction directory instead of /tmp.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Manual adjustments

OS adjustments

Adjust system parameter ncargs

If the value of the system parameter neargs is too low, some monitors may show the error message "arg list too long".

To avoid this message, you should increase the value of neargs to at least 16.

To check for the current value, enter the following command:

lsattr -EH -l sys0 | grep ncargs

or use the AIX smit(ty) tool (run 'smitty system' and then select 'Change show characteristocs of a operating system'.

The value should be 16 or higher. To change the setting of ncargs, enter the following command.

chdev -l sys0 -a ncargs=<value>

This change takes affect immediately and is preserved over boot.

Adjust system parameter maxuproc

If the value of the system parameter maxuproc (maximum allowed processes per user) is too low, processes like monitors, tasks or shell binaries cannot be executed and may hang.

To avoid this error, you should increase the value of maxuproc to at least 1024.

To check for the current value, enter the following command:

lsattr -EH -l sys0 | grep maxuproc

or use the AIX smit(ty) tool (run 'smitty system' and then select 'Change show characteristics of a operating system'.

The value should be 1024 or higher. To change the setting of maxuproc, enter the following command.

chdev -l sys0 -a maxuproc=<value>

This change takes affect immediately and is preserved over boot.

HP-UX

Required Perl and gawk versions ECM SM server

ECM SM server requires the following software to be installed on the server system:

- perl 5 (required but NOT installed during ECM SM server install
- gawk . Please check chapter Requirements of all Server platforms for HP-UX for additional information.

Creating filesystems

Please use **sam** to create the following HP-UX filesystems for ECM SM server installation:

Filesystem mount point	Filesystem minimum size (in GB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: /tmp)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is /opt/IBM/ECMSM</path></pre>	10.0

If the system temporary filesystem (/tmp) is not big enough to hold the temporarily extracted InstallAnywhere installer files it is possible to set the UNIX environment variable IATEMPDIR to a directory that has enough free space, which then is used as extraction directory instead of /tmp.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Installing required Software packages

The software mentioned below is delivered with HP-UX 11 Application Software CDs, or must be downloaded from the HP web site.

NOTE

gawk and the required libraries from the is *only required* if you do not have an awk installed, that can handle more than 3000 bytes per input line.

- gawk (3.1.5) or newer
- libiconv (1.10 or newer) [needed by gawk]

• gettext (0.14.5 or newer) [needed by gawk]

gawk and libraries

Due to limitations of the HP-UX awk tool it is necessary to install gawk, libiconv and gettext fro the HP Web site.

There you will find HP-UX depot files for gawk, libiconv and gettext. Copy or download these files to a directory, where you have write access, and uncompress them with gzip (gunzip); e.g.:

cp *.depot.gz /tmp ; cd /tmp ; gunzip *.depot.gz

Now you can install the software with the HP-UX **swinstall** command, entering the following command at the command line (/tmp/ is only an example path):

swinstall -s /tmp/<package>.depot *

The swinstall command needs the absolute path to the unzipped depot file.

NOTE If you are unfamiliar with the **swinstall** command, read its manual page or ask your HP-UX system administrator for assistance.

After the successful installation of gawk, you must create a symbolic link into /usr/bin/ named nawk, pointing to the gawk executable. Assuming the gawk tool is installed at /usr/local/bin/gawk enter the following:

In -sf /usr/local/bin/gawk /usr/bin/nawk

Control the success by entering the following at the command line:

which nawk

The response from the system should be:

/usr/bin/nawk #

Manual adjustments

Required environment variables

Make sure that the environment variable HOME is set to a valid directory that contains a file named **.rnd**. This file is required during creation of the CALA_REX server SSL certificates and is overwritten during creation of the certificate. The initial file can be any file that is sufficiently large (e.g. a binary).

Redhat Linux

Required Perl version ECM SM server

ECM SM server requires the following software to be installed on the server system:

• perl 5 (required but NOT installed during ECM SM server install

Software installation using 'Normal' Redhat mode

For RHEL 32 and for 64 bit based installations you have to install the following 32 bit package:

• compat-libstdc++-33.i686

For RHEL 32 bit based installations you have to install the following 32 bit packages:

- the file command
- the **perl** interpreter

For RHEL 64 bit based installations you have to install the 64 bit package containing the following components:

- the file command
- the **perl** interpreter

Also, if the error message "Graphical installers are not supported by the vm" is given while the installer tries to start, the following *32 bit* libraries must be installed:

- libXdmcp.i686
- libXext.i686
- libXrender.i686
- libXft.i686
- libXi.i686
- libXt.i686
- libXtst.i686
- libgcc.i686

Redhat Enterprise Linux 7.0 and newer additionally requires the following package:

• libstdc++.i686

These libraries can be installed by the yum package manager from the commandline; e.g.:

```
# yum install libgcc.i686
```

Creating filesystems

Please use cfdisk or fdisk, and mkfs to create the following filesystems for ECM SM server installation:

Filesystem mount point	Filesystem minimum size (in GB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: /tmp)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is /opt/IBM/ECMSM</path></pre>	10.0

If the system temporary filesystem (/tmp) is not big enough to hold the temporarily extracted InstallAnywhere installer files it is possible to set the environment variable IATEMPDIR to a directory that has enough free space, which then is used as extraction directory instead of /tmp.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Solaris

Solaris (all versions)

Required Perl version ECM SM server

ECM SM server requires the following software to be installed on the server system:

• perl 5 (required but NOT installed during ECM SM server install

Solaris 9

Creating filesystems

Please use **smc** (Solaris Management Console, if Solaris Volume Management is used) or **vea** (if the Veritas Volume Manager is installed) to create the following filesystems for ECM SM server installation:

NOTE It is not required but recommended to create these filesystems.

Filesystem mount point	Filesystem minimum size (in GB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: /tmp)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is /opt/IBM/ECMSM</path></pre>	10.0

If the system temporary filesystem (/tmp) is not big enough to hold the temporarily extracted InstallAnywhere installer files it is possible to set the UNIX environment variable IATEMPDIR to a directory that has enough free space, which then is used as extraction directory instead of /tmp.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Installing Solaris patches

Because Solaris 9 does not contain some required libraries and tools the system needs to be updated with the latest Solaris 9 recommended patches (check <u>http://www.sun.com</u> for more details).

Install the Solaris 9 cluster patch (download the latest cluster patch from http://www.sun.com)

NOTE You need to install the Solaris 9 recommended patches in Single user mode (init state *s*).

Log on to the system in single user mode and change into the patch directory, where the cluster patch is extracted.

Execute

./install_cluster

and follow the instructions. After this installation step you need to reboot the system (normal init state)

Installing required Software packages

Perl

Use the following command to check for perl:

pkginfo | grep - perl

The system should print out the following information:

```
SUNWop15m
                                                      SUNWopl5p
                          Perl 5.005_03 Referensystem
system
                                                                        Perl
5.005_03 (POD Dosystem
                         SUNWopl5u
                                     Perl 5.005_03system
                                                              SUNWp15m
                             ______SUNWp15p
                                           Perl 5.6.1 (POD Documsystem
   Perl 5.6.1 Referencesystem
                 Perl 5.6.1 (core)system SUNWpl5v
SUNWpl5u
                                                           Perl 5.6.1 (non-core)
                                Perl 5.005_03
Referensystem
               SUNWop15p
(POD Dosystem SUNWopl5u
Perl 5.005_03system SUNWpl5m
                                      Perl
                                        Perl 5.6.1
5.6.1 Referencesystem SUNWpl5p
                                   Perl
(POD Documsystem SUNWpl5u
5.6.1 (core)system
                   SUNWpl5v
                                     Perl 5.6.1
```

Install missing Perl packages from Solaris 9 Operating System CD 1.

Mount Solaris 9 Operating System CD 1, change into the **Solaris_9/Product** directory and install all missing file packages with the following command

pkgadd -d \$PWD SUNWpl5u SUNWpl5v SUNWopl5u SUNWpl5p

Solaris 10

Creating filesystems

Please use **smc** (Solaris Management Console, if Solaris Volume Management is used) or **vea** (if the Veritas Volume Manager is installed) to create the following filesystems for ECM SM server installation:

NOTE It is not required but recommended to create these filesystems.

Filesystem mount point	Filesystem minimum size (in GB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: /tmp)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is /opt/IBM/ECMSM</path></pre>	10.0

If the system temporary filesystem (/tmp) is not big enough to hold the temporarily extracted InstallAnywhere installer files it is possible to set the UNIX environment variable IATEMPDIR to a directory that has enough free space, which then is used as extraction directory instead of /tmp.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Installing Solaris patches

Because Solaris 10 does not contain some required libraries and tools the system needs to be updated with the latest Solaris 10 recommended patches (check <u>http://www.sun.com</u> for more details).

Install the Solaris 10 cluster patch (download the latest cluster patch from http://www.sun.com)

NOTE You may need to install the Solaris 10 recommended patches in Single user mode (init state *s*).

Log on to the system in single user mode and change into the patch directory, where the cluster patch is extracted.

Execute

./install_cluster

and follow the instructions. After this installation step you need to reboot the system (normal init state)

Installing required Software packages

Perl

Use the following command to check for perl:

pkginfo | grep - perl

The system should print out the following information:
GNOME2 SUNWpe	erl-xml-parser	XML::Parser PERL modu	leGNOME2
SUNWperl-xml-pars	er-devel-share XML::Pars	er PERL module develope	er files – platform
independent files	s, /usr/sharesystem S	UNWper1584core	Perl
5.8.4 (core)syste	em SUNWper1584man	Perl 5.8	.4 Reference Manual
Pagessystem	SUNWper1584usr	Perl 5.8.4 (nor	-core)
PERL moduleGNOME2	SUNWperl-xml-parser-	devel-share XML::Parse	er PERL module developer
files - platform	independent files,		
/usr/sharesystem	SUNWper1584core	Perl	
5.8.4 (core)syste	m SUNWper1584man	Perl 5.8	.4 Reference
Manual Pagessyste	m SUNWper1584usr	Perl	

Install missing Perl packages from Solaris 10 Operating System CD.

Mount Solaris 10 Operating System CD and install all missing Perl file packages with the following command

Manual adjustments

OS adjustments

Verify that OS kernel parameters are configured correctly. In some cases the following parameters need to be specified or adjusted in /etc/system file. Note: Do not decrease the values, if the parameters are specified with higher values.

set rlim_fd_max=4096
set rlim_fd_cur=1024

Note: /etc/system changes require system reboot.

SuSE Linux

Required Perl version ECM SM server

ECM SM server requires the following software to be installed on the server system:

• perl 5 (required but NOT installed during ECM SM server install

Software installation

It is recommended to use SuSE Linux Enterprise Server Version 10 (SLES 10) or 11 (SLES 11).

For SLES 32 or 64 bit based installations you have to install these packages/modules:

- the file command
- the **perl** interpreter
- libstdc++33-32bit

Also, if the error message "Graphical installers are not supported by the vm" is given while the installer tries to start, the following *32 bit* libraries must be installed:

- libXdmcp.so
- libXext.so
- libXrender.so
- libXft.so
- libXi.so
- libXt.so
- libXtst.so
- libgcc.so

These libraries can be installed by the zypper package manager from the commandline or yast2; e.g.:

```
# zypper install libstdc++33-32bit
```

Creating filesystems

Please use yast to create the following filesystems for ECM SM server installation:

Filesystem mount point	Filesystem minimum size (in MB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: /tmp)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is /opt/IBM/ECMSM</path></pre>	10.0

If the system temporary filesystem (/tmp) is not big enough to hold the temporarily extracted InstallAnywhere installer files it is possible to set the environment variable IATEMPDIR to a directory that has enough free space, which then is used as extraction directory instead of /tmp.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Windows

Required Perl version ECM SM server

ECM SM server requires the following software to be installed on the server system:

- perl 5 (automatically installed during ECM SM server installation)
- shell (installed during ECM SM server installation)

Creating filesystems

Please use the **disk management** tool to create the following filesystems for ECM SM server installation:

Filesystem mount point	Filesystem minimum size (in GB)
Filesystem containing Installer images	5.0
Temporary extraction directory (default: %TEMP%)	up to 3x the size of the installer image
<pre><path directory="" ecm="" installation="" server="" sm="" to="" your="">, default location is C:\Program Files\IBM\ECMSM</path></pre>	10.0

If the system temporary filesystem (%TEMP%) is not big enough to hold the temporarily extracted Instal-IAnywhere installer files it is possible to set the environment variable TMP to a directory that has enough free space, which then is used as extraction directory instead of %TEMP%.

The required database filesystem size depends on the database vendor, number of client and events handled by the ECM SM server.

Preliminary Considerations

Enhanced security - FIPS 140-2 compliant password encryption

Why must ECM SM store passwords?

Some ECM SM components, especially monitors, need access to services that are protected via credentials. E.g. a database monitor must log-in at the database to check if it is available.

Therefore the credentials (user and password) need to be stored in the configuration files. Although the credentials are stored encrypted, it is recommended to use a technical user with limited permissions for monitoring.

Improper chracters within passwords

The special characters double quotes ("), Dollar sign (\$), semi colon (;), hash (#) and grave accent (`) are not supported within passwords.

FIPS-140-2 compliant password encryption

ECM SM uses a FIPS-140-2 compliant encryption when storing passwords. There are three keys that are needed to encrypt sensitive data. All of these keys are also needed to decrypt the data.

username or filename

The first key is the username or filename the password is associated with.

keyfile

There is a key file in each ECM SM agent and server installation which contains the second key that is used for encryption. The key within this file is created at installation time and is specific to the ECM SM installation. The keyfile is stored in the **.keys** subdirectory of the server or agent installation. It is recommended to protect this directory using the operating system specific methods to avoid other users than the user running the agent having access to the keyfile.

The keyfile for an agent is generated by the server and stored on the agent by 'Accepting' an agent in the 'Connected Agents' view.

the agent id

The key within the keyfile is encrypted with the agent id of the ECM SM.

ECM SM uses a AES-128 algorithm twice with different keys (username/filename and keyfile content) to encrypt passwords.

Migration of configuration files from ECM SM prior 5.2

Prior versions of ECM SM used an other mechanism for password encryption. Passwords from older version can still be decrypted by the current version of ECM SM. So all monitors and tasks will still work. Once the configuration is changed, passwords are stored using the new algorithm described above. This requires an upgraded agent, use the task 'Upgrade CALA_REX Agent' to upgrade an old ECM SM agent.

SSL authentication in CALA_REX

Basics - How SSL authentication works

Overview

SSL authentication uses certificates and certificate chains. Each certificate must be signed by another certificate except of so called root certificates, which is self-certified.

The authenticity of an certificate can be verified by following the certificate chain up to one certificate which is known to be trustworthy.



A simple certificate chain for authenticating a client



Another example for certificate chains when authentication clients



Another certificate chain example with a longer certificate chain

For a further control, the applications should also do some additional checks after the validity of the certificates has been approved. It could for example check if the ip address or hostname of the client is the same as specified in the certificate. This avoids clients from connecting with a certificate copied from another client.

Certificate files

While installation, the following files are created in the keys subdirectory of the ECM SM server installation directory.

- **root_cert.pem**: the certificate of the root ca
- **root_cert.srl**: the serial number file of the root ca
- root_key.pem: the private key for the root certificate
- **serverca_cert.pem**: the server ca certificate
- serverca_cert.srl: the serial number file for the server ca
- serverca_key.pem: the private key for the server ca certificate

- trusted_cas.pem: the certificates of trusted cas (includes root_cert.pem and serverca_ cert.pem)
- cala_rex_srv_cert.pem: the certificate used by CALA_REX server
- **cala_rex_srv_priv.pem**: the private key of the CALA_REX server certificate file
 - **NOTE** The files starting with **root**_ should be moved to a safe place after successful installation. They are useful, if the server ca certificate is compromised.

See Creating an SSL certificate for the agent for a description for creating SSL certificates for clients.

The default passwords for the private keys

This table shows the default passwords for the private keys as they are created while installation of CALA_REX server and client.

root_key.pem	cAlarEXr00TCaPAssw0Rd
serverca_key.pem	cAlarEXSerV3rCaPAssw0Rd
cala_rex_srv_priv.pem	cAlarEXseRverPAssw0Rd
cala_rex_cli_priv.pem	cAlarEXcL1entPAssw0Rd

Integrating CALA_REX into an existing public key infrastructure

For integrating ECM SM into an existing public key infrastructure, the following files must be created:

- trusted_cas.pem: the certificates of trusted certificate authorities in PEM format
- **cala_rex_srv_cert.pem**: the certificate used by CALA_REX server in PEM format
- **cala_rex_srv_priv.pem**: the private key of the CALA_REX server certificate file in PEM format

The files need to be copied to the **keys** subdirectory of the ECM SM installation directory. If done so before the installation of CALA_REX server software, the files are detected while installation and are not replaced.

Certificate requirements

Custom generated certificates need to have some fields set to specified values when used with CALA_REX. See the sections below for a description of this fields. Certificates and certificate chain files used with CALA_REX need to be stored in the PEM format.

CALA_REX server

- the *commonName* field must contain the servers' hostname
- for each network interface CALA_REX server listens on, a *subjectAltName* entry must be present
- for each hostname alias of the ECM SM server, a *subjectAltName* entry must be present
- the *extendedKeyUsage* field must contain the entry for server authentication (OID 1.3.6.1.5.5.7. 3.1)

CALA_REX client

- the *commonName* field must contain the clients' hostname
- the network interface which is used to connect to CALA_REX server, a *subjectAltName* entry must be present
- for each hostname alias of the ECM SM client, a *subjectAltName* entry must be present
- the *extendedKeyUsage* field must contain the entry for client authentication (OID 1.3.6.1.5.5.7.3.2)

Configuration details for CALA_REX clients and servers

Default configuration

To make the user's life as easy as possible, the default configuration should work the following way:

- the default names for certificate files are:
 - **\$CENIT_ROOT/keys/trusted_cas.pem** (ECM SM client and server)
 - \$CENIT_ROOT/keys/cala_rex_srv.pem (ECM SM server only)
 - \$CENIT_ROOT/keys/cala_rex_cli.pem (ECM SM client only)
- if the necessary certificate files are found, CALA_REX automatically switches to authenticated mode
- using the default configuration, the server accepts both authenticated and anonymous client and application connections
- The certificates created by the webconsole have a well defined format. The default configuration verifies the certificate using fields from this format, further configuration is only needed, when a customer uses self created certificates.

new configuration parameters for CALA_REX clients and servers

	Les este d'a s	
name	aescription	default value
hostdb.col.ciphers	The database column to receive the cipher algorithms used on the client connection (CALA_REX server only)	CSM_CIPHERS
hostdb.col.cert	The database column to receive the client's certification data (CALA_REX server only)	CSM_CERT
ssl.allowanoncnx	Specifies for which connection types anonymous connections are allowed. One of the values: none, application, client, client_and_application (CALA_REX server only)	client_and_application
ssl.trustcert.file	The file containing a trusted cer- tificate	\$CENIT_ROOT/keys/trust- ed_⊣ cas.pem
ssl.trustcert.dir	A directory containing trusted cer- tificates	NULL
ssl.cipherlist	The list of ciphers to use (see OpenSSL documentation)	ALL:!LOW:!EXP:! MD5:@STRENGTH
ssl.verifydepth	The maximum length of the verify chain.	3
ssl.certificate	The certificate to be sent to the connection peer	\$CENIT ROOT/keys/cala rex_srv cert.pem (SrV) \$CENIT ROOT/keys/cala rex_cli
aal kovatoro	The keystore containing the pri-	cert.pem (Cli)
SSI.NEYSLUIE	vate key	<pre>\$CENIT ROOT/keys/cala rex_srv priv.pem (SrV) \$CENIT ROOT/keys/cala rex_cli priv.pem (Cli)</pre>

name	description	default value
ssl.keystore.password The (pwdcrypt encrypted) pass- word for the keystore.		
		11201e1900242a1b3e50171606₊ 31330b0116422a1600 (Cli)

Integrating ECM SM into an existing authentication system

The user management of ECM SM can be configured to used existing directory services for user authentication.

The currently supported directory services are:

- IBM Tivoli Directory Server
- Microsoft Active Directory Service
- Sun Java Directory Server
- Novell eDirectory Server
- the ECM SM native authentication service

See section Configuring LDAP authentication in the chapter Installing ECM SM Server.

The default roles used by ECM SM

The roles listed below are preconfigured afterECM SM installation. These roles may be modified or additional roles may be added afterwards.

fsm_user

User role for ECM SM WebConsole. Allow basic access to the web server (login, logout), see hosts and events.

fsm_operator

Operator role for ECM SM WebConsole. Additional right to acknowledge events and to see *Current CALA_REX Hosts*.

fsm_admin

Administrator for ECM SM WebConsole monitoring. Execute any CALA_REX action, close events, delete monitors and manage hosts.

fsm_useradmin

Administrator for ECM SM WebConsole monitoring and web server administration. Additional right to manage user (create, change and delete).

Installing ECM SM Server

Installation Prerequisites

Ensure all prerequisites listed in chapter Installation Requirements and Server Preparation are fulfilled.

Server Installation process

Starting the installer

During ECM SM server installation the following components will be installed and configured:

- JDBC parameters and the JDBC database connection to the database will be checked
- ECM SM Web Console will be installed and services will be created (unless WebSphere based installation is selected).
- ECM SM WebSphere application archives will be created (if WebSphere based installation is selected).
- All agent install and configuration files including the agents and platform specific JRE archives
- Database tables will be created and data will be imported (unless DDL-creation only is specified)
- ECM SM CALA_REX Server agent will be installed, configured and started

Note: for full ECM SM server installation you'd need the following three InstallAnywhere install Images:

ECM SM server install image

This platform specific installer image contains all server-related components.

ECM SM All JRE's archives

This package contains JRE archives for all platforms. These archives are required for using ECM SM Admin GUI tools and to update existing ECM SM CALA_REX 4.0x agents.

Note: There is a Windows-based JRE-archives InstallAnywhere install image and an All-UNIX InstallAnywhere install image available.

This installation image can automatically be installed as sub-package of the ECM SM server install image. If installed separately on UNIX systems this image requires manual extension of the system variable PATH to a Java JRE version 7 binary, which is required during installation. Note: Add the Java JRE installation directory \$CENIT_ROOT/jre/bin provided by the server installer to the path variable.

ECM SM CALA_REX All agents images

This installation image contains CALA_REX agent InstallAnywhere images for all platforms. This Image is required, if any kind of agent (managed systems) is to be installed.

Note: There is a Windows-based CALA_REX InstallAnywhere install image and an All-UNIX Instal-IAnywhere install image available.

This installation image can automatically be installed as sub-package of the ECM SM server install image. If installed separately on UNIX systems this image requires manual extension of the system variable PATH to a Java JRE version 7 binary, which is required during installation. Note: Add the Java JRE installation directory \$CENIT_ROOT/jre/bin provided by the server installer to the path variable.

If you do not have enough temporary space at /tmp (UNIX/Linux) you can specify the variable IATEMPDIR, that should point to a filesystem with enough space to extract the installAnywhere archive.

If you do not have enough temporary space at %TMP% and %TEMP% (Windows) you have to set the variable TEMP and TMP. The variables must point to a local partition with enough space to extract the installAnywhere archive. The directory cannot be located on a file share, it must be on a local disc.

Starting the InstallAnywhere install image on UNIX:

./IBM_ECM_SM_SERVER.bin

Starting the InstallAnywhere install image on Windows:

./IBM_ECM_SM_SERVER.exe

NOTE If using Windows 2012 as operating system, set the compatibility mode to "Windows 7" in the properties of the file "IBM_ECM_SM_SERVER.exe".

Files Currently	on the Disc (2)			
IBM_ECM_SM-	5.2.0-001-Win	27.04.2015 15:49	Application	979.458 KB
BM_ECM_SM-	5.2.0-001-Win.exe.MD5	27.04.2015 15:49	MD5 File	1 KB
	 BM_ECM_SM General Compatibility If this program isn't work try running the compatibility round Run compatibility trout How do I choose compatibility mode Compatibility mode Run this program in Windows 7 	1-5.2.0-001-Win Pro Details king correctly on this vers bility troubleshooter. bleshooter tibility settings manually? n compatibility mode for:	ion of Windows,	
	Settings Reduced color mod S-bit (256) color Run in 640 x 480 se Disable display scal Enable this program Run this program a Change settings for	le creen resolution ling on high DPI settings in to work with SkyDrive fi is an administrator is all users OK Cancel	les Apply	

Changing the Compatibility Mode for the InstallAnywhere install image on Windows:

InstallAnywhere options:

-D NOADDITIONALSPACE=true

Normally the installer including sub-images requires a lot of free space in the installation directory. If you'd want to overwrite an existing installation (same or previous version) than you can force the installer to just check for the minimum free space in the installation directory. Set the variable NOADDITIONALSPACE to true.

After starting the InstallAnywhere install image the Intro panel is displayed.

InstallAnywhere	and the second s	
() "	nstallAnywhere bereitet die Installation vor	
	81%	
		Abbrechen
(C) 2012 Flexera	Software LLC	

ECM SM Installation: Intro panel

The ECM SM splash image is displayed short term afterwards.



ECM SM Installation: ECM SM Splash screen

You'd need to confirm the ECM SM license agreement to proceed with the installation.

IBM Enterprise Content Manager	ment System Monitor Server
	Softwarelizenzvereinbarung
	Please read the following license agreement carefully.
	International Program License Agreement
IBM.	Part 1 - General Terms
Enterprise Content Management System Monitor	BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
	* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND
	* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT FAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.
	1. Definitions
	"Authorized Use" - the specified level at which Licensee is authorized 🔻
	I accept the terms in the license agreement.
	I do not accept the terms in the license agreement.
	Print
InstallAnywhere	
Cancel Help	Previous Next

ECM SM Installation: ECM SM license agreement

Carefully read the license agreement and select I accept ... and press Next to continue or press I do not accept ... or cancel to exit the installation.

A short introduction text is displayed on the next panel. Press the 'Next' button to proceed.

IBM Enterprise Content Manager	nent System Monitor Server
	Introduction
	InstallAnywhere guides you through the installation of IBM Enterprise Content Management System Monitor Server.
	It is strongly recommended to close all programs before you proceed with the installation.
Enterprise Content Management	Press 'Next' to open the next windows, press the 'Previous' button if you want to re-open the previous window.
System Monitor	You can stop the installation at any time by pressing the 'Cancel' Button.
	Help for the displayed panel is available through the 'Help' button.
InstallAnywhere	
Cancel Help	Previous Next

ECM SM Installation: Introduction screen

Detecting previous installations

The installer detects previously installed ECM SM server components.

IBM Enterprise Content Managen	ment System Monitor Server	
	Update / Reinstallation of t	he product
Elever Enterprise Content Management System Monitor	Update / Reinstallation of t An existing 4.5+ ECM SM installation at location C:\Program Files (x86)\IBM\ECMSM was detected. Please select one of the following options: New Install Selecting 'New Install' means that the previous installation of ECM SM server at C:\Program Files (x86)\IBM\ECMSM can no longer be used, because only one ECM SM server installation instance is supported on a server. Note: The previous installation directory will be unchanged, until a new installation directory is selected.	ne product
InstallAnuukara		
Cancel Help	Previous	Next

ECM SM Installation: Installation type screen - New Install

If this is not an initial installation of the software on this system you can select the installation type.

IBM Enterprise Content Manager	nent System Monitor Server
	Update / Reinstallation of the product
IBM.® Enterprise Content Management	An existing 4.5+ ECM SM installation at location C:\Program Files (x86)\IBM\ECMSM was detected. Please select one of the following options:
System Monitor	Reconfigure Only
	Reconfigure only means the installer will not install components of ECM SM on the system into the existing installation directory C:Program Files (x86)JBMECMSM. This selection is used to change global configuration settings (ports, LDAP settings, etc) of the installation. Note: Activating the 'Re-Initialize Database' will delete all existing data.
	If you'd want to re-initialize the database activate check the following checkbox!
InstallAnywhere	Provious Nevt
	T TEVIOUS TVEAL

ECM SM Installation: Installation type screen - Reconfigure Only

In the case the system detects an previous installation the installation type 'Reconfigure Only' can be selected.

Note: Only check the 'Re-Initialize database', if you want to clear the complete database.

IBM Enterprise Content Managem	ment System Monitor Server	. • X
	Update / Reinstallation of th	e product
IBM. Enterprise Content Management	An existing 4.5+ ECM SM installation at location C:\Program Files (x86)\IBM\ECMSM was detected. Please select one of the following options:	
System Monitor	Upgrade Update means the installer will use the existing installation directory C:Program Files (x86)\IBM\ECMSM. All product components will be installed and configured again. Existing service / agent settings will be removed and installed again. Note: This selection will update the existing database including content! It is recommended to create a backup before you proceed.	
InstallAnywhere Cancel Help	Previous	Next

ECM SM Installation: Installation type screen - Upgrade

If you want to upgrade an existing installation select the installation type 'Upgrade'.

Configuration Options

Setting the installation directory

IBM Enterprise Content Managemen	nt System Monitor Server	Terms.	
		Insta	llation folder
Enterprise Content Management	Please specify the ECM SM server installation folder.		
System Monitor	Vhere do you want to install the ECM SM server component	s?	
	C:\Program Files (x86)\IBM\ECMSM		
		Restore Default Folder	Choose
InstallAnywhere		Drov forum	Next
Cancel Help		Previous	Next

ECM SM Installation: Specify the installation folder

Select Choose... to adjust the installation location of the ECM SM software and click the Next button.

NOTE Press **Restore Default Folder** to reset the selected installation folder.

Selecting the Server installation type



ECM SM Installation: Specify the Server installation type (Complete installation)

Adjust the detected full qualified hostname, in the case the detected network settings aren't correct. Enable of disable the checkbox 'Enable ECM SM server installer debugging' in the case you expect issues or you need additional installation information.

Select *Complete installation* in the case you want to install all ECM SM Server components. All components are: Database initialization, CALA_REX server, Event Server and GUI Server. A ECM SM CALA_REX Agent can optionally be installed on the server by activating the corresponding checkbox.

IBM Enterprise Content Manager	ment System Monitor Server
	Select Installation type and local host name
	Select one of the available installation types
Enterprise Content Management System Monitor	Local Hostname (correct name resolution required - full qualified host name) N7P00157B64BIT.de.cenit-group.com
	 Enable ECM SM Server installer debugging Primary Server - Core component installation Primary Server contains the following components: CALA_REX Server, Database initialization, Download Server. Optionally the Download Server can be replaced by the GUI Server component. Note: This installation type requires at least another installation on a remote system running the Event Server and the GUI Server component (unless the Download Server wasn't replaced ba the GUI Server).
	It is recommended to install a CALA_REX agent to be able to monitor and controll Server components.
InstallAnywhere	Add CALA_REX Agent - recommended for all Servers

ECM SM Installation: Specify the Server installation type (Primary Server installation)

Adjust the detected full qualified hostname, in the case the detected network settings aren't correct. Enable of disable the checkbox 'Enable ECM SM server installer debugging' in the case you expect issues or you need additional installation information.

Select *Primary Server - core component installation* in the case you want to install only the core ECM SM Server component. Minimum core components are: Database initialization, CALA_REX server, Download Server or optionally instead of the Download Server a GUI Server.

NOTE The Primary Server is a subset of the Complete installation, without an additional GUI Server and Event Server installation as Secondary Server installation the ECM SM System architecture is not complete. A ECM SM CALA_REX Agent can optionally be installed on the server by activating the corresponding checkbox.

IBM Enterprise Content Manager	ment System Monitor Server
	Select Installation type and local host name
IBM _e	Select one of the available installation types
System Monitor	Local Hostname (correct name resolution required - full qualified host name) N7P00157B64BIT.de.cenit-group.com Finable ECM SM Server installer debugging
	Secondary Server - select dedicated components Secondary Server means the components GUI Server, Event Server and / or CALA_REX Agent can be installed locally. A communication to the Primary Server is required during the installation, the CALA_REX Server Service / daemon has to run on the Primary Server. It is recommended to install a CALA_REX agent to be able to monitor and controll Server
	Image: Add Event Server component Image: Add GUI Server component Image: Add CALA_REX Agent - recommended for all Servers
InstallAnywhere	Previous Next

ECM SM Installation: Specify the Server installation type (Primary Server installation)

Adjust the detected full qualified hostname, in the case the detected network settings aren't correct. Enable of disable the checkbox 'Enable ECM SM server installer debugging' in the case you expect issues or you need additional installation information.

Select Secondary Server - select dedicated components in the case you want to install ECM SM an Event Server and / or GUI Server component. A ECM SM CALA_REX Agent can optionally be installed on the server by activating the corresponding checkbox.

IBM Enterprise Content Manager	ment System Monitor Server
	Specify Update settings for existing server
	The installer found an existing ECM SM Server installation at C:\Program Files (x86)\IBM\ECMSM.
IBM.	Adjust or confirm the full qualified hostname and debugging settings of the installer.
System Monitor	Local Hostname (correct name resolution required - full qualified host name)
	N/PUU15/B64B11.de.cenit-group.com
	Enable ECM SM Server installer debugging
	Install a CALA_REX Agent to the Server to be able to monitor and automatically restart Server components (fixed Service-Prefix: _srvagnt, Agent CALA_REX port: 23804)
	Install CALA_REX Agent on the Server system
InstallAnywhere]
Cancel Help	Previous Next

ECM SM Installation: Specify Update settings for existing server (5.1 Upgrade installation)

Adjust the detected full qualified hostname, in the case the detected network settings aren't correct. Enable of disable the checkbox 'Enable ECM SM server installer debugging' in the case you expect issues or you need additional installation information.

A ECM SM CALA_REX Agent can optionally be installed on the server by activating the corresponding checkbox.

Setting the installation directory

IBM Enterprise Content Manageme	ent System Monitor Server	x
	Specify the Primary Server informat	ion
IBM.	Please specify the required information from the primary server. Note: the values are required and cannot be specified later. The Primary server components have to be started, network access is mandatory.	
System Monitor	Primary Server name (full qualified hostname) N7P00157B64BIT Primary Server CALA_REX Port 23802 Primary server administrative user name admin Primary server administrative password •••••	
InstallAnywhere Cancel Help	Previous Next	

ECM SM Installation: Specify the Primary Server settings for a Secondary Server installation

In the case a Secondary Server installation the installation process need CALA_REX communication to the Primary Server. Therefore specify the full qualified Primary Server name and the Primary Server CALA_REX port (Default value 23802). In addition the administrative user account and password has to be specified to download required files (settings information, JDBC driver files, etc) from the Primary Server. Once you specified the parameters click the **Next** button. The download will proceed. In the case of an error a error panel will be displayed and the installer will go back to the Settings panel. Correct the settings in this case and / or verify the network communication and check whether CALA_REX Server is activated on the Primary Server.

Configuring basic ECM SM parameters

The next four panels show the *Basic ECM SM Server Settings*. The first screen shot shows the basic parameters, if the *Embedded Jetty Server* is selected as web application server to be used.

IBM Enterprise Content Manager	nent System Monitor Server
	Primary Server Basic settings
IBN.	Specify the appropriate ECM SM server settings here.
System Monitor	Mich Application Corport to a
	Embedded Jetty Server
	ECM SM Web Server GUI and download port 23990
	Unsecure / http access
	Event Reception Port (Monitoring / CALA) 23840
	Optional: Services/Agents User (required for MSSQL Windows authentication) .\srvuser
	Windows only: Password of Services/Agents user
	CALA_REX Server port 23802
	If the system has more than 1 network adapter, but CALA_REX needs to be bound to one specific adapter specify the IP address of the adapter here (IP version 4 only) Optional: CALA_REX IP address
InstallAnywhere	
Cancel Help	Previous Next

ECM SM Installation: Basic Settings for Unsecured / HTTP-based Jetty Web Server

Embedded Jetty Server

The embedded *Jetty Web Application Server* will be used as *GUI* and *Event Server* web application server.

IBM WebSphere

An existing *IBM WebSphere Application Server* will be used as *GUI* and *Event Server* web application server.

NOTE The license for the IBM WebSphere Application Server needs to be purchased separately. See *Hardware and Software Requirements Guide* for information about supported IBM WAS versions.

If Embedded Jetty Server with Unsecure / HTTP access is selected, the GUI port must be specified.

ECM SM Web Server GUI and Download Port

Default value is 23990, any unused port can be chosen.

IBM Enterprise Content Managen	nent System Monitor Server
	Basic Server settings
IBM. Enterprise Content Management	Specify the appropiate ECM SM server settings here.
System Monitor	Web Application Server type
	Embedded Jetty Server
	ECM SM Web Server GUI and download port 23990
	Secured / https access
	Specify either an existing keystore or a new keystore to be created
	Full qualified keystore file name including path
	Restore Default Choose
	✓ Generate specified keystore
	Keystore password
	Optional: SSL key password. If unset the store password will be used.
	Event reception port (CALA) 23840
	ECM SM Server name N7P0015764Bit.de.cenit-group.com
InstallAnywhere	
Cancel Help	Previous Next

ECM SM Installation: Basic parameters for secured / HTTPS-based Jetty Web Server

If Jetty Web Application Server with Secured / HTTPS access is selected, the following additional parameters need to be specified:

ECM SM Web Server GUI and Download Port

Default value is 23990, any free port can be chosen.

Full Qualified Keystore File Name

Specify the full qualified file name of the keystore file.

Generate Specified Keystore

Check the checkbox in the case, the installer shall create a temporary script, that contains the commando to generate the keystore file.

Keystore Password

Required: Specify the password of the keystore.

Optional: SSL Key Password

The SSL key password of the Jetty application. If unset, the keystore password will be used.

Event Reception Port (Monitoring / CALA)

This port is used to receive events from agents (managed systems). The default value of the ECM SM server monitoring port (CALA Port) is 23840

Checkbox: Enable or disable Allow only current CALA_REX Agents

Check this, if only the newest version of the CALA_REX Agent should be allowed to connect to the server. Don't enable this checkbo ig you plan to connect old agents.

NOTE This option isn't available during upgrade installation.

ECM SM Server Name

This parameter contains the full qualified IP name of the ECM SM server

Checkbox: Enable or disable ECM SM Installation Debugging

Check this, if you encountered issues installing ECM SM Server for detailed information / logging.

NOTE Checking this checkbox does not enable debugging of the application itself.

Optional: Services / Agents User

If this parameter is specified, the services / agents will be installed via this user account. Otherwise the service / daemon will be started as *Local System* (Windows) or *root* (UNIX / Linux). For Windows domain accounts use either <*domain-name*>\<*user-name*> Or <*user-name*>@<*domain-name*>.

- **NOTE** On Windows systems the installing user as well as the service user need to be member of the Administrators and Users groups (or have corresponding permissions) and must also have the *Log on as a service* permission.
- **IMPORTANT** MS SQL Server *Windows Authentication* requires this parameter to be set.

Windows Only: Password of the Services User

On Windows-based systems the password is required, if a Services / Agents User is specified.

CALA_REX Server Port

This parameter defines the server-side port of the agent that is responsible for agent installation, task execution and other action taken on agents.

	See documentation for further information regarding CALA_REX Server libpathadd variable. Optional: CALA_REX libpathadd variable: CALA_REX additional parameters	
	Authentication / LDAP No LDAP / ECM SM internal authentication	ш
	Enable RAP (WEB GUI) OSGi console Enable EventServer OSGi console	
	Enable ECM SM Event Server and GUI Debugging	•
InstallAnywhere Cancel Help	Previous Next	

ECM SM Installation: Basic Server Settings (All Web Application Servers)

Optional: CALA_REX IP Address

If specified, the CALA_REX agent is bound to this IP address only. Specify a value here, if a *multi-IP* address system should be bound to one specific IP address only.

NOTE Use 0.0.0, if the CALA_REX service shall bind to all network devices.

Checkbox: CALA_REX Additional Parameters

If checked, you can specify another CALA_REX relevant property and its value.

The next *Basic Server Settings* screen shot shows the required parameters, if *IBM WebSphere Application Server* is selected as web application server.

	ł	Basic Server se	ttings
	Presify the engraphists FCH CH converte attings here		
	Specily the appropriate ECM SM server settings here.		
System Monitor			
	Web Application Server type		<u> </u>
	IBM WebSphere		-
	WebSphere Server name (hostname) N7P0373464BIT.de.cenit-group.com		
	WebSphere Server port 23990		_
	ECM SM GUI application context root ECM_SM_SERVER		
	Datasource name ECM_SM_DS		
	ECM SM download port 23990		
	Event reception port (CALA) 23840		
	ECM SM Server name N7P0373464BIT.de.cenit-group.com		
	Enable ECM SM Server installer debugging		
	Optional: Services / Agents User (required for MSSQL Windows authentication)		_
			-
InstallAnywhere			
Cancel Help		Previous	ext

ECM SM Installation: IBM WebSphere AS Parameters

WebSphere Server Name (Hostname)

Specify the IP or hostname of the IBM WebSphere Application Server, on which the ECM SM enterprise applications will be deployed.

WebSphere Port

The default value is 9080. Verify the port settings via your WAS Administrator.

ECM SM GUI Application Context Root

Default value of the context root is ECM_SM_SERVER. This is the name of the ECM SM GUI enterprise application within *WebSphere Application Server*.

WebSphere Datasource Name

A data source with this name needs to be defined within *IBM WebSphere Application Server* for the database connection. The creation of a data source is described in the Creation of a datasource on IBM WebSphere chapter.

NOTE All data source settings should match the database settings specified later.
ECM SM Download Port

The JRE archives and CALA_REX agent installer packages, located on the *ECM SM Server*, are downloaded from this port. This is a minimized Embedded *Jetty Web Application Server* running on the *ECM SM Server*.

The third Basic Server settings screen shot shows the lower part of the scroll area. It contains the LDAP authentication type parameter and two parameters for debugging and advanced server settings.

	See documentation for further information regarding CALA_REX Server libpathadd variable. Optional: CALA_REX libpathadd variable: CALA_REX additional parameters	
	Authentication / LDAP	
	Enable RAP (WEB GUI) OSGi console	
	Enable EventServer OSGi console	
InstallAnywhere	Enable ECM SM Event Server and GOI Debugging	*
Cancel Help	Previous	Next

ECM SM Installation: Basic server settings lower screen area

Enable RAP (Web GUI) OSGi Console

Check this box, if you want to enable ECM SM RAP (Web GUI) service/agent OSGi console. For further information about OSGi consoles see the related chapter.

Enable Server OSGi Console

Check this box, if you want to enable ECM SM Server service/agent OSGi console. For further information about OSGi consoles see the related chapter.

Enable ECM SM Event Server and GUI Debugging

Enabling this will slow down the performance of the *ECM SM Event Server* and *GUI component*. This parameter should only be activated for debugging purposes. If you have this option enabled, check whether the debug ports for Java remote debugging are set correctly for the Event Server and GUI debugging on the **Advanced Server Settings** panel. You may use the default debug port values.

Furthermore, the enabled option will activate trace files for the Event Server and GUI component, i.e. the **\$CENIT_ROOT/<component_name:** gui or eventserver>/cfg/logging.conf file will be adjusted automatically during the installation process to enable tracing.

NOTE This feature takes effect without defining any additional ports.

0001	# Adjustment of logging.conf trace file entry depending on selected ${\scriptscriptstyle {\rm cl}}$
	or deselected installer option:
0002	<pre>de.cenit.eb.sm.finca.helper.loghandler.TraceFileHandler.level = OFF</pre>
0003	# Trace files are deactivated (default value - unchecked "Enable $_{ m a}$
	Event Server and GUI Debugging" checkbox)
0004	<pre>de.cenit.eb.sm.finca.helper.loghandler.TraceFileHandler.level = FINE</pre>
0005	# Trace files are activated (checked "Enable Event Server and GUI $_{\!$
	Debugging" checkbox)

To disable tracing, set the value of the variable above back to OFF after you finished debugging.

In case, secure LDAP over SSL is selected from the drop-down list box under Authentication / LDAP, additional *Basic Server Settings* are displayed (further LDAP parameters) beneath.

	Authentication / LDAP	
	LDAP OVER SSL	
	Keystore file including full path	
	C:\/daptrust\/dap	
		Restore Default Choose E
	Password of Keystore	
	Configure advanced Server settings	
	Enable RAP (WEB GUI) OSGi console	-
InstallAnowhere		
Cancel Help		Previous Next

ECM SM Installation: LDAPS Keystore parameters

In case, you selected the secure Jetty-based implementation and checked the Generate specified keystore checkbox, the following panel will be displayed:

IBM Enterprise Content Managen	nent System Monitor Server			
Manual creation of your keystore for the Jetty Application Server				
LIBITE Enterprise Content Management System Monitor	Manual creation of your keystore for the Jetty Application Server Please open a Windows Comamnd rompt (CMD.exe) NOW and execute the following command: C:\Users\faas\AppData\Local\Temp\112303.tmp\createkey.cmd The script will prompt for several parameters. It is absolutely required that you enter the exact values provided below: Parameter 1: N7P0015764Bit.de.cenit-group.com Parameter 3: IBM ECM SM Parameter 4: Press enter without typing any value Parameter 6: Press enter without typing any value Parameter 6: Press enter without typing any value Confirmation: Specify the language specific requested confirmation string (yes, ja, si, etc)			
	Press the 'Next' button after you've created the key store. The command will create the previously configured keystore file. Press the 'Next' button to proceed.			
InstallAnywhere Cancel Help	Previous			

ECM SM Installation: Jetty keystore generation instructions (Windows)

A similar panel will be opened for UNIX/Linux-based systems with instructions about the creation of the keystore. Do not proceed without successful manual execution of the displayed command.

Configuring event forwarding

The next four screen shots show the ECM SM event forwarding functionality.

Detailed event forwarding setup like Recipients, etc is done in the ECM SM Event Console after setup.

Event forwarding as E-Mail

The first event forwarding settings screen shows the required SMTP (email) forwarding parameters.

IBM Enterprise Content Manager	ment System Monitor Server	×
	Event forwarding set	tings
	Specify the ECM SM event forwarding settings here.	
IBM.		
System Monitor		
	Forwarding via Email (SMTP)	<u> </u>
	Enable Email Forwarding (SMTP)	
	SMTP Server name (full qualified DNS name) mysmtp.example.com	
	SMTP Server port 25	
	SMTP email account to forward events ecmsm@examply.com]
	SMTP authentication user (optional) ecmsm	E
	Password of authentication user]

ECM SM Installation: SMTP (eMail) Event forwarding

The following SMTP parameters are required for email forwarding.

SMTP full qualified IP Server name

Specify the name of the email server

SMTP Server port (default: 25)

Specify the port of the SMTP server to be used

SMTP email address to be used

Specify the email-address to be used, e.g. myaccount@domain.com

SMTP Authentication method

Select on of the supported authentication methods (LOGIN, PLAIN, DIGEST-MD5, NTLM or SASL) or 'Disable SMTP authentication'. If authentication is enabled the following two parameters (SMTP user and password) are required.

SMTP Authentication user

If Email authentication is required use this email account to authenticate emails

Password of the SMTP authentication user

Use this password to authenticate the user.

NOTE The password will be displayed shadowed.

Event forwarding via SNMP

The second Event forwarding settings screen shows SNMP (Simple Network Management Protocol) parameters.

IBM Enterprise Content Manager	nent System Monitor Server
	Event forwarding settings
	Specify the ECM SM event forwarding settings here.
IBM.	
Enterprise Content Management	
System Monitor	
	Forwarding via SNMP protocol
	Enable SNMP Event Forwarding
	SNMP Server name or IP address 10.23.30.40
	SNMP Version 2C Inform
	SNMP port 161
	SNMP Enterprise OID 1.3.6.1.4.1.8235

ECM SM Installation: SNMP Event forwarding

The following SNMP parameters are required for SNMP-Trap forwarding.

SNMP manager full qualified IP name

Specify the name of the SNMP manager to be used for SNMP forwarding.

SNMP type

Select one of the following SNMP types from the list: SNMP v1, SNMPv2 or SNMPv2 Inform Contact your SNMP Manager administrator for further information about SNMP versions

SNMP manager port (default: 162)

Specify the required SNMP port of the server

SNMP OID (default: 1.3.6.1.4.1.8235)

You may want to adjust the SNMP OID. If you change the OID you'd need to adjust the prepared SNMP MIB and trap definition files shipped with the product

Event forwarding to HP Operations (HP OVO)

The third Event forwarding settings screen shows HP Operations (HP OVO) settings.

	Forwarding to HP OVO
	Enable Forwarding to HP OVO
	HP OVO Server name (full qualified DNS name) myovoserv.example.com
	HO OVO port 381
	HO OVO Java library directory (location of jopcagtbase.jar and jopcagtmsg.jar)
	C: \ovolibs
	Restore Default Choose
	*
InstallAnywhere	
Cancel Help	Previous Next

ECM SM Installation: HP OVO Event Forwarding

Event forwarding to HP Operations (HP OVO Forwarding) depends on the following parameters.

HP OVO server name

Full qualified name of the HP OVO server

HP OVO port (default: 381)

Specify the HP OVO server port

HP OVO Java Library directory

Specify the directory where the HP OVO Java libraries jopcagtbase.jar and jopcagtmsg.jar are located

Event forwarding to IBM Tivoli Enterprise Console or Omnibus

The next Event forwarding settings screen shows the required parameters for IBM EEIF Event forwarding to IBM Tivoli Enterprise Console or Omnibus.

	Forwarding via IBM Tivoli EEIF (to IBM Tivoli T/EC or Omnibus)	
	Enable IBM EEIF Event Forwarding	
	IBM Tivoli EEIF Event Server name or IP address mytivoliserv.example.com	
	IBM Tivoli EEIF port 5529	
	IBM Tivoli EEIF Java library directory (where evd.jar and log.jar are located)	
	C:\eeifibs	
	Restore Default Choose	
		*
InstallAnywhere		
Cancel Help	Previous Nex	t



Event forwarding to IBM Tivoli Enterprise Console or Omnibus depends on the following parameters.

IBM EEIF server name

Full qualified name of the Tivoli Enterprise Console or Omnibus server

IBM EEIF server port (default: 5529)

Specify the port of the EEIF-based IBM Event server

IBM EEIF Java Library directory

Specify the directory where the IBM EEIF Java libraries evd.jar and log.jar are located

Event forwarding via Log file

The last Event forwarding settings screen shows the required parameters for log file based event integration.

	Forwarding via Logfile	=
	Enable Logfile Event Forwarding	•
	Logfile with path relative to <install-dir>/server or absolute path (directory must exist)</install-dir>	
	/var/rep/reportEventToFile.rep	
	Default Multi Line output format	•
	Report all except HARMLESS and WARNING events	•
InstallAnywhere		
Cancel Help	Previous	Next

ECM SM Installation: Log file Event forwarding

Event forwarding via log file depends on the following parameters.

Log file name

Log file including relative path to **\$CENIT_ROOT/eventserver** or absolute path to the file.

NOTE The directory must exist.

Type of template format file

Specify the template format file type. Select either 'Default Multi Line output format' or 'Default Single Line output format' or 'Custom Event forwarding template file'

Custom Event forwarding template file

In the case the type 'Custom Event forwarding template file is selected specify the custom template file including the path.

Custom Event forwarding selection

Select whether all events are forwarded (Report all events) or all events except HARMLESS (Report all except HARMLESS events) or all events except HARMLESS and WARNING events (Report all except HARMLESS and WARNING events) are stored in the log file.

Configuring LDAP authentication

If LDAP authentication is activated the user has to decide which LDAP type to use.

Background

The settings for the LDAP authentication are all based on the same principles regardless of the concrete LDAP server used. These principles are described here to give a better understanding about the input parameters described in the following sub-sections.

NOTE In the following the placeholders $\{0\}$ and $\{1\}$ will be replaced with the username and the password during runtime. So you should not enter these values directly in your configuration, but use the shown placeholders.

Server Name and Port

These parameters are necessary to establish a network connection to the LDAP server. They are the normal hostname of the machine, the LDAP server is running at, plus the port used by the LDAP server.

Group (Provider) URL

It is the LDAP search pattern (aka filter) used to get those elements from the LDAP tree, that do contain groups.

These elements can be groups itself or users. That depends on the LDAP implementation. On some systems the user elements hold the information to which groups a user belongs to and on some systems the group elements store the users as members of the group.

To get the groups from these elements, the Group Attribute is used.

Group Attribute

That is the attribute of the elements selected by the Group URL (see above) to get the concrete groups defined in the LDAP system.

E.g. in case the users contain the groups, the filter can be *memberOf*. In case the elements are groups, the filer can be something like (&(objectClass=groupOfUniqueNames)) (*uniqueMember=uid=*{0},*)).

Group Query

That LDAP filter pattern selects a distinctive element, normally a user, to retrieve the groups the element belongs to.

Group Name Pattern

The LDAP filter to get a distinctive group entry from the LDAP tree. It should at least contain the name of the group. The name is later selected by the Group Name Index.

Group Name Index

This is the index of the group's name in the list of values returned by the Group Name Pattern. The counting starts by 1 (*one*).

User URL

This is the LDAP filter to retrieve a distinctive user from the LDAP tree.

Configuring connection to MS AD LDS

	LDAP Advanced settings
IBM.	Specify the appropiate LDAP settings here
Enterprise Content Management System Monitor	 ✓ Requires internal ECM SM user ✓ Use LDAP for authentication and groups
	Please specify the required LDAP type and required parameters MS ADAM LDAP Server name msadamsrv
	LDAP Group URL (e.g. OU=User,O=fsm,C=com) OU=User,O=fsm,C=com LDAP Group attribute memberOf
	LDAP Group query (default value: distinguishedName=CN={0},OU=Users,O= <domain>,C=<do distinguishedName=CN={0}, OU=User,O=fsm,C=com LDAP User URL (e.g. CN={0},OU=User,O=fsm,C=com) CN={0},</do </domain>
InstallAnywhere	LDAP Group name pattern

ECM SM Installation: MS AD LDS LDAP settings

If the checkbox 'Requires internal ECM SM user' is selected an internal ECM SM user is required for external authentication. Otherwise the user is created automatically.

If the checkbox 'Use LDAP for authentication and groups' is selected, the external LDAP system is used to authenticate the user and to transmit its group memberships to ECM SM. Inside ECM SM the user will be member of the intersecting set of LDAP and ECM SM groups. If unchecked, the external LDAP system is used for authentication only, group memberships are solely managed using the ECM SM user management.

The following parameters are required for MS AD LDS based LDAP server authentication.

Server Name

Specify the full qualified MS AD LDS LDAP server name

Server Port

Specify the MS AD LDS LDAP server port (default unsecure port: 389, secured: 636)

Group URL

Specify the Group URL pattern to search for groups

Example: OU=User, O=fsm, C=com

NOTE Do NOT add $CN = \{ 0 \}$ to this parameter

Group Attribute

Specify the attribute of an entry in the LDAP database that contains group information.

Default: memberOf

Group Query

Adjust the Group filter if required.

Default value is distinguishedName=CN={0},OU=Users,O=<domain>,C=<domain-suffix>

If the MS AD LDS server is configured to use the LDAP displayName instead of the distinguished-Name please use the following value without any extension: $displayName = \{ 0 \}$

User URL

Specify the User URL pattern to search for users

Example: CN={0},OU=User,O=FSM,C=COM

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: CN=([^ ,] *) , . *

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Configuring connection to a MS Active Directory Server

	LDAP Advanced setting	js
IBNG Enterprise Content Management	Specify the appropiate LDAP settings here	
System Monitor	Requires internal ECM SM user	
	✓ Use LDAP for authentication and groups	
	Please specify the required LDAP type and required parameters	
	MS ADS (with SASL/GSSAPI authentication)	
	ADS Server name (Domain Controller without DNS suffix, e.g. adsserv)	
	msadamsrv	
	ADS Server port 389	
	Domain name (lowercase letters, e.g. mydomain.com) example.com	
	LDAP Group provider URL CN=Users,*	
	LDAP Group query sAMAccountName={0}	
	LDAP Group attribute memberOf	
	LDAP Group name pattern CN=([^,]*),.*	
	LDAP Group name index 1	-
InstallAnywhere	,	
Cancel Help	Previous Next	

ECM SM Installation: MS Active Directory settings

The following parameters are required for MS ADS based LDAP server authentication. Be aware ECM SM supports two different authentication methods for MS ADS.

- MS ADS (with SASL/GSSAPI authentication)
- MS ADS (with simple authentication method)

Depending on your MS ADS server settings the appropriate authentication method should be selected.

NOTE Selecting the wrong method requires manual adjustment after the installation process.

The following MS ADS parameters apply to both MS ADS authentication types:

Server Name

Specify the MS ADS server name without DNS suffix (for instance adsserv1).

Server Port

Specify the MS ADS server port (default port: 389).

Domain Name

Specify the ADS Domain name in lowercase letter.

Group Provider URL

Specify the Group provider URL pattern to search for groups.

Group Query

Adjust the Group filter if required.

Default: *sAMAccountName=*{0}

Group Attribute

Specify the attribute of an entry that contains group information.

Default: memberOf

Group Name Pattern

Adjust the Group name pattern settings, if required.

Default: CN=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

LDAP Security principal (non GSSAPI-authentication only)

Default value. { 0 } or { 0 }@<domain-name>

Use { 0 }@<domain-name> in the case the ADS server requires 'Bind with Credentials', otherwise use { 0 }

The domain name can be obtained from the Active Directory Users and Computers dialog which is started via Start Administrative Tools Active Directory Users and Computers .



Obtaining the domain name from the Active Directory configuration

Configuring connection to a SUN Java Directory Server

The required SUN Java Directory Server settings are displayed in the following screen shot.

	L	DAP Advanced settings
IBM. Enterprise Content Management	Specify the appropiate LDAP settings here	
System Monitor	Requires internal ECM SM user	A
	☑ Use LDAP for authentication and groups	
	Please specify the required LDAP type and required parameters	
	SUN Java System Directory Server	•
	LDAP Server name (e.g. sun.mydomain.com) mysunsrv	
	LDAP Server port (e.g. 389, 636 if SSL activated) 389	
	LDAP Group URL (e.g. ou=Groups,dc=mydomain,dc=com)	=
	ou=Groups,dc=mydomain,dc=com	
	LDAP Group attribute Con	
	LDAP Group query	
	(&(objectClass=groupOfUniqueNames)(uniqueMember=uid={0},*))	
	LDAP User URL (e.g. uid={0},ou=People,dc=mydomain,dc=com)	
	uid={0},ou=People,dc=mydomain,dc=com	
	LDAP Group name pattern ou=([^,]*),.*	•
InstallAnwhere		
Cancel Help		Previous Next

ECM SM Installation: SUN Directory Server settings

The following parameters are required for SUN Java System Directory Server authentication.

Server Name

Specify the full qualified SUN Directory server name.

Server Port

Specify the SUN Directory LDAP server port (default: 389)

Group URL

Specify the Group URL pattern to search for groups.

Group Attribute

Specify the attribute of an entry that contains group information.

Default: cn

Group Query

Adjust the Group filter if required.

Default: (&(objectClass=groupOfUniqueNames)(uniqueMember=uid={0},*))

User URL

Specify the User URL pattern to search for users.

Group Name Pattern

Adjust the Group name pattern settings, if required.

Default: *ou*=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Sun Java(TM) System Server Console	
Console Edit View Object Help	
Sun Java™ System Server Console	
Servers and Applications Users and Groups	
Default View	
wzkasmicom wzkasmicom Domain name: wzk3fsm.com	
Description: Stand Low and House Structure and House Structur	
User directory host and po 5 w2k3fsm.w2k3fsm.com:39566	
Bind DN:	
Bind password:	
	Þ
Edit	Help

Obtaining the LDAP server name and port from the Sun Java System Server Console

Find LDAP Server name (e.g. w2k3fsm.w2k3fsm.com) and LDAP Server port (e.g. 39566) in the Server Console.



Obtaining the LDAP user URL from the SGun Java System Directory Server Console

Find LDAP specify LDAP User information regarding the needed tree to LDAP URL (e.g.uid={0},ou=People,dc=fsmdomain,dc=com) and Group URL (e.g. ou=Groups,dc=fsmdomain,dc=com) in the Directory Server Directory tab.

Configuring connection to IBM Tivoli Directory Server

If IBM Tivoli Directory server based authentication is planned the following parameters need to be specified.

LDAP Advanced settings
Specify the appropriate LDAP settings here
System Monitor Requires internal ECM SM user Image: Comparison of the system
InstallAnywhere

ECM SM Installation: IBM Tivoli Directory Server LDAP settings

The following parameters are required for IBM Tivoli Directory Server authentication.

Server Name

Specify the full qualified IBM Tivoli Directory server name.

Server Port

Specify the IBM Tivoli Directory LDAP server port (default: 389)

Group URL

Specify the Group URL pattern to search for groups.

Ex.: ldap[s]://<ldap-server-name>>:<ldap-port>

Group Attribute

Specify the Group attribute that contains group information.

Default: cn

Group Query

Adjust the Group filter if required.

Default: (&(objectClass=accessGroup)(member=cn={0}*))

User URL

Specify the User URL pattern to search for users.

Group Name Pattern

Adjust the Group name pattern settings, if required.

Default: cn=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

To obtain the required data start the Tivoli Directory Server Web Administration Tool and select the Directory management folder.

Tivoli Directory Server Web Administration Tool		
Introduction	⊜	
Ser properties	Manage entries	
Server administration	Content location :	
Carter Strength Construction	dap://tivtds61:389 > cn=localhost > cn=fsmtest	
) <u> Schema management</u>		
Directory management	Expansion Floor I Add. I Foll allege too Delete	
Add an entry	📅 😰 😰 🔳 🛛 Select Action 🔽 Go	
Anage entries	Select Expand A RDN A Object class A Created A Last	
Eind entries	← 🕂 <u>cn=groups</u> container Oct 31, 2007 Oct	
Replication management	← ♣ <u>cn=users</u> container Oct 31, 2007 Oct	
Realms and templates	Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2	
Logout	Close	

Obtaining LDAP configuration data from the Tivoli Directory Server Web Administration Tool

- Find LDAP Server name (e.g. tivtds61) and LDAP Server port (e.g. 389) in the first part of the LDAP URL.
- LDAP User URL is the LDAP URL to the user entries, { 0 } is replaced with the login name. (example: cn={0}, cn=users, cn=fsmtest, cn=localhost)
- LDAP Group URL is the LDAP URL to get the groups (example: cn=groups, cn=fsmtest, cn=localhost).

Configuring connection to Novell eDirectory

Novell eDirectory LDAP authentication requires the following settings:

	LDAP Advanced settings
IBM. Enterprise Content Management	Specify the appropiate LDAP settings here
System Monitor	Requires internal ECM SM user
	Use LDAP for authentication and groups
	Please specify the required LDAP type and required parameters
	Novell eDirectory
	LDAP Server name mynedirsrv
	LDAP Server port (e.g. 389, 636 if SSL activated) 389
	LDAP Group URL (e.g. Idap[s]:// <idap-server>:<idap-port>/T=<novell-tree-name>)</novell-tree-name></idap-port></idap-server>
	ldap://mynedirsrv:239/T=exampletree
	LDAP Group attribute an
	LDAP User URL (e.g. CN={0},O=mydomain,O=com)
	CN={0},O=mydomain,O=com
	LDAP Group query (e.g. (member=cn={0},OU=Users,O= <company-name>))</company-name>
	(member=cn={0},OU=Users,O= <organization>)</organization>
	LDAP Group name pattern (example Idap://[^]*/cn=fsm_([^,]*),.*) cn=([^,]*),.*
InstallAnvwhere	
Cancel Help	Previous Next

ECM SM Installation: Novell eDirectory LDAP settings

The following parameters are required for Novell eDirectory LDAP server authentication.

Server Name

Specify the full qualified Novell eDirectory server name.

Server Port

Specify the Novell eDirectory LDAP server port (default: 389).

Group URL

Specify the Group URL pattern to search for groups.

Ex.: ldap[s]://<ldap-server-name>:<ldap-port>... /T=<Novell-Tree-Name>

Group Attribute

Specify the attribute of an entry that contains group information.

Default: none (unset)

User URL

Specify the User URL pattern to search for users

Default: CN={0}, O=mydomain, O=com

Group Query

Adjust the Group filter if required.

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: cn=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Running the LDAP connection test

If LDAP-based authentication is configured the following message panel is displayed next:

?	The LDAP settings can now be verified with a connection test using an existing user account. The user password is required.
	It is recommended to test the LDAP settings now. Note: If the LDAP settings are incorrect manual adjustment is required.
	Run the LDAP Connection test Continue without LDAP connection test Change LDAP settings

ECM SM Installation: LDAP Connection Test

You can decide whether to test the LDAP connection, proceed without LDAP test or chance the LDAP settings. If you press the 'Run the LDAP Connection test' button a panel that requests credential will open.

	LDAP Connection test - credentials required
IBM.	Please enter a valid user and password to test the configured LDAP connection
Enterprise Content Management System Monitor	LDAP user name myname
	Password of specified user
InstallAnywhere	

ECM SM Installation: LDAP User and Password

Enter appropriate values for user and password and press 'Next' to process with the LDAP Connection test. If the specified parameters or the user credentials were incorrect the following message will rise:

LDAP Connection test failed! LDAP Connection test failed! Please verify the settings
Adjust LDAP settings

ECM SM Installation: LDAP Connection Test failed

Press the 'Adjust LDAP settings' button to change the LDAP settings and retry the LDAP connection test. Once the connection test was successful the following message is displayed:

<u>^</u>	LDAP Connection test was successful
	LDAP Connection test was successful - press 'Next' to proceed with the installation
	Next

ECM SM Installation: LDAP Connection Test successful

Configuring Advanced Server and embedded Agent settings

This panel shows advanced Server settings (debugging ports) as well as the RAP UI server name. In addition to can adjust the Agent IP address and port to bind the optional embedded Agent to.

IBM Enterprise Content Managen	nent System Monitor Server
	Advanced Server and embedded agent settings - Complete installation
IBM. Enterprise Content Management	Specify advanced ECM SM server settings. Note: Only users with advanced knowledge of ECM SM server should adjust these settings.
System Monitor	Server parameters: Server Console port 127.0.0.1:23960 Server InitDB Console Port 23962 RAP (Web GUI) settings: RAP Http Server name N7P001578648IT.de.cenit-group.com RAP Console port 127.0.0.1:23980 Ports for advanced debugging - do not specify values for production use! Server Remote Debugging port (Default: 8000) Server RAP Remote Debug port (Default: 8001) Server INIT Remote Debug port (Default: 8006) Embedded Agent Settings (if activated): Agent IP-address and port to bind
InstallAnywhere Cancel Help	Previous



Server Console port (default: 23960)

Port of the OSGi console of the event server. Allows access to the OSGi console of the event server. Only used for maintenance. For normal production it is not necessary to access the OSGi console directly.

Server InitDB Console port (default: 23962)

Port of the OSGi console of the database initialization process. Allows access to the OSGi console of the database initialization process of the installer. Only used for maintenance. After the application is installed, the database initializer is offline, so the console cannot be accessed.

RAP http Server name

Full qualified IP name or address of the ECM SM RAP (Remote Application Platform), formally known as (Rich Ajax Platform) Web server. This parameter is not displayed if you run a Primary Server installation.

RAP Console port (default: 23980)

Default console port of the RAP (Remote Application Platform) Web server

Server Remote Debug port (default: unset, otherwise 8000)

Port used for development or maintenance. It allows remote debugging access via JDWP (Java Debug Wire Protocol) to the event server. For that, the parts to be debugged must be build with debug information included. In production this is not the case

Server RAP Remote Debug port (default: unset, otherwise 8001)

Port used for development or maintenance. It allows remote debugging access via JDWP (Java Debug Wire Protocol) to the RAP GUI server. For that, the parts to be debugged must be build with debug information included. In production this is not the case

Server INIT Remote Debug port (default: unset, otherwise 8006)

Port used for development or maintenance. It allows remote debugging access via JDWP (Java Debug Wire Protocol) to the database initialization process. For that, the parts to be debugged must be build with debug information included. In production this is not the case and after the installation has finished the process is not running at all

The last parameter of the panel allows adjusting IP address and port of the embedded Agent to bind to.

Embedded Agent IP address and port to bind (default: listenport:127.0.0.1:23804)

In the case more than one agent should be installed locally on the ECM SM Server the following parameter may requires adjustment. Do not use the same port by more than one agent.

Configuring Database Settings

The next panel is used to configure the database settings used by the ECM SM Server system.

		Database settings
Enterprise Content Management	Please specify the appropriate database settings	
	DB2 DB2 instance Database name ECMSMDB Schema name (upper case) ECM51 JDBC driver location C:\idbc\db2 Restore D JDBC connection string jdbc:db2://localhost:50000/ECMSMDB;currentSchema=ECM51; JDBC driver class com.ibm.db2.jcc.DB2Driver Database user ECM51 Password of Database user	efault Choose =
InstallAnywhere Cancel Help	·	Previous Next

Configuring a Connection to an IBM DB2 Database

ECM SM Installation: IBM DB2 Settings - First Part

This screen shot shows the required IBM DB2 parameters.

IBM DB2 Database Instance

Specify the IBM DB2 instance name.

Database Name

Specify the IBM DB2 database name for use with the ECM SM Server system.

NOTE This database must exist before you start the installation.

Schema Name

You can specify an IBM DB2 schema name here. If unset, the default schema name is used.

NOTE When you define a value for this parameter, that differs from the default schema, you must also extend the JDBC connection string by the currentSchema parameter, which is required in this case (see below).

JDBC Driver Path

Specify the location of the IBM DB2 JDBC driver files.

NOTE This parameter is not displayed during Secondary Server installation.

JDBC Connection String

Replace the connection string template with the values of your system. The default string is:

```
jdbc:db2://<server-name>:<port>/<database-name>[:
currentSchema=<schemaName>;]
```

NOTE Parts enclosed in [] square brackets are optional. Parts enclosed in <> angle brackets mark place holders, that have to be replaced by the respective values of your system.

Depending on the *IBM DB2* installation settings and user rights, the following parameter needs to be added to the connection string in case the *ECM SM Server* installation failed: [deferPrepares=false;]. Perform a server re-installation with the enhanced settings in this case.

JDBC Driver Class (Default: com.ibm.db2.jcc.DB2Driver)

Only adjust this, if you want to use a non-default IBM DB2 JDBC driver.

Database user

Specify the technical database user, that is to connect to the *IBM DB2* database.

Password of the Database User

Specify the password of the database user.

Database Host Name

Specify the full qualified host name or IP address of the IBM DB2 database server.

Database Port (Default value of the first instance: 50000)

Specify the port of the ECM SM IBM DB2 database.

Configuring a Connection to an MS SQL Server Database

The following screen shot shows all parameters required, if MS SQL Server with database authentication (*SQL Server Authentication*) is selected as ECM SM database vendor.

	Database settings
IBMe Enterprise Content Management	Please specify the appropriate database settings
	MSSQL Database authentication MSSQL Instance name ECMSM51\mymssqlsrv Database name ECMSM51 Schema name (enter the default schema name of the MSSQL user) ecmsmusr JDBC driver file name (full name of file sqljdbc4.jar) C:\jdbc\mysql\sqljdbc4.jar IDBC connection String jdbc:sqlserver://localhost: 1433;instanceName =ECMSM;databaseName =ECMSM51;responseBuffering=adapti JDBC driver class com.microsoft.sqlserver.jdbc.SQLServerDriver Database user Password of Database user
InstallAnywhere Cancel Help	Previous Next

ECM SM Installation: MS SQL Server parameter settings using SQL Server Authentication

The following screen shot shows all parameters required, if MS SQL Server with Windows authentication is selected as ECM SM database vendor.

	Database setting
IBM. Enterprise Content Management	Please specify the appropriate database settings
System Monitor	MSSQL Windows authentication MSSQL Windows authentication file sqljdbc_auth.dll incl. full path \ividbc\mssql\sqljdbc_auth.dll R Choose
	MSSQL Instance name ECMSM51\mymssqlsrv Database name ECMSM51 Schema name (enter the default schema name of the MSSQL user) ecmsmusr JDBC driver file name (full name of file sqljdbc4.jar) C:\jdbc\mysql\sqljdbc4.jar
	Restore Default Choose JDBC connection String jdbc:sqlserver://localhost:1433;instanceName =ECMSM;databaseName =ECMSM51;responseBuffering=adapti JDBC driver class com.microsoft.sqlserver.jdbc.SQLServerDriver
InstallAnywhere Cancel Help	Previous Next

ECM SM Installation: MS SQL Server parameter settings using Windows Authentication

The first parameter block describes the supported MS SQL Server database user authentication methods.

Database authentication (SQL Server Authentication)

The technical user, that connects to the database, requires database authentication only.

Windows authentication (Integrated Authentication)

This authentication method requires access to an integrated authentication Windows DLL file. You should specify the full path to the sqljdbc_auth.dll MS SQL Server Windows authentication file (32 bit version).

WARNING This parameter is not displayed during Secondary Server installation.

NOTE Windows Authentication does not work on UNIX-based servers using *MS SQL Server* as database. UNIX/Linux servers can only connect to an MS SQL Server database by using the database authentication method (*SQL Server Authentication*).

Important note Activating *Windows Authentication* requires the specification of the Windows service account and password on the **Basic Server settings** panel of the installer. Please go back to this panel and verify the mentioned parameters before you proceed.

WARNING When configuring a JDBC connection to your *MS SQL Server* database using the *Windows Authentication* method, make sure that the *Windows* user, by which you run the *ECM SM Server* installation program, is identical to the specified *Windows* user you want to use for database connection via *Windows Authentication*. If the mentioned *Windows* users are not identical, the database connection test will fail.

NOTE In case you use the *Windows Authentication* method to connect to your MS SQL Server database, and only in this case, *you must add* the integratedSecurity=true string to your *JDBC connection string* (see below).

Database Instance

Specify the SQL Server instance name. Leave this parameter empty, if you use the default SQL Server instance.

Database Name

Specify the SQL Server database name for use with the ECM SM Server system.

NOTE This database must exist before you start the installation.

Schema Name

Specify the SQL Server default schema name of the SQL Server database user. Do not leave this parameter unset.

NOTE The installer does not create the schema specified in this field. The schema must exist and must be defined as default schema for the database user. Check user settings in the SQL Server Management Console. See also the MS SQL Server chapter.

JDBC Driver File

Specify the full file name of the SQL Server JDBC driver file.

NOTE This parameter is not displayed during Secondary Server installation.

JDBC Connection String

Replace the connection string template with your system's values.

The default string using SQL authentication is:

jdbc:sqlserver://<server-name>:<port>;instanceName=<instancename>;databaseName=<DBname>; responseBuffering=adaptive

The default string using Windows authentication is:

jdbc:sqlserver://<server-name>:<port>;instanceName=<instancename>;databaseName=<DBname>; responseBuffering=adaptive;integratedSecurity=true

NOTE Parts enclosed in [] square brackets are optional. Parts enclosed in <> angle brackets mark place holders, that have to be replaced by the respective values of your system.

```
JDBC Driver Class (Default: com.microsoft.sqlserver.jdbc.SQLServerDriver)
```

Only adjust this, if you want to use a non-default MS SQL Server driver.

Database User

Specify the technical database user, that is to connect to the MS SQL Server database.

Password of the Database User

Specify the database user's password.

Database Host Name

Specify the full qualified host name or IP address of the MS SQL Server database host.

Database Port (Default value of the first instance: 1433)

Specify the port of the ECM SM MS SQL Server database.

The following screen shot shows all additional parameters available for the *MS SQL Server*-based *ECM SM Server* installation.

	Database host localhost Database port 1433
	Create database and DDL file
	Directory for created DDL's
	C:\Program Files (x86)\IBM\ECMSM DDL
	Restore Default Choose
InstallAnywhere	,
Cancel Help	Previous Next

ECM SM Installation: More MS SQL Server parameters

Configuring a Connection to an Oracle Database

The following screen shot shows all parameters required, if Oracle is selected as ECM SM database vendor. The provided examples show standard Oracle database settings as well as Oracle RAC based settings.

	Database settings
IBNL® Enterprise Content Management	Please specify the appropriate database settings
	Orade Database name ECMSM51 Schema name (enter the default schema name of the Oracle user, upper case) ecmsm51usr JDBC driver file name (full name of file ojdbc5.jar or ojdbc6.jar) C:\/dbc\orade\ojdbc6.jar Restore Default Choose JDBC connection string jdbc:orade:thin:@localhost:1521:ECMSM51 JDBC driver class orade.jdbc.driver.OradeDriver Database user ecmsmusr Password of Database user ••••••• Database host localhost
InstallAnywhere Cancel Help	Previous Next

ECM SM Installation: Oracle parameter settings

This screen shot shows the required Oracle parameters.

ORACLE_SID or Oracle Service Name

Specify the *Oracle* SID (ORACLE_SID) or the Oracle Service Name *ECM SM*. Note: In the case an Oracle Service name based configuration is used the leading / is required. This parameter applies to Oracle standard and Oracle RAC configuration.

Database Name

Specify the *Oracle* database name for use with *ECM SM*. This parameter applies to Oracle standard and Oracle RAC configuration.

NOTE This database must exist before you start the installation.

Schema Name

Specify the *Oracle* default schema name of the *Oracle* user. Do not leave this parameter unset. This parameter applies to Oracle standard and Oracle RAC configuration.

JDBC Driver File

Specify the full path to the *Oracle* JDBC driver file. This parameter applies to Oracle standard and Oracle RAC configuration. Note: This parameter is not displayed during Secondary Server installation.

NOTE This parameter is not displayed during Secondary Server installation.

JDBC Connection String (Oracle standard configuration)

Replace the connection string template with the values of your system. The default string for an *Oracle SID*-based configuration is:

jdbc:oracle:thin:@<server-name>:<port>:<database-name>

The default string for an Oracle Service Name-based configuration is:

jdbc:oracle:thin:@<server-name>:<port>/<service-name>

NOTE Parts enclosed in <> angle brackets mark place holders, that have to be replaced by the respective values of your system.

JDBC Connection String (Oracle RAC configuration)

The following examples can vary for your *Oracle RAC*-based configuration, contact your Oracle administrator for details. Configuration example 1:

jdbc:oracle:thin:@<oracle-scan-server-name>:<port>/<service-name>

Configuration example 2:

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on) (ADDRESS=(PROTOCOL=TCP)
(HOST=<Ora-server-name-1>) (PORT=<port>)) (ADDRESS=(PROTOCOL=TCP)
(HOST=<Ora-server-name-2>) (PORT=<port>)) (CONNECT_DATA=(SERVICE_
NAME=<service-name>)))
```

Note: Parts enclosed in <> angle brackets mark place holders, that have to be replaced by the respective values of your system.

JDBC Driver Class (Default: oracle.jdbc.driver.OracleDriver)

Only adjust this, if you want to use a non-default *Oracle* driver. This parameter applies to Oracle standard and Oracle RAC configuration.

Database User

Specify the technical database user, that is to connect to the *Oracle* database. This parameter applies to Oracle standard and Oracle RAC configuration.

Password of the Database User

Specify the password of the database user. This parameter applies to Oracle standard and Oracle RAC configuration.

Database Host Name

Specify the full qualified host name or IP address of the Oracle database server.

In the case of an *Oracle RAC* configuration the IP name or IP address of the Oracle SCAN server should be specified here.

Database Port (Default value: 1521)

Specify the port of the *ECM SM Oracle* database. This parameter applies to Oracle standard and Oracle RAC configuration.

Configuring a Connection to a PostGreSQL Database

NOTE *PostGreSQL*-based *ECM SM Server* installation is only supported for demo and testing environments.

	Database settings
IBM.	Please specify the appropriate database settings
Enterprise Content Management System Monitor	Postgre/SQL Database name ecmsm51 Schema name (enter the default schema name of the PostGreSQL user) public JDBC driver file name (full path to postgresql* jdbc4.jar) C:\Program Files (x86)\PostgreSQL\pgJDBC\postgresql-9.1-903.jdbc4.jar BBC connection string jdbc:postgresql:ecmsm51 JDBC driver class org.postgresql.Driver Database user ecmsmusr Password of Database user •••••••
InstallAnywhere	Database host localhost
Cancel Help	Previous Next

ECM SM Installation: PostGreSQL parameter settings

This screen shot shows the required PostGreSQL parameters.

Database Name

Specify the *PostGreSQL* database name for use with *ECM SM Server*.

NOTE This database must exist before you start the installation.

Schema Name

Specify the *PostGreSQL* default schema name of the *PostGreSQL* user. Don't leave this parameter unset.

JDBC Driver File

Specify the full path to the PostGreSQL JDBC driver file (a JDBC type 4 driver has to be used).

NOTE This parameter is not displayed during Secondary Server installation.

JDBC Connection String

Replace the *PostGreSQL* connection string template with the values of your system. The default string is:

jdbc:postgresql:<database-name>

NOTE Parts enclosed in <> angle brackets mark place holders, that have to be replaced by the respective values of your system.

JDBC Driver Class (Default: org.postgresql.Driver)

Only adjust this, if you want to use a non-default *PostGreSQL* driver.

Database User

Specify the technical database user, that is to connect to the PostGreSQL database.

Password of the Database User

Specify the password of the database user.

Database Host Name

Specify the full qualified host name or IP address of the *PostGreSQL* database host.

Database Port (Default value: 5432)

Specify the port of the ECM SM PostGreSQL database.

Configuring the Creation of DDL Files (Optional)

	Database port 50000 Create database and content	•
InstallAnywhere Cancel Help	Previou	IS Next



At the bottom of the *Database settings* installer panel, the user can make his choice between three options of how the database creation is to be dealt with by the subsequent installation process. The **Create database and content** option is selected by default.

The overview of all available options is as follows:

Create database and content

The database is created with all required content.

Create database and DDL files

The database is created with all required content, and database description (DDL) files are created additionally.

Create DDL files only (manual DB creation)

Only the DDL files are generated and stored in the specified folder location, that are required for creating the database later on manually. The user has to build the database and content by means of the DDL files during the installation process.

NOTE The installation process stops at a later point and waits until the user has built the database from the generated DDL files.

The following screen shot shows the folder selection, in case Create DDL files only (manual DB creation) is selected.

	Create DDL file only (manual DB creation)	
	Directory for created DDL's	
	C:\Program Files (x86)\IBM\ECMSM\DDL	
	Re	store Default Choose
InstallAnywhere	,	
Cancel Help		Previous Next

ECM SM Server Installation: Selection of DDL Folder Location (Create DDL files only)

The next screen shot shows the folder selection, in case Create database and DDL files is selected.

	Create database and DDL file	•
	Directory for created DDL's	
	C:\Program Files (x86)\IBM\ECMSM\DDL	
		Restore Default Choose
InstallAnywhere		
Cancel Help		Previous Next

ECM SM Server Installation: Selection of DDL Folder Location (Create database and DDL files)

Running the Database Connection Test

To proceed with the *ECM SM Server* installation, the database connection test has to be successful. Press the **Test the DB connection for user xxxxx** button to verify, whether a database connection can successfully be established.

Database	connection test
?	To proceed with the installation the database connection need to be verified.
	Before the installation can proceed a successful connection to the database fsm51 (database type POSTGSQL, JDBC URL jdbo:postgresql:fsm51, JDBC class org.postgresql.Driver) is required.
	Start the database now if it's not yet started.
	Cancel Installation and Exit Change DB Settings Test the DB connection for user fsm51

ECM SM Server Installation: Database Connection Test Message

If you enabled installer debugging (Enable installer debugging checkbox on the Basic server settings panel) you will receive detailed connection test output. In case, the connection test was unsuccessful, pressing the Next or Previous button will open the Database settings panel again to allow changing the incorrect database settings.

IBM Enterprise Content Manager	nent System Monitor Server
	Connection test result
	Database connection test result.
	Database connection test result was:
IBM.	Connection test was successfull.
Enterprise Content Management System Monitor	Standard error output: Sun Sep 14 14:07:56 CEST 2014 Set default values for attributes which are not already set. Sun Sep 14 14:07:56 CEST 2014 Default DB-Port is 0 for POSTGSQL. Sun Sep 14 14:07:56 CEST 2014 Default DB-Port is 0 for POSTGSQL. Sun Sep 14 14:07:56 CEST 2014 Default output-separator is ;; Sun Sep 14 14:07:56 CEST 2014 Default output-separator is ;. Sun Sep 14 14:07:56 CEST 2014 Default output-separator is ;. Sun Sep 14 14:07:56 CEST 2014 Default query-separator is ;. Sun Sep 14 14:07:56 CEST 2014 Default query-separator is ;. Sun Sep 14 14:07:56 CEST 2014 Period evec parameter Sun Sep 14 14:07:56 CEST 2014 Found evec parameter Sun Sep 14 14:07:56 CEST 2014 Found evec parameter Sun Sep 14 14:07:56 CEST 2014 Checking sql-command DoNothing Sun Sep 14 14:07:56 CEST 2014 Create DbClient with DB-AccessData: - DB-Type: POSTGSQL - DB-Subtype: null - Server: NTP00157B64BIT - User: Smuser - Password: - Password:
	KE/pH/u2+iktN8PuASPi9S4UhmZFrlpeh5mRONCfotU= - ID
	- JDBC-Driver-Class: org.postgresql.Driver - JDBC-Driver-URL: jdbc:postgresql://N7P00157B64BIT:5432/smdb?schema=public
InstallAnywhere	
Cancel Help	Previous

ECM SM Installation: Database Connection Test Result

Optional: JDBC Driver Location for Database Monitoring and other 3rd Party Components

This screen shot shows the optional parameters to prepare the ECM SM server for later database monitoring of managed systems (agents) and for VMware ESX monitoring.
Optional:	JDBC driver location for agent DB monitoring and other 3rd Party compo	onents
IBM.	Specify directories on the ECM SM server that contain appropriate JDBC drivers to access IBM DB2, Microsoft SQL Server and Oracle Database servers. Note: Only one JDBC driver (version) is supported for each DB vendor VMWare ESX monitoring driver location (Note: specify version 4.x and version 5.x drivers seperately)
System Monitor	C: \jdbs\db2 Restore Default Choose	^
	Microsoft SQL server driver location No MSSQL JDBC driver files V Oracle Database driver location V No Oracle JDBC driver files V VMWare ESX driver location V	=
	VMWare ESX Version 4.x driver file (file name vim25.jar) C:\vmware_api4\vim25.jar Restore Def Choose VMWare ESX Version 5.x driver file (file name vim25.jar) C:\vmware_api5\vim25.jar Restore Def Choose Restore Def Choose	~
InstallAnywhere Cancel Help	Previous	lext

ECM SM Installation: JDBC Driver Location for Database Monitoring and other 3rd Party Components

If you have selected to activate the IBM DB2 driver location, the following parameter will be displayed:

IBM DB2 driver location for remote DB monitoring

Specify the full qualified path to the DB2 driver files.

If you have selected to activate the Microsoft SQL Server driver location, these parameters will be displayed:

Microsoft SQL Server driver location

Specify the full qualified path to the Microsoft SQL Server driver file.

In addition, you may want to specify the MS SQL Server Windows authentication DLL file for using the Microsoft SQL Server Windows authentication. Specify the full qualified file name including full path.

If you have selected to activate the Oracle Database driver location, these parameters will be displayed:

Oracle JDBC driver location

Specify the full qualified path to the Oracle Database driver file.

If you have selected to activate the VMware ESX Monitoring, these parameters will be displayed:

VMware ESX driver location

Specify the full qualified filename including full path to the **vim25.jar** VMware ESX driver file. There is an input field for API version 4.1 and 5.x.

Daemon Settings

The next panel shows the Service / Daemon startup settings. You might want to change the default settings (automatic startup) to manual startup.

IBM Enterprise Content Manager	nent System Monitor Server
	Services / Daemon behaviour
IBM.	Select the ECM SM Server Service / Daemon startup behaviour and whether to start the software after the installation or not
Enterprise Content Management System Monitor	Automatic Startup
	Start after installation
InstallAnywhere	
Cancel Help	Previous

ECM SM Installation: service / Daemon startup settings

Automatic Startup

All ECM SM services / daemons installed on the system will be configured for automatic startup.

Manual Startup

All ECM SM services / daemons installed on the system will be configured for manual startup. This may be useful in High Availability environment, if services are started by dedicated HA tools.

If you selected the checkbox 'Start after installation' the ECM SM services will be started after the installation finished.

NOTE If you selected IBM WebSphere based installation then manual WAS deployments are necessary at the end of the installation.

Downloading Open Source components

For full functioning ECM SM Windows based servers and agents an OpenSource component needs to be downloaded from sourceforge.net.

ECM SM n	requires a GPL component for fully functioning Windows based systems (ECM SM server and clients)
?	ECM SM requires the UNIX like Shell from sourceforge.net for fully functioning Windows ECM SM server and clients.
	This ECM SM server installer can use a previously downloaded Sourceforge.net shell archive (see documentation) or can automatically download the file from the internet.
	Please select the desired way to copy the UNIX like Windows shell into the correct directory on this ECM SM server or cancel this task. For further information verify the ECM SM Hardware & Software requirements guide and the install guide.

ECM SM Installation: GPL Windows Shell Download message box

The required 3rd Party download can be done manually or automatically by the installer. Select the appropriate button. If you don't want to install the OpenSource/GPL requirement please contact your Sales representative for further details.

If you selected the 'Automatic download' button the following progress bar will be displayed.

IBM Ente	erprise Content Management System Monitor Server	
	Download UNIX like Windows Shell from http://sourceforge.net:80	3

ECM SM Installation: Shell sourceforge.net download bar

If you've already manually downloaded the UNIX-Like Shell archive from sourceforge.net you can specify the file location with the file browser.

IBM Enterprise Content Manager	nent System Monitor Server		X
		UNIX-like Windows	Shell location
Enterprise Content Management	Please specify the location of the downloaded shell archive si You'd need to download the file from sourceforge.net to enabl of Windows based ECM SM server and clients (managed sys For further details see ECM SM Hardware & Software requirer	hell.w32-ix86.zip. e full functioning tems). nents guide and the Install g	uide.
System Monitor	Please Choose the shell archive shell.w32-ix86.zip File:		
	C:\shell.w32-ix86.zip		
		Restore Default File	Choose
InstallAnwwhere			
Cancel Help		Previous	Next

ECM SM Installation: Shell location file browser

Specify the location of the UNIX-like Windows shell zip-archive you've downloaded from sourceforge.net. The complete path including the file itself has to be given.

IBM Enterprise Content Manager	nent System Monitor Server
	Windows Shell archive verification
IBM.	The verification of the Windows Shell archive was successfull
Enterprise Content Management System Monitor	
Cancel Help	Previous

ECM SM Installation: Shell archive verification result

This screen shot displays the result of the content verification of the specified or downloaded shell archive. In the case of an incomplete archive or of missing files an error screen is displayed. The installation process will continue with the previously displayed selection panel.

NOTE The GPL-licensed UNIX-like Windows shell is required for Windows based ECM SM servers as well as for full functioning Windows agents.

Completing the installation

Subpackage location

The location of the ECM SM JRE and CALA_REX InstallAnywhere install images has to be defined next.

IBM Enterprise Content Manager	ment System Monitor Server
	Install required ECM SM software sub-packages
IBNC Enterprise Content Management System Monitor	To be able to install and update ECM SM agents the following components need to be installed: IBM_ECM_SM CALA_REX agent images IBM_ECM_SM JRE archives These components are part of seperate install images. Note: Previous agent versions will be removed from the server installation directory.
	✓ Install CALA_REX agent images
	Full path to CALA_REX agent images (IBM_ECM_SM_CALA_REX_images.exe)
	C:\fsm_images\51_installer\IBM_ECM_SM_CALA_REX_images.exe
	Restore Default Choose
	✓ Install JRE archives Full path to JRE archives (IBM_ECM_SM_JRE_archives.exe) C:\fsm_images\51_installer\IBM_ECM_SM_JRE_archives.exe Restore Default Choose
InstallAnywhere	Provinue
Cancer Help	Plevious

ECM SM Installation: JRE and CALA_REX agent subpackage location

As mentioned above the complete ECM SM server installation process requires the separate JRE and the ECM SM CALA_REX agent install images. The installer automatically tries to find the required InstallAnywhere Images in the source directory where the Server image is installed from. If the Install images are located somewhere else or if they are renamed please specify them within this panel.

Parameter Check

Before you can start the installation the installer runs a parameter check and displays the results, in the shown screenshot a pre-check error 20.

Important notice: the pre-check stops on the first detected issue. You may have to re-run the parameter check several times until the parameter check returns with exit code 0 (all tests passed).

IBM Enterprise Content Manager	nent System Monitor Server	
		Output of ECM SM pre-check
	Exit code of the Pre-Check is 20	•
Enterprise Content Management System Monitor	Checking for Event reception port: Starts Checking for Event reception port: Passed. Checking for RAP console port: Starts Checking for RAP console port: Starts Checking for RAP host name: Starts Checking for RAP host name: Starts Checking for RAP port Starts Checking for RAP port Starts Checking for RAP port Passed. Checking for RAP port Passed. Checking for RAP http server name: Passed. Checking for RAP http server name: Passed. Checking for RAP port: Starts Checking for RAP port: Starts Checking for RAP JMX port: Starts Checking for RAP JMX port: Starts Checking for RAP REST port: Starts Checking for RAP SCP port: Starts Checking for SCP host name: Starts Checking for SCP host name: Starts Checking for SCP host name: Passed. Checking for SCP port Starts Checking for SCP port Starts Checking for SCP port passed. Checking for SCP port passed. Checking for SCP port Starts Checking for SCP port Starts	
	Checking for Server console port. Starts Checking for Server console port. Passed. Checking for Server database initialization port. Starts	-
InstallAnwhere	Checking for Server database initialization port. Stafts	· · ·
Cancel Help		Previous Next

ECM SM Installation: Installer Pre-check results

In the case of an error (exit code not 0) the following message will be displayed in addition to the display panel:

Pre-check	completd with errors
	The Pre-check completed with errors.
	Please go back and verify the settings again or ignore the test results in the case you are sure about your selections and settings.
	Ignore Pre-check result and proceed Go back to the settings panels

ECM SM Installation: Installer Pre-check error message

In the case of an detected error you may need to adjust settings. Press the appropriate button or proceed ignoring the pre-check errors.

Note: Ignoring the pre-check errors may result in a failed installation.

If you have not selected the embedded Jetty Application Server, you must stop and undeploy any previous version of the application. This message box reminds you to stop and undeploy the application before you proceed.

Stop and undeploy applications		
?	Please stop and undeploy older version of the application 'IBM ECM SM GUI Server' and 'IBM ECM SM Server' before proceeding with the new installation.	
	Press the 'Proceed with installation' button after you've undeploed and uninstalled previous versions or press exit 'Cancel and Exit'.	
	Cancel and Exit Proceed with installation	

ECM SM Installation: WAS message box

All required parameters are specified now. Review the displayed parameters and press the 'Install' button, if no changes are required.



ECM SM Installation: Pre-installation overview panel

The installation has started. Depending on the installation parameters different packages are installed now.

IBM Enterprise Content Manager	ment System Monitor Server
	Installing IBM Enterprise Content Management System Monitor Server
IBM.	IEM.
Enterprise Content Management	
	IBM® Enterprise Content Management System Monitor Version 5.1.0 Usensed Materials - Property of IDM Corp. 5724-F91 © Cocyright 2000-2012 CENIT AC, Cermany: © Copyright 2005, 2012 IDM Corporation. IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions workdwide. Built on Eblices is a tracemark of Eclipse - Rundation, Inc. Java and al Java-based trademarks and logos are trademarks or registered trademarks of oracle and/or its affiliates. This Program is Icensed under the terms of the icense agreement accomparying the Program. This Icense agreement: may be either located in a Program cirectory tolder or Ibrary identified as "License" or "Non_IBM_License", il applicable, or proviced as a printed license agreement. Plasse read this agreement carefully before using the Program. By using the Program, you agree to these terms.
	Installing Java Runtime Environment
InstallAnywhere	
Cancel	

ECM SM Installation: Installation packages are being installed

After the package installation step is finished, the new ECM SM configuration, database environment as well as the required services are being installed.

IBM Enterpr	rise Content Management System Monitor Server
BI	uilding ECM SM configuration, Building ECM SM database, generating services/daemons

ECM SM Installation: ECM SM configuration progress bar

Installing DDL files

If 'Create DDL files only' was specified at the Database settings panel then the following progress bar is displayed:



ECM SM Installation: DDL-only ECM SM configuration progress bar (first part)

After finishing the first installation and configuration steps the installer shows the following panel:

IBM Enterprise Content Managem	nent System Monitor Server
	Manual DB interaction is required
Enterprise Content Management System Monitor	Now a generated DDL file need to be executed on the database server to create additional database tabels before you proceed with the update process. Please copy all SQL files from the folder C:\Program Files (x86)\IBM\FSM\DDL\ to the database server (if remote) and run the scripts with sufficient Database rights. After successful completion select the 'Proceed with installation' button.
Cancel Help	Previous

ECM SM Installation: Manual database interaction required

The created Database description files need to be executed by a database administrator. After successful manual creation of the ECM SM database tables select the 'Process with installation' checkbox and press the 'Next' button.

Note: the installation will fail, if the manual database creation wasn't successful and complete.

There are two DDL files like <db_name>.sql and <db_name>_monitoring.sql. First execute the <db_name>.sql and after that <db_name>_monitoring.sql script.

NOTE The # is used as command separator for IBM DB2. For Microsoft MSSQL GO is used and for Oracle /. Tell your IBM DB2 to use # as command separator or change it in the created files <db_name>.sql and <db_name>_monitoring.sql. Using a semicolon is not possible in all cases because they are used in stored procedures. For IBM DB2 the DB2 Control Center (DB2CC) and the IBM Data Studio offer a input field to define the separator. Do not forget to commit the database action taken, depending on your db tool, via SQL action.

After pressing the 'Next' button the installer shows the following progress bar:



ECM SM Installation: DDL-only ECM SM configuration progress bar (second part)

Installation Status

At the end of the configuration step the installation status is displayed. If Installer debugging was enabled then the complete Installation process output is displayed in the scroll area.

IBM Enterprise Content Managen	nent System Monitor Server
	Output of ECM SM update
	Output
	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET S_PROD_TYPE_NAME=FSM_SERVER
IBM.	C:\Users\faas\AppData\Local\Temp\/1347421469\Windows>SET S_PROD_NAME=FSM
Enterprise Content Management System Monitor	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET INST_DIR=C:\Program Files (x86)\IBM\ECMSM
	C:\Users\faas\AppData\Local\Temp\l1347421469\Windows>SET CENIT_ROOT=C:\Program Files (x86)\IBM\ECMSM
	C:\Users\faas\AppData\Local\Temp\I1347421469\Windows>SET CENIT_ROOT_FW=C:/Program Files (x86)/IBM/ECMSM
	C:\Users\faas\AppData\Local\Temp\I1347421469\Windows>SET CREATE_DDL_FILE=false
	C:\Users\faas\AppData\Local\Temp\I1347421469\Windows>SET STEP_ONE=true
	C:\Users\faas\AppData\Local\Temp\I1347421469\Windows>SET STEP_TWO=true
	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET CALA_REX_SRV_PASSWD=
	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET CALA_REX_SRV_USER=
	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET INTERP=w32-ix86
	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET JAVA_DEBUG_PARAMETER= -Dde.cenit.eb.sm.installer.debug=true
InstallAnwhere	
Cancel Help	Previous

ECM SM Installation: Detailed installation output

At the end of the scroll area you will find the Exit code of the installation process.

IBM Enterprise Content Manager	ment System Monitor Server
	Output of ECM SM update
	C:UsersItaas\AppData\Local\I emp\l1347421469\Windows>SEI S_JDBC_PROVIDER_DIR=org.postgresql
IRM.	C:\Users\faas\AppData\Local\Temp\l1347421469\Windows>SET INT_LOG_FILE=IBM_ECM_SM_SERVER_install_internal_installer.log
Enterprise Content Management System Monitor	C:\Users\faas\AppData\Local\Temp\\1347421469\Windows>SET INT_ERR_FILE=IBM_ECM_SM_SERVER_install_error_internal_installer.log
	C:\Users\faas\AppData\Local\Temp\I1347421469\Windows>SET PACKAGE_NAME=
	C:\Users\faas\AppData\Local\Temp\l1347421469\Windows>del /F /Q "C:\Program Files (x86)\IBM\ECMSM\IBM_ECM_SM_SERVER_install_error_internal_installer.log" 1>NUL 2>NUL
	C:\Users\faas\AppData\Local\Temp\1347421469\Windows>del /F /Q "C:\Program Files (x86)\IBM\ECMSM\IBM_ECM_SM_SERVER_install_internal_installer.log" 1>NUL 2>NUL
	C:\Users\faas\AppData\Local\Temp\l1347421469\Windows>"C:\Program Files (x86)\VBM\ECMSM\jre\bin\java.exe" -Dde.cenit.eb.sm.installer.debug=true -cp "C:\Program Files (x86)\VBM\ECMSM\installtools\de.cenittfinca.functional.utils.jar,C:\Program Files (x86)\VBM\ECMSM\installtools\com.trustice\javatar.jar" -Djava.ext.dirs="C:\Program Files (x86)\VBM\ECMSM\jre\Vib\ext,C:\Program Files (x86)\VBM\ECMSM\JeNLet,C:\Program Files (x86)\VBM\ECMSM\extfinca.external.jdbc\org.postgresql" de.cenit.eb.sm.finca.functional.utils.tools.installer.Installer.SM_SERVER install 1>"C:\Program Files (x86)\VBM\ECMSM\VBM_ECM_SM_SERVER_install_internal_installer.log" 2>"C:\Program Files (x86)\VBM\ECMSM\VBM_ECM_SM_SERVER_install_error_internal_installer.log"
	STDERR
	Exit code:
InstallAnywhere	1
Cancel Help	Previous Next

ECM SM Installation: Exit code of the installation process

Installing JRE

Pressing the next button will start the installation of the previously selected JRE subpackage.

Note: No additional installations panels show up.



ECM SM Installation: JRE Installation progress bar

CALA_REX agent installation

Installing CALA_REX

Afterwards the CALA_REX agent images InstallAnywhere installer started.

Note: No additional installation panels show up.



ECM SM Installation: CALA_REX agent images Installation progress bar

Embedded agent installation

In the case the installation of the embedded CALA_REX agent was activated the following installation progress bar will be displayed:



Embedded CALA_REX agent installation progress bar

If the Installer debugging is enabled the agent installation result screen will be displayed afterwards.

Final steps

After the sub-packages are installed successfully the 'Installation Complete' panel is displayed with the overall Exit code.

IBM Enterprise Content Managem	nent System Monitor Server
	IBM Enterprise Content Management System Monitor server installation result
LEM. Enterprise Content Management System Monitor	The IBM Enterprise Content Management System Monitor server installation completed with return code 0 Press the 'Next' button to configure the system.
InstallAnywhere Cancel Help	Previous

ECM SM Installation: Installation completed panel

If the installation finished with Exit code '0' then the next panel shows up.

IBM Enterprise Content Managen	nent System Monitor Server
	Installation done
	Congratulation! IBM Enterprise Content Management System Monitor Server successfully installed at:
	C:\Program Files (x86)\ibm\ECMSM
IRM.	You can logon to the ECM SM Console with the following Link:
Enterprise Content Management	http://N7P0015764Bit.de.cenit-group.com:23990
System Monitor	Select "Done", to close the installer.
Installânwehere	
Cancel Help	Previous Done

ECM SM Installation: Installation successful panel

In the case the installation was based on WebSphere a successful installation is completed with the following panel. You'd need to deploy (install) and start the two displayed ear-files (Web Applications) to your WebSphere Server The deployment of the ECM_SM on IBM WebSphere. Before you start the WebSphere Application don't forget to define the Application Specific Data source and define the JVM custom properties as described in the JVM Properties for an IBM WebSphere Based Installation.

IBM FSM Server				
Installation done - Deploy WAS Applications now				
Hasic Server settings				
Event forwarding settings	Congratulation! IBM FSM Server successfully installed at:			
LDAP Advanced settings	O/Decement Files (#00)//DMOve Har			
Advanced Server settings	C.IProgram Files (x86)/IBM/SysMon			
Ø Database settings	Before can logon to the FSM Console you'd need to install and deploy the WebSphere Applications			
Connection test result	C:\Program Files (x86)\IBM\SysMon\application_server\FSM_SERVER_gui_app.ear			
Services / Daemon behaviour	and C:\Program Files (x86)\IBM\SysMon\application_server\FSM_SERVER_server_app.ear to your WebSphere Application_Server w7p00157 de cenit-group com (port: 23990)			
Shell download result	to your webophere Application cerver witpoortor. de.cenic group.com (porc 20000).			
Windows Shell location	Note: Do not forget to create the specified WebSphere Datasource FSM_DS before deployment.			
Install required software packages	See documentaion for further details.			
Pre-Installation - Overview	Select "Finish", to close the installer.			
Installing				
Output of configuration and services installation action				
Output of configuration and daemons installation action				
Output of configuration				
DDL - manual interaction				
S is				
Output of Conversion				
installation action				
Output of Server Agent installation action				
Cancel Help	Previous Done			

ECM SM Installation: WAS-based successful installation panel

In the case of an exit code '0' the installer will automatically start the ECM SM Web Application in your default browser.

Note: The Default browser will only be started, if the ECM SM application is installed based on the Embedded Jetty Application Server.

The first login

n7p0015764bit.de.cenit-grc ×	a. 1997	
$\leftrightarrow \rightarrow \mathbf{C}$ [] n7p0015764bit.de.cenit-group.com:23	990	🚖 🔧
		IBM Enterprise Content Management System Monitor
File Help		
1		
	×	
	Login	
	Please enter your credentials.	
	User	
	OK Cancel	

ECM SM Installation: ECM SM Login Screen

After login with the ECM SM admin user (startup-password is 'admin') you'll see a similar ECM SM Event Console. Process with the ECM SM Users guide for further information about the ECM SM Web Console handling.

n7p0015764bit.de.cenit-grc ×	5		10.1 deal late constants	
← → C 🗋 n7p0015764bit.de	e.cenit-group.com:23990			🚖 🤸
)) Fullscreen				IBM Enterprise Content Management System Monitor
File Window Desktop Tools Help				
Tree 🛛 🖓 🖓	🗖 Event List 🛛 📑 Event De	atails 📑 Business View	📽 De-/Select All 👏 Refresh 😋 Automatic R	lefresh 🎯 History View 🎾 Filter 🛛 🗢 🗖
SYSTEM SYSTEM SYSTEM SYSTEM SYSTEM SYSTEM HOST HOST INSTANCE	Timestamp =	Severity Value	Full Qualified Host Nar Application Nam	e Datastream Message Text
	Goto Page		Page 1 of 1	Event 0 - 0 of 0
	📑 Knowledge Base Entry 🛿			🛟 Add 💥 Delete 🔻 🗖 🗖
	Knowledge Base Entry No Entry No entry available.			
ECM SM Server Status 🛛 🗍				
Status:				
Check Now			adm	



Installation and configuration of the ICN integration (ECM SM plug-in)

This section describes the configuration steps to deploy the ICN integration ECM SM plug-in.

HTTPS-enabled ECM SM GUI server

In order to connect to an HTTPS-enabled ECM SM GUI server, the underlying WebSphere instance needs the servers signer information added to its TrustStore. To do so, log in to the WebSphere Console (https:// websphere:9043/ibm/console) and navigate to 'Security', 'SSL certificate and key management', 'Key stores and certificates', 'TrustStore', 'Signer certificates', 'Retrieve from port'.

Enter the hostname and port of each ECM SM GUI server you want to connect to including the one you want to load the plug-in from.

WebSphere. software	Welcome websphere	Help Logout I
	Cell=dev-machineNode01Cell, Profile=p8-dev	Close pa
View: All tasks	SSL certificate and key management ? -	Help
Welcome Guided Activities	SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > Retrieve from port	Field help For field help information,
± Servers	makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the signer from the server during the handshake.	select a field label or list
Applications	General Properties	displayed.
E Services	+ Host	Barra bata
Resources	minpuss/s	More information about this
j kourdy • Obbit sourty • Sourty density • Sourth extentions extentions • SSL certificate and key management • Security auditog • Bos sourthy	Port [23990 SSt.configuration for outbound connection NodeBealutISSLEettings Alas	Command Assistance View administrative scripting command for last action
Environment		
System administration	Retrieve signer information	
Users and Groups	Retrieved signer information	
Monitoring and Tuning	Saria number	
Troubleshooting	Jena namoei 102244201	
Service Integration	10/#767	
i noot	Issued to [N=ninp03575.de.cenit-group.com, OU=IBM FSM, O=IBM FSM, L=Unknown, [ST=Unknown, C=Unknown Issued by [Ch=ninp03575.de.cenit-group.com, OU=IBM FSM, O=IBM FSM, L=Unknown, [Ch=ninp03575.de.cenit-group.com, OU=IBM FSM, O=IBM FSM, L=Unknown, ST=Unknown, C=Unknown Fingerprint (SHA digest)	
	44:73:17:72:27:87:5C:02:4B:49:BE:4B:4F:21:8F:6F:99:03:4A:A2	
	Validity period Juli 3, 2016 Apply OK Reset Cancel	
	Appy UK Keset Cance	

ECM SM Installation: IBM Content Navigator ECM SM plug-in - Import server certificate in WebSphere.

Installation and configuration of the ICN integration (ECM SM plug-in)

This chapter describes the installation and configuration of the IBM Content Navigator (ICN) plug-in for IBM ECM SM. The plug-in enables users to view the overall status of their managed IBM ECM environment without opening the IBM ECM SM UI.

Please use the following description to install the ECM SM plug-in.

Login to the **IBM Content Navigator (ICN)** UI as administrative user. Click on the maintenance (gear) icon on the left side and select 'Plug-ins'. Press the **New** button to install the new ECM SM plug-in.

Desktops	E Desktops ×]		
Repositories Sync Services	You must use the adn	ninistration tool to reg	ister plug-ins	for the web	client. If a plu
FileNet Content Manager	Important: If you edit invoked in the order th	a plug-in that is refere at they are listed. If a	enced in anot plug-in need	her area of th Is to be run b	ne administra efore anothe
Daeja ViewONEViewer Maps	New Plug-in	dit Enable	Disable	Delete	Refresh
Plug-ins	Name				

ECM SM Installation: IBM Content Navigator Plug-in administration

Type the following URL into the text box and press the **Load** button to load the plug-in. The URL depends on the ICN version, the system name and the type of the server: http[s]://<ECM SM servername>:<GUI-or-Downloadserver-port>/downloads/ICN/ECMSystemMonitorPlugin[-2.0.2].jar. If you want to use the plug-in with ICN 2.0.2 please add the '-2.0.2' suffix to the URL. The recommended ICN version is 2.0.3.

Example URL for ICN 2.0.3 and HTTPS:

https://myserver:23990/downloads/ICN/ECMSystemMonitorPlugin.jar

Example URL for ICN 2.0.2 and HTTP:

http://myserver:23990/downloads/ICN/ECMSystemMonitorPlugin-2.0.2.jar

Desktops × - Plug-ins	× 📑 *IBM Enterprise Content Management System Monitor for IBM Content Navigator 🗙	
Save and Close Save Re	set Close	
Plug-in: IBM Enterprise Con	tent Management System Monitor for IBM Content Navigator	
A plug-in can be either a JAR file or a	compiled class file.	
Important: The IBM Content Navigator web application server must be able to access the plug-in file on the local file system or through a URL.		
JAR file path: ?	https://myserver:23990/downloads/ICN/ECMSyster	
Class file path: ?	Load	
Class name: 🧃		
Name:	IBM Enterprise Content Management System Monitor for IBM Content Navigator	
Version:	5.2.0	

ECM SM Installation: IBM Content Navigator Plug-in - adding a new plug-in

After pressing the **Load** button the systems loads the plug-in. The version, the description and the required parameters of the plug-in will be displayed below.

Server Alias: ?	
Server URL: ?	
	Save Remove
Configured Servers:	http://nlinp04063:23990
Reset Configuration:	RESET User Settings RESET Plugin Settings

ECM SM Server Configuration

ECM SM Installation: IBM Content Navigator Plug-in - speficy plug-in settings.

Please make sure to press the **Save** button before proceeding with the server configuration.Specify the ECM SM server URL and an alias for each entry. The format looks like: http(s)://<ECM SM servername>:<GUI-port>, example: https://myserver:23990

Press the **Save** button below the URL input field to store the new server in the ICN configuration. The configured servers are global for all ICN users. The ECM SM user-specific credentials are stored later separately for each ICN user.

Press the **Close** button to finish the plug-in configuration. Next, select **Desktop** from the sidebar and select either an existing desktop or create a new desktop.

B Desktops × ECM_SM	<			
Save and Close Save Res	et Close			
Desktop: ECM_SM				
			141 1 1	
General Repositories	Layout Appea	irance • Iv	Ienus Workflows	Mobile
* Name: 🥐	ECM SM	N		
	_			
* ID: 🥐	ECMSM			
Description:				
 Authentication 				
* Repository: P8DEV		•		
Limit access to specific users and g	roups 🔿 Enable	Disable		
	Desktops × ECM_SM > Save and Close Save Rese Desktop: ECM_SM General • Repositories • Name: Description: Authentication Repository: P8DEV Limit access to specific users and g			Desktops × ECM_SM × Save and Close Save Reset Close Desktop: ECM_SM • General • Repositories • Layout Appearance • Menus Workflows • Name: ? ECM_SM • ID: ? ECMSM Description: • Authentication • Repository: P8DEV Limit access to specific users and groups O Enable O Disable

ECM SM Installation: IBM Content Navigator ECM SM plug-in - editing an existing desktop

If you plan to create a new desktop the desktop name will be used later to login to the ICN. Add the ECM SM plug-in to the ICN desktop you selected or created and store the new / updated desktop.

Desktops	B Desktops	× 🔝 New De	esktop ×				
E Repositories		_					
Sync Services	Save and Clo	ose Save	Reset Clo	ose			
FileNet Content Manager							
OD Content Manager OnDemand	Desktop: New Desktop						
Daeja ViewONE							
 Viewer Maps 	A desktop det	ermines what the us	er can see and	do when they log i	n to the web cli	ient. After you cre	ate a desktop,
	General	 Repositories 	 Layout 	Appearance	Menus	Workflows	Mobile
Menus							
T Labels	Name. ?						
Themes	* ID: 0						
🚊 Icon Mapping							
🚘 Settings	Description:						
-	-						
	- Authentie	cation					
	* Repository	Select a reposito	ory		•		

ECM SM Installation: IBM Content Navigator ECM SM plug-in - Create a new desktop (1 of 2)

Specify the desktop name and the desktop ID in the General tab.

NOTE The desktop ID will later be used within the desktop URL. The selection of a Content Repository in the **Repositories** tab is recommended. Access to the desktop can be limited in the Authentication section of the General tab. Please check the IBM Content Navigator documentation for details.

B Desktops	s × 📑 ECM_S	M ×					
Save and Cl	ose Save	Reset	se				
Desktop: E	CM_SM						
General	Repositories	• Layout	Appearance	Menus	Workflows	Mobile	
 Desktop Specify whi * Layout 	Features ich features users car ? ecm.	n access from th	is desktop. Additic NavigatorMainLay	onally, you can yout 🔹	customize the be	Phavior of each	feature that is included in the desktop. onfiguration
* Display features:	Yed Mov	e Up Move Feature Home Browse Search Event M	a Down				Select a feature to configure

ECM SM Installation: IBM Content Navigator ECM SM plug-in - Create a new desktop (2 of 2)

Select the Layout tab and tick the Event Management feature. PressSave to add the plug-in's feature to the sidebar of the configured desktop.

The IBM Content Navigator ECM SM plug-in can now be used.

Open the browser and type in the URL of the new ICN desktop containing the ECM SM plug-in with the following URL: http(s)://<hostname-hosting-ICN>:<port>/navigator/?desktop=<ECM SM ICN-Desktop ID>, example: http://myicnserver:9081/navigator/?desktop=ECMSM

In the sidebar select the **Event Management** feature and choose one of the previously configured ECM SM servers from the server dropdown list. Enter your ECM SM credentials and press the **Connect** button to load the configured Custom Trees of the selected ECM SM server.



ECM SM Installation: IBM Content Navigator ECM SM plug-in - Overview

Activating monitoring for the ECM SM server

After installing the ECM SM server, monitoring for the server must be activated to receive events in the console.

- Login to the console as described in section The first login
- Choose Tools ECM SM Base agents and non Core ECM Agent Installer from the menu
- Depending on your browser settings, a warning similar to the following may be shown. Select **Run** to start the installer.

Warning - Secu	rity	×
The applic Do you wa		
Name:	IBM FSM Non Core System Setup	
Publisher:	CENIT AG	
From:	http://nxpp00902.de.cenit-group.com:23990	
🥅 Always t	rust content from this publisher.	
	Run	Cancel
Part of trust	of the application is missing a digital signature. Only run if you <u>M</u> ore I the origin of the application.	nformation

Browser security warning

• A login window will be opened. Log in with the same credentials you used for the console login.

User:	
Password:	
	Ok Cancel

Installer Login

• The installer opens. Select **Remote machine** in the **Install Method** section on the right, then select the ECM SM server in the **Hostname** combobox. Press the **Install and configure** button to start the installation.

File Help					
	IBM* Enterprise Content Management Syste Version 5.1.0	em Monitor		IBM	
Install information		Install met	hod		
				O Local machine	
Product:	cala			Remote machine	•
Hostname:	N7P02471B64BIT.de.cenit-group.com	File transf	ег:	cala_rex	•
Operating system:	Windows NT/2000/XP	Remote ex	kecution:	cala_rex	-
	LI			Copy files only	
Install directories					
Source directory	crx://renos/install				
Target directory:	C:/opt/ia_stuff/ia_fp2/cala				
JDK path	C:\opt\programs\java\jre_1_6_26				
Install options					
Keep monitor se	ettings Autos	start mode:	After inst	tall and at boot time	-
Reconfigure only	Y .				
Create environm	nent file				
Uninstall					
- Selected configurat	tion				
Configuration: FCM	A SM CLIENT WINDOWS				
This is an IBM ECM SM agent configuration set for Microsoft Windows operating systems.					
	Set configuration variables	Copy config	uration fro	om	
	Install and configure	Exit	Help		

Installer Window

• After the installation has finished, events from the ECM SM server will arrive in the console.

How to update expired ECM SM server certificates

ECM SM server installations generate several certificates for the communication between server, managed systems and the Web Console at installation time. If the ECM SM server was updated several times it may happen that the certificates expire (after 2 years). If the communication between the ECM SM server and the managed systems use the server certificate be aware that all agents require new certificates that apply to the updated server certificate, too.

To generate new certificates the following steps are required.

Delete existing certificates

Delete the ECM SM server certificate files <ECM SM-install-directory>/keys/*.pem on the ECM SM server.

Update the Server with the latest Fixpack

Install the latest ECM SM Fixpack. It will create new server certificates.

Optional: Generate new certificates for agents.

If the agent communication is based on the server certificates generate new agent certificates, too. See chapter 'Creating an SSL certificate for the agent' in the Installation Guide for further information.

CALA_REX and Task execution logging on the Server and Agents

Since version 5.2.0 the logfiles for tasks and monitors will be logged to \$CENIT_ROOT/cala/temp. Create the ".plusdebug" debugging directory in this directory. The CALA_REX logfile (cala_rex logging) will be written to \$CENIT_ROOT/cala_rex/logs when configured using the "Configure Debug Settings" task.

Troubleshooting

If the login fails you should verify all log files in the **\$CENIT_ROOT** directory (for InstallAnywhere and internal log files) and in the **\$CENIT_ROOT/var/log** directory.

Event forwarding to an ESM System via Logfile

ECM SM supports the generation of report (log) files. Besides SNMP trap based event forwarding this is the most common way to forward events from one event management system to another. ECM SM server supports the generation of free formatted report / logfiles that can be parsed by other systems.

Please refer to section Event forwarding via Log file for detailed information on how to activate and configure this functionality. Additional information about the filesink component that writes to report (log) files can be found in the ECM SM Users Guide, chapter 'Webconsole - Serverconf Console' in the section 'The Server Configuration Console', sub-section 'The Rules Engine Plug-Ins'. A description of possible place-holders in logfile names can be found in the ECM SM Users Guide, chapter Webconsole - Serverconf Console - Serverconf Console in the section 'The Rules Engine Plug-Ins'. A description of possible place-holders in logfile names can be found in the ECM SM Users Guide, chapter Webconsole - Serverconf Console in the section 'The Event Mapping View', sub-section 'ReplacementHandlers'.

Note: This is the common way to forward ECM SM events to IBM Tivoli Monitoring Version 6 and to IBM Tivoli Enterprise Console.

Event integration to an ESM System via SNMP

ECM SM servers support forwarding of ECM SM events as SNMP traps to any SNMP Manager.

This is the easiest and most common way to forward ECM SM events into an existing Enterprise System Management environment.

The system supports the following SNMP versions:

- SNMP V1
- SNMP V2C
- SNMP V2C inform

The SNMP forwarding mechanism needs to be configured during ECM SM Server installation.

ECM SM SNMPv1 traps and variable settings

The following SNMPv1 traps of enterprise 1.3.6.1.4.1.8235.0 (enterprise CENIT) are generated by ECM SM:

Name	Trap number	Severity
cenitGeneric	0	Warning
cenitHarmlessLogfile	101	Normal
cenitWarningLogfile	102	Warning
cenitMinorLogfile	103	Minor
cenitCriticalLogfile	104	Major
cenitFatalLogfile	105	Critical
cenitHarmlessMonitoring	201	Normal
cenitWarningMonitoring	202	Warning
cenitMinorMonitoring	203	Minor
cenitCriticalMonitoring	204	Major
cenitFatalMonitoring	205	Critical

Each ECM SM SNMPv1 trap contains the following SNMP variables

Name	OID	Туре	Note
Event	1.3.6.1.4.1.8235.1.1.1.1	STRING	Error Id, Event Class or Monitor name
Source	1.3.6.1.4.1.8235.1.1.1.2	STRING	Logfile name or Monitor cmdline parameters
Message	1.3.6.1.4.1.8235.1.1.1.3	STRING	Logfile Message text or monitor result
Timestamp	1.3.6.1.4.1.8235.1.1.1.4	STRING	Timestamp of event

Name	OID	Туре	Note
Original Error Text	1.3.6.1.4.1.8235.1.1.1.5	STRING	Original error text from logfile or Monitor debug output
Error cause	1.3.6.1.4.1.8235.1.1.1.6	STRING	Error cause or empty
Corrective Action	1.3.6.1.4.1.8235.1.1.1.7	STRING	Corrective action or empty
Repeat count	1.3.6.1.4.1.8235.1.1.1.8	NUMERIC	Number of identical events
Hostname	1.3.6.1.4.1.8235.1.1.1.9	STRING	Hostname, where the events was detected

ECM SM SNMPv2c or SNMPv2c Inform traps and variable settings

The following SNMPv2c traps of enterprise 1.3.6.1.4.1.8235.2.0 (enterprise cenitNotifications) are generated by ECM SM:

Name	Trap number	Severity
cenitGeneric	0	Warning
cenitHarmlessLogfile	101	Normal
cenitWarningLogfile	102	Warning
cenitMinorLogfile	103	Minor
cenitCriticalLogfile	104	Major
cenitFatalLogfile	105	Critical
cenitHarmlessMonitoring	201	Normal
cenitWarningMonitoring	202	Warning
cenitMinorMonitoring	203	Minor
cenitCriticalMonitoring	204	Major
cenitFatalMonitoring	205	Critical

Each ECM SM SNMPv2 trap contains the following SNMP variables

Name	OID	Туре	Note
snmpTrapEnterprise	1.3.6.1.6.3.1.1.4.3.0	OBJID	Enterprise of the received v2 trap (cenit)
Agent Timestamp	1.3.6.1.2.1.1.3.0	TIMETICKS	Timestamp of the CALA SNMP Agent
snmpTrapOID	1.3.6.1.6.3.1.1.4.1.0	OBJID	SNMP Trap OID of the received trap
Trap OID	1.3.6.1.4.1.8235.0	OBJID	Trap OID of this event
Event	1.3.6.1.4.1.8235.1.1.1.1	STRING	Error Id, Event Class or Monitor name
Source	1.3.6.1.4.1.8235.1.1.1.2	STRING	Logfile name or Monitor com- mand line parameters
Message	1.3.6.1.4.1.8235.1.1.1.3	STRING	Logfile Message text or monitor result
Timestamp	1.3.6.1.4.1.8235.1.1.1.4	STRING	Timestamp of event
Original Error Text	1.3.6.1.4.1.8235.1.1.1.5	STRING	Original error text from logfile or Monitor debug output
Error cause	1.3.6.1.4.1.8235.1.1.1.6	STRING	Error cause or empty

Name	OID	Туре	Note
Corrective Action	1.3.6.1.4.1.8235.1.1.1.7	STRING	Corrective action or empty
Repeat count	1.3.6.1.4.1.8235.1.1.1.8	NUMERIC	Number of identical events

Prepared MIB files

If you plan to forward SNMP messages to an SNMP Manager you need to import the appropriate MIB files into your SNMP Manager.

You will find prepared MIB files on the installation media in the directory <INSTALL_MEDIUM_DIR>/MISC/ SNMP.

SNMP Version	MIB Filename
cenit_snmp_v1.mib	SNMPv1
cenit_snmp_v2.mib	SNMPv2c and SNMPv2c inform

Please consult the SNMP Managers user guide for further information.

NOTE You can import both files into your SNMP Manager.
Prepared trap definition files

SNMP Managers (IBM Tivoli NetView, HP OpenView, Enterasys Networks NetSight Element Manager, e.g.) need trap definition files to handle SNMP traps correctly.

You will find trap definition files for different SNMP Managers <Installation-directory>/MISC/SNMP directory on the ECM SM server.

Filename	Function
cenit_trapd_IBM_NV_UNIX.conf	ECM SM SNMPv1 and SNMPv2 trapd.conf extensions for IBM NetView for UNIX Version 7 and newer
cenit_trapd_IBM_NV_Windows.conf	ECM SM SNMPv1 trapd.conf extensions for IBM NetView for Windows and IBM NetView for UNIX prior Version 7
cenit_trapd_HPOV_and_NEM.conf	ECM SM SNMPv1 and SNMPv2 trapd.conf extensions for HP Openview Node Manager and Enterasys Networks NetSight Element Manager
cenit.trapdef	Enterasys Networks NetSight Element Manager trap definition file for ECM SM SNMPv1 traps (enterprise cenit)
cenitNotifications.trapdef	Enterasys Networks NetSight Element Manager trap definition file for ECM SM SNMPv2 traps (enterprise cenitNotifications)

If you want to forward ECM SM SNMP traps to another SNMP Manager you may need to change one of the prepared trap definition files.

Please consult your SNMP Manager's user guide for further information about trap definition settings.

Event forwarding to HP OpenView Operations (OVO)

ECM SM supports forwarding of ECM SM events to HP OpenView Operations (OVO). On ECM SM server a HP OpenView Operations Agent has to be installed to forward events to HP OpenView Operations. Events from ECM SM managed systems (clients) are forwarded by the ECM SM server communication via HP OpenView Agent to the HP Open View Server.

IMPORTANT There are different types of HP OpenView Agents available. ECM SM message forwarding is only supported with the https-Agents (HP OpenView OVO 8.x HTTPS Agent for Windows, HP-UX and Solaris). Refer to the HP OpenView documentation about details on how to install and configure the required HP OpenView Agent from the HP OpenView Server on the ECM SM server. There is no need to install any HP OVO agent or software on ECM SM managed systems (clients). The ECM SM forwarding component uses the same mechanism as the HP OpenView command "opcmsg". If there are any issues with the transaction of ECM SM messages to the OVO system (for example the sent events are not received by the server), it is recommended to check the HP OpenView documentation about "how to send messages via opcmsg". If "opcmsg" works correctly from the ECM SM server then the ECM SM component will work correctly, too.

Please refer to the ECM SM Release Notes regarding supported OVO agent version and required OVO patches.

Customizing the ECM SM Web Console

Changing Fonts and Colors

ECM SM is based on the <u>Eclipse Rich Ajax Platform</u>. HTML properties can be configured via a cascading style sheet definition file. Find the file at <installation path>/ext/finca.gui.style/theme/fsm/fsm.css.

For details refer to the RAP Theming documentation located at <u>http://wiki.eclipse.org/RAP_Theming</u>.

Note that the ECM SM gui service must be restarted in order to make use of a changed style sheet.

Icon Sets

A user can choose between multiple icon sets (see Window Views User Preferences Presentation Iconset). ECM SM provides two icon sets by default: *ECM SM45* and *ECM SM40*.

To add a own icon set, the following steps are necessary:

- Copy the directory structure from <installation path>/gui/icons/ECM SM45 to <installation path>/gui/icons/<name of your icon set>.
- Adjust icons to your needs.
- Load the file <installation path>/eventserver/cfg/finca-cfg.xml into an editor, search for the lines

```
0001 <property name="de.cenit.eb.sm.finca.functional.usermgmt.icondir" d
    type="listbox">
0002 <listitem name="ECM SM40"/>
0003 <listitem name="ECM SM45"/>
0004 </property>
```

and create an entry for the new icon set

```
0001 <property name="de.cenit.eb.sm.finca.functional.usermgmt.icondir" 
    type="listbox">
0002 <listitem name="ECM SM40"/>
0003 <listitem name="ECM SM45"/>
0004 <listitem name="name of your icon set"/>
0005 </property>
```

Note that the ECM SM gui service must be restarted in order to make use the new icon set.

How to Configure and Use the UnifiedDatabaseClient (UDC)

General

The UnifiedDatabaseClient (UDC) is a command line tool to execute SQL queries on several RDBMS and display the result in a uniform database independent way.

Requirements

To use the UnifiedDatabaseClient, you need the JDBC driver of your RDBMS. Download the driver from the homepage of the database vendor. Please refer to chapter *Databases* in the *ECM SM Hardware & Software Requirements* guide for details.

UDC requires Java 7 or higher.

Usage

Parameters for the UDC are read from command line arguments. The following parameters are supported:

Configuration file property	Command line switch	Description/Allowed values/Defaults
udc.database.type	-d <type></type>	Database type. Optional. Default <i>DB2</i> . Valid values: <i>DB2</i> , <i>MSSQL</i> , <i>ORACLE</i> , <i>MYSQL</i> , <i>DER-BY</i> .
udc.database.type.subtype	-d <type>:<subtype></subtype></type>	Database version depending on the data- base type; e.g. 9.1 for database type ORA- CLE or 2000 for database type MSSQL. Optional. The default is database type dependent.
udc.database.server.id	-s <database server=""></database>	Hostname or IP address of the database server to connect to. Optional. Default is <i>localhost</i> .
udc.database.user.id	-u <database id="" user=""></database>	The ID of the database user, who is con- nected to the database and executes SQL statements. Non optional. No default. Empty string is not allowed.
udc.database.user.pwd	-p <database user<br="">password></database>	The password (pwdcrypt coded) of the data- base user, who is connected to the database and executes SQL statements. Non optional. No default. Empty string is allowed.
udc.database.db.id	-db <database id=""></database>	ID of the database to connect to. This can be a database specific formated string. Non optional. No default. E.g. to allow the spec- ification of database instances for MS SQL Server or table spaces for Oracle.
udc.database.jdbc.port	-jp <jdbc port=""></jdbc>	Port used for the JDBC connection. Option- al. The default is JDBC driver/database type dependent (50000 for IBM DB2).
udc.database.jdbc.driver.class	-jc <jdbc driver<br="">class></jdbc>	The JDBC driver class. Optional. The default is JDBC driver/database type dependent. Optional. Default is RDBMS specific.
udc.database.jdbc.driver.url	-ju <jdbc driver="" url=""></jdbc>	The JDBC driver URL. Optional. The default is JDBC driver/database type dependent. Default is RDBMS specific. If not defined, the values will be taken from the -d, -s, -jp and - db parameters.
udc.output.type	-o <output type=""></output>	The output should be in the specified format. Optional. The default is <i>udc</i> . Valid values: <i>csv</i> , <i>xm</i> 1, <i>htm</i> 1, <i>udc</i> .
udc.output.separator	-outsep <output sepa-<br="">rator></output>	Separator for output. Used for <i>csv</i> , <i>udc</i> and if none of the above listed output types is defined. Optional. Default is ; ; ; ;

Configuration file property	Command line switch	Description/Allowed values/Defaults
udc.output.resultseparator	-resultsep <output result separator></output 	Separator between results of SQL state- ments in the output. Used for <i>csv</i> , <i>udc</i> and if none of the above listed output types is defined. Optional. Default is
udc.query.separator	-querysep <query sepa-<br="">rator></query>	Separator for multiple queries to be executed. Optional. Default is ;
udc.action.commit	-nc	The client will not commit any data changing SQL statement, if the database is not config- ured as autocommit. Optional. The default is to commit the changes.
udc.action.testconnection	-t	The client will only test the JDBC connec- tion and not execute any SQL statement Any SQL statement given on the command line will be ignored. In case the connection could be established and closed successfully, o (zero) is returned. In all other cases 1 (one) or higher is returned.
-	-exec	Query to be executed. Surrounded by double quotes (e.g. "SELECT * FROM").
-	-execfile	Read queries (one ore more) to be executed from given filename.
-	-debug	Print debug information to stderr. Optional. Default is to use no debug output.
udc.action.time	-calc	Three additional time spans (in milliseconds) are calculated and displayed on the com- mand line: The time span, it took to con- nect to the database (login time span), the time span, it took to execute SQL statements (execution time span) and the complete time (adding up login and execution time spans in milliseconds).

Some optional parameters will be set by the UDC on runtime depending on the provided parameters.

For the JDBC Driver URL the parameters -d, -s, -jp and -db are used.

The JDBC Driver Class will be set using the -d parameter for the database type and subtype. In some cases the Driver Class and Driver URL are different for different subtypes of the database. If the default value doesn't match your affords, provide it as an command line argument.

The following examples are UDC calls from the command line for some different RDBMS. The minimal needed parameters are given, all other are default for the database type. For other subtypes the needed parameters may differ. For these examples the Java binary is in the path variable.

MySQL

java -Djava.ext.dirs=/opt/jdbc/mysql/:/opt/IBM/ECMSM/tools/de.cenit/ -cp . -jar /opt/IBM/ECMSM/ tools/de.cenit/universalDatabaseClient.jar -exec "SELECT * FROM MYTABLE" -d MYSQL -s myserver -u myuser -p <encrypted password> -db /MYDB

Defaults

- DB-Subtype: 5.0
- JDBC Driver Class: com.mysql.jdbc.Driver
- JDBC Port: 3306
- JDBC Driver URL: jdbc:mysql://<database server>:<jdbc port><database id>

Specials

• The parameter "?tinyIntlisBit=false" is used for the connection to the database to show tinyint fields as number, not as boolean values.

IBM DB2

java -Djava.ext.dirs=/opt/jdbc/db2/:/opt/IBM/ECMSM/tools/de.cenit/ -cp . -jar /opt/IBM/ECMSM/tools/ de.cenit/unifiedDatabaseClient.jar -exec "SELECT * FROM MYTABLE" -d DB2 -s myserver -u myuser -p <encrypted password> -db /MYDB

Defaults

- DB-Subtype: 9.5
- JDBC Driver Class: com.ibm.db2.jcc.DB2Driver
- JDBC Port: 50000
- JDBC Driver URL: jdbc:db2://<database server>:<jdbc port><database id>

Oracle

java -Djava.ext.dirs=/opt/jdbc/oracle/:/opt/IBM/ECMSM/tools/de.cenit/ -cp . -jar /opt/IBM/ECMSM/ tools/de.cenit/unifiedDatabaseClient.jar -exec "SELECT * FROM MYTABLE" -d ORACLE -s myserver -u myuser -p <encrypted password> -db :MYDB

Defaults

- DB-Subtype: 10g
- JDBC Driver Class: oracle.jdbc.driver.OracleDriver
- JDBC Port: 1521
- JDBC Driver URL: jdbc:oracel:thin:@<database server>:<jdbc port><database id>

Specials

- If you want to connect as sysdba or sysoper use "user as sysdba" or "user as sysoper" for the -u parameter (double quotes are needed around these value).
- You have to use the ORACLE_SID for connecting to an remote Oracle database, not the SQL-Netname.

MSSQL

java -Djava.ext.dirs=/opt/jdbc/mssql/:/opt/IBM/ECMSM/tools/de.cenit/ -cp . -jar /opt/IBM/ECMSM/ tools/de.cenit/unifiedDatabaseClient.jar -exec "SELECT * FROM MYTABLE" -d MSSQL -s myserver -u myuser -p <encrypted password> -db ;instanceName=MYINSTANCE

Defaults

- DB-Subtype: 2005
- JDBC Driver Class: com.microsoft.sqlserver.jdbc.SQLServerDriver
- JDBC Port: 1433
- JDBC Driver URL: jdbc:sqlserver://<database server>:<jdbc port><database id>

Windows authentication over JDBC driver

UDC requires the JDBC driver file sqljdbc4.jar from the Microsoft JDBC Driver for SQL Server version 4.0 package. Other Microsoft JDBC Driver for SQL Server versions and files are not supported.

Make sure that the directory contains only the JDBC driver file sqljdbc4.jar and remove the file sqljdbc.jar.

If you plan to use Windows Authentication for the MSSQL database connection, the file sqljdbc_auth.dll from the Microsoft JDBC Driver for SQL Server version 4.0 package is required, too. Make sure that the 32-bit version of the DLL is copied to the same directory as the JDBC driver file sqljdbc4.jar. The DLL is initially located in <installation directory>\sqljdbc_<version>\<language>\auth\x86.

Specials

- You can use -db instanceName=<instance>;databaseName=<databasename> for defining the database.
- To connect to an SSL secured SQL server, you can specify the required parameters with the -db parameter as well, e.g. -db instanceName=LOCAL;databaseName=mydb;encrypt=true;trustServerCertificate=true. See <u>http://</u> <u>msdn.microsoft.com/en-us/library/bb879935%28v=sql.105%29</u> for a list of possible parameters and more details.

Output

The UDC supports different output types. Default is the UDC format.

You could change the output type using the *-o <output type>* commandline switch. If you define an invalid value the UDC will use the default format.

UDC

```
java -Djava.ext.dirs=/opt/jdbc/mysql:/home/_____/development/workspace/
bin/java/libs/de.cenit/ -cp . -jar unifiedDatabaseClient.jar -exec "SELECT
 * FROM CALA.CSM_AREA LIMIT 0,5" -d mysql -u webadmin -p 0000060f13000d0f0
0 -db /CALA
CSM_AREANAME;;;;CSM_AREA;;;;
Apache;;;;apache;;;;
CALA Check;;;;cala_check;;;;
Filesystem;;;;filesystem;;;;
Sendmail;;;;sendmail;;;;
System;;;;system;;;;
```

Default output for UDC.

xml

```
java -Djava.ext.dirs=/opt/jdbc/mysgl:/home/millionality/development/workspace/
bin/java/libs/de.cenit/ -cp . -jar unifiedDatabaseClient.jar -exec "SELECT
 * FROM CALA.CSM AREA LIMIT 0,5" -d mysql -u webadmin -p 0000060f13000d0f0
0 -db /CALA -o xml
<?xml version="1.0" encoding="UTF-8"?>
<DbResultSet>
<ResultRow number="0">
<cell name="CSM AREANAME">Apache</cell>
<cell name="CSM AREA">apache</cell>
</ResultRow>
<ResultRow number="1">
<cell name="CSM AREANAME">CALA Check</cell>
<cell name="CSM AREA">cala check</cell>
</ResultRow>
<ResultRow number="2">
<cell name="CSM AREANAME">Filesystem</cell>
<cell name="CSM AREA">filesystem</cell>
</ResultRow>
<ResultRow number="3">
<cell name="CSM AREANAME">Sendmail</cell>
<cell name="CSM AREA">sendmail</cell>
</ResultRow>
<ResultRow number="4">
<cell name="CSM AREANAME">System</cell>
<cell name="CSM AREA">system</cell>
</ResultRow>
</DbResultSet>
```

XML output for UDC.

html

```
java -Djava.ext.dirs=/opt/jdbc/mysgl:/home/m=image/development/workspace/
bin/java/libs/de.cenit/ -cp . -jar unifiedDatabaseClient.jar -exec "SELECT
* FROM CALA.CSM AREA LIMIT 0,5" -d mysql -u webadmin -p 0000060f13000d0f0
0 -db /CALA -o html
<thead>
CSM AREANAMECSM AREA
</thead>
Apacheapache
CALA Checkcala check
Filesystemfilesystem
Sendmailsendmail
Systemsystem
</tbodv>
```

HTML output for UDC.

CSV

```
java -Djava.ext.dirs=/opt/jdbc/mysql:/home/n____/development/workspace/
bin/java/libs/de.cenit/ -cp . -jar unifiedDatabaseClient.jar -exec "SELECT
* FROM CALA.CSM_AREA_LIMIT 0,5" -d mysql -u webadmin -p 0000060f13000d0f0
0 -db /CALA -o csv
"CSM_AREANAME";;;;"CSM_AREA";;;;
"Apache";;;;"apache";;;;
"CALA Check";;;;"cala_check";;;;
"Filesystem";;;;"filesystem";;;;
"Sendmail";;;;"sendmail";;;;
```

CSV output for UDC.

Agent Installation Requirements

AIX

ECM SM agent platforms

ECM SM agents require the following software to be installed on the agent system:

- perl 5 or higher (required but NOT installed during ECM SM agent installation)
- Alternate shell like the bash shell (recommended): Due to limitations of the AIX sh and ksh shells monitoring and task execution can fail. To prevent these errors it is recommended to install the bash-shell to each agent before the monitoring agent is installed (if not yet installed). The bash-shell can be installed from the IBM AIX Toolbox CD.
 Within the ECM SM agent installer use the Set configuration variables configuration window, item Custom Shell binary, to specify the full qualified name of the bash (for instance /usr/local/bin/bash) to be used for all ECM SM agent components like the agent installer, monitors and tasks. A link to the specified binary is created in the directory <ECM SM-install-dir>/fsmsh.
- gawk (recommended): Due to limitations of the AIX awk and nawk (which is a copy of awk) monitoring and task execution (for instance IBM WebSphere monitors and tasks) can fail. To prevent these errors it is recommended to install gawk to each agent before the monitoring agent is installed (if not yet installed). gawk can be installed from the IBM AIX Toolbox CD.
 Within the ECM SM agent installer use the Set configuration variables configuration window, item Custom AWK binary, to specify the full qualified name of gawk (for instance /usr/local/bin/gawk) to be used for all ECM SM agent components like the agent installer, monitors and tasks. A link to the specified binary is created in the directory <ECM SM-install-dir>/fsmsh.

You must add the path to the perl binary to the CALA_REX configuration manually if perl is not found in the standard path .

Adjust system parameter ncargs

If the value of the system parameter neargs is too low, some monitors may show the error message "arg list too long".

To avoid this message, you should increase the value of ncargs.

To check for the current value, enter the following command:

lsattr -EH -l sys0 | grep ncargs

The value should be 16 or 32. To change the setting of ncargs, enter the following command.

chdev -l sys0 -a ncargs=<value>

This change takes affect immediately and is preserved over boot.

Adjust system parameter maxuproc

If the value of the system parameter maxuproc (maximum allowed processes per user) is too low, processes like monitors, tasks or shell binaries cannot be executed and may hang.

To avoid this error, you should increase the value of maxuproc to at least 1024.

To check for the current value, enter the following command:

lsattr -EH -l sys0 | grep maxuproc

or use the AIX smit(ty) tool (run 'smitty system' and then select 'Change show characteristics of a operating system'.

The value should be 1024 or higher. To change the setting of maxuproc, enter the following command.

chdev -l sys0 -a maxuproc=<value>

This change takes affect immediately and is preserved over boot.

Installing CALA_REX or CALA without root permissions

- the directory /etc/cenit must exist
- the user needs full access (read/write) to this directory
- if the root directory of the CALA installation (normally /opt/IBM/ECMSM/cala already exists, the user needs full access (read/write) to this directory

HP-UX

ECM SM agent platforms

ECM SM agents require the following software to be installed on the agent system:

- perl 5 or higher (required but NOT installed during ECM SM agent installation)
- gawk (recommended): Due to limitations of the HP-UX awk binary agent installation, monitoring and task execution can fail. To prevent these errors it is recommended to install gawk to each agent before the monitoring agent is installed (if not yet installed). The gawk or nawk for HP-UX is not provided by HP and therefore need to be downloaded from the Internet. Note: gawk might require the components 'gettext' and 'libiconv'.
 Within the ECM SM agent installer use the Set configuration variables configuration window, item

Custom AWK binary, to specify the full qualified name of gawk (for instance /usr/local/bin/ gawk) to be used for all ECM SM agent components like the agent installer, monitors and tasks. A link to the specified binary is created in the directory <ECM SM-install-dir>/fsmsh.

You must add the path to the perl binary to the CALA_REX configuration manually if perl is not found in the standard path .

Installing CALA_REX or CALA without root permissions

- the directory /etc/cenit must exist
- the user needs full access (read/write) to this directory
- if the root directory of the CALA installation (normally /opt/IBM/ECMSM/cala already exists, the user needs full access (read/write) to this directory

Redhat Linux

ECM SM agent platforms

Note: Installation might fail, if Redhat Data Protection is enabled. Please consult Redhat documentation for further details.

ECM SM agents require the following software to be installed on the agent system:

- perl 5 or higher (required but NOT installed during ECM SM agent installation)
- compat-libstdc++-33.i686

You must add the path to the perl binary to the CALA_REX configuration manually if perl is not found in the standard path .

Installing CALA_REX or CALA without root permissions

- the directory /etc/cenit must exist
- the user needs full access (read/write) to this directory
- if the root directory of the CALA installation (normally /opt/IBM/ECMSM/cala already exists, the user needs full access (read/write) to this directory

Solaris

ECM SM agent platforms

ECM SM agents require the following software to be installed on the agent system:

- perl 5 or higher (required but NOT installed during ECM SM agent installation)
- Alternate shell like the bash shell (recommended): Due to limitations of some SUN shells sh and ksh monitoring and task execution can fail. To prevent these errors it is recommended to install the bash-shell to each agent before the monitoring agent is installed (if not yet installed). The bash-shell can be installed from the SUN Companion CD. Note: The bash shell might require additional prerequisite components to be installed.
 Within the ECM SM agent installer use the Set configuration variables configuration window, item Custom Shell binary, to specify the full qualified name of the bash (for instance /usr/local/bin/bash) to be used for all ECM SM agent components like the agent installer, monitors and tasks. A link to the specified binary is created in the directory <ECM SM-install-dir>/fsmsh.
- gawk (recommended): Due to limitations of the SUN Solaris / SunOS awk and nawk monitoring and task execution (for instance IBM WebSphere monitors and tasks) can fail. To prevent these errors it is recommended to install gawk to each Solaris / SunOS agent before the monitoring agent is installed (if not yet installed). gawk can be installed from the Solaris Companion CD or the Internet. Within the ECM SM agent installer use the Set configuration variables configuration window, item Custom AWK binary, to specify the full qualified name of gawk (for instance /usr/local/bin/gawk) to be used for all ECM SM agent components like the agent installer, monitors and tasks. A link to the specified binary is created in the directory <ECM SM-install-dir>/fsmsh.

You must add the path to the perl binary to the CALA_REX configuration manually if perl is not found in the standard path .

Required file /usr/lib/charset.alias

ECM SM Agents version 5.2.0 support nationalized data analyzation, which includes multi byte character support. This functionality is realized based on the iconv Library.

The required system configuration file /usr/lib/charset.alias is not installed out of the box in some Solaris versions (e.g. Solaris 8). As a result the monitoring component of the ECM SM agent does not work on these systems with missing configuration file. To fix this problem, just copy this file from another Solaris machine where this file exists, or create it manually (see An example charset.alias file for an example charset.alias file).

NOTE On Solaris 9 this file is part of the Solaris package *SUNWgnome-base-libs*, which is installed on every Solaris 9 systems by default.

Manual OS adjustments

Verify that OS kernel parameters are configured correctly. In some cases the following parameters need to be specified or adjusted in /etc/system file. Note: Do not decrease the values, if the parameters are specified with higher values.

set rlim_fd_max=4096
set rlim_fd_cur=1024

Note: /etc/system changes require system reboot.

Installing CALA_REX or CALA without root permissions

- the directory /etc/cenit must exist
- the user needs full access (read/write) to this directory
- if the root directory of the CALA installation (normally /opt/IBM/ECMSM/cala already exists, the user needs full access (read/write) to this directory

SuSE Linux

ECM SM agent platforms

ECM SM agent require the following software to be installed on the agent system:

- perl 5 or higher (required but NOT installed during ECM SM agent installation)
- libstdc++33-32bit

You must add the path to the perl binary to the CALA_REX configuration manually if perl is not found in the standard path .

Installing CALA_REX or CALA without root permissions

- the directory /etc/cenit must exist
- the user needs full access (read/write) to this directory
- if the root directory of the CALA installation (normally /opt/IBM/ECMSM/cala already exists, the user needs full access (read/write) to this directory

Windows

ECM SM agent platforms

ECM SM agents require the following software to be installed on the agent system:

- perl 5 or higher (automatically installed during ECM SM agent installation)
- UNIX Like Windows shell (installed during ECM SM agent installation), unless Limited Agent version is used.

A perl implementation is included on the installation media in subdirectory TOOLS/w32-ix86/shell. It is automatically installed during installation of ECM SM server and agents.

Note: Full functioning Windows based ECM SM server and agents require a UNIX-like Windows shell, which is licensed under GPL. The shell can be downloaded manually from <u>sourceforge.net</u> or automatically during ECM SM server and agents installation. You can run a ECM SM Limited Windows agent version without having the GPL component installed. The ECM SM server requires the UNIX-like shell for Windows systems.

WMI requirements

The service user account has to be a member of the "Performance Monitor Users" (in German: "Systemmonitorbenutzer") group to be able to access WMI counters. In addition to the group membership, the service user needs the permission "Enable Account" in the WMI Control Security settings. By default, the group "Everyone" has permissions "Execute Methods", "Provider Write" and "Enable Account". If that's the case the service account inherits the permission through that group. To access WMI from remote the "Remote Enable" permission is required.

For more detailed information how to configure WMI permissions refer to the Microsoft documentation:

Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012

Configuring and installing ECM SM clients

CALA_REX Installation

The communication between the ECM SM server and agents is based on the CALA_REX (CALA remote execution) server and agent service. This service is used and needed to install and configure monitoring and logfile management components.

Since version 5.2.0 ECM SM supports multiple CALA_REX agents on one system. The ECM SM UI components identify the agents by its hostname, the so called 'Service / Agent ID Postfix'. In the case more than one agent will be installed on the system the 'Service / Agent ID Postfix' has to be unique and each agent has to use its own communication port (default value: 23804). Use a short string as the parameter 'Agent ID Service Postfix' #, {};\$_ or white spaces (blanks, tabs) maximum 8 characters on AIX) that adds information about the agent.

Location of CALA_REX agent images

The CALA_REX agent install images can be downloaded from the ECM SM Web Console. Open the ECM SM Web Console in your browser, navigate to the 'Client Administration' Console or open the view 'GUI Tools and downloads' directly. Select the platform specific ECM SM CALA_REX agent install image and either execute the installer image directly or download the image to the local system.

List of CALA_REX agent install images:

WINDOWS_IBM_ECM_SM_CALA_REX_AGENT.exe (InstallAnywhere image for MS Windows) AIX_IBM_ECM_SM_CALA_REX_AGENT.bin InstallAnywhere image for IBM AIX) Solaris-SPARC_IBM_ECM_SM_CALA_REX_AGENT.bin (InstallAnywhere image for Solaris 9 and 10 - SPARC base Solaris-Intel_IBM_ECM_SM_CALA_REX_AGENT.bin (InstallAnywhere image for Solaris 10 - Intel based) HP-UX-Itanium_IBM_ECM_SM_CALA_REX_AGENT.bin (InstallAnywhere image for HP-UX 11 - Itanium based) Linux-Intel_IBM_ECM_SM_CALA_REX_AGENT.bin (InstallAnywhere image for Linux on Intel platform) Linux-PPC_IBM_ECM_SM_CALA_REX_AGENT.bin (InstallAnywhere image for Linux on PowerPC platform) Linux-S390_IBM_ECM_SM_CALA_REX_AGENT.bin (InstallAnywhere image for Linux on s390)

Installing the CALA_REX agent

Go to the download page and click on the platform specific link in the *CALA_REX agents* section. Save the InstallAnywhere install-image on the machine where the CALA_REX agent is to be installed.

Double-click the binary that has just been downloaded to start the CALA_REX agent installation process. InstallAnywhere will guide you through the installation process.

NOTE On UNIX and Linux systems you might have to add execution rights (x-flag) to the installer image before you can run the installation process.

IMPORTANT On the Intel based Solaris platform you must start the installer with bash and not with the standard sh shell of the system. This is due to some limitations of the InstallAnywhere scripts of the self-extracting installer archives.

	InstallAnywhere bereitet die Installation vor		
		47%	
			Abbrechen
(C) 2012 Flexe	a Software LLC.		

CALA_REX Installation: Intro screen.

Press on the Next button to start the installation process.

	Software License Agreement
	Please read the following license agreement carefully.
	International Program License Agreement
IBM.	Part 1 - General Terms
Enterprise Content Management System Monitor	BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
	* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND
	* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.
	1. Definitions
	"Authorized Use" - the specified level at which Licensee is
	I accept the terms in the license agreement.
	I do not accept the terms in the license agreement.
	Print
InstallAnywhere	
Cancel Help	Previous

CALA_REX Installation: License information.

Carefully read the license agreement and select I accept ... and press Next to continue or press I do not accept ... or cancel to exit the installation.

IBM Enterprise Content Managem	nent System Monitor CALA_REX Agent
	Introduction
	InstallAnywhere guides you through the installation of IBM Enterprise Content Management System Monitor CALA_REX Agent.
	It is strongly recommended to close all programs before you proceed with the installation.
IBNL® Enterprise Content Management	Press 'Next' to open the next window, press the 'Previous' button if you want to re-open the previous window.
System Monitor	You can stop the installation at any time by pressing the 'Cancel' button.
InstallAmwhere	
Cancel Help	Previous

CALA_REX Installation: Installation introduction.

Select **Choose...** to adjust the installation location of the CALA_REX agent software and click the **Next** button. Note: Press **Restore Default Folder** to reset the selected installation folder.

(1) IBM Enterprise Content Manager	nent System Monitor CALA_REX Agent		x
		Installation fold	ler
IBM.	Please specify the CALA_REX Agent installation folder:		
System Monitor	Where do you want to install the CALA_REX Agent componen	ts?	
	C:\Program Files (x86)\IBM\ECMSM_AGENT		٦
		Restore Default Folder Choose	
InstallAnywhere			_
Cancel Help		Previous	

CALA_REX Installation: Installation folder.

Press the Next button to continue.

IBM Enterprise Content Manager	nent System Monitor CALA_REX Agent
	Specify the IBM ECM SM CALA_REX Agent settings
IBM. Enterprise Content Management	Specify the IBM ECM SM CALA_REX Agent settings here
System Monitor	Agent settings CALA_REX Agent IP name N7P00157B64BIT.de.cenit-group.com Additional CALA_REX parameters - for instance CALA_REX agent port settings listenport=127.0.0.1:23804 Agent ID Service Postfix (8 first characters used to identify multiple agents) P8-5.2.0 Agent description IBM ECM SM CALA_REX Agent Optional: CALA_REX user
InstallAnywhere Cancel Help	Previous Next

CALA_REX Installation: Installation settings.

Specify the agent settings for the CALA_REX installation.

Agent settings:

ECM SM CALA_REX IP name

Specify or adjust the IP name of the CALA_REX agent.

Additional CALA_REX parameters

Specify the parameters with the following format: *variablename=value*, separate parameter-pairs with semicolons. Example: *debugfile=logs/cala_rex_cli.log;* debuglevel=0.

Note: If you plan to install more than one CALA_REX agent on the system you need to add a *listenport=127.0.0.1:<adjusted-port-value>*, Example: *listenport=127.0.0.1:23804*. The default port number is 23804. Additionally you need to add an Service instance in this case, otherwise the agent cannot be detected correctly.

Agent ID Service Postfix

Required. Enter a postfix for the Service/Agent ID. If no postfix is given, the default value 'agent' will be used. The Agent-ID will be used to identify the agent-name within the Agent Installer, the

Monitoring Manager and the Task Execution Manager. The hostname 'MyServer1' with Agent-ID 'ECM-Server1' will be displayed as 'myserver1_ecm-server1'.

NOTE: Blanks, special characters and '_' aren't supported

The Agent ID Daemon Postfix have to be unique on each system in the case more than one agent will be installed per system, since it will be added to the Windows Service name cala_rex_cli.

Example: 'ECM-Server1' will generate a Windows Service called 'cala_rex_cliecm-server1'. The corresponding service for the Monitoring Agent (CALA) will be 'cala_srv_ecm-server1'.

On UNIX/Linux systems the Agent-ID will be used to generate the System startup/shutdown scripts (AIX: /etc/inittab entry)

Note: If you enter a postfix you must adjust the configuration of the CALA_REX services monitor as well.

NOTE Note: The agent ID postfix for AIX should not be longer than 8 characters. The postfix should not contain any of the following characters #, { } ; \$_ or white spaces (blanks, tabs).

Agent Description

Required. Specify a short descriptive text. This text will be visible in the result of a list-clients request executed on the CALA_REX server (current CALA_REX view).

User

Optional. Specify the user under which the CALA_REX agent will be running. If you do not specify a user, the CALA_REX agent will be running under the Local System account.

CAUTION If the desired user account is an LDAP / ADS domain user, specify the user account with domain format, for instance MYDOMAIN/myuser.

NOTE On Windows systems the installing user as well as the service user need to be a member of the Administrators and Users groups (or have corresponding permissions) and must also have the permission *Log on as a service*. The automatic startup of the installed service will fail at the moment although it was selected in the installation process. This is because of technical limitations regarding the update of the access rights for the

installed service by the installer. So after the installation it is necessary to manually fix the permissions for the installed service. To do this, open the service manager and re-enter the correct credentials for the service or add the user permission Log on as a service to the specified Windows service account.

NOTE Please keep in mind that all Image Services and Process Engine related monitors (IS, PE Mini-IS, PE-Core, PPM, PE-Memory and PE-

Cache) require that the CALA_REX and the CALA Windows service run under a service account that follow the Images Services or P8 PE group requirements. Please verify the Image Services or Process Engine service account requirements documented in the IBM FileNet Image Services and Process Engine installation guides.

Password

Windows only. Specify the password for the user given above. If no user is specified this parameter is ignored

Optional: CALA_REX adapter IP address to bound to.

Specify the IP address (IP version 4) of the network adapter to be used. This parameter is only required, if more than one network card is installed in the system.

Optional: CALA_REX libpathadd parameter

Specify optional CALA_REX libpathadd setting. See parameter section for detailed information.

Enable or disable CALA_REX installer debugging

Enable or disable CALA_REX installer debugging. If enabled an additional output and output panel is displayed.

IBM Enterprise Content Managen	nent System Monitor CALA_REX Agent
	Server related IBM ECM SM CALA_REX Agent settings
IBM. Enterprise Content Management	Specify the server related IBM ECM SM CALA_REX Agent settings here
System Monitor	Server settings IBM ECM SM Server CALA_REX Server name N7P00157864BIT IBM ECM SM Server CALA_REX port 23802 HTTP based communication to GUI / Download Server IBM ECM SM Server RAP (Web GUI) port 23990
InstallAnywhere Cancel Help	Previous

CALA_REX Installation: Server related Agent settings.

Specify the ECM SM server related agent settings for the CALA_REX installation.

Server settings:

ECM SM Server IP name

Required. Specify the IP name or address of the CALA_REX server.

ECM SM CALA_REX server port

Required. Specify the port of the CALA_REX server. Default value is 23802.

ECM SM Web / Download Server protocol type (http or https)

Required. Specify the ECM SM Web / Download protocol type (http or https). Default value is http.

ECM SM Web / Download server port

Required. Specify the port of the ECM SM Web / Download server. Default value is 23990.

Press the Next button to continue with the Windows specific settings.

The next few panels only apply to Windows based installations. The CALA_REX automatically tries to download the UNIX-Like Windows-shell archive from the monitoring server. During the download action a similar following progress bar will be displayed.

Download UNIX like Windows Shell from N7P02471B64BIT.de.cenit-group.com, port 23990

CALA_REX Installation (Windows only): Shell download bar from Monitoring server

If the download from the server was successful a message window will be displayed.

	UNIX-like Windows Shell download from the monitoring server was successful
	The UNIX-like Windows Shell download from the monitoring server was successful.
	The UNIX-like Windows Shell download from the monitoring server was successful.
	You can proceed with the installation.
IBNL	
Enterprise Content Management	
System Monitor	
Cancel <u>H</u> eip	<u>Previous</u>

CALA_REX Installation (Windows only): Shell download successful from Monitoring server

If the download action failed and installer debugging is active the following panel will be displayed:

	UNIX-like Windows Shell download from the monitoring server FAILED
	The UNIX-like Windows Shell download from the monitoring server failed due to an error.
	The UNIX-like Windows Shell download from the monitoring server failed due to an error.
IBM.	Please check the network and server settings (use the Previous' button) or check the message below and retry the download.
Enterprise Content Management System Monitor	Error Message was: java.net.UnknownHostException: N7P02471B64BIT.de.cenit-group.commm at java.net PlainSocketImpl.connect(PlainSocketImpl.java:227) at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:377) at java.net.Socket.connect(Socket.java:488) at java.netSocket.connect(Socket.java:488) at java.netSocket. at java.netSocket.connect(Socket.java:359) at java.netSocket. at java.netSocket.connect(Socket.java:385) at java.netSocket. at gava.netSocket.connect(Socket.java:259) at org.apache.commons.httpclient.protocol.DefaultProtocolSocketFactory.createSocket(DefaultProtocolSoc ketFactory.java:80) at org.apache.commons.httpclient.protocol.DefaultProtocolSocketFactory.createSocket(DefaultProtocolSoc ketFactory.java:122) at org.apache.commons.httpclient.HttpConnection.open(HttpConnection.java:707) at org.apache.commons.httpclient.HttpMethodDirector.executeWithRetry(HttpMethodDirector.java:387) at org.apache.commons.httpclient.HttpClient.executeWithRetry(HttpMethodDirector.java:387) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:387) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:387) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:37) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:37) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:37) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:37) at org.apache.commons.httpclient.HttpClient.executeWethod(HttpClient.java:37) at de.cenit.eb.sm.fsmtools.httpmon.Httpmonitor.main(Httpmonitor.java:76)
InstallAnywhere	
Cancel Help	Previous

CALA_REX Installation (Windows only): Shell download error from Monitoring server

Pressing the 'next' button will display a message window with several options:

?	IBM ECM SM CALA_REX Agent requires the UNIX like Shell from sourceforge.net for fully functioning Windows IBM ECM SM CALA_REX Agent agents. This IBM ECM SM Server installer can use a previously downloaded shell archive (see documentation) or can automatically download the file from the internet.			
	Please select the desired way to copy the UNIX like Windows shell into the correct directory or cancel this task. For further information verify the IBM ECM SM Server Release Notes and Install guide.			
	I don't want to install the GPL component. Automatically download the archive from sourceforge.net Specify the location of the downloaded shell archive			

CALA_REX Installation (Windows only): Message bar for UNIX-like shell download selection

If you press the **Specify the location of the downloaded shell archive** button then the file-browser panel will be displayed.

	Choose the GPL	Windows Shell Arcl	nive location	
	Please specify the location of the downloaded shell archive shell.w32-ix86.zip.			
IBM.	You'd need to download the file from sourceforge.net to enable full functioning of Windows based IBM ECM SM Server and agents (managed systems). For further details see IBM ECM SM Server documentations and Release Notes.			
Enterprise Content Management System Monitor				
	Please Choose the shell archive shell.w32-ix86.zip File:			
	C:\shell.w32-ix86.zip			
		Restore Default File	Choose	
	_			
InstallAnywhere				
Cancel Help		Previous	Next	

CALA_REX Installation (Windows only): Shell download bar from Monitoring server

If you press the **Automatically download the archive from sourceforge.net** button then the download progress bar will be displayed.



CALA_REX Installation (Windows only): Shell sourceforge.net download bar

If you press the I don't want to install the GPL component button or the downloads weren't successful the following message panel will be displayed.

	Windows Limited Functionality only selected
	Please Read Before Continuing:
IBM. Enterprise Content Management System Monitor	Please Read Before Continuing: Important notice: If you proceed with the installation by pressing the 'Next' button only Limited functionality without comprehensive monitoring will be available on this system. For full functionality please download the UNIX-Like Shell package shell.w32-ix86.zip for Windows systems to the IBM ESM SM Server and press the 'Back' button to start the download of the package from the IBM ECM SM Server to this agent again. This shell package is licensed under GPL and needs to be downloaded from http://www.sourceforge.net to the IBM ECM SM Server only once. For further information consult the related documentation.
InstallAnywhere	
Cancel Help	Previous Next

CALA_REX Installation (Windows only): Only Limited Windows agent available

In the case you proceed with the **Next** button then the Limited agent monitoring and Windows Eventlog settings panel will show up.

	Specify IBM ECM SM CALA_REX Agent monitoring set	tings
IBM. Enterprise Content Management	Please specify all relevant monitoring / logfile analyzation settings here.	
System Monitor	Remote Monitoring Server port 23840 Local start port for monitoring components: 23831 Activate Windows Eventlog monitoring Windows Eventlog names to be monitored system,application Prefilter for incoming events Publisher_Service,AEEngine,CSMGR,ftserver,MSSQLSERVER,FileNETPrintSer Prefilter for outgoing events application:eventtype=Information%system:eventtype=Information Activate Basic monitoring CPU Usage Critical threshold (more than x percent) 95 Disks to check for free space (for example C:) ALL Disk space free (minimum value) in percent of MB	vice
InstallAnywhere Cancel Help	Previous	ext

CALA_REX Installation (Windows only): Limited Windows agent parameter settings

Remote Monitoring Server port

Normally the specified default value (23840) should not be changed. If the server-port was adjusted during server installation then this value should be changed, too.

Local start port for monitoring components

If more than one instance of the ECM SM monitoring agent is installed on the system then adjust this value. In this case it's useful to increase the value for each agent instance by 100

Activate or deactivate Eventlog monitoring

If activated then the following 3 parameters have to be specified

Eventlog names

system, application are the default. You can add more existing eventlog names

Incoming event filter settings

This parameters defines which Eventlogs are processed (read). The default value processes a list of event logs, where the source column fit to IBM, VWServices, ...
Outgoing Event filter settings

This parameter defined which Eventlogs are filtered out. The default settings (application:eventtype=Information%system:eventtype=Information) suppresses event log entries of eventtype 'Information'

CPU Usage Critical threshold

Above this threshold (default: 90%) the CPU usage monitor alerts an error

Disks to check for free space

The listed disks (C:,D:) or ALL (default value) are checked for free space

Disk space free (minimum value) in percent of MB

A minimum of x% (default: 10) need to be free, otherwise the system alerts an error

Press the Next button to continue with the Agent Startup behaviour panel.

IBM Enterprise Content Managen	nent System Monitor CALA_REX Agent
	Agent Startup behaviour
IBM.®	Optional: Specify the Service/Agent ID and the descriptive name used in the 'Connected Agents' view for the IBM ECM SM CALA_REX Agent.
System Monitor	Agent Startup behaviour
	Automatic Startup
	Start after installation
InstallAnywhere	
Cancel Help	Previous Next

CALA_REX Installation: Agent instance and name settings.

Agent Startup behaviour

Select either Automatic Startup or Manual Startup of the Service/daemon.

Start after installation

Enable or disable startup of the Windows Service after successful installation.

Press Next to continue.



CALA_REX Installation: Pre-Installation Overview.

This panel displays the specified installation parameters. Press the Previous button to change settings.

Press Next to start the installation process.

During installation the Installation progress panel is displayed. You will see a popup message bar during the agent configuration at the end of the installation step.



CALA_REX Installation: Installation finished.

Note: At the end of the installation you might see a detailed installation result. This depends on the Installer debugging checkbox setting.

IBM Enterprise Content Manager	nent System Monitor Server
	CALA_REX agent installation result
	The installation completed with return code 0
IBM	C:\Users\faas\AppData\Local\Temp\I1411360060\Windows>SET
System Monitor	TEMPDIR=C:\Users\faas\AppData\Local\Temp\998969.tmp
	C:\Users\faas\AppData\Local\Temp\I1411360060\Windows>SET USERINSTALLDIR=C:\Program Files (x86)\IBM\ECMSM\agent
	C:\Users\faas\AppData\Local\Temp\l1411360060\Windows>SET S_AGENT_ID=n7p00157b64bit_srvagnt
	C:\Users\faas\AppData\Local\Temp\\1411360060\Windows>SET S_SERVER_SERVICE_NAME=IBM ECM SM CALA_REX Agent
	C:\Users\faas\AppData\Local\Temp\I1411360060\Windows>SET CENIT_ROOT_DOS=C:\Program Files (x86)\IBM\ECMSM\agent
	C:\Users\faas\AppData\Local\Temp\I1411360060\Windows>SET CR_CLI_USER=/mathias
	C:\Users\faas\AppData\Local\Temp\l1411360060\Windows>echo OFF
	C:\Users\faas\AppData\Local\Temp\/1411360060\Windows>SET CR_CLI_SERVERADDR=N7P00157B64BIT.de.cenit-group.com:23802
	C:\Users\faas\AppData\Local\Temp\I1411360060\Windows>SET CR_CLI_DESC=N7P00157B64BIT.de.cenit-group.com (Agent on Primary Server)
InstallAnywhere	
Cancel Help	Previous

CALA_REX Installation: CALA_REX installation debug output

After the installation the Installation done panel is displayed, which sometimes recommends a restart of the Windows system.

	Installation done
	Congratulation!
	IBM Enterprise Content Management System Monitor CALA_REX Agent successfully installed at:
TRM	C:\Program Files (x86)\IBM\ECMSM_AGENT
Enterprise Content Management	Select "Done", to close the installer.
System Monitor	
InstallAnywhere	
Cancel Help	Previous Done

CALA_REX Installation: installation done

Press the **Done** button to finish installation.

Accepting a new or updated CALA_REX Agent

Since version 5.2.0 CALA_REX agents have to be accepted by an administrative ECM SM user. Only accepted agents can be managed by the ECM SM server. Open the 'Client Administration' console in the Web UI, select the appropriate agent from the list (colored red, status 'not_accepted').

	Connected Agents 🔀			🔊 Refres	sh ▽ □ I
	Name 🔻	Calarex Versio	Description	Status	IP
Ø	N7P00157B64BIT.de.	02.01-000	ECM SM Server [n7p00157b64bit_primary]	online	10.0.40.
Ø	N7P00157B64BIT.de.	02.01-000	[n7p00157b64bit_srvagnt]	online	10.0.40.
×	N7P00157B64BIT.de.	02.01-000	IBM ECM SM CALA_REX Agent [n7p00157b64bit_agent1]	not accepted	10.0.40.

CALA_REX activation: new, not yet accepted agents

To accept the agent open the context menu on the selected agent.

	Connected Agents	×		
	Name 💌		Calarex Version	Description
Ø	N7P00157B64BIT	.de.	02.01-000	ECM SM Server [n
Ø	N7P00157B64BIT	.de.	02.01-000	[n7p00157b64bit
8	N7000157864BIT	.de.	02.01-000	IBM ECM SM CALA
	Nefresh			
	💥 Delete			
	🕑 Accept			

CALA_REX activation: Context menu with 'Accept' menu item.

Press the accept menu item. The new agent will now be accepted, the security key file will be generated and stored on the agent system at **\$CENIT_ROOT/.keys** directory. Secure this directory to minimize unauthorized access. This directory only requires read-access for the Service / Daemon user that runs the CALA_REX agent.

	Connected Agents 🔀			💙 Refres	h ▽ 🗖
	Name 💌	Calarex Versio	Description	Status	IP
Ø	N7P00157B64BIT.de.	02.01-000	ECM SM Server [n7p00157b64bit_primary]	online	10.0.4
	N7P00157B64BIT.de.	02.01-000	[n7p00157b64bit_srvagnt]	online	10.0.40
Ø	N7P00157B64BIT.de.	02.01-000	IBM ECM SM CALA_REX Agent [n7p00157b64bit_agent1]	online	10.0.40

CALA_REX activation: Accepted agent status changed to 'online', colored green.

CALA_REX and Task execution logging on the Agent

Since version 5.2.0 the logfiles (incl .plusdebug directory location of the CALA_REX agent) are located at \$CENIT_ROOT/cala/temp. Create the .plusdebug and cala_rex debugging directory in this directory.

NOTEThe key file is missing if you reinstall the CALA_REX agent on a machine which
was already accepted in the previous installation. The CALA_REX agent is still
accepted after the installation, even though there is no key file yet.
Before you reinstall the CALA_REX agent, please delete the agent from the
Connected Agents view. Accept the CALA_REX agent again.
If you have already reinstalled the CALA_REX agent delete the CALA_REX
agent from the CALA_REX agent delete the CALA_REX
agent from the Connected Agents view. Restart the CALA_REX server. Accept
the CALA_REX agent again.

Unattended installation of the CALA_REX agent

ECM SM provides InstallAnywhere CALA_REX agent images for all platforms with full unattended installation functionality.

To record a response file for use as input parameter file for later unattended installation steps run the installer with the following command (example for Windows installer, others are similar):

WINDOWS_IBM_ECM_SM_CALA_REX_AGENT.exe -r responsefile-name

The specified parameters will be recorded in the response file. If no filename is specified the settings are recorded into the file installer.properties (default name of the response file).

To start an unattended installation with a previously recorded input parameter file, run the installer with the following command:

WINDOWS_IBM_ECM_SM_CALA_REX_AGENT.exe -i silent -f input-file

Note: If running the unattended (silent) installation the system will not be restarted after the installation (Windows only).

Creating an SSL certificate for the agent

If the CALA_REX server is configured to accept only SSL encrypted connections from a agent, you must create and activate an SSL certificate for the agent. This process consists of several steps.

Create an SSL agent certificate request

Go to the directory \$CENIT_ROOT/tools/ssl on the agent and execute the script create_client_req.sh. The script creates a configuration file, a agent certificate request and the private key file for the agent. If the option -k is not given, the request and the configuration will be stored in a single file named \$CENIT_ROOT/keys/client_combined.<clientname>.

NOTE The variable CENIT_ROOT must be set before the script can be executed.

Start the script with the following command:

sh create_client_req.sh [-k] [-p]

Options:

-k

Optional. Tells the script to keep the agent certificate request and the corresponding configuration file as two separate files instead of combining them into one file. Recommended if you use an existing PKI infrastructure and process the certificate request with existing tools.

-p

Optional. The script does not use the password from the CALA_REX configuration file or the standard password but waits for user input on stdin. The encrypted password is automatically stored in the CALA_REX configuration file.

Transfer agent request file to the server

Transfer the file created in the step above to your ECM SM server. The file can be stored in a temporary directory, it will be removed after the certificate has been signed.

Sign the certificate request.

Go to the directory \$CENIT_ROOT/tools/ssl on the server and execute the script sign_cert.sh. The script signs the agent certificate request with the server CA certificate of the ECM SM server. The script prompts the user for the password of the server CA certificate (see The default passwords for the private keys). The signed certificate will be stored on the server in the file \$CENIT_ROOT/keys/client/cala_rex_cli_cert.<clientname>.pem.

NOTE The variable CENIT_ROOT must be set before the script can be executed.

Start the script with the following command:

sh sign_cert.sh filename

Options:

filename

Required. Name of the file that contains the agent certificate request.

Transfer and activate agent certificate

Transfer the files \$CENIT_ROOT/keys/client/cala_rex_cli_cert.<clientname>.pem and \$CENIT_ROOT/keys/trusted_cas.pem from the server to the agent and rename the agent certificate file to \$CENIT_ROOT/keys/cala_rex_cli_cert.pem.

To disable anonymous connections for this agent call

sh cr_cli_cfg.sh configure "ssl.cipherlist=ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH"

in the CALA_REX installation directory (*\$CENIT_ROOT/cala_rex*) on the agent.

NOTE The variable CENIT_ROOT must be set before the script can be executed.

Restart the CALA_REX agent to activate the agent certificate by calling

sh cr_rex.sh restart

Distinctions when installing the CALA_REX agent in a cluster environment

When installing several CALA_REX agent daemons on one machine, like one would like to do in a cluster environment, the following things need to be taken care of:

- Each installation needs an *unique postfix and cenit-root directory*. (The -I and -r parameters in the Unix installer, the appropriate fields in the Windows installer.)
- The daemons listenport must be unique. The default value for the listenport is 127.0.0.1:23804, this must be changed for subsequent installations. Specify -o listenport=127.0.0.1<:port> when calling the Unix installer or add listenport=127.0.0.1:<port> to the additional parameters field in the Windows installer.
- In a cluster environment it's likely, that some instances should not use the systems default *IP* address, but that of any cluster resource. Use the -i <ip address argument of the Unix installer for setting the IP address, add ip-address=<ip-address> to the additional parameters field of the Windows installer.

For starting and stopping the CALA_REX daemon, the script **\$CENIT_ROOT/CALA_REX/CALA_REX.sh** can be used. Use the **net** command on Microsoft Windows.

Further CALA_REX installation and configuration options

For further CALA_REX installation and configuration options see chapter Further CALA_REX installation and configuration options

Preparation

Preparing the ECM SM clients

Before you can configure the IBM Enterprise Content Management System Monitor on the machines, you must install a CALA_REX client on each server that you want to monitor. See the CALA_REX Installation for details.

Preparing JMX Support

This chapter introduces JMX, the "Java Management Extensions". It shows the JMX functionality in principle, how it works, communicates and which components are needed to use JMX. Additionally, this chapter gives an overview of how the various application servers support JMX.

An introduction to JMX



Infrastructure of JMX

JMX is the abbreviation for Java Management Extensions. This technology is used to provide read and write access to resources of a web application server. The upper graphic shows the infrastructure of JMX. It is divided into three levels.

Distributed Service Level

This level is responsible for the provisioning of an interface to the agent level.

Agent Level

The agent level defines agents which are responsible for the communication with the resources.

Instrumentation Level

The instrumentation level contains the resources which can be managed.

MBeans

"MBeans" is an abbreviation for Managed Beans. The programming model of "Beans" is an official Java "technology" to provide program parts with a kind of "plug and play" mechanism.

The following screen shot shows the JMX MBeans structure.



MBeansMBeans

Beans have uniquely defined interfaces and therefore can be used as exchangeable modules. MBeans use this idea of modularity within a web application server environment.

This way MBeans act as interfaces to the application server's resources (see "Instrumentation Level" in figure "Infrastructure of JMX"). The client in the 'MBeans' figure is the MBeanMonitor software component in this specific case. Via the standard interface, provided by the application server, the MBeans can be accessed.

The client can get an instance of the object, which is represented by the MBean. So, it is possible to access the application server's resources from an external Java program, the JMX Application Server Monitor.

What MBeans are used for

Figure "MBeans" above shows an application server having several MBeans. An application server can have an arbitrary number of MBeans. Two kinds of MBeans exist: static and dynamic MBeans.

Static MBeans exist directly after the start of the application server.

Dynamic MBeans are created during runtime.

The provided MBeans depend on vendor and version of the application server. Each application server has its own set of MBeans. Therefore, there is no standard, which MBeans must be provided by each server.

MBeans can manage several resources of the application server, similar to the administration console of the application server. An MBean represents a collection of mechanisms to access / manage the application server.

As the figure shows, an MBean can have three different kinds of mechanisms:

Attributes

Attributes are mostly used to read or set the attributes of an MBean. An attribute can store almost any information in different kinds of datatypes. For example, a deployed web application can have a hit counter. Other user-specific parameters like groups or user names are stored in attributes, too. Another example for an attribute definition is the maximum allowed cache or memory, which can be used. Each attribute has a rights management. Some attributes cannot be accessed in write mode, yet they are available for read operations. Finally, the description information itself of an MBean can be stored in an attribute.

Operations

The term "Operation" in this context is a synonym for a function or a method in programming languages. Operations are mostly used to perform actions on the server or to access the attributes (even if this is not necessary, as it is possible to access the attributes directly). Operations are often used to run tasks, for example to start or stop an application or resource of the application server. Also, more detailed responses can be realized via operations, like getting one element out of an array of information. For that purpose, operations have parameters, just as functions and methods, which can also have parameters (arguments). Mainly, operations have the bean-specific getter and setter methods to read and write information from respectively to an MBean.

NOTE

'Operations' are used for a more complex and powerful access than 'Attributes' can provide.

Notifications

Notifications are sent, when special, predefined events occur. The used MBean can be configured in such a way, that it sends a notification each time, something special happens. In most cases, a notification informs about a parameter, that has been changed. To receive notifications, a client, that listens permanently, must be running (the notification listener). This mechanism is different to the use of 'Operations' or 'Attributes', where the client explicitly asks for the server response. In the case of notifications, the server performs the action and the client gets the information only, in case it is listening. The client has to enable the notification mechanism on the server, if it wants to receive the information.

How IBM Enterprise Content Management System Monitor works on the basis of MBeans

The JMX monitor uses MBeans to monitor the application server. This means, that JMX is used to read information from the server, but no write or other executive actions are initiated. Thus, attributes can be read out and operations, that only do read access, can be invoked. Furthermore, the IBM Enterprise Content Management System Monitor JMX monitoring component does not listen for notifications.

JMX versions

There are two different releases of JMX:

JMX1.0

The old specification does neither have very strictly nor exactly defined interfaces and directives and therefore it is no consistent standard. That is why almost every application server vendor created his own interfaces to access the MBeans. This means, that every application server comes with some libraries (jar files) to access the MBeans from this specific application server. Mostly, these libraries are even not compatible from one application server's release to another. Only the server's libraries, that need to be accessed, have to be used. For some of the servers, like JBoss, Oracle WebLogic and IBM WebSphere, this technology is used.

JMX1.2

JMX 1.2 is the successor of the JMX1.0 standard, because no real JMX 1.1 specification exists. The JMX1.2 standard has a more strictly defined interface. At least the JSR160 API defines a unique interface for application server vendors to provide access to their MBeans. If JMX1.2 is used, the way to connect to the server is different from the JMX1.0 method, in as much as other libraries are needed.

Note: Java 5 already contains these libraries. If JMX1.2 is needed to be used with Java 1.4.x a subset of libraries from the project MX4J are used by ECM SM. To access the MBeans via JMX1.2 this technology has to be enabled on the application server itself. Depending on the application server this is done in the starting script, with a special command line call or on the administration console of the server. Older versions of some application servers do not provide JMX1.2 support.

Application Server	JMX Version	Connection Type	Java Version (Server side)
Oracle WebLogic 7	JMX1.0	WebLogic specific class- es	Java 1.4.2
Oracle WebLogic 8.1	JMX1.0	WebLogic specific class- es	Java 1.4.2

Overview of Supported Application Servers

Application Server	JMX Version	Connection Type	Java Version (Server side)
Oracle WebLogic 9	JMX1.2	WebLogic specific class- es	Own Java (JRockit)
Red Hat JBoss 3.x	JMX1.0	JBoss specific classes	Java 1.4.2
Red Hat JBoss 4.0.1	JMX1.0	JBoss specific classes	Java 1.4.2
	JMX1.2	JSR160	Java 5
IBM WebSphere AS 5.1	JMX1.0	WebSphere specific classes	WebSphere Java
IBM WebSphere AS 6.0.x	JMX1.0	WebSphere specific classes	WebSphere Java
IBM WebSphere AS 7.0.x	JMX1.0	WebSphere specific classes	WebSphere Java
IBM WebSphere AS 6, 7 and 8 Versions	JMX1.2	WebService	Java 6
Sun Java Application Server 8.1	JMX1.2	JSR160	Sun Application Server own Java 5
Oracle Application Server 10g	JMX1.2	JSR160	Oracle J2EE
IBM WebSphere AS 6, 7 and 8	JMX1.2	JSR160	Oracle J2EE

The table above lists the different application servers, that are supported by the *IBM ECM SM* MBean Monitor. It gives an overview of which application servers need their specific classes and which use the JSR160 standard.

Oracle WebLogic 7

Needed jar files

• weblogic.jar

Default server lib path

The path has to point to the lib directory of the server installation.

<WebLogicHome>/server/lib

Example: E:\bea\weblogic700\server\lib

Default address to admin console

http://<host>:7001/console

Default JMX Port 7001

Default server lib path

The path has to point to the lib directory of the server installation.

<WebLogicHome>/server/lib

Example: E:\bea\weblogic700\server\lib

Oracle WebLogic 8.1

Needed jar files

- weblogic.jar
- wsclient.jar

Default server lib path

The path has to point to the lib directory of the server installation. The mx4j jar files are referenced automatically.

<WebLogicHome>/server/lib

Example: E:\bea\weblogic81\server\lib

Default address to admin console

http://<host>:7001/console

Default JMX Port

7001

Oracle WebLogic 9

Needed jar files

- weblogic.jar
- wlclient.jar
- wljmxclient.jar

Default server lib path

The path must point to the lib directory

<WebLogicHome>/server/lib

Example: E:\bea\weblogic9\server\lib

Default address to admin console

http://<host>:7001/console

Default service URL

Even if WebLogic9 supports JMX1.2 no service URL is needed, because connection is built up via server own libraries.

Recommended Java Path

Most times Oracle WebLogic is installed with it's own JDK. The Java path given in the monitor or task configuration should point to this.

Example: C:\bea\jdk150_04

Default JMX Port

7001

Red Hat JBoss 3.x

Needed jar files

- jbossall-client.jar
- jboss-jmx.jar
- jmx-client.jar

Default server lib path

The path must point to the Red Hat JBoss home directory, which contains the lib and client directories.

<JBossHome>/

Example: E:\JBoss-328

Default address to admin console

http://<host>:8080/[web-console]

Default JMX Port

1099

Red Hat JBoss 4.0.1

Needed jar files

• mx4j.jar

- mx4j-remote.jar
- mx4j-rjmx.jar
- (or Red Hat JBoss own libs, when using JMX1.0 see Red Hat JBoss 3.x)

Default server lib path

The path must point to the Red Hat JBoss home directory, which contains the lib and client directories.

<JBossHome>/

Example: E:\JBoss-4

Default service URL when JMX1.2 is activated

service:jmx:rmi:///jndi/rmi://<host>:<port>/jmxrmi

Default address to admin console

http://<host>:8080/[web-console]

Default JMX Port

1099 (JMX1.0)

depending on configuration (JMX1.2)

IBM WebSphere 5.1

Needed jar files

- admin.jar
- bootstrap.jar
- ecutils.jar
- emf.jar
- ffdc.jar
- ibmjsse.jar
- ibmorb.jar
- idl.jar
- iwsorb.jar
- j2ee.jar
- j2ee_2.jar (This file is not contained in the directory by default. It is part of the j2ee (Java Enterprise Edition) and must be copied out of it into the lib directory of the WebSphere installation.)

- jmxc.jar
- mejb.jar
- messaging.jar
- messagingClient.jar
- messagingImpl.jar
- migrate.jar
- Improxy.jar
- pmiclient.jar (only on WebSphere 5)
- ras.jar
- runtime.jar
- sas.jar
- security.jar
- utils.jar
- wasjmx.jar

Default server lib path

The path must point to the WebSphere directory, which contains the lib and bin directory.

<WebSphereHome>/

Example: E:\WebSphere5\AppServer

Default address to admin console

http://<host>:9090/admin

Default JMX Port

2809 (Bootstrap port - RMI)

IBM WebSphere 6.0.1

Needed jar files

see WebSphere 5.1 jar list

Default server lib path

The path must point to the WebSphere directory, which contains the lib and bin directory.

<WebSphereHome>/

Example: E:\WebSphere601\AppServer

Default address to admin console

http://<host>:9043/ibm/console

Default JMX Port

2809 (Bootstrap port - RMI)

Sun Application Server 8.1

Needed jar files

- mx4j.jar
- mx4j-remote.jar
- mx4j-rjmx.jar

Default server lib path

The mx4j jar files are referenced automatically.

Default address to admin console

http://<host>:4850/admingui

Default service URL

service:jmx:rmi:///jndi/rmi://<host>:3353/management/rmi-jmx-connector

Default JMX Port

3353

Oracle Application Server 10g

Needed jar files

- mx4j.jar
- mx4j-remote.jar
- mx4j-rjmx.jar

Default server lib path

The mx4j jar files are referenced automatically.

Default address to admin console

http://<host>:8888/em/console/ias/cluster/topology

Default service URL

service:jmx:rmi:///jndi/rmi://<host>:<port>/jmxrmi

Default JMX Port

depending on configuration (JMX1.2)

Tomcat 5.x

Needed jar files

- mx4j.jar
- mx4j-remote.jar
- mx4j-rjmx.jar

Default server lib path

The mx4j jar files are referenced automatically.

Default address to admin console

http://<host>:8080/

Default service URL

service:jmx:rmi:///jndi/rmi://<host>:<port>/jmxrmi

Default JMX Port

depending on configuration (JMX1.2)

Additional hints

Default address to admin console

The URL to the admin console can vary, depending on the configuration of the application server.

Default service URL

The service URLs can vary, depending on the configuration of the application server.

Default JMX Port

The ports can vary, depending on the configuration of the application server.

WebSphere 5 and Stats Objects

The MBeanMonitor Java program needs components, that are not delivered with the WebSphere 5 Application Server. They are shipped with Java 5 or J2EE (Java Enterprise Edition). This concerns the "j2ee.jar" file. It has to be copied into the libs directory of the WebSphere 5 Application Server and it must be renamed to "j2ee_2.jar".

Additional Information on JMX relevant for the IBM ECM SM JMX Monitors

This chapter describes some keywords, which are related to the JMX topic and are used by the JMX monitors. It is written for a better understanding of which parameters / values have to be specified for JMX monitors.

JSR160 and Service URL

JSR160 is a specification, which defines an interface to use JMX. With it, it is possible to connect to a server via the javax.management classes. The connection is made via a so called service URL. A service URL can look like the following example:

Example: service:jmx:rmi:///jndi/rmi://192.168.240.154:8765/jmxrmi

The prefix "service:jmx:rmi:" is available in every service URL. Sometimes it may start with "service:jmx:iiop" or "service:jmx:soap". It is recommended to use the "rmi-connection type" because this is the most robust communication type.

The fact, that it works on different servers this way, makes JSR160 very useful, because one implementation works for all servers supporting this technology.

JSR160 is supported by the following Java versions:

Java 1.4.2

When JSR160 shall be used with Java 1.4.2 the open source libraries MX4J from the website http://mx4j.sourceforge.net are needed. The libraries are also provided on the ECM SM installation disc. These libraries implement the JSR160 API and make it possible to use the JMX1.2 technology. Based on the information from the MX4J website, MX4J should work with Java 1.3, too.

Note: The combination Java 1.3.x and MX4J is not supported for ECM SM JMX monitors at present.

Java 5

Java 5 supports the JSR160 API by default. No special libraries like MX4J are needed.

Host and Port

Host is the name of the application server or the IP of the system. The port depends on the application server configuration. The previous chapters give an overview of the default ports of the different application servers.

ObjectName

Several MBeans can be accessed by the ObjectName at once. The ObjectName must exist. One way to find out which ObjectName provides access to which information is the "View JMX Parameters" Task. Object-Names may look cryptic. Mostly these names describe an element in the hierarchy of the application server's MBean structure.

Example: jboss.jca:name=DefaultDS,service=ManagedConnectionFactory

User Name and Password

Application servers can enable access via authentication, which makes it necessary to specify user and password for the request. The required user and the password are normally not identical with the system user, but they are administered by the application server itself. Depending on the application server, the user and the password are defined during the server installation, when activating JMX on the application server's administration console or when starting the server.

On WebSphere 6 Application Server, JMX monitoring was tested successfully with an administrative user as well as a user having the "monitor" role of the WebSphere security model. Since the JMX monitors and tasks are just designed for reading operations, it is recommended to use a user, which has only monitoring rights.

The different application servers have different policy models and different default configurations for security handling with JMX. The administrator should be able to configure the correct security policies. Some application servers like WebLogic also separate between different levels of security in the MBean hierarchy. Red Hat JBoss has to be configured in its web.xml file. It is not the part of this manual to handle security configuration for every application server in detail. So only some helpful links are included:

JBoss:

https://community.jboss.org/wiki/SecureTheJmxConsole

WebLogic 8:

http://docs.oracle.com/cd/E13222_01/wls/docs81/secwlres/secroles.html

WebLogic 9:

http://docs.oracle.com/cd/E13222_01/wls/docs92/ConsoleHelp/taskhelp/ security/DefinePoliciesforMBeans.html

WebSphere:

http://www.redbooks.ibm.com/redbooks/pdfs/sg246316.pdf

Attributes, Operations and Stats

As already mentioned the monitors can get information by calling attributes or invoking operations. Every MBean can be accessed via an ObjectName. When having the ObjectName it is possible to tell the MBean whether an attribute shall be requested or an operation shall be invoked. For the monitors this is done via the parameter "Action". This parameter can have the value "attribute" or "operation". The monitor only can do one thing, either attributes are requested or operations are invoked.

After the monitor knows which action to take (attribute request or operation invocation) it also must know the name of the attribute to request or which operation to invoke. For the monitor this is done via the parameter "ActionNames". The action names and operation names can be found out with the "View JMX Parameters" task or with a JMX browser.

Stats (stats_attribute and stats_operation) are no real action type, but an action to tell the monitor, that in the following monitor configuration has to handle stats return values. Depending on if attributes are requested or operations are invoked, "stats_attribute" and accordingly "stats_operation". Stats objects have a special format when they are returned. stats_statsName_attribute. In chapter 1.3.8 there is an example for how to configure the monitor, when stats objects are requested.

Parameters and Signatures

As operations may have parameters the monitor provides two field: "parameters" and "signatures". With parameters the value(s) of the parameters are specified to the program. This values may be numbers, for example 0, if the operation returns elements of an array (which is a realistic scenario). So 0 would return the first element of the array (just as usual in programming languages). The signature in this case would be "java.lang.Integer" to tell the program that this is a numeric value.

It has to be kept in mind that only primitive datatypes have to be specified as the according Java object to the program.

- int java.lang.Integer
- long java.lang.Long
- float java.lang.Float
- double java.lang.Double
- boolean java.lang.Boolean

Example: An operation may be implemented like this: int getConnectionArrayElement(int element)

So the parameter will be the number of the requested array *element*. For example 0, 1 or 2.

The value for signature will be *java.lang.lnteger*, because the parameter element if of the type int.

NOTE Prior to configuring an individual JMX monitor, parameters for the monitor, the number of parameters and their data type have to be verified with a JMX browser or the task "View JMX Parameters" to prevent erroneous return values.



Example for ObjectName, operationNames, parameters and signatures with real values

Example - parameters and signatures

Imagine the task would return the following (This example uses entirely fictitious ObjectNames, operations, parameters and signatures).

You want to guarantee, that the user "admin" from the group "Administrators" has the rights "allAccess.

You want to guarantee, that the processor load is less 0.8 -> 80%.

You want to guarantee, that the myImportantServlet is the servlet on index 2.

```
0001 +-----
                  _____
0002 myDomain:name=UserManagement,type=myApplicationServer 1
0003 +-----
0004 ClassName: org.this.is.just.nice.to.Have
0005 Description: This information is only to get all of the possible information which \dashv
   is provided
0006 +-----
      OPERATIONS
0007
0008
      +----+
0009
      Operation: getUserRights
0010 Description: getter for UserRights
0011
     ReturnType: java.lang.String;
      Parameter 0: pl
0012
      Type: java.lang.String
Description: The user's Name
Parameter 1: p2
Type: java.lang.String
0013
0014
0015
0016
0017
        Description: The user's Group
0018 ...
0019 +-----
0020 myDomain:name=ApplicationServer,type=myDomain
                                                      8 |
0021 +-----
0022 ClassName: org.this.is.just.nice.to.Have
0023 Description: This information is only to get all of the possible information which \downarrow
   is provided
0024
      +----+
```

```
0025
        OPERATIONS
                         0026
        +----+
0027
       Operation: getprocessorLoad
0028
       Description: returns the load as floating value, where 1.0 means 100% processor \dashv
    load.
0029
        ReturnType: double;
0030 ...
0031
       Operation: getServlet
0032
       Description: getter for an element of the servlet list
       ReturnType: javax.management.ObjectName
0033
0034
          Parameter 0: p1
0035
          Type: int
0036
          Description: The index of the servlet in the array.
0037
```

Imagine, the following rules shall be defined:

- You want to guarantee, that the user "admin" from the group "Administrators" has the rights allAccess.

- You want to guarantee, that the processor load is less 0.8 -> 80%.
- You want to guarantee, that the myImportantServlet is the servlet on index 2.
- ObjectNames: "myDomain:name=UserManagement,type=myApplicationServer;myDomain: name=ApplicationServer, ↓ type=myDomain"
- operation names: "getUserRights,!=,allAccess;::;getprocessorLoad,>,0.8;getServlet,!=,myDomain: name=myImportantServlet,type=Servlet"
- parameters: "admin;Administrators;::;;:;2"
- signature: "java.lang.String;java.lang.String;::;;;java.lang.Integer"

How to configure stats requests

In principal the stats requests "stats_attribute" and "stats_operation" are configured the same way as the normal "attribute" and "operation" actions. There is only one thing to keep in mind: stats objects have a special structure when they are returned. So it is not enough to just write "stats".

The Task will return you the following, if the application server returns supported stats objects:

```
0001
        Attribute: stats
0002
        Value:
0003 Stats name=DefaultApplication#DefaultWebApplication.war, type=servletSessionsModule
0004 {
0005 name=LiveCount, ID=7, description=The number of sessions that are active at the \dashv
    moment , unit=NV, type=RangeStatistic,
0006 lowWaterMark=0, highWaterMark=0, current=0, integral=0.0
0007 }
0008
        Description: Provides access to the implementation of the specific Stats \dashv
     interface that this managed
0009 object is required to support if it implements the StatisticsProvider model.
0010
        Type: javax.management.j2ee.statistics.Stats
0011
        Readable: true
        Writable: false
0012
0013
```

What is a stats object?

A stats object is a collection of several attributes in one single object. Most times this object is just called "stats". This technology is mainly used by WebSphere Application Servers. The stats object makes it possible to bundle several attributes together if that makes sense. Most times the stats object has a name and a description and some other information, describing the data which is also contained in the stats object.

There is also some information which is not needed to configure the monitor. For example the "Stats name=DefaultApplication#DefaultWebApplication.war, type=servletSessionModule". The monitor only uses the "name" between the curly braces {}.

To make it possible to identify the different attributes (With "attributes" in this case the "highWaterMark", "current" or "integral" are meant) of the stats objects correctly, the naming of the several attributes has to be extended, compared to the single attribute requests.

A stats attribute is requested as follows: *attributeName_statsName_statsAttributeName*. The following example will give a closer look in that.

The MBeanMonitor Java program will return the output in the following format:

```
0001 #host::label::stats_LiveCount_name::LiveCount
0002 #host::label::stats_LiveCount_ID::7
0003 #host::label::stats_LiveCount_description::The number of sessions that are active at 
the moment
0004 #host::label::stats_LiveCount_unit::NV
0005 #host::label::stats_LiveCount_type::RangeStatistics
0006 #host::label::stats_LiveCount_lowWaterMark::0
0007 #host::label::stats_LiveCount_highWaterMark::0
0008 #host::label::stats_LiveCount_current::0
0009 #host::label::stats_LiveCount_integral::0.0
```

Build a stats attribute request - step by step:

It is easy to understand this, when comparing the output of the Java program with the output of the task.

The first line of the task output is: "Attribute: stats"

This means, that every request is started with "stats_". This is the "attributeName".

The Java program extracts the name of the stats object (In the curly braces of the task output it is "name=LiveCount". This is the "statsName"

Sometimes stats objects can have several collections included in curly braces. To differ them the name (in this case "LiveCount") is added to the attribute request. So it would look like that now: "stats_LiveCount_"

Finally the "*statsAttributeName*" is requested. Imagine "lowWaterMark" shall be requested, so the final call of that attribute is "stats_LiveCount_lowWaterMark".

Example for monitor configuration:

ObjectName: Just the object name which contains the stats attribute.

Action: stats_attribute

Action Names: stats_LiveCount_lowWaterMark,>,10;stats_LiveCount_highWaterMark,>,40;stats_LiveCount_current,>,25

Tools - JMX Browsers

There are some tools available which make it possible to browse the MBeans of the application server and to change values with a graphical user interface. The following chapters will introduce some of these tools.

JConsole

JConsole is a tool delivered with the Java 5 distribution. With JConsole it is possible to view different statistics of the JVM and browse through the MBeans structure. It can be used with JSR160 compatible servers. The JConsole.exe can be found in the /bin directory of the Java 5 JDK. JConsole is recommended for JSR160 servers, running in a Java 5 system. This program is not part of IBM Enterprise Content Management System Monitor.

Tree Security Security	Attributes	Operations	v			
Tree All Mimplementation	Attributes	Operations	v			
Tree JMImplementation Security Combea	Attributes	Operations		1/		
JMimplementation Security com.bea			Notifications	Info		
Calify Combea		Name			Value	
Com.bea	AllowsPersis	stentDowngrade		tru	e	
	BlockingSendPolicy		FIF	0		
🕈 🔚 DatabaseName	BytesMaxim	um		-1		
🔶 🗂 MBeanTypeService	BytesPaging	Enabled		fals	se	
∽ □ ReliableWseeSAFAgent	BytesThresh	oldHigh		-1		
← C RuntimeService	BytesThresh	oldLow		-1		
C C Samples Search WebApp	Consumptio	nPausedAtStartu	lb	de	fault	
	Deployment	Order		10	00	
WiseeFileStore	ExpirationSc	aninterval		30		
- WseeJMSServer	HostingTem	poraryDestinatio	ns	fal	false	
- JMSMessageLogFile	InsertionPausedAtStartup		de	default		
- 🧐 JMSServer	JMSMessag	eLogFile		CO	m.bea:Name=WseeJMSServer,Type=JMSMessag.	
🕈 🗂 ejb20BeanMgedEar	JMSSession	Pools		jav	rax.management.ObjectName[0]	
🗢 🗂 exampleJDBCStore	MaximumMe	ssageSize		21	47483647	
🔶 🗂 exampleQueue	MessageBut	ferSize		-1		
🗣 🗂 exampleTopic	MessagesM	aximum		-1		
← C exampleTrader	MessagesP	agingEnabled		fals	se	
← C evamples-demo	MessagesTh	nresholdHigh		-1		
~ C examples demoVA	MessagesTh	nresholdLow		-1		
examples-demoxA	Name			VVs	seeJMSServer	
examples-demoxA-2	Notes			-		
← 🔄 examples-jms	PagingDirec	tory				
🔶 🛄 examples-jms	Parent	- 2000		COL	m.bea:Name=wl_server,Type=Domain	
🔶 🔚 examples-multiDataSource-dem	PersistentSt	ore		COL	m.bea:Name=VVseeFileStore,Type=FileStore	
🔶 📑 examples-oracleXA	ProductionP	ausedAtStartup		de	fault	
- C examplesJMSServer	SessionPoo	is .		jav	ax.management.ObjectName[U]	
← C examplesServer	StoreEnable	a		tru	e	
• C evernlesServer	Targets			jav	ax.management.ObjectName[1]	
	emporaryl	emplateivame				

JConsole

MBean Inspector

This is a tool for IBM WebSphere Application Servers. It can be downloaded from http://www.alphaworks.ibm.com/tech/mbeaninspector. The components of the tool have to be unzipped to the "lib" and "bin" folder of the WebSphere installation directory. MBeanInspector is recommended to be used with WebSphere Application Servers. This program is not part of IBM Enterprise Content Management System Monitor.

6)MBeanInspector	
File View Connect Operation Notification	Help
CataSource (cells/p2pp02471/node Attribute Description Attribute InactiveConnectionSup Attribute TransactionResourceR Attribute authMechanismPrefere Attribute category	General Properties Canonical name: WebSphere:JDBCProvider=Samples Cloudscape JDBC Provider,Server=server1 Cell: p2pp02471 MBean identifier: cells/p2pp02471/servers/server1/resources.xml#DataSource MBean type: DataSource Node: p2pp02471 Process: server1
Attribute connectionFactoryType Attribute dataSourceName Attribute dataSourceName Attribute dataSourceName Attribute dataSourceName Attribute dataStoreHelperClass Attribute description Attribute indiName Attribute indiName Attribute indiName Attribute loginTimeout Attribute loginTimeout Attribute statementCacheSize Operation getAllPoolContents Operation getAuthMechanismPr Operation getCategory Operation getDataSourceName Operation getDataSourceName Operation getJndiName Operation getJndiName Operation getJndiName Operation getJndiName Operation getLoginTimeout	Attributes connectionFactoryType dataSourceName dataStoreHelperClass description loginTimeout statementCacheSize TransactionResourceRegistration itaEnabled InactiveConnectionSupport authMechanismPreference Operations getConnectionFactoryClass getDataSourceName getDataSourceName getDataSourceName getDataStoreHelperClass getDat
Operation getPoolContents Operation getStatementCaches	imx.attribute.changed

MBean Inspector

Red Hat JBoss - JMX Console

Red Hat JBoss comes with its own JMX console. It can be started when connecting to the following URL (http://<host>:8080/jmx-console). The JBoss - JMX Console is recommended to be used for JBoss Application Servers. This program is not part of IBM Enterprise Content Management System Monitor.

🚰 JBoss JMX Management Console - Microsoft Internet Explorer provided by Cenit Internet Access		
File Edit View Favorites Tools Help		-
🖛 Back 🔻 🔿 🗸 😰 🚰 🥘 Search 📷 Favorites 🛞 Media 🥵 🛃 🗙 🎝 🔀 🔹 🧮 📖		
Address 🕖 http://192.168.240.154:8080/jmx-console/	• (∂Go Links '
		-
•••		
JMX Agent View w2kfsmen		
		_
N		
ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*") :		
ApplyFilter		
Catalina		
Catalilla		
• type=Server		
type=StringCache		
JMIMplementation		
 name=Default.service=LoaderRepository 		
• type=MBeanRegistry		
 type=MBeanServerDelegate 		
iava lang		
Javanany		
<u>name=Code Cache.type=MemoryPool</u>		
name=CodeCacheManager.type=MemoryManager		

Red Hat JBoss - JMX Console

JManage

JManage is a universal tool to browse and monitor application servers via web console and command line. It supports several application servers. The official website of this open source tool is on http://www.jmanage.org/. It comes with its own Jetty web server. Some configurations have to be made, like loading some application server own libraries. JManage is recommended to be used with every application server. In tests there were some problems when connecting to WebSphere. On all other servers it worked without any bigger problems. The product is documented very well on the website. This program is not part of IBM Enterprise Content Management System Monitor.

🚰 jManage - JMX Client - Microsoft Internet Explorer provided by Cenit Internet Access	
File Edit View Favorites Tools Help	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100
🗘 Back 🔹 🔿 🖉 🛐 🚮 📿 Search 💿 Favorites 🛞 Media 🧭 🛃 🚽 🗐 🗒	
Address 🖉 http://localhost:9095/app/mbeanList.do	▼ 🔗 Go Links ≫
<i>jManage</i>	Home Profile Admin Logout Logged-in as admin
Applications > iboss isr160 > Query	U
: Filter by object name	
Catalina	
type=Server	
type=StringCache	
Mimplementation	
service=LoaderRepository.name=Default	
type=MBeanRegistry	
type=MBeanServerDelegate	
java.lang	
type=ClassLoading	
type=Compilation	
type=GarbageCollector,name=Copy	
type=GarbageCollector,name=MarkSweepCompact	
type=Memory	
type=MemoryManager,name=CodeCacheManager	
type=MemoryPool,name=Code Cache	
type=MemoryPool,name=Eden Space	
har Manageria and Anna Car	

JManage

The structure of an MBean

The MBean is an object on the web application server which is referenced by a unique ObjectName. With this ObjectName as reference the attributes can be called and the operation can be invoked. The ObjectName can look as follows:

abstract example of an ObjectName

testServer:type=com.test,name=com.test

real example of an ObjectName

jboss.jca:name=DefaultDS,service=ManagedConnectionFactory

Preparing Application Servers for JMX

On most application servers (especially the JSR160 compatible servers) JMX has to be activated before it can be used. The following list remarks the steps which have to be done on principle. For further information check the application server's instruction manual.

WebLogic 7 and 8

As these Weblogic versions use the standard application server connection libraries no further configuration is needed.

WebLogic 9

WebLogic 9 supports JMX1.2 per default. No additional configuration has to be made.

Red Hat JBoss 3.x and 4.x (using JMX1.0)

As these JBoss versions use the standard application server connection libraries, no further configuration is needed.

Red Hat JBoss 4.x using JMX1.2

JMX1.2 has to be enabled in the startup script.

WebSphere 5.0

JMX has to be enabled in the administrative console. The monitor works with RMI as connection type. So the server has to enabled for JMX connection via RMI.

WebSphere 6.0.1

JMX has to be enabled in the administrative console. The monitor works with RMI as connection type. So the server has to enabled for JMX connection via RMI.

Sun Application Server

JMX has to be enabled in the administrative console. If it has been enabled correctly, the server log-file contains an entry with the service URL.

Oracle Application Server 10g

JMX1.2 has to be activated with the OC4J service of the Oracle Application Server.

Which attributes and Object Names the status monitors use

This chapter handles the status shell scripts. It describes which MBeans and which attributes are requested in the status request. MBean names are written in bold letters. Attributes which are used as maximum border of the threshold (for percentage use) are prefixed with an "B" like border value.. All other attributes have no style change.

```
0001 JBoss 3 + 4
0002 ------
0003 jboss.system:type=ServerInfo
0004 FreeMemory
0005 TotalMemory
0006 jboss.system:service=ThreadPool
0007 (B)MaximumQueueSize
0008 QueueSize
0009 jboss.web:name=<threadPoolName>,type=ThreadPool maxSpareThreadS
0010 (B)maxThreadS
0011 currentThreadCount
```

0012 currentThreadsBusy 0013 jboss.web:host=localhost,path=/<WebApplication>,type=Manager 0014 maxActiveSessions 0015 activeSessions 0016 expiredSessions 0017 maxActive 0018 rejectedSessions 0019 duplicates 0020 jboss.jca:service=ManagedConnectionPool,name=DefaultDS 0021 (B)AvailableConnectionCount 0022 MaxConnectionsInUseCount 0023 ConnectionCount 0024 InUseConnectionCount 0025 Oracle WebLogic 7 and Oracle WebLogic 8 0026 -----0027 <DomainName>:Location=<ServerName>,Name=<ServerName>,ServerRuntime= <ServerName>, Type=JVMRuntime 0028 HeapFreeCurrent 0029 HeapSizeCurrent 0030 <DomainName>:Name=default,Server=<ServerName>,Type=ExecuteQueue 0031 ThreadsMaximum 0032 ThreadCount 0033 <DomainName>:ApplicationRuntime=<ServerName>_<ApplicationName>, -Location=<ServerName>,Name=<ServerName> <ServerName> <ApplicationN $\verb+ame>_<ApplicationName>,ServerRuntime=<ServerName>,Type=WebAppComponentRu+$ ntime 0034 OpenSessionsHighCount 0035 OpenSessionsCurrentCount 0036 <DomainName>:Location=<ServerName>,Name=<ServerName>.jms, -ServerRuntime=<ServerName>, Type=JMSRuntime 0037 ConnectionsCurrentCount 0038 ConnectionsHighCount 0039 Oracle WebLogic 9 0040 ----0041 com.bea:Name=<ServerName>,ServerRuntime=<ServerName>,Location= <ServerName>, Type=JRockitRuntime 0042 FreeHeap 0043 TotalHeap 0044 UsedHeap 0045 HeapSizeCurrent 0046 HeapFreeCurrent 0047 HeapFreePercent 0048 (B)TotalPhysicalMemory 0049 FreePhysicalMemory 0050 UsedPhysicalMemory 0051 TotalNumberOfThreads 0052 AllProcessorsAverageLoad 0053 JvmProcessorLoad 0054 com.bea:Name=ThreadPoolRuntime,ServerRuntime=<ServerName>,Location=MedRecServer, Type=ThreadPoolRuntime 0055 PendingUserRequestCount 0056 ExecuteThreadIdleCount 0057 HoggingThreadCount 0058 ExecuteThreadTotalCount 0059 MinThreadsConstraintsPending 0060 QueueLength 0061 WebSphere 5 0062 -----0063 WebSphere:platform=common,cell=<CellName>,version=5.0.1,name=JVM,mbeanIdentifier

=JVM,type=JVM,node=<NodeName>,process=<ServerName>

0064 stats

```
0065 WebSphere:platform=common,cell=<CellName>,version=5.0,name=ORB.thread.pool, 
     mbeanIdentifier=cells/<CellName>/nodes/<NodeName>/servers/<ServerName>~
     /server.xml#ThreadPool_1,type=ThreadPool,node=<NodeName>,process=<ServerName>
0066 stats
0067 WebSphere:platform=common,cell=<CellName>,version=5.0,name=MessageListenerThread.
     Pool,mbeanIdentifier=cells/<CellName>/nodes/<NodeName>/servers/
     <ServerName>/server.xml#ThreadPool 3,type=ThreadPool,node=<NodeName>, 
    process=<ServerName>
0068 stats
0069 WebSphere:platform=common,cell=<CellName>,version=5.0,name=SoapConnectorThreadPo-
     ol, mbeanIdentifier=com.ibm.websphere.models.config.process.impl.ThreadPoolImpl,
     type=ThreadPool,node=<NodeName>,process=<ServerName>
0070 stats
0071 WebSphere:platform=common,cell=<CellName>,version=5.0,name=Servlet.Engine.
     Transports,mbeanIdentifier=cells/<CellName>/nodes/<NodeName>/servers/
     <ServerName>/server.xml#ThreadPool_2,type=ThreadPool,node=<NodeName>, -
    process=<ServerName>
0072 stats
0073 WebSphere:platform=common,cell=<CellName>,version=5.0,name=<ApplicationName>,J
     #<WarFileName>,mbeanIdentifier=default_host/<ApplicationName>,type=...
     SessionManager,node=<NodeName>,process=<ServerName>
0074 stats
0075 WebSphere 6
0076 -----
0077 WebSphere:name=JVM,process=<ServerName>,platform=dynamicproxy,node=<NodeName>,J
     , j2eeType=JVM, J2EEServer=<ServerName>, version=<Version>, type=JVM, ⊣
    mbeanIdentifier=JVM,cell=<CellName>
0078 heapSize
0079 freeMemory
0080 stats
0081 WebSphere:platform=dynamicproxy,cell=<CellName>,version=<Version>, -
     name=MessageListenerThreadPool,mbeanIdentifier=cells/<CellName>/nodes/
     <NodeName>/servers/<ServerName>/server.xml#ThreadPool_<MessageListenerID>,J
     ,type=ThreadPool,node=<NodeName>,process=<ServerName>
0082 stats
0083 WebSphere:platform=dynamicproxy,cell=<CellName>,version=<Version>, -
     name=ORB.thread.pool,mbeanIdentifier=cells/<CellName>/nodes/<NodeName>+
     /servers/<ServerName>/server.xml#ThreadPool_<ORB_ID>,type=ThreadPool,→
    node=<NodeName>,process=<ServerName>
0084 stats
0085 WebSphere:platform=dynamicproxy,cell=<CellName>,version=<Version>, -
     name=WebContainer,mbeanIdentifier=cells/<CellName>/nodes/<NodeName>.
     /servers/<ServerName>/server.xml#ThreadPool_<WebcontainerID>,type=→
    ThreadPool, node=<NodeName>, process=<ServerName>
0086 stats
0087 WebSphere:platform=common,cell=<CellName>,version=<Version>,name=.J
     <ApplicationName>#<WarFileName>,mbeanIdentifier=default_host<+</pre>
    ApplicationName>, type=SessionManager, node=<NodeName>, process=<ServerName>
0088 stats
0089 WebSphere 6.1
0090 -----
0091 WebSphere:name=__X__,process=<ServerName>,platform=__X__,node=<NodeName>, 4
```

```
mbeanIdentifier=_X_,cell=<CellName>,spec=_X_
0092 heapSize
0093 freeMemory
0094 stats
0095 WebSphere:name=__X__, process=<ServerName>, platform=__X__, node=<NodeName>, 4
    version=<Version>,type=_X_,mbeanIdentifier=cells/<CellName>/nodes/
    <NodeName>/servers/<ServerName>/server.xml#ThreadPool <MessageId>, -J
    cell=<CellName>,spec=__X_
0096 stats
0097 WebSphere:name=ORB.thread.pool,process=<ServerName>,platform=_X_,node=,J
    <NodeName>, version=<Version>, type=_X_, mbeanIdentifier=cells/<CellName>,
    /nodes/<NodeName>/servers/<ServerName>/server.xml#ThreadPool <ORB -J
    Id>,cell=<CellName>,spec=__X
0098 stats
0099 WebSphere:name=_X_,process=<ServerName>,platform=_X_,node=<NodeName>, 
    version=<Version>,type=_X_,mbeanIdentifier=cells/<CellName>/nodes/+
    <NodeName>/servers/<ServerName>/server.xml#ThreadPool_<WebContainerId>+
     ,cell=<CellName>,spec=__X___
0100 stats
0101 WebSphere:name=__X_, process=<ServerName>, platform=__X_, node=<NodeName>, -
    version=<Version>,type=ThreadPool,mbeanIdentifier=cells/<CellName>/nodes/+J
    <NodeName>/servers/<ServerName>/server.xml#ThreadPool_<TCP_Id>, -
    cell=<CellName>,spec=_X_
0102 stats
0103 WebSphere:name=<ApplicationName>#<WarFileName>, process=<ServerName>,
    ,platform=__X__,node=<NodeName>,version=<Version>,type=__X__,mbeanIdentifieJ
    r=__X__/<ApplicationName>,cell=<CellName>,spec=__X_
0104 stats
```

How to find out the actual configured port of the several application servers

This chapter shows a short description how to find out the port of the application server if it is not the default value.

Red Hat JBoss 3 and 4

On starting up the JBoss Application Server a lot of startup information is given out. The port can be read out in the following line of this output:

15:42:40,593 INFO [NamingService] JNDI bootstrap JNP=/0.0.0.0:1099, RMI=/0.0.0.0:1098, backlog=50, no client SocketFactory, Server SocketFactory=class org.jboss.net.sockets.DefaultSocketFactory

The bootstrap port is 1099, as written in the default information.

If JBoss 4 is configured for JMX 1.2, the administrator has defined the port itself in the startup script and so should know the correct port.

Weblogic 7, 8 and 9

On starting up the WebLogic servers, a lot of startup information is given out. The port can be read out at the end of the startup sequence.

At the end a conclusion is generated and a line following to this is printed out: "http://192.168.240.159:7011/ index.jsp"

This is the address to the administration console, but the port is the same for JMX connections as known.

WebSphere 5

To get the port of the WebSphere application server it is necessary do go into the administration console. Expand "server" and click on "Application Server". After that click on the server whose port shall be found out. On the left side there is the link "Endpoints". Click it to enter the port configuration menu. The bootstrap port is the port, which is needed to build up JMX connections. For usual it is port 2809. Beside the "Endpoints" link, there is also an "Administration Services" link which leads to a menu where the connection Type (whether RMI or SOAP) can be chosen. It might be necessary to switch this port to RMI. In some case it was, in some others it was not.

WebSphere 6 and WebSphere 6.1

To get the port of the WebSphere application server it is necessary do go into the administration console. Expand "server" and click on "Application Server". After that click on the server whose port shall be found out. On the left side there is the link "Ports". Click it to enter the port configuration menu. The bootstrap port is needed to build up JMX connections. For usual it is port 2809. Under the sub heading "server infrastructure" there is a link "administration" (the second link) which can be expanded. There is the "Administration Services" link which leads to a menu where the connection Type (whether RMI or SOAP) can be chosen. It might be necessary to switch this port to RMI. In some case it was, in some others it was not.

How to use JMX monitoring and tasks with Tomcat 5.x

As Tomcat is very popular this chapter describes how to configure Tomcat 5.x and run it with JMX 1.2.

Configure Tomcat 5.x

The Jakarta website describes how the startup script must be pre configured to activate JMX. The manual is on <u>http://tomcat.apache.org/tomcat-5.5-doc/monitoring.html</u>.

Tomcat 4 and 6 have not been tested to JMX functionality.

The web site shows some mix between Linux and Windows config. Windows needs a "set" to define the variable but can not handle double quotes around the whole expression. Take the examples below in the configuration. In the example the port 9004 is chosen. Every other free port could be used.

Windows:setCATALINA_OPTS=-Dcom.sun.management.jmxremote-Dcom.sun.management.jmxremote.port=9004-Dcom.sun.management.jmxremote.ssl=false-Dcom.sun.management.jmxremote.authenticate=false-Dcom.sun.management.jmxremote.ssl=false-Dcom.sun.

Linux / Unix: CATALINA_OPTS="-Dcom.sun.management.jmxremote - Dcom.sun.management.jmxremote.port=9004 -Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"

The web site says to enter the variable in the startup script. It also can be written in the catalina script, since it is called by the startup script. The startup scripts *catalina.bat* or *catalina.sh* are in the bin directory of the Tomcat install directory. \$CATALINA_HOME/bin/catalina.sh. Just as the startup script itself.

Hint for Windows: There is also a version of Tomcat 5.x which can be setup via installer and executed as a Windows service. It is recommended not to use this version, because it owns no startup script and it is not known if and where the JMX settings can be configured in the service version.

Java version: To execute Tomcat with JMX enabled, Java version 5 is needed. It should also work, when Tomcat runs with a J2EE 1.4, but Java Standard Edition 1.4.x is not supported out of the box. The web site describes how to configure Tomcat, when Java 1.4.x shall be used. In this case a special adaptor of the MX4J project is needed. The JMX monitors and task need whether Java version 5 or 1.4.x.

Security: The website also describes how to activate security (user authentication). The upper example only shows the basic configuration, without user and password required.

Service URL: Tomcat can be accessed via JSR160 just like all other application servers which support JSR160. The service URL is "service:jmx:rmi://jndi/rmi://HOST:PORT/jmxrmi"

Monitors which Support Tomcat: Configured like that, Tomcat can be accessed via "JMX WebApplication Thresholds" Monitor, "JMX WebApplication Thresholds" Monitor and "View JMX Parameters" Task.

How to configure sas.client.props for WebSphere

To access the MBeans, when security on WebSphere is enabled, the following steps have to be executed, before this will work.

The file sas.client.props is found in the \$WASHOME/AppServer/propertires (WebSphere 5) or \$WASHOME/AppServer/profiles/<profilename>/properties (WebSphere 6.0.x.x and WebSphere 6.1.x.x). In the sas.client.props file the following variables have to be changed:

- com.ibm.CORBA.loginUserid=<UserName>
- com.ibm.CORBA.loginPassword=<PasswordAsClearText>

To encrypt the password the following WebSphere command has to be used:

Windows:

\$WASHOME/AppServer/bin/PropFilePasswordEncoder <pathToSasFile>/sas.client.props com.ibm. CORBA.loginPassword

• Unix:

\$WASHOME/AppServer/bin/PropFilePasswordEncoder <pathToSasFile>/sas.client.props com.ibm. CORBA.loginPassword

This command will encode the password(s) and will also delete all comments. A file with the name sas.client.props.bak will be created with the old version of the file (The new file will not have the comments anymore, because they are deleted by the algorithm . Even if the sas.client.props contains the login data now, the user and password have still to be defined in the monitor because the credentials in the props file only does the CORBA authentication.
How to create the keystore and truststore files for WebSphere 6.1.x.x and newer

By default WebSphere 6.1.x.x application servers have stronger security configurations compared with previous WebSphere versions. A keystore and truststore have to be generated for authentication when JMX data is going to be requested. It is recommended to perform the following steps before configuring WebSphere 6.1.x and newer monitors. It is possible to use the resources of an existing WebSphere profile, but this should only be done, when the WebSphere Administrator has no concerns about that. The following steps were verified on WebSphere 6.1 machines and might differ on newer WebSphere environments.

Important: The following steps are best practices, which are proposed for the JMX monitoring, without changing already existing WebSphere profile configurations. If you are familiar with the WebSphere security configuration, you don't need to perform these steps. But make sure, that the keystore and truststore exists. The JMX monitoring program is using SAS_PATH setting. Therefore the monitors and tasks are looking for the ssl.client.props file at the same place (relative file path).

The following steps have to be performed:

- Open a shell / command line interface.
- Copy the properties directory of a WebSphere profile of your choice to CENIT_ROOT/cala/monitors/pam
 cp -r \$WAS_HOME/profiles/<profile_name>/properties \$CENIT_ROOT/cala/monitors/pam
- Edit the file \$CENIT_ROOT/cala/monitors/pam/properties/sas.client.props Perform the actions described in the chapter How to configure sas.client.props for WebSphere: For <pathToSasFile> use \$CENIT_ROOT/cala/monitors/pam/properties/sas.client.props.
- Edit the file \$CENIT_ROOT/cala/monitors/pam/properties/ssl.client.props
 Perform the changes in the file as shown in the snippets below. Except of these changes, the file
 should be left in it's origin
 Attention: Replace the text between the pointed brackets <> through real paths

```
0001 ...
0002 # Has to be set to false later, but now it must be set to true.
0003 com.ibm.ssl.enableSignerExchangePrompt=true
0004 ...
0005 # KeyStore information
0006 ...
0007 com.ibm.ssl.keyStore=<$CENIT_ROOT>/cala/monitors/pam/key.p12
0008 ...
0009 # TrustStore information
0010 ...
0011 com.ibm.ssl.trustStore=<$CENIT_ROOT>/cala/monitors/pam/trust.p12
0012 ...
```

- Copy setupCmdLine.bat/setupCmdLine.sh and to \$CENIT_ROOT/cala/monitors/pam cp \$WAS_HOME/profiles/<profile_name>/bin/setupCmdLine.* \$CENIT_ROOT/cala/ monitors/pam cp \$WAS_HOME/profiles/<profile_name>/bin/retrieveSigners.* \$CENIT_ROOT/ cala/monitors/pam
- Edit the file \$CENIT_ROOT/cala/monitors/pam/setupCmdLine.bat or .../
 setupCmdLine.sh and change the following line

*Windows:*set USER_INSTALLATION_ROOT=<CENIT_ROOT>/cala/monitors/pam *Unix:*export USER_INSTALLATION_ROOT=<CENIT_ROOT>/cala/monitors/pam

 Edit the file \$CENIT_ROOT/cala/monitors/pam/retrieveSigners.bat or .../ retrieveSigners.sh and change the following line Windows: set WAS_USER_SCRIPT=<CENIT_ROOT>/cala/monitors/pam/setupCmdLine. bat Unix: export WAS_USER_SCRIPT=<CENIT_ROOT>/cala/monitors/pam/setupCmdLine.sh

• Change to the directory \${CENIT_ROOT}/cala/monitors/pam/profiles/<profile-Name>/bin

Request the remote keystore names and the local keystore names.
 Windows: retrieveSigners.bat -listRemoteKeyStoreNames -listLocalKeyStoreNames

 ${\sf Unix: retrieveSigners.sh\ -listRemoteKeyStoreNames\ -listLocalKeyStoreNames}$

- An output similar to this will be returned:
 - 0001 CWPKI0306I: The following remote keystores exist on the specified → server: CMSKeyStore, NodeLTPAKeys, NodeDefaultTrustStore, NodeDefaultKey→ Store
 - 0002 CWPKI0306I: The following remote keystores exist on the specified → server: CMSKeyStore, NodeLTPAKeys, NodeDefaultTrustStore, NodeDefaultKey→ Store

If no output like that, but an error message occurs, try to copy the files from \${WAS_HOME}/
profiles/<profileName>/etc/trust.pl2 and \${WAS_HOME}/profiles/<profileName>/etc/key.pl2 to the pam directory.

 Use one of the keystores, which are returned by the previous command to execute the following command:

0001 retrieveSigners <remoteKeyStoreName> <localKeyStoreName>

Example:

Windows:retrieveSigners.bat NodeDefault TrustStore ClientDefaultTrustStore *Unix*:retrieveSigners.sh NodeDefault TrustStore ClientDefaultTrustStore

- It might be necessary to authenticate with user and password. For usual a login dialog will appear. After an administrative user and password are entered, a new keystore and truststore are generated in \$CENIT_ROOT/cala/monitors/pam/trust.pl2 and \$CENIT_ROOT/cala/monitors/pam/key.pl2.
- The JMX monitors and tasks will give the ssl.client.props file to the Java program as a property. When a sas.client.props path is defined, the monitors and tasks will use this path to refer to the ssl.client.props. For basic use, this file has not to be edited.
- In the monitors the SAS_PATH needs not to be set, when the files are stored in the pam directory. But since there are several profiles on WebSphere and each one might have its own security handling it is proposed not to store this data in the pam directory, but in pam/<profileName> directory. Also all paths which point to the pam directory in this scenario must be changed to pam/<profile-Name>. But in this case, the SAS_PATH must be set for each monitor, depending to which profile's servers it shall connect.
- For more information go to the following web sites:

https://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rsec_sslclientpropsfile.html https://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_retrievesigners.html

The jmx_classpaths.props file

On the client, there is a props file, which contains all class paths for the supported application servers. This file is stored at CENIT_ROOT/cala/monitors/pam/jmx_classpaths.props. It can be used, when the class path has to be extended, because of missing jar files. Therefor a task exists in the STANDARD task archive, to load and edit this task. It is called "JMX Class Path Edit Task". Refer to the task guides for more information. All monitors and tasks use this file. If the file does not exist, hard coded class paths are defined inside the script, so the monitors and tasks will not fail.

Workaround for pwdcrypt problem with Unix systems

There may be problems with pwdcrypt on Unix systems, when the JMX monitors are called. An exception will occur in the task output (for tasks) and in the monitor plusdebug output (for monitors) which looks similar to the following.

```
0001 -----Standard Output-----
0002 java.lang.reflect.InvocationTargetException
0003
     at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
0004 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
0005 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.J
     java:25)
0006 at java.lang.reflect.Method.invoke(Method.java:324)
0007 at com.ibm.ws.bootstrap.WSLauncher.run(WSLauncher.java:219)
0008 at java.lang.Thread.run(Thread.java:534)
0009 Caused by: java.lang.UnsatisfiedLinkError: no PwdCrypt.solaris2 in java.library.path
0010 at java.lang.ClassLoader.loadLibrary(ClassLoader.java:1517)
0011 at java.lang.Runtime.loadLibrary0(Runtime.java:788)
0012 at java.lang.System.loadLibrary(System.java:834)
0013 at de.cenit.eb.sm.cala.utils.PwdCrypt.<clinit>(Unknown Source)
0014 at de.cenit.eb.sm.mbeanmonitor.MonitorMBeans.decryptPassword(Unknown Source)
0015 at de.cenit.eb.sm.mbeanmonitor.MonitorMBeans.fillProperties(Unknown Source)
0016
     at de.cenit.eb.sm.mbeanmonitor.MBeanMonitorMain.getOutput(Unknown Source)
0017
      at de.cenit.eb.sm.mbeanmonitor.MBeanMonitorMain.main(Unknown Source)
0018
     ... 6 more
```

The most important line is "Caused by: java.lang.UnsatisfiedLinkError: no PwdCrypt.solaris2 in java.library. path".

Workaround for tasks and monitors:

- 1 Create the folder pwdcrypt_libs in the directory \$CENIT_ROOT/tools.
- 2 Change directory to \$CENIT_ROOT/tools/de.cenit.
- 3 Extract the pwdcrypt jar file with the command "jar -xvf pwdcrypt.jar" and execute the following copy command. "cp libPwdCrypt.linux.so ./pwdcrypt_lib/libPwdCrypt.linux.so" so that this file is in the previously created directory.

- 4 Change to the CALAdirectory and edit the file cala_rex_cli.cfg. Execute "cp libPwdCrypt.linux.so ./ pwdcrypt_lib/libPwdCrypt.linux.so".
- 5 Append the following line to the file: <property name="libpathadd" value="\$CENIT_ROOT/tools/pwdcrypt_libs">
- 6 Restart CALA.
- 7 Change to cala directory and edit cala_env.sh.
- 8 Add the following line export LD_LIBRARY_PATH=.:\$LD_LIBRARY_PATH. This works as well on Solaris.

AIX: export LIBPATH=.:\$LIBPATH

HP-UX: export SHLIB_PATH=.:\$SHLIB_PATH

9 Save and restart CALA.

How to enable basic JSR160 functionality on Red Hat JBoss 4.x

To enable basic JSR160 functionality in JBoss 4.x, JBoss must be executed with a Java version 5 or later and the following adjustments must be made in the run.bat or run.sh of the JBoss which are in the bin directory.

The example uses port 9999. Any other usable port can be chosen. Also no security is enabled with this configuration. For further information about how to configure security please refer to the JBoss administration manuals.

```
0001 Windows in run.bat
0002 ...
0003 set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m -Dsun.rmi.dgc.client.gcInterval=3600000 斗
     -Dsun.rmi.dgc.server.gcInterval=3600000
0004 set JAVA_OPTS=%JAVA_OPTS% -Djavax.management.builder.initial=org.jboss.system.server.4
     jmx.MBeanServerBuilderImpl
0005 set JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver
0006 set JAVA OPTS=%JAVA OPTS% -Dcom.sun.management.jmxremote -Dcom.sun.management.J
     jmxremote.port=9999 -Dcom.sun.management.jmxremote.authenticate=false -Dcom.sun.J
    management.jmxremote.ssl=false
0007 ...
0008 Unix in run.sh
0009 ...
0010 JAVA_OPTS=$JAVA_OPTS -Xms128m -Xmx512m -Dsun.rmi.dgc.client.gcInterval=3600000 +
     -Dsun.rmi.dgc.server.gcInterval=3600000
0011 JAVA_OPTS=$JAVA_OPTS -Djavax.management.builder.initial=org.jboss.system.server.jmx.J
    MBeanServerBuilderImpl
0012 JAVA_OPTS=$JAVA_OPTS -Djboss.platform.mbeanserver
0013 JAVA_OPTS=$JAVA_OPTS -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.J
     port=9999 -Dcom.sun.management.jmxremote.authenticate=false -Dcom.sun.management.4
     jmxremote.ssl=false
0014 ...
```

```
© Copyright Cenit AG 2000, 2016, © Copyright IBM Corp. 2005, 2016
```

JMX Support via WebService

There is the possibility to deploy web application with web service а (monitortools.applicationserver.jmx.adaptor.war monitortools.applicationserver.imx.adaptor.ear) on a application server and request the data from this service, avoiding to configure the sas client.props and ssl-client.props files as in the usual connection way. This is only available for the JPS JMX Monitor.

The following figure illustrates the dependencies between the web application server (IBM WebSphere, Oracle WebLogic or JBoss) and the JMX Client (monitors and tasks). The JPS Monitor is called as usual and as described in the monitoring guide.

For HTTPS some additional steps have to be performed. The following figure shows in basic, what the following sub sections will describe



WebService dependencies

Note: The web service gets information of the server and its JVM in which it is running. So if a WebSphere cluster (WebSphere Network Deployment) environment shall be monitored, the monitortools.applicationserver.jmx.adaptor application must be deployed on every server instance via ND.

Create or get a keystore for IBM WebSphere 6.x and IBM WebSphere 7.x and IBM WebSphere 8.0.x

The simplest solution is to use an existing keytstore. However, if none exists one must be generated. A keystore is a container for server certificates. First the server's certificate is required. This can be acquired from the WebSphere system administrator or simply downloaded and exported using a common web browser. Make sure that the file is stored in "der" format.

Assuming the certificate is named "mycert.cert" it must be added to a keystore using this command:

0001 \$JAVA_HOME/bin/keytool -import -file mycert.cert -alias WAS-certificate -keystore - mystore

The keytool will ask you if you want to trust the keystore. Accept it by typing "yes". Furthermore it will ask you for a password. Use a password you like, e.g. adminadmin.

It is recommended to create the truststore on the CALAagent (and use the JRE of the CALA installation), on which the monitor is executed, since the keystore must be stored on the agent machine anyway, to reference it in the Configure Keystore Settings task.

Exporting a certificate for IBM WebSphere 8.5.x, using the Integrated Solutions Console

On *IBM WebSphere 8.5* the certificate can be exported from the Integrated Solutions Console as follows:

Select Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates > Extract certificate in the IBM WebSphere 8.5 Integrated Solutions Console.

SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates Manages personal certificates. + Preferences Create
Delete Receive from a certificate authority... Replace... Import... Export... Revoke... Renew Extract... Select Alias Issued To Issued By Serial Number Expiration You can administer the following resources: 93 CN=svwap003di.de.cenit-CN=svwap003di.de.cenit-6301472591628 Valid from default group.com, OU=SMRDcell02, group.com, OU=Root Jun 20, Certificate, OU=SMRDcell01, OU=SMRDnode01, O=IBM, 2013 to Jun C=US OU=dmgrNode01, O=IBM, 20, 2014. C=US CN=svwap003di.de.cenit-CN=svwap003di.de.cenit-4343476569927 Valid from ٦ group.com, OU=Root aroup.com, OU=Root lun 20. Certificate, OU=SMRDcell01, Certificate, OU=SMRDcell01, 2013 to Jun OU=dmgrNode01, O=IBM, OU=dmgrNode01, O=IBM, 16, 2028. C=US C=US Total 2

Store it to an arbitrary name, e.g. websphere85_store.cert

Extract certificate under IBM WebSphere 8.5

Hint: The cert file is stored in a directory of your IBM WebSphere installation directory. If you click the Apply button twice, the console will show the message below, where you can see, in which directory the cert was saved to.

SL certificate and k	key management
	Messages
	CWPKI0621E: D:/IBM/WAS85/AppServer/profiles/DMgr01/etc/websphere85_store.cert already exists.
SSL certificate an	nd key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates > Extract certificate
Extracts a certifica	ate from the key store to be added to another key store.
Conoral Properties	
a where the second	
Certificate alias to	io extract
default	
* Certificate file n	name
websphere85_st	tore.cert
Data type	
Base64-encode	ed ASCII data 💌
Apply OK I	Reset Cancel

Save certificate under IBM WebSphere 8.5

Import the Store Into the Agent's Monitoring Environment

Execute the Configuration > Configure Keystore Settings task in the IBM ECM SM Task Execution Manager on the agent, where the *JMX* client is running.

Enter the path to your keystore in the field Keystore Name of the task.

The field Keystore Type is not important for *JMX* requests. You can enter a default value.

Enter the password for the keystore in the Keystore Password field. In the previously shown examples it was adminadmin.

File Tools	Help		
Global Set	tings		
Product:	Configuration		-
Task:	Configure Keystore Settings		-
Task Spec	ific Settings		
	Servers:	N7P02471B64BIT.de.cenit-group.com	
		p6sysmlp03	
	Keystore Filename incl. Path:	C:\cenitroot\mystore	
	Keystore Type:	pkcs12	
	Keystore Password:	•••••	
Store as	a task definition	Run task About this	s task
Connected to	o N7P02471B64BIT.de.cenit-group.com	n:23802 as admin	

Configuration Task

The file ts_conf.prop will be stored in the cala/monitors/pam directory of the client.

The JPS JMX component requests the keystore data automatically from the $ts_conf.prop$ file, if an HTTPS URL is requested.

How to deploy the monitortools.applicationserver.jmx.adaptor application as WebSphere Enterprise Application

This section describes the deployment of the monitortools.applicationserver.jmx.adaptor enterprise application onto a standalone *IBM WebSphere Application Server version 7.0*. A separate description of an ND system is not included. For special adjustments of *IBM WebSphere Application Server version 6.0* see the following chapter.

The application is provided as a WAR (Web Archive) and an EAR (Enterprise Archive) file.

Both file types can be found under <CENIT_ROOT>/repos/install/web_apps in your IBM ECM SM Server installation.

Perform the following steps to deploy the EAR file onto your IBM WebSphere Application Server.

Note: Certain changes you make in the *Integrated Solutions Console* of your IBM WebSphere Application Server require a "Save directly to the master configuration." to become effective. Perform this action by clicking the **Save** link, that is displayed in the **Messages** section on the console.

WebSphere. software		Welcome wasadmin			
View: All tasks	Cell=SMRDcell01, Profile=DMgr01				
Welcome	Enterprise Applications	?			
Guided Activities	Entrumine Annline line				
Servers					
New server	ose this page to manage installed applications. A single application can be deproved onto multiple servers.				
Server Types	H Preterences				
	Start Stop Install Uninstall Update Rollout Update Remove File Export DDL Export File				
DataPower					
Applications	Select Name 🗘 Application Status 🖸				
New Application	You can administer the following resources:				
Application Types	DefaultApplication				
WebSphere enterprise applic	Total 1				
 Business-level applications Assets 					
Global deployment settings					
+ Jobs					
± Services					
+ Resources					
± Security					
Environment					
System administration					
Monitoring and Tuning					
+ Troubleshooting					
Service integration					
± UDDI					
	1				

Enterprise Applications Page

Press the Install button to install the monitoring application.

WebSphere. software		Welcome wasadmin
View: All tasks	Enterprise Applications	
Welcome	Preparing for the application installation	2 -
Guided Activities Guided Activities Subscript Activities Subscrite Subscript Activities Subscript Activities Subs		
 Servers 	Specify the EAR, WAR, JAR, or SAR module to upload and install.	
New server	Path to the new application	
Clusters	 Local file system 	
DataPower	Puil parn	
± Core Groups	Dubisuciermonitorcoos.appicationserver.jmx.adaptor.ear	
Applications	Remote file system	
New Application	Full path	
Application Types	Browse	
 Business-level applications 		
Assets	Next Cancel	
Global deployment settings		
± Jobs		
± Services		
Resources		
Security		
Environment		
System administration		
Monitoring and Tuning		
Troubleshooting		
Service integration		
± UDDI		

Specifying the path to the new application

Select the monitortools.applicationserver.jmx.adaptor.ear file and press Next.

WebSphere. software		Welcome wasadmin		IBM.
View: All tasks	Enterprise Applications		Clo	ise page
Welcome	Preparing for the application installation			? =
Guided Activities				
 Servers 	How do you want to install the application?			
New server	Fast Path - Prompt only when additional information is required.			
Clusters	Detailed - Show all installation options and parameters.			
DataPower				
	Choose to generate default bindings and mappings			
Applications				
New Application	Previous Next Cancel			
WebSphere enterprise applic				
Business-level applications				
Assets				
Global deployment settings				
🛨 Jobs				
± Services				
Resources				
E Security				
Environment				
∃ System administration				
Monitoring and Tuning				
Troubleshooting				
Service integration				
■ UDDI				
	1			

Preparing for the application installation

Choose Detailed and press Next.

ll=SMRDcell01, Profile=D	Mgr01 Close pa
stall New Application	2
Specify options for ins	stalling enterprise applications and modules.
→ Step 1: Select	Select installation options
installation optior	ns Specify the various options that are available for your application.
<u>Step 2</u> Map modules to server	rs 🛛 Precompile JavaServer Pages files
<u>Step 3</u> Provide JS	Directory to install application
reloading options Web modules	for The second sec
Step 4 Map shar	ed Distribute application
libraries	
<u>Step 5</u> Map share library relationship	ed Application name
 Step 6 Map virtu: 	Monitortools_Applicationserver_JM
hosts for Web	Create MBeans for resources
modules	Override class reloading settings for Web and EJB modules
roots for Web	Ext Relad interval in seconds
modules	Deploy Web services
<u>Step 8</u> Map secu roles to users or	Validate Input off/warn/fail
<u>Step 9</u> Map JASP provider	Process embedded configuration
<u>Step 10</u> Metadat	a Allowall files to be read but not written to
for modules	Allow executables to execute
<u>Step 11</u> Display module build Ids	.*dll=755#.*so=755#.*a=755#.*sl=755
<u>Step 12</u> Summar	ry Application Build TD
	Unknown
	Allow dispatching includes to remote resources
	Allow servicing includes from remote resources
	Business level application name Create New BLA
	Asynchronous Request Dispatch Type
	Disabled 💌
	Allow E)B reference targets to resolve automatically
	Deploy client modules Client deployment mode
	Isolated
	Validate schema
Next Const	
wext Cancel	

Select installation options

Make sure the Precompile JavaServer Pages files checkbox is checked.

Cell	=SMRDcell01, Profile=DMgr(01		Close page
Ins	stall New Application			
	Specify options for installi	ng enterprise applications and modules.		
	<u>Step 1</u> Select	Map modules to servers		
	 Step 2: Map modules to servers 	Specify targets such as application servers or clusters of application servers where you want to insta Modules can be installed on the same application server or dispersed among several application s serve as routers for requests to this application. The plug-in configuration file (plugin-cfg.xml) for e applications that are routed through.	ill the mo irvers. Al each Wel	odules that are contained in your iso, specify the Web servers as tai b server is generated, based on th
	<u>Step 3</u> Provide options to compile JSPs	Clusters and servers: WebSphere:cell=W2K8R264WAS855Node01Cell,node=W2K8R264WAS855Node01,server=server1		pply
	<u>Step 4</u> Provide JSP reloading options for Web modules			
		Select Module URI		Server
	<u>step 5</u> map snared libraries	monitortools.applicationserver.jmx.adaptor INF/web.xml	war,WEB-	WebSphere:cell=W2K8R264WAS
	<u>Step 6</u> Map shared library relationships			·
*	 <u>Step 7</u> Map virtual hosts for Web modules 			
	<u>Step 8</u> Map context roots for Web modules			
	<u>Step 9</u> Map security roles to users or groups			
	<u>Step 10</u> Map JASPI provider			
3	<u>Step 11</u> Metadata for modules			
	<u>Step 12</u> Display module build Ids			
	Step 13 Summary			
	Previous Next C	ancel		

Map module to server

Check the monitortools.applicationserver.jmx.adaptor module checkbox in the table and select the application server on which you want to install the selected module from the **Clusters and servers:** drop-down list box. Click the **Apply** button to carry over the selected server into the table's **Server** column. Click **Next**.

The next steps can be left in their default state. Just check the *Select* checkboxes and click *Next* until you get to the *Map virtual hosts for Web modules* panel.



Map virtual hosts for Web modules

Select the monitortools.applicationserver.jmx.adaptor web module, map it to the default_host and press Next.

<u>Step 1</u> Select	Map context roots for Web modules		
installation options	Configure values for context roots in web m	odules.	
<u>Step 2</u> Map modules to servers	Web module	URI	Context Root
<u>Step 3</u> Provide options to compile JSPs	monitortools.applicationserver.jmx.adaptor	monitortools.applicationserver.jmx.adaptor.war,WEB-INF/web.xml	jmxmonitor
<u>Step 4</u> Provide JSP reloading options for Web modules			
<u>Step 5</u> Map shared libraries			
<u>Step 6</u> Map shared library relationships			
<u>Step 7</u> Map virtual hosts for Web modules			
Step 8: Map context roots for Web modules			
<u>Step 9</u> Map security roles to users or groups			
<u>Step 10</u> Map JASPI provider			
<u>Step 11</u> Metadata for modules			
Step 12 Display			

Map context root

Enter the context root. The default value is *jmxmonitor*. Press Next. In the EAR file's installation process, this step is skipped and the context root is automatically set to *jmxmonitor*.

installation options <u>Step 2</u> Map modules to servers <u>Step 3</u> Provide options to compile 1506	Each role that is defi registry. accessIds: domain scenario. Fo based on the user of	ned in the appli The accessIds a	cation or module mus	t map to a user	or group from the domain us
Step 2 Map modules to servers Step 3 Provide options to compile	Each role that is defi registry. accessIds: 7 domain scenario. For based on the user of	ned in the appli The accessIds a	cation or module mus re required only when	t map to a user	or group from the domain us
options to compile	for Java Platform, En	r all other scena r group name. T Iterprise Edition	rios the accessId will t 'he accessIds represen authorization when us	using cross real be determined d nt the user and sing the WebSph	m communication in a multi luring the application start group information that is used lere default authorization
3513	engine. The format f wrong information in indicates that any va	or the accessId these fields will lid user in the t	s is user:realm/unique cause authorization t rusted realms be give	eUserID, group: to fail. AllAuthen n the access. All	realm/uniqueGroupID. Enterin ticatedInTrustedRealms: This Authenticated: This indicates
Step 4 Provide JSP	that any valid user in	n the current rea	Im be given the acces	55.	
reloading options for Web modules	Map Users	Map Groups	Map Special Subje	cts 🔻	
<u>Step 5</u> Map shared libraries					
	Select Role	Spe	ecial subjects	Mapped users	Mapped groups
<u>Step 6</u> Map shared library relationships	jmx_monitor	ing Nor	1e		
<u>Step 7</u> Map virtual hosts for Web modules					
<u>Step 8</u> Map context roots for Web modules					
Step 9: Map security roles to users or groups					
<u>Step 10</u> Map JASPI provider					
<u>Step 11</u> Metadata for modules					

Map Users...

Select the jmx_monitoring role and press the Map Users... button.

Cell=SMRDcell01, Profile=DMgr01	
Enterprise Applications	? -
Enterprise Applications > Enterprise Applications > Map users/groups	
Use this page to search for users or groups and add them to the selected roles.	
■ jmx_monitoring	
Search and Select Users	
Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users in the Available list and add t the Selected list.	hem to
Display a maximum of	
20 results	
*	
Search	
The selected realm cannot be accessed at this time. You might need to start the server. Otherwise, you can use the following fields to ac	ld users
by their unique user IDs.	
User short name Selected:	
Unique user ID	
*	
UK Cancel	

Search and Select Users

Initially, there are no users in the **Available** list. Specify an appropriate search string and click on **Search** to find users, you want to assign to the application's security realm.

Cell=SMRDcell01, Profile=DMgr01		
Enterprise Applications		? -
Enterprise Applications > Enterprise Applications	plications > Map users/groups	
Use this page to search for users or gro	ups and add them to the selected roles.	
jmx_monitoring		
Search and Select Users		
Decide how many results to display, ent the Selected list.	er a search string (use * for wildcard), and click	c Search. Select users in the Available list and add them to
Display a maximum of	- .	
20 Search string	results	
*]	
Search		
Available:		Selected:
wasadmin 🔺		
	•	
~		Ŧ
OK Cancel		

Map users/groups

Add the desired OS users (here: *wasadmin*) to the **Selected** list. The application requires the following minimum access roles: 'Monitor' and 'Auditor'.

CHILLE	MDDaall	01 0-		110-0-
Cell-3	MRDCell	01, PI	onie-L	лмаго.

Step 1 Select	Map se	curity roles	s to users o	r groups				
Installation options <u>Step 2</u> Map modules to servers <u>Step 3</u> Provide options to compile JSPs Step 4 Provide JSP	Each ro registry domain based for Java engine, wrong i indicate that an	Each role that is defined in the application or module must map to a user or group from the domain user registry. accessIds: The accessIds are required only when using cross realm communication in a multi domain scenario. For all other scenarios the accessId will be determined during the application start based on the user or group name. The accessIds represent the user and group information that is used for Java Platform, Enterprise Edition authorization when using the WebSphere default authorization engine. The format for the accessIds is user:realm/uniqueUserID. group:realm/uniqueGroupID. Entering wrong information in these fields will cause authorization to fail. AllAuthenticatedInTrustedRealms: This indicates that any valid user in the trusted realms be given the access. AllAuthenticated: This indicates that any valid user in the current realm be given the access.						
reloading options for Web modules	Ма	Map Users Map Groups Map Special Subjects 👻						
<u>Step 5</u> Map shared libraries		6						
<u>Step 6</u> Map shared library relationships	Select	Kole jmx_monito	ring	None	wasadmin	irs	Mapped groups	
<u>Step 7</u> Map virtual hosts for Web modules								
<u>Step 8</u> Map context roots for Web modules								
Step 9: Map security roles to users or groups								
<u>Step 10</u> Map JASPI provider								
<u>Step 11</u> Metadata for modules								
Step 12 Display								

Map security role

The *wasadmin* user is now mapped to the jmx_monitoring role.

Leave the settings of the following steps at their default values and click the Next button.

cify options for installing er	nterprise applications and modules.				
Step 1 Select	Summary				
installation options	Summary of installation options				
Step 2 Map	Options	Values			
modules to servers	Precompile JavaServer Pages files	Yes			
<u>Step 3</u> Provide	Directory to install application				
JSPs	Distribute application	Yes			
Step 4 Provide JSP	Use Binary Configuration	No			
reloading options for	Deploy enterprise beans	No			
Web modules	Application name	Monitortools_Applicationserver_JMX_Adaptor			
Step 5 Map shared	Create MBeans for resources	Yes			
Step 6 Map shared	Override class reloading settings for Web and EJB modules	No			
library relationships	Reload interval in seconds				
Step 7 Map virtual	Deploy Web services	No			
hosts for Web modules	Validate Input off/warn/fail	warn			
	Process embedded configuration	No			
<u>Step 8</u> Map context roots for Web modules	File Permission	.*\.dll=755#.*\.so=755#.*\.a=755#.* \.sl=755			
modules	Application Build ID	Unknown			
<u>Step 9</u> Map security roles to users or	Allow dispatching includes to remote resources	No			
	Allow servicing includes from remote resources	No			
Step 10 Map JASPI	Business level application name				
provider	Asynchronous Request Dispatch Type	Disabled			
<u>Step 11</u> Metadata	Allow EJB reference targets to resolve automatically	No			
	Deploy client modules	No			
Step 12 Display	Client deployment mode	Isolated			
module build Ids	Validate schema	No			
Step 13: Summary	Cell/Node/Server	Click here			

Summary

Review the deployment summary page and click Finish.

Check the monitortools.applicationserver.jmx.adaptor checkbox and start the installed application by pressing Start.

The web service is running now and acts as an interface to WebSphere's internal MBeans. These are accessed by the JPS JMX Monitor and its components.

Special Adjustments for WebSphere Application Server (Adapting the JDK Source Level in the Integrated Solutions Console)

The JDK Source Level may be set to JDK 1.3 for your *WebSphere Application Server* by default. At monitor runtime, this setting leads to an output, that contains an HTML coded error message.

To avoid this error message, you must set the JDK Source Level to version 1.5 in the *Integrated Solutions Console*. The procedure is as follows:

- Log in to the Integrated Solutions Console
- Click on the link of the application server, whose JDK source level you want to adapt under Server Types > WebSphere application servers
- On the Configuration tab under Container Settings, click on Web Container Settings and then on Web container
- Under Additional Properties click on Custom properties
- On the Custom properties page, click the New button
- Under General Properties specify a name for the custom property (e.g. *jdkSourceLevel*) and enter 15 in the Value field to set the JDK source level to the 1.5 JDK version. Optionally, enter a description. Note, that the values of textual properties are case sensitive.
- Click Apply or OK
- Click Save in the Messages box, that appears
- Restart the server for the adapted JDK source level custom property to take effect

Special Adjustments for WebSphere Application Server (Adapting the JDK Source Level in the Configuration File)

Alternatively to the adaptation on the *WebSphere Integrated Solutions Console*, the JDK source level can also be adapted in a configuration file.

In order to set the JDK source level to version 1.5, proceed as follows (if you have an environment with a DMGR, the changes must be made for the DMGR and the other nodes have to be synchronized):

- Dependent on your WebSphere Application Server version, open the following file in a text editor: WebSphere AS 6: {WAS_ROOT}/profiles/<profilename>/config/cells/<cellname>/applications/ <enterpriseappname>/deployments/<deployedname>/<webmodulename>/WEB-INF/ibm-web-ext.xmi
 WebSphere AS 7, 8 and 8.5: {WAS_ROOT}/profiles/<profilename>/config/cells/<cellname>/applications/ <enterpriseappname>/deployments/<deployedname>/deployed-name>/deployments/<deployed-
- The file contains several configuration parameters. Add the following XML element to the configuration

WebSphere AS 6: <jspAttributes xmi:id="JSPAttribute_NUMBER" name="jdkSourceLevel" value="15"/> WebSphere AS 7, 8 and 8.5: <jsp-attribute name="jdkSourceLevel" value="15"/> The placeholder NUMBER in the *WebSphere AS 6* configuration must be a unique ID within the XML file. Check the existing IDs to learn, which ID you can allocate.

• Restart the monitortools.applicationserver.jmx.adaptor application.

How to change the user / role mapping after the deployment

If you want to adjust your user-role mapping afterwards (in case of some permissions changed), perform the following steps:

WebSphere. software							Welcom	e wasadmin
	Cell=SMRD	cell01, Profile=DMgr01						
	Enternrise	Applications						
Welcome	enterprise	Applications						
Guided Activities	Enterp	rise Applications						
Servers	Use thi	is page to manage installed app	ications. A sir	gle application can	be deployed ont	o multiple	servers.	
New server	± Pref							
								· · ·
	Star	t Stop Install Uninstal	Update	Rollout Update	Remove File	Export	Export DDL	Export File
DataPower	R	1 4 9						
Core Groups								
Applications	Select	Name 🗘			Application S	tatus 🖸		
New Application	You ca	an administer the following resou	rces:					
Application Types		DefaultApplication			€>			
WebSphere enterprise applications		ECM SM SERVER						
Business-level applications					-			
Global deployment settings		ECM SM SERVERSERVER			=>			
clobal deproyment settings		Monitortools Applicationserver	JMX Adaptor]	*			
Jopz		ivt0.co		-	4			
Services		INCROP			v			
Resources		query			€			
Security	Total (6						
Environment								
System administration								
Users and Groups								
Monitoring and Tuning								
Troubleshooting								
Service integration								

Application settings

Click on the name of the application.

onfiguration	
General Properties	Modules
* Name	Manage Modules
applicationserver_jmx_monitor_ear	Metadata for modules
Application reference validation	Display module build Ids
Issue warnings	Web Module Properties
Detail Properties	Session management
Target specific application status	Context Root For Web Modules
Startup behavior	JSP and JSF options
Application binaries	Virtual hosts
Class loading and update detection	Enternrice Java Rean Dronerties
Request dispatcher properties	
Security role to user/group mapping	Default messaging provider references
JASPI provider	Client Module Properties
Custom properties	Client module deployment mode
View Deployment Descriptor	
Last participant support extension	Database Profiles
References	SQL) profiles and pureQuery bind files
Shared library references	
Shared library relationships	

Application settings

Click on Security role to user/group mapping. The Security role to user/group mapping page will be displayed. For a more detailed description of the following steps, look up the *How to deploy the monitortools.applicationserver.jmx.adaptor application as WebSphere Enterprise Application* chapter.

NOTE To retrieve the maximum of MBeans and their attributes, WebSphere application security has to be enabled. Since some MBeans provide system internal information, some of the MBeans need the user's authentication, before the information is provided. With security disabled, no authentication challenge is performed and so the MBean requests return with an exception, due to a missing authentication.

	Cell=W2K8R264WAS855Node01Cell, Profile=AppSrv01
iew: All tasks 🔹	Global security
Velcome	olobal secondy
Guided Activities	Global security
Servers	Use this panel to configure administration and the default application security
Applications	applications, security domains can be defined to override and customize the s
Services	Security Configuration Wizard Security Configuration Report
esources	
Security	Administrative security
Global security	Enable administrative security Administrative user roles
Security domains	Administrative group roles
Administrative Authorization Groups	Administrative authentication
Security auditing	
Bus security	Application security
Environment	Enable application security
System administration	
Users and Groups	Java 2 security
Monitoring and Tuning	Use Java 2 security to restrict application access to local resources
Troubleshooting	Warn it applications are granted custom permissions
- Service integration	
UDDI	User account repository
	Realm name
	defaultWIMFileBasedRealm
	Current realm definition
	Federated repositories
	Available realm definitions
	Federated repositories Configure Set as current
	Apply Reset

How to deploy the monitortools.applicationserver.jmx.adaptor Web Application under Oracle WebLogic

First, it is necessary to set up the security settings. The application uses the *jmxmonitoring* group to define permissions.

etting	gs for myre	alm						
Config	guration U	sers and Groups	Roles and Policies	Credential Mappings	Providers	Migration		
Users	Groups							
This Cus Grou	page displays tomize this	information about (each group that has b	een configured in this se	ecurity realm.			
Ne	New Delete Showing 1 to 7 of 7 Previous Next							
	Name 🚕	D	escription					Provider
	AdminChann	elUsers A	dminChannelUsers acc	ess the admin channel				DefaultAuthenticator
	Administrato	rs A	Administrators can view and modify all resource attributes and start and stop servers DefaultAuthenticator					
	AppTesters	A	AppTesters can test applications that are in admin mode DefaultAuthenticator					
	CrossDomair	Connectors O	rossDomainConnector	s can communicate with	other domain	s		DefaultAuthenticator
	Deployers	D	eployers can view all r	esource attributes and	deploy applica	itions		DefaultAuthenticator
	Monitors	м	onitors can view all re	source attributes and p	erform operat	ions not restricted by i	roles	DefaultAuthenticator
	Operators	0	perators can view all r	esource attributes and	perform serve	er lifecycle operations		DefaultAuthenticator
Ne	w Delete						Showing 1	to 7 of 7 Previous Next

Add a new group

Create a New Group	
OK Cancel	
Group Properties	
The following proper	ties will be used to identify your new Group.
* Indicates required fie	lds
What would you like to	o name your new Group?
* Name:	jmxmonitoring
How would you like to	describe the new Group?
Description:	
Please choose a provi	der for the group.
Provider:	DefaultAuthenticator 💌
OK Cancel	

Create jmxmonitoring group

It is recommended to specify a different user (here: the weblogic user).

es Credential Mappings Provide	rs Migration
s been configured in this security real	n.
	Showing 1 to 1 of 1 Previous Next
'n	Provider
	DefaultAuthenticator
	Showing 1 to 1 of 1 Previous Next
	es Credential Mappings Provide s been configured in this security real

Assign User to Group

Settings for wel	blogic	
General Pass	swords Attributes Groups	
Save		
Use this page t	o change the description for the selected user.	
Name:	weblogic	The login name of this user. More Info
Description:	weblogic	A short description of this user. For example, the user's full name. More Info
Save		

Select Groups Tab

eneral	Passwords	Attributes	Groups	
Save Use this	page to config	gure group me	nbership for this user.	
arent G Availab Adı Adı Cro Dej Dej Mo	Froups: le: minChannelL pTesters issDomainCo ployers nitors erators	Jsers	Chosen: Chosen: Administrators jmxmonitoring	This user can be a member of any of these parent groups. Mo Info

Add jmxmonitoring Group to User

- Create a directory on the WebLogic application server (e.g. c:\jmxdeployment).
- Within this directory create a subdirectory "app". (e.g. c:\jmxdeployment\app).
- Copy the JMX WebApplication from \$CENIT_ROOT\repos\install\webapps
 \monitortools.applicationserver.jmx.adaptor.war to the recently created app directory. (e.g. c:\jmxdeployment\app\monitortools.applicationserver.jmx.adaptor.war).
- Copy the plan directory from \$CENIT_ROOT\repos\install\webapps\plan to the recently created jmxdeployment directory (e.g. c:\jmxdeployment\plan).
- Retrieve the values for the agentId and keyFileContent from the agent which is used to monitor the application server, as follows and replace the placeholders with the values in the plan.xml file (e.g. c:\jmxdeployment\plan.xml).
 - agentId

The value for the agentId can be found on your ECM SM agent in the file \$CENIT_ROOT/
set_cenit_env.sh. The variable is named S_AGENT_ID. The value might look like
hostname_agent. Replace the placeholder enterAgentIdHere from the plan.xml file with
the agent id (e.g. hostname_agent).

keyFileContent

Copy the content of the keyfile of the ECM SM agent, which monitors your application server via JMX. The keyfile can be found at \$CENIT_ROOT/.keys/keyfile.Copy the whole string (including the prefix :AES12B:BASE64:) and replace the placeholder enterKeyFile-ContentHere from the plan.xml file with the key file content (e.g. :AES12B:BASE64:5om3/Crypt3d/P455w0rd=).

Path to plan.xml

Replace the text enterDirectoryPathToPlanXmlHere with the path to the plan.xml file on your application server. Specify the directory only, without file name (e.g. c:\jmxdeploy-ment\plan).

Deploy the monitortools.applicationserver.jmx.adaptor application.

Summary	of Deployments					
Summary	of Deployments					
Control	Monitoring					
This pag be starte To instal Custon Deployn	e displays a list of Ja ed, stopped, update I a new application or nize this table nents	va EE applications a d (redeployed), or d module for deployr	nd stand-alone applic leleted from the domai ment to targets in this	ation modules tha n by first selectin domain, dick the :	t have been installed to th g the application name an install button.	nis domain. Installed applications and modules can d using the controls on this page.
Install	Update Dele	te Start v	Stop ~			Showing 0 to 0 of 0 Previous Next
🔳 Na	me 🗠	State	Health	Туре	Targets	Deployment Order
			The	ere are no items t	o display	
Install	Update Dele	te Start v	Stop 🗸			Showing 0 to 0 of 0 Previous Next

Install the Monitoring Application

Click the Install button.

nstall Application Assista	nt
Back Next Finish	Cancel
Locate deployment to i	install and prepare for deployment
Select the file path that rep You can also enter the path	resents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. In of the application directory or file in the Path field.
Note: Only valid file paths required deployment descri	are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the ptors.
Path:	c:\jmxdeployment
Recently Used Paths:	c:\ c:\deployment\plan c:\deployment\app
Current Location:	192.168.240.3 \c:
Documents and S jdbc jmxdeploymen Program Files RECYCLER WINDOWS wmpub Back Next Finish	ettings It (open directory) Cancel

Select the deployment directory

Select the folder, in which you previously copied the monitortools.applicationserver.jmx.adaptor.war file and the plan.xml file and click Next.

Install Application Assistant
Back Next Finish Cancel
Choose targeting style
Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.
Install this deployment as an application
The application and its components will be targeted to the same locations. This is the most common usage.
Install this deployment as a library
Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.
Back Next Finish Cancel

Select Install this Deployment as Application

Select "Install this deployment as an application" and click Next.

Install Application Assistant						
Back Next Finish Cancel						
Optional Setting	<u>15</u>					
You can modify the	ese settings or accept the defaults					
* Indicates required	fields					
— General ——						
What do you want	to name this deployment?					
* Name:	monitortools.applicationserver.jm					
- Security						
What security mode	el do you want to use with this application?					
OD Only: Use	only roles and policies that are defined in the deployment descriptors.					
Custom Roles deployment dese	x: Use roles that are defined in the Administration Console; use policies that are defined in the criptor.					
Custom Roles	and Policies: Use only roles and policies that are defined in the Administration Console.					
Advanced: Us	e a custom model that you have configured on the realm's configuration page.					
- Source Access	ibility					
How should the sou	rce files be made accessible?					
Ose the defau	Its defined by the deployment's targets					
Recommended select	ction.					
Copy this app	lication onto every target for me					
During deployment,	the files will be copied automatically to the Managed Servers to which the application is targeted.					
🔘 I will make th	e deployment accessible from the following location					
Location:	c:\jmxdeploymenf\app\monitortools.applicationserver					
Provide the location and that each targe	n from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location at can reach the location.					
— Plan Source Ac	cessibility					
How should the plar	n source files be made accessible?					
O Use the same	accessibility as the application					
Recommended select	ction.					
Copy this plan	n onto every target for me					
During deployment,	the plan files will be copied automatically to the Managed Servers to which the application is targeted.					
Do not copy t	his plan to targets					
You must ensure the plan files exist in the shared location and that each target can reach the location.						
Back Next	Fnish Cancel					

It is recommended to use DD Only Mode

Select the options as on the screenshot and click Next.

Install Application Assistant							
Back Next Finish Cancel							
Review your choices and click Fin	ish						
Click Finish to complete the deployment	:. This may take a few moments to complete.						
— Additional configuration ———							
In order to work successfully, this applic	ation may require additional configuration. Do you want to review this applic	ation's configuration after completing this assistant?					
Yes, take me to the deployment Output Description: According to the deployment According to the deployment	t's configuration screen.						
No, I will review the configuration	on later.						
— Summary —							
Deployment:	c: \jmxdeployment \app \monitor tools.applicationserver.jmx.adaptor.war						
Name:	monitor tools. applicationserver.jmx.adaptor						
Staging Mode:	Copy this application to every target for me						
Plan Staging Mode:	Copy the plan to every target for me						
Security Model:	DDOnly: Use only roles and policies that are defined in the deployment descriptors.						
Target Summary							
Components 🗞	Targets						
monitor tools.applicationserver.jmx.adaptor AdminServer							
Back Next Finish Cancel							

Finish Deployment

Click Finish.

verview	Deployment Plan	Configuration	Security	Targets	Control	Testing	Monitoring	Notes		
ave										
Jse this pa	ge to view the insta	lled configuration	of a Web ap	plication.						
	-	-								
ame:		monitor tools.appl	icationserve	er.jmx.adap	tor		The nar	me of this	application deployment. More Info	
Context Root:		/monitortools.applicationserver.jmx.adaptor					The spe servlet.	The specific path at which this Web application is found by a servlet. More Info		
Path:		c:\jmxdeploymer adaptor.war	it\app\mor	iitortools. a	pplicationse	erver. jmx.	The pat Adminis	th to the s tration Se	source of the deployable unit on the erver. More Info	
)eployme	nt Plan:	c:\jmxdeploymer	it\plan\plai	n. xml			The pat Adminis	th to the o tration Se	deployment plan document on the erver. More Info	
Staging Mo	ode:	stage					Specifie on the area du	es whethe Administra Iring appli	r an application's files are copied from a sou ation Server to the Managed Server's stagin cation preparation. More Info	
Plan Stagir	ng Mode:	stage					Specifie source staging	es whethe on the Ad area duri	r a deployment plan's files are copied from a lministration Server to the Managed Server's ing application preparation. More Info	
Security M	odel:	DDOnly					The sec secured	urity mod J. More I	lel specifies how this deployment should be Info	
🚰 Deploy	ment Order:	100					An integ relative startup	ger value to other . More I	that indicates when this unit is deployed, deployable units on a server, during info	
🚰 Deploy lame:	ment Principal]			A string when d shutdov when ca Applicat then th	y value tha eploying t wn. This p alling out i tionLifecy e anonym	at indicates the principal that should be used the file or archive during startup and vrincipal will be used to set the current subje into application code for interfaces such as cleListener. If no principal name is specified, ous principal will be used. More Info	

Save the Configuration

How to deploy the monitortools.applicationserver.jmx.adaptor Web Application under Red Hat JBoss

Deploying the application on Red Hat JBoss application server depends on the configuration. With standard settings it is possible to deploy the application simply by putting the file into the {jboss install dir}/server/default/deploy folder of the JBoss application server installation. The application will automatically be deployed on the next restart. If your system has another configuration please contact your administrator.

The security settings are defined in the {jboss install dir}/server/default/conf/loginconfig.xml file. Add the following content to the <application-policy> element.

```
<application-policy name="monitortools.applicationserver.jmx.adaptor">
    <authentication> <login-module
    code="org.jboss.security.auth.spi.UsersRolesLoginModule" flag="required" >
        <module-option name="usersProperties">props/users.properties</module-option>
        <module-option name="rolesProperties">props/users.properties</module-option>
        <module-option name="rolesProperties">props/roles.properties</module-option>
        <module-option>
        <module>
        <modu
```

<module-option

</authentication>

This configuration defines two files for users and roles: **users.properties** and **roles.properties**. The files can be given different names.

The users.properties file contains the users and passwords for the monitoring application.

Sample { jboss install dir }/server/default/conf/props/users.properties:

admin=admin

All users must be mapped to the jmx_monitoring role. This is done in the {jboss install dir}/ server/default/conf/props/roles.properties file:

admin=jmx_monitoring

The default URL for connectiontest.jsp to test the connection is:

http://localhost:8080/monitortools.applicationserver.jmx.adaptor/connectiontest.jsp

Preparing IBM FileNet Listener functionality

To enable IBM FileNet Listener functionality for Listener tasks and monitors it is necessary to activate Listener functionality within IBM FileNet and IBM Content Manager before ECM SM specific Listener configuration.

Configuring/enabling the Listener of IBM FileNet and IBM Content Manager applications

Some IBM FileNet products and IBM Content Manager (supported since Version CM 8.4.2) require different configuration steps to activate the IBM product Listener. Check the related product installation guide for details. Note: This step normally requires administrative rights to the application.

Configuring/enabling the Listener during ECM SM client configuration

After activation of the Listener functionality for IBM FileNet and IBM Content Manager products the ECM SM Listener configuration need to be done for each system. For IBM FileNet P8 4.x systems the Listener configuration is part of the core configuration itself. For all other IBM FileNet products that support the Listener interface and for IBM Content Manager the ECM SM Listener configuration need to be done as additional configuration step. See chapter 'Configuring a FileNet Listener' for further information.

Preparing WMI functionality

The monitor can only be run on Windows systems with a 32bit JRE. The 64bit version is currently not supported by com4j.

Preparing VMware ESX/ESXi functionality

ECM SM supports monitoring for VMware ESX/ESXi server. That will monitor the virtual machine that run on this server. To activate this monitoring it is necessary to download free 3rd Party Java JAR files from http://www.vmware.com.

The new monitor can be found in the STANDARD monitoring collection.

Downloading required 3rd party Library

Perform the following steps to download **vim25.jar**, which is required to establish connection to the VMware ESX/ESXi server.

Download the binary file of VMware vSphere Management SDK from vmware.com

ECM SM supports the vSphere Web Service API in version 4.1 and 5.x.

To download the SDK open the URL <u>https://developercenter.vmware.com/web/sdk/51/vsphere-management</u> and download the binary zip file <u>VMware-vSphere-SDK-5.1.0-774886.zip</u> (vSphere 5.1 Management SDK) or newer.

- **NOTE** The URL might change over time. So if it is not available the vSphere 5.1 Management SDK has to be searched on the Internet manually.
- **NOTE** vSphere 4.1 Web Management SDK is not available anymore on the official VMware WebSite. Refer to your ESX/ESXi administrator to receive the SDK.

Extract the zip file

Extract the downloaded file VMware-vSphere-SDK-5.1.0-774886.zip.

Copy the file vim25.jar to the ECM SM Server

Copy the file vim25.jar from folder VMware-vSphere-SDK-5.1.0-774886.zip/SDK/ vsphere-ws/java/JAXWS/lib to the directory

- <ECM SM-installation-Dir>/repos/install/tools/com.vmware4,0r
- <ECM SM-installation-Dir>/repos/install/tools/com.vmware5

(related on which API you use) on the ECM SM primary Server. This directory does not exist and must be created, when it was not yet set in the ECM SM Fix Pack 1 installer.

Adjust the access rights as well as the user/group membership

Adjust the access rights as well as the user/group membership of the new directory and the copied file. Make sure that they are identical to the directory **org.apache** and the files located in that directory.

Keystore certificate import for use with Java based monitors

This chapter describes how to import a certificate into a keystore on a monitored system for use with secure Java based monitors like the Web Status monitor that checks https Web pages. The following description can differ on your system, because you might use a different Web browser or browser version.

Exporting the certificate of the Web page / application on the local desktop

At this point the certificate of the Web Page / application that need to be monitored has to be imported into your browser already. If this is not yet done open the Application in your browser and import the relevant certificate first.

If you use Microsoft Internet explorer open the 'Tools' menu and select 'Internet Options'. Within options select the 'Content' tab and press the 'Certificates' button. Select the certificate you'd want to export, select Encoded binary X.509 format, specify a filename and export the file.

If you use Firefox open the 'Options' menu, select the 'Advanced' tab, then the 'Encryption' sub tab. Press the 'View certificates' button and select the certificate to export from the various types of certificates. Press the export button, select X.509 certificate file type, specify a file and save the certificate.

Import of previously exported certificate into a keystore

The previously exported X.509 certificate need to be imported into a keystore on the server where the monitor will run. Due to security reasons you may want to create a custom keystore and import the certificate into this keystore and not into the default keystore. Talk to the local administrator before importing the certificate.

Logon to the remote server and copy the exported certificate file in binary mode to the remote server.

Change to the directory where the Java to be used by the monitor is located.

Import the certificate with the Java keytool program by for executing

```
./keytool -import -v -trustcacerts -alias myCertAliasName -file myCert-
FileName
```

Enter the password twice and answer 'Yes' to trust the certificate. The keystore now contains the Web page / application certificate and can be used by monitors.

Starting the ECM SM agent installer

Agents may be installed locally (from the agent machines console) or remote via CALA, the CALA Remote Execution protocol that is installed with the ECM SM server.

The graphical installer depends on a Java runtime environment (Java 7 or newer) installed on the desktop where the installer is started. Supported JREs for various platforms are available on the Client Administration console (menu Window Consoles) on the ECM SM web interface.

The ECM SM agent installer is started via the ECM SM web interface. Start your browser and enter http:// ServerName:23990/rap?startup=fsm in its address line (replace *ServerName* with the IP address or hostname of your ECM SM server). Additionally you may need to adjust the port.

NOTE In the case of a WAS-based installation the URL need to be adjusted, too.

When the ECM SM main page is displayed, change to the **Client Administration** console and select one of the installers in the left frame:

IBM ECM SM ECM Core Agents (P8, IM, CM8, etc) Installer

IBM P8 AE, CE, PE, Process Analyzer IS/IM incl. Content Services IBM Content Manager, Content Manager OnDemand IBM Enterprise Records IBM IICE and CommonStore IBM Content Collector, IBM FileNet Email Mgr and Rec. Crawler IBM FileNet Capture

Start IBM ECM SM ECM Core Agents (P8, IM, CM8, etc) Installer

IBM ECM SM Base agents and non Core ECM Agent Installer

IBM P8 CE FileStore IBM P8 ObjectStore Only Servers IBM P8 Content Search Services IBM Datacap IBM eDiscovery IBM Case Manager IBM Content Navigator IBM II4C servers Other not above listed FileNet or Other non core IBM ECM servers Database and Web Application servers

Start IBM ECM SM Base agents and non Core ECM Agent Installer

Launch installer - Client Administration console

The installers can be started from the **Tools** menu as well, without changing to the **Client Administration** console:

File Window Desktop	Tools Help
GUI-Tools, JRE arch	IBM ECM SM ECM Core Agents (P8, IM, CM8, etc) Installer
	IBM ECM SM Base agents and non Core ECM Agent Installer
 IBM Enterprise C 	IBM ECM SM Monitoring Manager
Launch the IBM Ente	IBM ECM SM Task Execution Manager
too.	IBM ECM SM V2S Editor (supports 32 Bit Java Webstart only)

Launch installer - Tools menu
There are two different installer tools available:

- IBM ECM SM IBM ECM Core Agents (P8, IM, CM8, etc) Installer: This is the installer for machines running any IBM FileNet and IBM CM8 software to be monitored. On these machines, the CALA agent components will be installed. The following chapters describe the installation procedure for this kind of servers.
- IBM ECM SM Base agents and non Core ECM Agent Installer: This is the installer for additional machines to be monitored that do not run any IBM FileNet or IBM CM8 core software (e.g. machines running WebServices or the ECM SM server itself). On these machines, the CALA agent components will be installed as well.
 - **NOTE** An agent of this type must be installed on the ECM SM server as well to allow monitoring of the server itself.

Press the appropriate button or select the menu entry to start the Java WebStart based installer tool.

The ECM SM installation - main screen

NOTE In case of an HTTPS connection with a self-signed certificate, you will get two warnings about an untrusted connection/certificate. Your browser and Java will warn you separately.

Either you should use an official certificate issued by a trusted certification authority or you must confirm that you know what your are doing and you are trusting the self-signed certificate. For Java you can make this decision permanent by selecting the checkbox *Always trust content from this publisher*. For the browser warning, it depends on the browser how you can handle this situation in the future; ask your administrator for further help.

Before the ECM SM Installer starts, a login window for the ECM SM CALAserver is shown:

User:	admin
Password:	*****
	Login Cancel

Login window

Log in with a user that has the appropriate permission to execute the ECM SM installer. The ECM SM installer window opens.



Installer main window

The main screen shows information about the existing configuration and contains the buttons to open further configuration windows.

The field **Configuration Directory** shows the location of the directory containing the ECM SM configuration. The default value for this is the configuration directory on the ECM SM server. Press the **Change** ... button to choose another directory.

If there is already a configuration for IBM FileNet Image Manager, the installer checks for newer versions of the configured cdb files at startup. If a newer CDB file is found on the server, the following message will be displayed:

The currently used cdb file is outdated, press ok to load the new cdb file.	
Currently used file: D:\tmp\sd\conf_db\IMS_21.cdb New file: D:\tmp\sd\conf_db\IMS_27.cdb	
Ok	Cancel

Dialog: New CDB file available

Press Ok to load the new CDB file. Press Cancel to keep the old file.

If a CDB file cannot be loaded (e.g. because the server is unreachable), the following warning message is displayed:

Error loa	ding file 📉 🔜 🔤 🔤 🔜 🔜 🔀
	The following CDB files could not be loaded:
	crx.ccco.stgt.cenit.deminswhocausu/coni_dumins_12.cdu
	Using values stored on FSM server instead. Be aware that these configuration data may be outdated!
	OK

Warning: CDB file cannot be loaded

The configuration for all domains that are defined in the listed CDB files may be based on outdated configuration data.

Configuring ECM SM clients for IBM FileNet Image Manager

NOTE

It is required to copy the current CDB file prior to configuration to any Storage Server where you plan to run one or more of the following monitors:

- Integral_SDS_DevaiceStatus
- Integral_SDS_DeviceThresholds
- EmptyDisksInOsar
- OsarDemandStatus
- OsarDriveContents
- OsarDriveInfo
- OsarGripperConfig
- OsarGripperContents
- OsarGripperDisabled
- OsarLibraryMode
- OsarSlotContents
- OsarSlotInfo

The file must be located in the subdirectory **sd/conf** of the path specified as **FileNet local path**. Make sure you update the file and perform a reconfigure of the respective client each time you change the definition of your storage libraries.

To configure IBM FileNet Image Manager properties, press the **Configure Image Manager** button and the configuration dialog file dialog appears.

Domain: hqdemo1:FileNet	Ŧ	Add	Remove
NLS (CSAR / SSAR / ISAR)			
FNIS HPIL/MRI		Ser	verLink
Server:	h	qdemo1 (h	qdemo1:F 💌
Hostname:	N	ONE	•
FileNet administrator:			
FileNet path:			Browse
FileNet local path:			Browse
FileNet report path:			Browse
Start Order:	1		Change
Stop Order:	1		Change
Database type:	M	ISSQL	-
Database path:			
Database name:			
Remote database identifier:			
Database maintenance user:			
Password of DB maintenance use	r:		
Database runtime user:			
Database OS user:			
TWO_TASK variable:			
Ok Cancel		Help	

The IBM FileNet Image Manager configuration dialog

The upper section of the window is for choosing the domain for what IBM FileNet Image Manager is to be installed. The tabbed section below is for the parameters of configuration. If there is no domain chosen, they will be greyed out. To choose a domain to configure, click the **New** ... button next to the domain combobox and you will get the CDB file dialog.

The CDB file dialog

CDB file:	crx:\w2kfsmtest.stgt.cenit.de//C:/IMS_3.cdb	•	Add CDB file
hqdemo1:	FileNet		
	OK Close Help		

The CDB file dialog

The CDB file listbox shows which IBM FileNet Image Manager cdb files are currently known. The listbox is empty if the installer is started the first time. To add a IBM FileNet IM configuration file press the Add CDB file button, which shows the Add a cdb file ... dialog.

Add a CDB file

There are different methods how a CDB file can be loaded. Depending on the selection in the **Selection mode for CDB file** listbox, the fields in the dialog box change.

Choose automatically using CALA to load the file via cala_rex from the IBM FileNet IM server. This method requires that the CDB file is located in the subdirectory sd/conf_db of the specified IBM FileNet IM local path.

The root server must be chosen from the listbox. The entry field FileNet local path must be filled in as well.

FileNet root server	w2kfsmtest.stgt.cenit.de	
Selection mode for CDB file:	automatically using cala_rex	
FileNet local path:		
Ok Car	ncel Help	

Add a CDB file using CALA_REX

Choose manually to load the configuration from a local file or from a non-standard location.

The name of the IBM FileNet IM root server has to be entered in the textfield. Pressing the **Filename** button opens a filechooser where you can navigate to the CDB file that must be loaded.

FileNet root server	w2kfsmtest.stgt.cenit.de
Selection mode for CDB file:	manually 💌
Filename	
Ok Car	cel Help

Manually add a CDB file

Press Ok to load the cdb file and get back to the CDB file dialog.

If any CDB files are loaded, the **CDB file** combobox shows a list of loaded CDB files. The listbox in the center of the dialog shows the IBM FileNet IM domains configured in the selected CDB file. To start further configuration, select a domain and press the **OK** button to see the domain configuration window.

The configuration window knows four server types: *FNIS*, *HPII/MRII*, *ServerLink* and *NLS* (*CSAR/SSAR/ISAR*). The tabs choose the server type to configure. Depending on the selected server type, different entry fields are visible.

Configuration of IBM FileNet IM servers

Note: Latest versions of IBM FileNet IS, Process Engine FileNet P8 PE support remote MSSQL servers without installed MSSQL client software on the FileNet server. ECM SM now supports DB2, MSSQL and Oracle-based IS installations that monitor the IS/Process Engine-related DB monitors on local and remote database by using Java (UDC / JDBC), too.

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

FNIS HPIL/MRII ServerLink	NLS (CSAR/SSAR/ISAR)				
Server:	hqdemo1 [hqdemo1:FileNet]				
Hostname:	w2kfsmtest.stgt.cenit.de				
FileNet administrator:	fnsw				
FileNet path:	/fnsw	Browse			
FileNet local path:	/fnsw/local/	Browse			
FileNet report path:	/fnsw/local/logs/perf	Browse			
Start Order:	1	Change			
Stop Order:	1	Change			
Database type:	MSSQL				
Database path:	C:/Program Files/Microsoft Server/90/Tools				
Database name:	indexdb				
Remote database identifier:					
Database maintenance user:	f_maint				
Password of DB maintenance user:	• *****				
Database runtime user:	f_sw				
Database OS user:					
TWO_TASK variable:					

Configure IBM FileNet IM server

Servers

This combobox shows all servers that are part of the specified IBM FileNet IM domain. The settings for the currently selected server can be edited in the text fields below. If a server is already configured, the current values will be shown as default.

General Settings

Hostname

Required. The listbox shows all machines that have a CALA_REX client installed. Choose the correct hostname of the server selected in the **Server** listbox. This is the name that will be used in the Web Console.

FileNet Administrator

Required. Enter the IBM FileNet IM administrator name, in most cases *fnsw*. The user you specify should have access to all IBM FileNet IM tools and database devices.

FileNet Path

Required. Enter the IBM FileNet IM base directory, for UNIX normally /fnsw, for Windows <drive letter>:/fnsw. Instead of /, \\ can also be used on Windows.

FileNet Local Path

Required. Enter the IBM FileNet IM local directory, for UNIX normally /fnsw/local, for Windows <drive letter>:/fnsw_loc. Instead of /, \\ can also be used on Windows.

FileNet Report Path

Required. Enter the IBM FileNet IM report directory: This directory is used as output location for IBM FileNet IM tools **perf_report** and **getstatus**. You can use the standard output path for **perf_report** (for UNIX normally /fnsw/local/logs/perf, for Windows <drive letter>:/fnsw_loc/logs/perf) or any other path. Instead of /, \\ can also be used on Windows.

Start Order

Required. Enter a numerical value that indicates the start order of the server. Pressing the **Change** button opens a dialog box where you can see all servers and set the start order as well.

Stop Order

Required. Enter a numerical value that indicates the stop order of the server. Pressing the **Change** button opens a dialog box where you can see all servers and set the stop order as well.

Additional settings for Database server

Database Type

This setting is read from the configuration file and cannot be changed except if the database type is **NONE**.

If the type is shown as **NONE**, the selected server does not have a IBM FileNet IM RDBMS installed (e.g. Cache server). You can change the value and fill in the remaining database related fields if the server has the appropriate database client software installed.

Database Path

Required for database servers. Enter the path to your RDBMS installation.

- Oracle: Path to the **bin** directory where the Oracle tools are installed:
 - Unix: /usr/oracle
 - Windows: <drive letter>:/orant
- Oracle using JDBC client (UDC): Path to the **bin** directory where the Oracle tools are installed (without /bin) and Java install Path (without /bin), separated by ,:
 - Unix: /usr/oracle,<JavaInstall-Dir>
 - Windows: <drive letter>:/orant,<JavaInstall-Dir>
- MSSQL: Path to the **binn** directory where the MSSQL tools are installed. The location of this directory depends on the MSSQL Server version:
 - MSSQL Server 2000 or MSDE 2000: <drive letter>:/Program Files/ Microsoft Server/80/Tools
 - MSSQL Server 2005: <drive letter>:/Program Files/Microsoft Server/90/Tools
 - MSSQL Server 2008: <drive letter>:/Program Files/Microsoft Server/100/Tools

The installation script searches the **binn** directory for the tools **sqlcmd.exe**, **osql.exe** or **isql.exe**.

- MSSQL using JDBC client (UDC) If the JDBC based UDC communication to the DB should be used, specify the Java install path here (without /bin at the end) instead of the DB installation path. UDC supports Java version 7 and newer.
- DB2: Path to the **bin** directory where the DB2 tools are installed:
 - Unix: /home/<instancename>/sqllib
 - Windows: <drive letter>:/Program Files/IBM/SQLLIB

The installation script searches the **bin** directory for the tool **db2sql92**.

- DB2 using JDBC client (UDC): Path to the **bin** directory where the DB2 tools are installed (without /bin) and Java install Path (without /bin), separated by ,:
 - Unix: /home/<instancename>/sqllib,<JavaInstall-Dir>
 - Windows: <drive letter>:/Program Files/IBM/SQLLIB,<JavaInstall-Dir>

Leave this path blank if there is no RDBMS installed.

NOTE Use / instead of \setminus in the pathname.

Database Name

Required for database servers. Enter the name of your database if it does not match the shown default value (*IDB* for Oracle, *indexdb* for MSSQLServer and DB2).

For Oracle, this field corresponds to the setting of ORACLE_SID (in most cases IDB).

Remote Database Identifier

This field changes its label depending on the selected database type. If the type is **NONE**, the label changes to **Remote Database Identifier**.

DB2 Database Instance name using DB2 client tools:

Label if database type is DB2.

Required. Enter the name of the DB2 instance.

DB2 JDBC settings using Java JDBC client access:

Label if database type is DB2.

Required. If your database is configured for remote access based on JDBC-communication the following parameter set is required: <db-server-name>,<db2-jdbc-driver-path>,<db-port>,com.ibm. db2.jcc.DB2Driver,jdbc:db2://<db-server-name>:<db-port>/<DB2-db-name>

Example: mydb2server,D:/db2/driver,50000,com.ibm.db2.jcc.DB2Driver,jdbc:db2://mydb2server: 50000/IDB

Remote Oracle DB name using Oracle client tools (sqlplus)

Label if database type is Oracle.

Optional. If your database is configured for remote access, enter the TNS name (service name) of the database.

Remote Oracle DB name using Java JDBC client access

Label if database type is Oracle.

Required. If your database is configured for remote access based on JDBC-communication the following parameter set is required: <db-server-name>,<oracle-jdbc-driver-path>,<db-port>,oracle. jdbc.driver.OracleDriver,jdbc:oracle:thin:@<db-server-name>:<db-port>:<Oracle-db-name>

In addition to this format the Oracle service name format is supported, too: <db-server-name>,<oracle-jdbc-driver-path>,<db-port>,oracle.jdbc.driver.OracleDriver,jdbc: oracle:thin:@<db-server-name>:<db-port>/<Oracle-service-name>

Example with DB name: myoraserver,D:/oracle/driver,1521,oracle.jdbc.driver.OracleDriver,jdbc: oracle:thin:@myoraserver:1521:IDBW2K

Example with Service name: myoraserver,D:/oracle/driver,1521,oracle.jdbc.driver. OracleDriver,jdbc:oracle:thin:@myoraserver:1521/idbserv

MSSQL Server/Instance name using MSSQL client tools

Label if database type is MSSQL.

Optional: The following combinations are possible for the parameter MSSQL Remote Server or Servername/Instancename:

Leave this parameter unset, if the local Default MSSQL instance should be monitored

Specify the remote MSSQL server name, if the Default instance should be monitored on a remote server

Specify MSSQL Server name/Instance name, if a custom MSSQL instance on the local or remote server should be monitored.

Note: Use "/" instead of "\" between MSSQL Server and Instance name!

MSSQL JDBC settings using Java JDBC Client access

If the JDBC based UDC communication to the MSSQL DB should be used the configuration for a Default MSSQL instance looks like: <MSSQL server name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port]. The default port number is 1433. Example: mssqlServ1,C:/Pro-gram Files/sqljdbc11/enu,1433. A MSSQL custom instance UDC configuration looks like: <MSSQL server name>/<Instance name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port]. Example: mssqlServ1/INSTANCE1,C:/Program Files/sqljdbc11/enu,1433.

NOTE For information on how to connect to an SSL secured MSSQL Server see Chapter *How to configure and use the UnifiedDatabaseClient* in the *ECM SM Install Guide*.

Database maintenance user

Required for DB2 and Oracle, optional for MSSQL. Specify the database maintenance user (in most cases f_{maint}).

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Password of DB maintenance user

Required for DB2 and Oracle, optional for MSSQL. Specify the password of the database maintenance user. The password will be encrypted before it is stored in the environment file **fnis_srv_ env.sh**.

Database runtime user

Required. Specify the database runtime user (in most cases *f_sw*).

Database OS User

Optional for Oracle and DB2 database servers on UNIX only. Specify the user that is owner of the Oracle or DB2 database installation, e.g. *oracle*.

TWO_TASK variable

Optional for Oracle. Specify the value of the *TWO_TASK* variable that is required to connect to a remote Oracle database (direct connect via SQLNet without specifying a Oracle Remote service name (variable Remote Database identifier, see above).

Configuration of HPII/MRII servers

FNIS	HPIL/MRIL	ServerLink	NLS (CSAR / S	SAR	/ISAR)	
Server:	w2kfsmtes	t.stgt.cenit.de [hqdemo1:File	-	Add	Remove
Туре:	() HPII) MRII				
					В	rowse
HPII user	:filenet				-	
HPII user HPII path	: filenet : C:/fnsw_loc	/bin				
HPII user HPII path	: <mark>filenet</mark> : C:/fnsw_loc	/bin				
HPII user HPII path	: <mark>C:/fnsw_loc</mark>	/bin				
HPII user HPII path	: <mark>C:/fnsw_loc</mark>	/bin		1		
HPII user HPII path	: C:/fnsw_loc	/bin		1		
HPII user HPII path	: <mark>C:/fnsw_loc</mark>	/bin		1		
HPII user HPII path	: <mark>C:/fnsw_loc</mark>	/bin				

Configure ImageImport server

Servers

This combobox shows all HPII/MRII servers already configured for the specified IBM FileNet IM domain. The serverlist can be modified using the Add and Remove buttons.

The settings for the currently selected server can be edited in the text fields below. If a server is already configured, the current values will be shown as default.

Туре

Select HPII for High Performance Image Import, MRII for Mid Range Image Import.

HPII user

Required for UNIX servers. Specify the user that must used to start ImageImport.

HPII path

Required. Specify the path to your ImageImport installation, e.g. /fnsw/local/bin for UNIX, <drive letter>:/fnsw_loc/bin for Windows.

Configuration of ServerLink servers

FNIS	HPIL/MRI	ServerLink	NLS (CSAR / S	SAR	/ISAR)	
Server:		w2kfsmtest.	stgt.cenit.de [•	Add	Remove
Converti		filement				
ServerL	ink user:	menet				
ServerLi	ink user: ink path:	C:/fnsw/srvlin	ik		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes	C:/fnsw/srvlir	k		Br	owse
ServerLi ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	C:/fnsw/srvlir	ik		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	C:/fnsw/srvlir	ik		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	C:/fnsw/srvlir	lk		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	c:/fnsw/srvlir	lk		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	c:/fnsw/srvlir	lk		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	s	IK		Br	owse
ServerLi ServerLi ServerLi	ink user: ink path: ink processes ink NT service	s	IK		Br	owse

Configure ServerLink server

Servers

This listbox shows all ServerLink servers already configured for the specified IBM FileNet IM domain. The serverlist can be modified using the **Add** and **Remove** buttons.

The settings for the currently selected server can be edited in the text fields below. If a server is already configured, the current values will be shown as default.

ServerLink User

Required for UNIX servers. Specify the user that must used to start ServerLink.

ServerLink Path

Required. Specify the path to your ServerLink installation, e.g. /fnsw/srvlink for UNIX, <drive letter>:/fnsw/srvlink for Windows.

ServerLink Processes

Required for UNIX servers. Specify all processes that must be started for ServerLink to work properly (UNIX). These process names are used as default setting when executing the *ServerLink Processes* monitor.

ServerLink NT Services

Required for Windows servers. Specify all services that must be started for ServerLink to work properly. These service names are used as default setting when executing the *ServerLink Processes* monitor. Additionally, they are used by the task *Start ServerLink* on Windows.

Configuration of NLS (CSAR/SSAR/ISAR) servers

-NLS archive mode-		
	Database mode	
	🔾 Family mode	Filelist mode
	Surface mode	Custom mode



Servers

This listbox shows all NLS (CSAR/SSAR/ISAR) servers already configured for the specified IBM FileNet IM domain. The serverlist can be modified using the Add and Remove buttons.

The settings for the currently selected server can be edited in the text fields below. If a server is already configured, the current values will be shown as default.

NLS Install Path

Required. Specify the path to your NLS installation, e.g. /fnsw/local/bin for UNIX, <drive letter>:/fnsw_loc/bin for Windows. You can also use the Browse... button to the right of the entry field to open a file browser and navigate to the correct directory.

NLS.cfg file with PATH

Required. Specify the full qualified name if the **NLS.cfg** file, e.g. /fnsw/local/bin/NLS.cfg for UNIX, <drive letter>:/fnsw_loc/bin/NLS.cfg for Windows. You can also use the **Browse...** button to the right of the entry field to open a file browser and navigate to the correct file.

NLS Tools PATH

Optional. Specify the path where either EMC's tool **c-ping** or **CenteraPing** is installed, e.g. /fnsw/ emc_tools for UNIX or <drive letter>:/fnsw_loc/emc_tools for Windows. You can also use the **Browse...** button to the right of the entry field to open a file browser and navigate to the correct directory.

NLS User

Optional, UNIX only. Specify the user that must be used to start and stop NLS. Default is *fnsw*.

NLS Archive Mode

Required. Select one of the predefined NLS archive modes. **Database mode** is default. No additional information is required for this mode.

For archive modes Family mode, Surface mode and Filelist mode, NLS Archive parameters must be specified:

NLS archive mode		
	Database mode	
	Family mode	🔾 Filelist mode
	Surface mode	🔾 Custom mode
NLS archive parameters:		

Archive mode Family

NLS Archive Parameters

Required. Specify the required NLS parameters.

For Surface mode, enter the surface id you want to process. You can add -both to process both sides of the surface.

For Family mode, enter the family name,

For Filelist mode, enter the full qualified file name.

If NLS is not installed as recommended by FileNet and a customized startup and shutdown script is required select **Custom mode**.

NLS archive	e mode	
	🔾 Database mode	
	🔾 Family mode	 Filelist mode
	Surface mode	Custom mode
Start script:		
Stop script:		

Archive mode Custom

Start script

Required. Specify a custom start script. Use forward slashes instead of backslashes.

Stop script

Required. Specify a custom stop script. Use forward slashes instead of backslashes.

Debug NLS:

Required. Specify whether NLS should be started with the DEBUG flag or not. Default: No debugging.

Excluding servers of a IBM FileNet IM Domain

If you want to exclude one or more servers of an IBM FileNet Image Manager Domain from being managed, you need to create a file fnis_do_not_manage.<Domain name>, which contains the server names to be excluded. The : in the domain name must be replaced by _. The file must be located on the ECM SM server in the directory where the configuration files are stored (normally /opt/FileNet/SysMon/repos/ config/PAM).

Example

If you want to exclude the server *w2kim40* from the Domain *im54db:FileNet*, you need to create the exclude file:

/opt/FileNet/SysMon/repos/config/PAM/fnis_do_not_manage.↓ im54db FileNet.

This is the example content of

```
/opt/FileNet/SysMon/repos/config/PAM/fnis_do_not_manage.↓
im54db_FileNet:
```

This is the server exclude file of Domain im54db:FileNet w2kim40

The name of the Domain and the name of the server are case sensitive.

Configuring ECM SM clients for IBM FileNet P8

Configure IBM FileNet Image Manager

To configure IBM FileNet Image Manager properties, press the Configure Image Manager ... button.



Configure Image Manager ...

For a complete description of the IBM FileNet Image Manager configuration see the Configuring ECM SM clients for IBM FileNet Image Manager.

Configure Process Engine

To configure FileNet P8 Process Engine properties, press the Configure Process Engine ... button.



Configure Process Engine ...

The Process Engine configuration dialog opens:

fo					
Global settin	gs				
System:	Virtual_P8			▼ New	Remove
M Domain:	IS40SQL:FileNet			•	
Server:	W2K3IS40			▼ New	Remove
Woheenvor	Innlication Server	Company	vi Manameriniomator	Drococe (makzor	
menserver	Components	Compone	PPM	Rout	iers
	•				
Routers					
Web App	lication Server				
Compone	ent Manager/Integra	tor			
Dracess	Analyzer				
_ Process	Апануден				
			0		
		OK	Cancel Help		

The Components tab

The dialog consists of an upper part in the Global settings box and a bottom part containing some tabs.

Global settings:

System

Required. Select the Process Engine System you want to configure. Press the New ... button to create a new P8 system. You can choose any name you like. The currently selected system is removed from the configuration by pressing the **Remove** ... button.

NOTE The System name must not contain blanks.

IM Domain

Required. Select the IBM FileNet Image Manager Domain that is associated with the Process Engine that you want to configure. If you selected an existing Process Engine, the corresponding IBM FileNet IM Domain will appear in the listbox.

Server

Required. Select the server you want to configure. Press the New ... button to add a server to the list.

The Components tab

nfo							
Global settin	gs						
System:	Virtual_P8				•	New	Remove
IM Domain:	IS40SQL:FileNet				•		
Server:	W2K3IS40				•	New	Remove
Webserver	Application Server	Componer	ni Manameril	nteorator	Proces	s Analyzer	
	Components	- 5511/51151	F	PPM		Rout	ers
PPM							
Routers							
- Weh Ann	lication Server						
	and Manager Internet	0.5					
Compone	ent Manager/Integrat	or					
Process	Analyzer						
			01				
		Ok	Cancel	Help			

The Components tab

The **Components** tab shows the components that have been configured for this server. If a component is installed, select the appropriate checkbox. For each selected component, additional settings must be specified in the appropriated tab.

PPM

Optional. Mark this checkbox if the server has the PPM installed.

Routers

Optional. Mark this checkbox if the server has one or more routers installed.

Web Application Server

Optional. Mark this checkbox if the server has a web server installed. (Only enabled if **Routers** is checked)

Component Manager / Integrator

Optional. Mark this checkbox if the server has a Component Manager / Component Integrator installed. (Only enabled if **Web Application Server** is checked)

Process Analyzer

Optional. Mark this checkbox if the server has a Process Analyzer installed.

Info								
-Global settin	igs							
System:						-	New	Remove
IM Domain:	tivhpit1:File	Net				-		
Server:						-	New	Remove
			V					
Webserver	Application	Server	Component	Manager/ V	integrator F	Proce	ss Analyzer	
 	Compor	nents			PPM		Rout	ers
FileNet Path: JAVA Path: Max. Pro Registry Por Return Port: Additional Pa VWJs Delay vwtool User: vwtool Pass Debug:	cesses: t: arameters: : word:	 	Processes s Processes					
			Ok	Cancel	Help			

PPM tab

FileNet Path

Required. Enter the path to the PPM jar-archive pw.jar, e.g. C:/fnsw/bin on Windows, /fn-sw/bin on UNIX.

Java Path

Required. Enter the path to Java bin directory, e.g. C:/Program Files/JDK on Windows or / usr/local/java on UNIX.

Max Processes

Required. Maximum number of VWJs server processes that the PPM can run at the same time.

Registry Port

Required. The RMI port the PPM runs on. The PPM port number must be greater than 1024.

NOTE

The port number is not optional because it is required by the CENIT Java tools.

Return Port

Optional. The port number where the remote PPM object receives calls. If the return port is 0 (the default value), an anonymous port is chosen. It is only necessary to enter a value other than 0 if you are also specifying the Local Host parameter to accommodate a firewall or Network Address Translator (NAT).

See FileNet documentation for details.

Local Host

Optional. Fully qualified name of the Process Engine, required for communication via a firewall or NAT.

VWJs Delay

Required. Automatically starts the total number of VWJs processes specified in **Max processes** and indicates the delay, in seconds, between starting each process.

vwtool User

Required for P8 3.0 and newer. Specify a valid user for vwtool.

vwtool Password

Required for P8 3.0 and newer. Specify the password for the user for vwtool.

PPM Debugging

Optional. Turns on/off debugging for the PPM processes, including all calls to the RMI registry.

Turning this option on creates trace files called **vwppm.trc** and **vwrmi.log** in the directory from which the PPM is started (\$TEMP for the ECM SM tasks).

VWJs Debugging

Optional. Turns on/off debugging for the VWJs processes. Changing this option affects only those processes started after you make the change. If you want to change the debugging setting for existing processes, you must stop and restart the PPM.

Turning this option on creates two trace files called jVWServer#.trc and jVWServer#.exc, where # is the number of the server process. The files are created in the directory from which the PPM is started (\$TEMP for the ECM SM tasks).

The Routers tab

Global settin	gs							
System:	Virtu	ial_P8				• I	New	Remove
IM Domain:	IS40	SQL:FileNet				•		1
Server:	W2K	(31540				▼ 1	New	Remove
						1/=====		
Webserver	Appli	cation Server	Compone	nt Manage	nintegrator	Process	Analyzer	
Router Name	:	vwrouter		•	New	Remove		
FileNet Path:	Į	/opt/FileNet/Vo	rkplace/WEB	3-INF/lib				
JAVA Path:	Į	/opt/FileNet/Rou	uter/JRE					
PPM Server:		aixrt12.cardiff.gl	lobalbs.co.u	k				
FileNet User:								
User Name:	-	-1					G	et user info
User Passwe	ord: 🗄	*****	******	*****				
Isolated Regi	ion: [1						
Registry Port	t: 🛓	32771						
PPM Port:		32771						
RMI Backlog	:	100						
Localhost	ē	55						
Debug Level	e.	0	1	2	3		4	
Connect Reti	ry:	180						

The Routers tab

Router Name

Required. Select a router or add a new router by pressing the **New** ... button. The currently selected router is removed from the configuration by pressing the **Remove** ... button.

FileNet Path

Required. Enter the path to the Router jar file. Name and location of this jar file depend on the FileNet version and the component on which the router runs:

- eProcess 4.2.2 and 5.0: path to pw.jar, e.g. /fnsw/bin on UNIX, c:/fnsw/bin or C:/ Program Files/FileNET/IDM/Web/IDMWS/Redist/WF_Extras on Windows
- P8 Content Engine: path to WFLauncher.jar, e.g. c:/Program Files/FileNet/Content Engine
- P8 Application Engine: path to eProcess.jar, e.g. /opt/ae/FileNet/Workplace/WEB-INF/lib

Java Path

Required. Enter the path to Java bin directory, e.g. C:/Program Files/JDK on Windows or / usr/local/java on UNIX.

PPM Server

Required. Network name of the PPM Server to which the router connects.

FileNet User

Optional, UNIX only. If you specify a user name, the router will be started with this user instead of the *root* user.

User Name

Required. User name to connect to the PPM Server, e.g. Administrator, SysAdmin or vwuser. Use the Get user info... button to get the user and password information directly from the FileNet server.

User Password

Required. Password of the user specified above. The password will be encrypted before it is stored in the environment file.

Isolated Region

Required. Number of the Isolated Region to connect to.

Registry Port

Required. The RMI port the router uses.

NOTE The port number is not optional because it is required by the CENIT Java tools.

PPM Port

Required. The RMI port that the PPM running on the Process Engine is using (Registry Port in the PPM configuration window for the PPM server).

RMI Backlog

Optional. Maximum queue length for incoming RMI connection indications before connections are refused.

Local Host

Optional. Fully qualified name of the Process Engine, required for communication via a firewall or NAT.

See FileNet documentation for details.

Debug Level

Optional. Debug Level for the router. Debug level 0 turns debugging off.

Selecting a value greater than 0 creates a trace file called <routername>.trc. The file is created in the directory from which the router is started (\$TEMP for the ECM SM tasks).

Connect Retry

Required. Time in seconds for retry to connect to the PPM Server.

Svetom		il P8			•	New	Remove
M Damain	15405	:OL :FileNet					10110101
	10/263				•	Now	Domano
server:	112113	л <u>э</u> чо				14644	Remove
Webserver	Applica	ation Server	Componen	t Manager/Integrator	Proce	ss Analyzer	
	Co	mponents		PPM		Rout	ers
Web Serve	r Settir	ngs					
Туре:		BEA WebLog	jic 8				•
User:							
Start Com	mand:	cmd.exe /k c:/	bea/user_pro	jects/domains/P8dom	ain/start/	VebLogic.ba	t
Stop Comr	nand:	cmd.exe /k c:/	bea/user_pro	jects/domains/P8dom	ain/stopV	VebLogic.ba	t
Processes	:	java					
Services:							
IMX Settin	us						
Connection	type:	BEA Webl o	aic				•
Server:		heal 2 fn glo	halhs coluk		Port [•] 70		
Service URI	L:	bour z.m.gro	baibo.co.ait				
User:		weblogic					
Password:		******					
Timeout:		60000					
Debug Leve	el:	Errors only					•
Debug File:							
Server libra	ry path	°. c:/bea/weblo	gic81/server/l	ib			
Java path:		c:/program fi	les/java/j2re1	.4.2_10			

The Web Application Server tab

The Web Application Server tab

Web Server Settings

Туре

Required. Select the type of web server you are configuring.

User

Optional, UNIX only. Select the user that must be used to start the web server processes. If no user is specified, the web server start and stop scripts will started as *root*.

Start Command

Required. Specify the command to start the web server. This can be a single command as well as a script or binary.

NOTE This script name must not contain blanks! Use the short name (DOS name) of the script instead. To determine the short name of a command, you can enter the following command: cpath_to_fsm_installation/tools/cosst.exe shortname ''<very long path/that contains blanks/and points to script''</pre>

Stop Command

Required. Specify the command to stop the web server. This can be a single command as well as a script or binary.

NOTE This script name must not contain blanks! Use the short name (DOS name) of the script instead. To determine the short name of a command, you can enter the following command: command: command. <pre

Processes

Required. Specify a list of processes that indicate that the web server is up and running. The processes that are specified here will be used by the task *View Process Engine Status* and by the monitor *ComponentStatus*.

Services

Optional, Windows platforms only. Specify a list of services that indicate that the web server is up and running. The services that are specified here will be used by the task *View Process Engine Status* and by the monitor *ComponentStatus*.

JMX Settings

Connection Type

Select the connection type. If the webserver supports JMX 1.2 or higher, you can select JMX 1.2 **Connectivity.** In all other cases, select the type that matches the Webserver type selected above.

Server

Required for connection types JBoss, BEA WebLogic, BEA WebLogic 9 and WebSphere. Enter the name of the server for the JMX connect.

Port

Required for connection types JBoss, BEA WebLogic, BEA WebLogic 9 and WebSphere. Enter the port of the server for the JMX connect.

Service URL

Required for connection type JMX 1.2 Connectivity. Enter the service URL for the JMX connect. This URL contains server name, port and other information.

User

Required. Specify the user for the JMX connect.

Password

Required. Specify the password of the user given above.

Timeout

Optional. Specify a timeout in seconds for the JMX request. If no timeout is given, the program will use 40 second as default timeout.

Debug Level

Required. Errors only logs only error messages. Debug provides more detailed information.

Debug File

Required. Specify the name of the output file where debug output must be written to.

Server library path

Required. Enter the path to the libraries of your web application server. The location of the libraries depends on the webserver type.

Java path

Required. Enter the path to Java bin directory, e.g. C:/Program Files/JDK on Windows or / usr/local/java on UNIX.

Note: For WebSphere and WebLogic 9 support the product own Java should be used. More detailed information about that is listed in the "prepare JMX support" documentation in the "Install Guide".

Global settin	gs					
System:	Virtual_P8		New	Remove		
IM Domain:	IS40SQL:FileNe	t		•		1
Server:	W2K3IS40			•	New	Remove
Webserver	Application Serv	/er Compone	nt Manager/Integrator	Process	s Analyzer	
	Components	\$	PPM		Rout	ters
Workplace H	lome:	/opt/FileNet/Worl	kplace			
JAVA Path:		/opt/FileNet/Rout	ter/JRE			
Router URL:		aixrt12.cardiff.glo	balbs.co.uk			
FileNet User:						
User:		-1			G	iet user info
Password:		*****	****			
JNDI Initial C	ontext Factory:					
Registry Por	t:	32771				
Event Port:		32773				
Required Lib	raries:					

The Component Manager/Integrator tab

The Component Manager / Integrator tab

Workplace Home

Required. Enter the path to the Workplace installation directory, e.g. C:/Program Files/ FileNet/Workplace on Windows or /opt/ae/FileNet/Workplace on UNIX.

JAVA Path

Required. Enter the path to Java bin directory, e.g. C:/Program Files/JDK on Windows or / usr/local/java on UNIX.

Router URL

Required. Enter the URL of the Process Router to be used for authentication. Enter the information in the following format: <server>:<port>/<router-name>.

FileNet User

Optional. If you specify a user name, the Component Manager will be started with this user instead of the *root* user.

User Name

Required. User name to connect to the router. Use the **Get user info** ... button to get the user and password information directly from the FileNet server.

User Password

Required. Password for the user specified above.

JNDI Initial Context Factory

(JMS-based components only) Identifies the class responsible for managing the connection to the J2EE JNDI server through which the JMS adaptor connects to the JMS queue.

Registry Port

Required. The RMI port that the Component Manager runs on. The port number must be greater than 1024.

Event Port

Optional. The port that the Component Manager listens to for incoming events.

By entering an event port you configure the Component Manager to automatically respond to new events as they occur. Alternatively, if you set the event port to 0, the Component Manager does not automatically respond to new events as they occur; instead, the Component Manager polls periodically for new events.

Required Libraries

Required for external components. Specify the fully qualified names of the jar files that contain the class associated with each component queue. Each jar file must be specified in a single line.

The Start task for the Component Manager appends the jar file locations to the CLASSPATH when starting the Component Manager.

nto						
Global settin	gs					
System:	sys_pa			•	New	Remove
IM Domain:	IS40SQL:FileNet			•		
Server:	W2K3IS40			•	New	Remove
Webserver	Application Server	Component	ManagerIntegrator	Proces	s Analvzer	
	Components		PPM		Rout	ers
ileNet path: Java path:	c:/program files/FileI	Net/Process Ai	nalvzer Enginelina			
	c:/program files/File)	NEDProcess A	nalyzer Engine/_jvm			Browse Browse

The Process Analyzer tab

The Process Analyzer tab

FileNet Home

Required. Enter the path to the Process Analyzer installation directory, e.g. C:/Program Files/ FileNet/Process Analyzer Engine/jpa.

JAVA Path

Required. Enter the path to Java bin directory, e.g. C:/Program Files/FileNet/Process Analyzer Engine/_jvm.

Configure Content Engine

To configure FileNet P8 Content Engine properties, press the **Configure Content Engine** ... button.



Configure Content Engine ...

The Content Engine configuration dialog opens:
Global Setting	gs										
Domain Nam	e: P8_3	i						•	New	Ren	nove
Server Nam	e: w2kc	: w2kcm35 💌 New Remove									
Start/Stop or	der;										
Start	order: 1		Ch	ange	•		Sto	op ord	er: 1	Cha	ange
FileNet Conte	nt Engine	Settin	igs –								
FileNet Path:	c:/progra	ım file:	s/filen	et/cont	ent eng	ine					
JAVA Path:	c:/progra	ım file:	s/filen	et/cont	ent eng	ine/_jvm					
User:	P835TIV	OLI/Ac	minis	trator							
Password: Database(s):	********* Orac	le 🗹	MSSG)L Sen	/er 🗌	DB2					
Password: Database(s): Webserver S Apache	·····	le 🗹	MSSG)L Sen	/er 🗌	DB2	at Infori	matio	n Server —		
Password: Database(s) Webserver S Apache Path:	ettings	le 🗹	MSSC)L Sen	/er	DB2	et Infori	matio	n Server —		
Password: Database(s): Webserver S Apache Path: User:	ettings	le 🗹	MSSC he gro	QL Sen up/apa	ver	DB2	et Infori is requ	matio	n Server		
Password: Database(s): Webserver S Apache Path: User: Port:	ettings gram files	le 🗹	MSSC he gro	QL Serv	xer	DB2	et Infori is requ	matio uired	n Server		
Password: Database(s): Webserver S Apache Path: User: Vser: Port: Webpage:	ettings gram files 8008	le 🗹	MSSC he gro	QL Serv	ner	DB2	et Inforn is requ age:	matio uired	n Server		

The Content Engine configuration window

Global Settings

Domain Name

Required. Select a already configured domain or add a new by pressing the **New** ... button. The currently selected domain can be removed by pressing the **Remove** ... button.

NOTE The domain is shown in the FileNet Enterprise Manager and is casesensitive. The FileNet domain specified in this field is completely independent from the Windows logon domain in the username specified in the field **User**.

Server Name

Readonly the server is entered in the New Domain dialog.

Start/Stop order

Start order

Use the Change ... button to the right of this field to change the start order for the selected server.

Stop order

Use the Change ... button to the right of this field to change the stop order for the selected server.

FileNet Content Engine Settings

FileNet Path

Required. Specify the installation path of the Content Engine Software, e.g. C:/Program Files/ FileNet/Content Engine. The script checks if the file WFLauncher.jar (router implementation for CE) can be found in this directory.

JAVA Path

Required. Specify the installation path to the Java bin directory, e.g. C:/Program Files/ FileNet/Content Engine/_jvm.

Note: JAVA is required for CENIT JAVA tools for Content Engine monitoring only.

User

Required. Specify a user name to the Content Engine.

NOTE The user must be a valid user for the FileNet Enterprise Manager. It may be a domain user (windows_logon_domain/username). The FileNet domain specified as **Domain Name** above is completely independent from the Windows logon domain in the username.

Password

Required. Specify the password of the user given above.

Database

Required. Select the database type(s) that are used for Object Stores on the Content Engine.

Webserver Settings / Apache

Path

Required. Specify the installation path of the Apache Web Server Software, e.g. C:/Program Files/Apache Group/apache2.

User

Required on UNIX. Specify the user that must be used to start the Apache Web Server.

Port

Required. Specify the port number on which the Apache Web Server is listening. Default is 8008.

Webpage

Required. This Apache Webpage needs to exist and will be monitored.

Web Server Settings / Internet Information Server

Required

Select Yes if you use IIS to provide WebDAV functionality on the Content Engine.

Port

Required. Specify the port number on which IIS is listening.

Webpage

Required. This IIS (WebDAV) page needs to exist and will be monitored.

CFS-IS Settings

IS Domains

Select one or more IS domains that have been set up for CFS-IS.

Configure IBM Content Collector, Email Manager and Records Crawler

To configure IBM Content Collector, IBM FileNet P8 Email Manager and Records Crawler properties, press the Configure IBM Content Collector, Email Manager and Records Crawler... button.

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication see chapter "How to configure and use the UnifiedDatabaseClient (UDC)" in the Installation Guide.



Configure IBM Content Collector, Email Manager and Records Crawler...

The IBM Content Collector, Email Manager and Records Crawler configuration dialog opens:

Info									
Global Settings									
System name:	Email_Mgr				•	-	New	Remove	
Server name:	N7P009026	4BIT.de.ce	enit-grou	up.com	•				
		Reload c	onfigura	ation					
		Nelodu C	onngura						
Product:		● ICC EM	lail Serv	vices and l	Email Ma	na	ger		
		O ICC File	e systen	n settings	and Rec	:01	ds Crawler		
Version:		3.6							-
Database type:		MSSQL				_			-
Database path:		C:/progran	n files/m	nicrosoft s	ql server/	/90	/tools		
Database name	:	EM36							
Remote Databas	se Identifier:	EM36							
Database user:		sa							
Database passv	word:	•••••	•••••						
Database schen	na:								
Logfile name:									
		Ok	Ca	ncel	Help				

The IBM Content Collector, Email Manager and Records Crawler configuration window

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Global Settings

System Name

Required. Select an already configured system or add a new by pressing the **New** ... button. The currently selected system can be removed by pressing the **Remove** ... button.

Server Name

Readonly. The server is entered in the New System dialog.

Reload configuration ...

Press this button to reload the IBM Content Collector, Email Manager and Records Crawler settings from the registry of the given server.

Product

Select the product type for which the configuration must be saved. If the settings for one of the components cannot be read from the registry of the given server, the corresponding radio button is disabled.

Each server can have either an IBM Content Collector Email Services and Email Manager component or an IBM Content Collector File system settings and Records Crawler component. If both components must be configured on the same server, two distinct systems must be created.

Version

Readonly if the version can be determined from the registry. If the setting cannot be determined, the version can be selected.

NOTE Please select "4.0" as version number when configuring IBM Content Collector 2.1.x, 2.2.x or 3.0.

Database Type

Readonly if the database type can be determined from the registry. If the setting cannot be determined, the database type can be selected.

Database Path

Required. Enter the path to your RDBMS installation.

- Oracle: Path to the **bin** directory where the Oracle tools are installed:
 - Windows: <drive letter>:/orant
- MSSQL: Path to the binn directory where the MSSQL tools are installed. The location of this directory depends on the MSSQL Server version:
 - MSSQL Server 2000 or MSDE 2000: <drive letter>:/Program Files/ Microsoft Server/80/Tools
 - MSSQL Server 2005: <drive letter>:/Program Files/Microsoft Server/90/Tools

The installation script searches the **binn** directory for the tools **sqlcmd.exe**, **osql.exe** or **isql.exe**.

- DB2: Path to the **bin** directory where the DB2 tools are installed:
 - Windows: <drive letter>:/Program Files/IBM/SQLLIB
- JDBC client: Java install directory

If the JDBC based UDC communication to the DB should be used, specify the Java install path here (without /bin at the end) instead of the DB installation path. UDC supports Java version 7 and newer.

NOTE Use / instead of \setminus in the pathname.

Database Name

Required. Enter the name of the components database if it does not match the shown value from the registry.

For Oracle, this field corresponds to the setting of ORACLE_SID.

Remote Database Identifier

Oracle via Oracle Client access

If your database is configured for remote access, enter the TNS name (Service name) of the database (otherwise not required).

MSSQL via MSSQL client access

Specify the Server/Instance name. The value is optional.

The following combinations are possible:

- Leave this parameter unset, if the local Default MSSQL instance should be monitored.
- Specify the remote MSSQL server name, if the Default instance should be monitored on a remote server.
- Specify MSSQL Server name/Instance name, if a custom MSSQL instance on the local or remote server should be monitored.

NOTE Use / instead of \ between MSSQL Server and Instance name!

DB2 via DB2 client access

DB2 instance name (required).

Oracle via JDBC (UDC) access

If the JDBC based UDC communication to the Oracle DB should be used the configuration for an ORACLE DB server looks like: <Oracle server name>,<path to the Oracle JDBC driver location>,[optional Oracle port]. The default port number is 1521.

Example: oracleServ1,C:/Program Files/oraclejdbc,1521

MSSQL via JDBC (UDC) access

If the JDBC based UDC communication to the MSSQL DB should be used the configuration for a Default MSSQL instance looks like: <MSSQL server name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port]. The default port number is 1433.

Example: mssqlServ1,C:/Program Files/sqljdbc11/enu,1433

An MSSQL custom instance UDC configuration looks like; <MSSQL server name>/<Instance name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port].

Example: mssqlServ1/INSTANCE1,C:/Program Files/sqljdbc11/enu,1433

NOTE For information on how to connect to an SSL secured MSSQL Server see Chapter *How to configure and use the UnifiedDatabaseClient* in the *ECM SM Install Guide*.

DB2 via JDBC (UDC) access

If the JDBC based UDC communication to the DB2 database should be used the configuration for a DB2 instance/database looks like: <DB2 server name>,<path to the DB2 JDBC driver location>,[optional DB2 port]. The default port number is 50000.

Example: db2Serv1,C:/Program Files/db2jdbc,50000

User

Required for DB2 and Oracle, optional for MSSQL. Enter the user that must be used to access the components database.

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Password

Required for DB2 and Oracle, optional for MSSQL. Enter password for the user specified above. The password will be encrypted before it is stored in the environment file.

Schema name

DB2 only: Specify the DB2 components schema name (required).

Logfile Name

Readonly if the logfile name type can be determined from the registry. If the setting cannot be determined, the logfile name can be entered.

This logfile name (including full path) points to the IBM Content Collector, Email Manager or Records Crawler primary logfile.

NOTE The location of the log file can be gathered from the ICC configuration manager GUI. Verify the entry of **Log file location**.

Configuring FileNet Capture



To configure FileNet P8 Capture properties, press the Configure FileNet Capture... button.

Configure FileNet Capture ...

The FileNet Capture configuration dialog opens:

Info						
Global Se	ttings					
System:	Capture_5.0			New	v	Remove
Server:	w2kcap50mssql			▼ Nev	v	Remove
Remote	Capture Services	Remote Ca	apture Services Database	FileNet Print		
	Components		Captu	re Profession	al	
🗹 Captu	re Professional					
🗌 Remo	te Capture Service	s				
Remo	te Capture Service	s Database				
FileNo	t Print					
	a r tua					
		Ok	Cancel Help			

The FileNet Capture configuration window

The upper part of the dialog shows the **Global Settings**. The lower part shows the components that have already been configured for the selected server.

Global Settings

System Name

Required. Select an already configured system or add a new by pressing the **New** ... button. The currently selected system can be removed by pressing the **Remove** ... button.

Server Name

Required. Select an already configured server or add a new by pressing the **New** ... button. The currently selected server can be removed by pressing the **Remove** ... button.

If you mark a checkbox, the tab for the corresponding component will be activated. If you unmark a component, the data will be removed for the selected server.

The Capture Professional tab

Info									
_Global Set	ttings								
System:	vystem: Capture_5.0							New	Remove
Server:								New	Remove
Remote (Remote Canture Services Densite Canture Services Detabase FileNet Drint								
	Compor	nents	Tremore v			Captu	re Profe	ssional	
ODBC Dat	asource:	FileNet	t Loa						
Database	user:	sa							
Database	password:								
Java path		c:/Prog	ram Files/J	Java.	vj2re1.4.2_11				
FavEntry	lactilo	C'(EavE	Entry Journ	ol/ER	ETrace log				
Tanchayi	iognic.	0.71 876	Innyyoounn		L Hatelog				
			Ok	(Cancel	Help			

The Capture Professional tab

ODBC Datasource

Required if you want to monitor the Capture Trace log. Enter the name of the ODBC datasource where CALA must read from.

To enable tracing and find out the name of the ODBC datasource open **Programs FileNet Capture Professional** *Trace* from the Windows start menu. Mark the checkbox **Enable Tracing**. The datasource name is shown in the **Record to** combobox.

Database user

Optional. Enter the user if the ODBC datasource requires a logon.

Database password

Optional. Enter the password for the user specified above if the ODBC datasource requires a logon

Java path

Required if you want to monitor the Capture Trace log. Enter the path to the Java bin directory.

NOTE CALA uses the JDBC-ODBC-Bridge contained in the Java Runtime. Because of this, a Java must be installed on the client to enable reading of the Capture Tracelog.

FaxEntry logfile

Optional. Enter the full-qualified name of the FaxEntry trace file.

To find out the name of the Fax Entry tracefile open **Programs FileNet Capture Professional** *Fax Entry* from the Windows start menu. Select **Configure** *Trace* from the menu. The name of the tracelog file is shown in the field **Trace File Name**.

The Remote Capture Services tab

Info				
Global	Settings			
Syster	n: Capture_5.0	▼ New	Remove	
Serve	: w2k3caprcs		▼ New	Remove
Remo	te Capture Services	Remote Capture Services Database	FileNet Print	
	Components	Captur	e Professional	
Path to	logs directory: C:/fm	sw/client		
		Ok Cancel Help		

The Remote Capture Services tab

Path to logs directory

Required. Enter the path to the logs directory where the logfiles for RCS are located, e.g. c:/fnsw/client.

The Remote Capture Services Database tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Info				
-Global Se	ttings			
System:	Capture_5.0	•	New	Remove
Server:	w2k3is40	▼	New	Remove
Remote (fanium Sonsiens	Pomoto Canturo Sonvicos Databaso FiloNo	i Drivi	
Ttembte	Components	Capture Profe	ssional	
Databaco				
Database	type.	MSSQL		•
Path:		C:/Program Files/Microsoft SQL Server/80/Tools		
Database	name:	offlinerep		
Remote d	latabase identifier:			
User:		sa		
Password	d:	****		

The Remote Capture Services Database tab

Database Type

Required. Select the database type of the RCS database.

NOTE At the moment, only MSSQL is supported.

Database Path

Required. Enter the path to the **binn** directory where the MSSQL tools are installed. The location of this directory depends on the MSSQL Server version:

- MSSQL Server 2000 or MSDE 2000: <drive letter>:/Program Files/Microsoft Server/80/Tools
- MSSQL Server 2005: <drive letter>:/Program Files/Microsoft Server/90/Tools

JDBC client

If the JDBC based UDC communication to the DB should be used, specify the Java install path here (without /bin at the end) instead of the DB installation path. UDC supports Java version 7 and newer.

The installation script searches the **binn** directory for the tools **sqlcmd.exe**, **osql.exe** or **isql.exe**, if UDC is configured it searches for **java.exe** in the **bin** subdirectory of the path.

NOTE Use / instead of \setminus in the pathname.

Database Name

Required. Enter the name of the RCS database.

Remote Server / Instance name

The following combinations are possible for the parameter MSSQL Remote Server or Servername/Instancename:

Leave this parameter unset, if the local Default MSSQL instance should be monitored

Specify the remote MSSQL server name, if the Default instance should be monitored on a remote server

Specify MSSQL Server name/Instance name, if a custom MSSQL instance on the local or remote server should be monitored.

Note: Use "/" instead of "\" between MSSQL Server and Instance name!

If the JDBC based UDC communication to the MSSQL DB should be used the configuration for a Default MSSQL instance looks like: <MSSQL server name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port]. The default port number is 1433. Example: mssqlServ1,C:/Pro-gram Files/sqljdbc11/enu,1433. A MSSQL custom instance UDC configuration looks like; <MSSQL server name>/<Instance name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port]. Example: mssqlServ1/INSTANCE1,C:/Program Files/sqljdbc11/enu,1433.

NOTE For information on how to connect to an SSL secured MSSQL Server see Chapter *How to configure and use the UnifiedDatabaseClient* in the *ECM SM Install Guide*.

User

Optional. Enter the user that must be used to access the RCS database.

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Password

Optional. Enter password for the user specified above. The password will be encrypted before it is stored in the environment file.

The FileNet Print tab

nfo						
Global Se	ttings					
System:	Capture_5.0			-	New	Remove
Server:	w2kprint			-	New	Remove
Remote (Canture Services	Remote Can	ture Services Dat	ahase Filot	lot Drint	<u></u>
Tremore	Components	Tempte edp		Capture Pro	fessional	
Path to lo	gs directory: CC/FN	SW LOC				
		Ok	Cancel	Help		

The FileNet Print tab

Path to logs directory

Required. Enter the path to the logs directory where the logfiles for FileNet Print are located, e.g. $c:/FNISW_LOC$.

Configuring a FileNet Listener

NOTE The FileNet Listener monitors must be run with Java(TM) 7 or higher. They will not work with older Java(TM) versions.

To configure a FileNet Listener, select the appropriate plug-in in the main installer dialog:



Configure FileNet Listener ...

This is the main window for configuring FileNet Listeners:

Info		
Global settings		
Servername: W2KORA92	Add server	Remove
Java settings		
Path to java: C:/Program Files/Java/j2re1.4.1_01/bin		Browse
Listeners		
New listener Delet	e	
Application: Image Services Resource Adapter		
Listener port: 32775	Test por	t
Ok Cancel	Help	

Listener configuration window

Global Settings

Server

The listbox shows all servers already configured for FileNet Listeners, use the Add server... and Remove ... buttons to add or remove servers.

Java Settings

Path to java

Required. Specify the path to the Java bin directory. You can also use the **Browse** ... button to the right of the entry field to open a file browser and navigate to the correct directory.

Listeners

Use the **New listener** ... button to add new Listeners. Each Listener will be shown on its own tab in the lower area of the dialog.

Use the **Delete** ... button to delete a Listener configuration.

Port

Required. Enter the port number for communication with the Listener. This should be the port number of the primary Listener on the server. Use the **Test port** ... button to check the communication with the Listener.

This is the dialog shown after pressing the New listener ... button:

Application:	Content Services
	Image Services
	Image Services Resource Adapter
	Ok Cancel Help

New Listener dialog

Application

Choose an application from the list of predefined entries or add a new application in the entry field.

Configuring ECM SM clients for IBM FileNet Content Services

Configure IBM FileNet Content Services

Pressing the **Configure Content Services** ... button opens the IBM FileNet Content Services configuration dialog.

The dialog consists of an upper part in the **Global settings** box and a bottom part containing some tabs (see screenshot on the next page).

Global settings:

Library System

Select the Library System you want to configure. Press the New ... button to add a new Library System system. Press the Remove ... button to remove the selected Library System from the configuration.

Server

Select the server you want to configure. Press the **New** ... button to add a new Verity standalone server. The **Remove** ... button is only activated if a standalone Verity server is selected. The servers that form the IBM FileNet CS system (Storage Managers and Content Search Managers) are added automatically to the **Server** list when you press the **Get Configuration** ... button.

Hostname

Required. The list shows all machines that have a CALA_REX client installed. Choose the correct hostname of the server selected in the **Server** listbox. This is the name that will be used in the Web Console.

The Database tab

This tab is only activated if the Property Manager is selected. If another Library System is selected in the listbox, the Property Manager is selected automatically. To reload the configuration from the FileNet database, press the **Get Configuration** ... button.

nfo						
Global Settings						
Library System:	cstivhp			-	New	Remove
Server:	tivhp11i			•	New	Remove
Hostname	tivhp11i.stgt	.cenit.de		•		
Database Setting	js FileNet S	Settings	Verity Settings			
General Databas	e Settings					
Installation Path	: []	usr/ora/91	20			
Remote Databas	e Identifier:					
User:		stivhp_fn	SW			
Password:	-		*			
or doile collange						
Oracle SID:	CSTIV	ΉP				
Oracle NLS Lang	juage: AMER	ICAN_AM	ERICA.WE8MSWIN1252			
Oracle OS User:	oracle					
			Get Configuration			
		Ok	Cancel	Help		

Database Settings tab

General Database Settings

Installation Path

Required. Enter the path to your RDBMS installation.

The most common values are /usr/oracle for Oracle on UNIX or <drive letter>:/orant for Oracle on Windows.

For MSSQL Server databases, common values are <drive letter>:/Program Files/ Microsoft Server/80/Tools for SQL Server 2000 or <drive letter>:/Program Files/ Microsoft Server/90/Tools for SQL Server 2005.

Remote Database Identifier

Optional. If the database is a remotely hosted Oracle database specify the Oracle Global name (TNS name / Service name).

If the database is a remotely hosted MSSQL database specify one of the following combinations:

Leave this parameter unset, if the local Default MSSQL instance should be monitored

Specify the remote MSSQL server name, if the Default instance should be monitored on a remote server

Specify MSSQL Server name/Instance name, if a custom MSSQL instance on the local or remote server should be monitored.

Note: Use "/" instead of "\" between MSSQL Server and Instance name!

User

Required for Oracle, optional for MSSQL. Specify the Database User for all SQL-Statements.

If your database is Oracle, you can create a database user by executing the task *Create Library System Oracle User* with the ECM SM Task Execution Manager.

If your database is MSSQL, you can leave this field empty. In that case, the tasks and monitors will try to connect using Windows authentication. Make sure that CALA and the CALA_REX client are using an account that has permission to access the database.

Password

Required for Oracle, optional for MSSQL. Specify the password of the Database User.

Oracle Settings

Oracle SID

Required for Oracle only. Specify the ORACLE_SID, where the IBM FileNet CS tablespace is located (if Property Manager is based on Oracle).

Oracle NLS_LANG

Required for Oracle only. Specify the value of the Oracle NLS_LANG parameter.

Oracle OS User

Required for Oracle on UNIX only. OS user to execute Oracle commands.

Get Configuration

Press this button to load the configuration from the IBM FileNet CS database. This fills the **Server** listbox as well.

The FileNet tab

This tab is available for all Storage Managers and Content Search Managers of the IBM FileNet CS system.

Info					
Global Settings					
Library System:	.ibrary System: cstivhp 🗸 🗸				
Server:	tivhp11i	•	New	Remove	
Hostname	tivhp11i.stgt.cen	it.de 🗸 🗸		·	
Database Setting	gs FileNet Setti	ngs Verity Settings			
FileNet Settings					
FileNet Version:		5.3			
IDMDS Home:		/usr/cs53/filenet			
Storage Manage	er Device:	/usr/cs53/storage			
Content Search	Manager Device:	/usr/cs53/search			
FileNet OS User:	1	filenet			
		Ok Cancel Help			

FileNet Settings tab

FileNet Settings

FileNet version

Required, normally filled by Get Configuration The version of the installed software.

IDMDS Home

Required, normally filled by Get Configuration Home directory of the FileNet CS installation.

Storage Manager Device

Required for Storage Managers. Enter the installation device of the StorageManager if the value is not correctly shown.

Content Search Manager Device

Required, normally filled by Get Configuration Installation device of the Content Search Manager.

FileNet OS User

Required for UNIX only. OS user to execute FileNet commands.

The Verity tab

This is the only tab that is activated for standalone Verity servers.

nfo			
-Global Settings-			1
Library System:	cstivhp 🔹	New	Remove
Server:	tivhp11i 🔹	New	Remove
Hostname	tivhp11i.stgt.cenit.de 🗸 🗸		
Database Setting	gs FileNet Settings Verity Settings		
Verity Settings			
	Master Verity Server		
Verify OS User:	filenet		
Variables:	VeritvServerPort=9550	Nom	Romano
	VerityBrokerPort=9551	NGW	Trentove
	VerityIndexLanguage=		
	VerityBrokerName=CS_TIVHP11I_cstivhp_K2Broker		
	VerityServerName=CS_TIVHP11I_cstivhp_K2Server		
	VerityAdminMasterServer=tivhp11i.dud.cenit.de		
	VerityAdminMasterPort=8105		
Name:	VerityServerPort	Apply	
Value:	9550		
	Ok Cancel Help		

Verity Settings tab

Verity Settings

Master Verity Server

Optional. Check this box if this is the master Verity Server. If the IBM FileNet CS system contains only one Verity Server, this server will be marked automatically.

Verity OS User

Required for UNIX only. OS user to execute Verity commands.

Variables

Read-only. Shows all Verity variables defined for this server.

NOTE The New ... and Remove ... buttons are currently disabled because additional variables are not processed yet

Name

Read-only. Shows the name of the variable that is currently selected in the listbox.

Value

Required. Enter the value of the variable. Use the **Apply** button to transfer the new value to the listbox.

The New Library System dialog

This dialog is shown if you press the New ... button next to the Library System listbox in the Global Settings panel.

Library System:	cstivhp
Property Manager:	tivhp11i
Ok	Cancel

New Library System dialog

Library System

Required. Enter the name of the new Library System.

The name entered here must match the name of the Library System in the IBM FileNet CS configuration. Note that the Library System name is case sensitive.

Server

Required. Enter the name of the Property Manager as it is known in the IBM FileNet CS Library System. If the network name differs, you can select it from the **Hostname** listbox in the main window after pressing the **Ok** button.

After pressing the Ok button, you are returned to the main configuration window. The Database Settings tab will be selected automatically. Adjust the hostname if required and fill in the database details of the IBM FileNet CS database.

The Get Configuration ... button retrieves the information about the specified Library System from the database and fills the server listbox. Select each server and complete the settings on the FileNet tab and on the Verity tab.

The New Verity Server dialog

The New Verity Server dialog is shown if you press the New ... button next to the Server listbox in the Global Settings panel.

Hostname:	tiv_verity
	Ok Cancel

New Verity Server dialog

Hostname

Required. Enter the hostname of the server you want to add. This is the name that is added to the server listbox. You can select a different value in the **Hostname** field in the main configuration window.

Press the OK button to add the server to the listbox in the main configuration dialog. The Verity Settings tab will be selected automatically.

Excluding servers of a Library System

If you want to exclude one or more servers of a Library System from being managed, you need to create a file fnds_do_not_manage.<Library System name>, which contains the server names to be excluded. The file must be located on the ECM SM server in the directory where the configuration files are stored (normally /opt/FileNet/SysMon/repos/config/PAM).

NOTE You cannot exclude the Property Manager

Example:

If you want to exclude the server *W2KCS54* from the Library System *cs54db*, you need to create the exclude file /opt/FileNet/SysMon/repos/config/PAM /fnds_do_not_manage.cs54db.

This is the example contents of /opt/FileNet/SysMon/repos/config/PAM /fnds_do_not_man-age.cs54db:

This is the server exclude file of Library System cs54db
W2KCS54

The name of the Library System and the name of the server are case sensitive (server names are uppercase letters).

Configuring ECM SM clients for IBM FileNet P8 4.x/5.x

Configure IBM FileNet P8 4.x/5.x

To configure IBM FileNet P8 4.x/5.x properties, press the Configure FileNet P8 4.x and 5.x Client ... button.



Structure of the IBM FileNet 4.x / 5.x hierarchy structure.

The root element of the IBM FileNet 4.x/5.0x structure is the so called "Release". It is only an abstract element which is a container of several "Systems". The configuration can consist of several different configured "Systems", which are all stored in the "Release". A system is a whole configuration for a complete environment of several different servers, farms, clusters and products, just as Content Engine or Process Engine running on these machines. Every system has a set of different "Servers" which contain the connection information

of a physical machine. One server can have several "Instances" which contain JMX specific configuration parameters. Instances are abstract servers which are defined in a web application server environment, since application servers have internal structures just as Cells, Nodes and Servers. Several Instances are grouped in so called "WebEnvironments". WebEnvironments can contain also instances from several servers. The servers and instances which are used in the infrastructure, finally are used in the definitions of the products (CE, AE, PE, CM, PA...).

Release

The release is the top level root element. The user will never see the release as an element in the GUI, but since there should not be several root elements (in this case this would be the systems) there is one virtual root element (the release).

System

The system is a collection of all computers and resources of a P8 installation, including the servers and the configuration for the installed products like Process Engine or Content Engine. The system includes the whole configuration for a complete P8 4.x/5.x installation. It is possible to define several systems.

Infrastructure

The infrastructure contains all servers of the P8 system which shall be configured. It is only a logical element, like the release element. The collection of all servers and web environments is called the infrastructure, because these elements model the server infrastructure of the P8 system.

Server

The server element contains several server specific parameters like the host name or the Java path. A server also contains several (at least one) JMX instance(s) and exactly one FileNet Listener configuration. The idea is to store as much information as possible on the server level. These parameters are available for several products (PE, AE...) on the server and need not be entered several times for each product.

Instance

An instance is the configuration of the JMX specific parameters. The JMX port is stored the instance as well as the application server type. Also other basic connection data like the user, password and timeout are part of an instance. One of the most important parameters is the server connection data, which contains the most important structure information of the application server internals. The following picture shows how an application server is structured and which information must be contained in the infrastructure.



Structure of application servers.

The image shows one server which has two different application servers running which have several applications deployed. The yellow fields are parameters which are stored in the "server connection data" parameter of the instance parameters. The other fields (Java path, port, user, password...) will be the same for every instance. The following example shows how many instances must be created to monitor all applications.

- Instance 1: [WebSphere Cell Node1 Server 1] will be used for "Application 1" and "Application 2"
- Instance 2: [WebSphere Cell Node1 Server 2]
- Instance 3: [WebSphere Cell Node2 Server 3]
- Instance 4: [WebSphere Cell Node2 Server 4]
- Instance 5: [WebSphere Cell Node2 Server 5]
- Instance 6: [WebSphere Cell Node2 Server 5]

- Instance 7: [WebSphere Cell Node2 Server 6] will be used for the clustered "Application 3".
- Instance 8: [WebLogic Domain Server1] is used for "Application 4" and "Application 5"

Web Environment

The Web Environments contain several instances which belong to a logical group. The following Web Environments would be used in the example above:

- WebEnv1: Instance1
- WebEnv2: Instance2, Instance3, Instance4, Instance5, Intsance6, Instance7
- WebEnv3: Instance7

In this example the unusual case is used, that there is only one (physical) server which contains all the instances. In real environment there will be several servers. One web environment can also contain instances from several servers at the same time.

Products

The products contain the configuration of the Content Engine, Process Engine and the other P8 products. It is differentiated between "Server Products" and "Web Products". Content Engine and Application Engine are web products, which mean that they run on application servers. These products use the configuration of the web environments. Content Engine uses exactly one Web Environment and Application Engine can contain several Web Environments. Only web products contain JMX instance data. All other products (Process Engine, Component Manager, Process Analyzer) are server products. These products do not use web environments but can contain one or several servers, depending on which products are used.

Configure IBM FileNet 4.x / 5.x

To configure IBM FileNet 4.x / 5.x properties, press the Configure IBM FileNet 4.x and 5.x Client ... button.



The FileNet Installer Plug-in

The IBM FileNet 4.x / 5.x configuration dialog opens.

Tools						
iystem: Windows			🔘 New	🗊 Delete 📓 Help		
Infrastructure Products						
Hosts Environments						
Windows					New	
				D	Edit	
└─ @ WebSphere6Instance				1	Delete	
e Weblogic9Instance				12	Help	
or III w2kcm35						
🥌 🥔 Weblogic7Instance						
)k 🥘 Cancel					

The Installer for IBM FileNet 4.x/5.x dialog with expanded tree view

It consists of several tabs which represent the hierarchical structure of the image above. When the dialog is opened the first time, most of the tabs and buttons are disabled.

In this main window there is the menu Tools . If it is opened, the option View config as text can be clicked.

In this window the current configuration is shown as textual tree view. It is possible to refresh the view and save the configuration to a file to use it for monitor configuration.

```
_____
|The current system protptype|
 _____
System: Windows
  -----+
     Servers:
                I
  -----+
Ι
+- Managed Host: w2k3ws6
 | +- Managing Host: w2k3ws6
| +- This server is managing host of the following servers:
 | | +- w2k3ws6
 | +- Description:
 1
   +- Java Path C:\Program Files\Java\j2rel.4.2_10
 1 1
 | +- The server has the following instances:
 Т
      Т
 L
      +- Instance: WebSphere5Instance
      +- JMX Parameters:
 T
      | +- Application Server Type: WEBSPHERE5
 T
      | +- [Service URL]:
 | +- [Port]: 2809
 Т
      | +- [JMX User]:
 T
      | +- [Password]: Not showed...
 I
 T
      | +- [Timeout]: 30
      | +- Path to Java: Path to JMX Java: E:\WebSphere5\AppServer\java
 I
      | +- Path to Server Libs: E:\WebSphere5\AppServer
 T
      | +- Server Connection Data: server1;w2k3ws6;w2k3ws6;5.0
 Т
      +- Listener Parameters:
 1
 I
      | +- Listener Port null
 T
      Ι
      +- Instance: WebSphere6Instance
         THEY DOLLARS CALLER
•
                                                                           •
                          츟 Refresh
                                       💾 Save As ...
                                                      🔞 Help
                   0k
```

Dialog to view the already configured system as text

Create a new system by clicking on the New... button. The New System dialog will be displayed.



Dialog to create a new system

The New System dialog has one input field to enter the new system's name, an OK button to create the system and a Cancel button to leave the dialog without creating the system.

After a system is created the infrastructure tab is enabled and it is possible to create a new server. Clicking the **New...** button opens the **New Server** dialog.

The Infrastructure Tab

The infrastructure tab is used to define the environment in which the system is running. So hosts / servers can be created which contain instances. After creating the servers, the instances are grouped in web environments. The infrastructure tab itself contains two other tabs. The **Hosts** tab to define the server and the **Environment** tab to define the web environments. Both tabs consist of a hierarchical tree of the system, the defined servers and instances in the hosts tab. The environment tab also has a hierarchical tree view with the system, the defined web environments and the instances associated with the web environment. Both tabs have three buttons: **New..., Edit...** and **Delete...**.

The New Server dialog - Hosts New... button

Managed Host:	W2K3WL9						🖪 Copy	🚯 Copy from	
Managing Host:	W2K3WL9						_	-	
Description:									
Java Path	c:/Progra~1/Java/Jdk5 🔤 Browse								
JMX Liste	ner								
Insta	nce:	wl9inst	-	🥟 New	🖪 Copy From	1	🖥 Delete		
Appli	cation Server Type	Bea Wel	blog	ic 9			-		
[Serv	rice URL):								
[Port]:	7001							
[JMX	User]:	weblogic							
pass	word	*****							
[Time	out]: 500								
Path	to Java:	C:\bea\jrockit90_150_04 📾 Browse							
Path	to Server Libs:	C:\bea\weblogic91\server\lib				🚭 B	Browse		
Server Connection Data: FNCESUNdomain;AdminServer;JVMRuntime									
Addit	ional Options:	tions: IP_ADDRESS=127.0.0.1							
L			_						
		OF		Cancel	📓 Help				

Dialog to create a new server . The JMX tab.

The New Server dialog is called, when the New... button is pressed in the Hosts tab. The New Server dialog consists of several input fields which are explained in the following list.

Managed Host

This is the host which shall be defined in this dialog. The combo box contains all available CALA_REX clients. The Managed Host field also is editable to enter other servers which are not contained in the combo box.

Managing Host

The Managing Host needs further introduction:

As the FileNet P8 4.x/5.x configuration also must support server farms and clusters, the Managing Host is used. Farms and clusters are a collection of several servers which appear as only one machine to the other servers and clients in the network. So it may not be possible to request information of these machines directly in some cases. The only interfaces to these machines are JMX and FileNet Listener technology. The JMX and Listener requests are executed by the server which is accessible in the network. This server is called the Managing Host and requests the JMX and FileNet Listener parameters.
If a host is Managing Host itself and is not managed by another machine, the Managed Host and the Managing Host are the same machine. The combo box contains all servers which are already defined.

Description

In the description field it is possible to enter some comments about the server (for example if it is part of a cluster or what the name of the cluster is).

Java Path

This is the path of the Java which shall be used. A Java version 6 or higher is required.

NOTE If the host is an Application Engine where monitoring for the Component Manager will be activated, make sure that you specify the path to the Java installation of the Component Manager. Otherwise the Component Manager monitors may fail.

Copy from... Button

This button opens the **Copy Server From...** dialog which makes it possible to copy a whole server configuration of an already existing server.

JMX Tab

The JMX tab is used to define several JMX instances.

Listener Tab

The Listener Tab is used to define FileNet Listener parameters.

The JMX Tab

A server can have several JMX instances. These instances are defined in the JMX tab of the New Server dialog. The following fields can be configured and the following buttons are available to configure the instances:

Instance

The combo box contains all already defined instances of this server. When creating a new server this combo box will be empty. To create a new instance, the **New...** button has to be pressed. The instances can be switched via the combo box. All instances in this combo box are defined for the server (not only the selected instance).

Application Server Type

The following application servers are supported:

- Oracle WebLogic 7
- Oracle WebLogic 8
- Oracle WebLogic 8 via webservice

- Oracle WebLogic 9, 10, 11
- Oracle WebLogic 9, 10, 11, 10 or 11 via webservice
- IBM WebSphere 5
- IBM WebSphere 6
- IBM WebSphere 6 via webservice
- IBM WebSphere 6.1
- IBM WebSphere 6.1 via webservice
- IBM WebSphere 7, 8 or 8.5 via webservice

A WebService based connection to a application server, which has the *applicationserver.jmx.monitor.war* / ~.ear application running. In this case the **ServiceUrl** has to be used instead of **host** and **port**. For further information about how to install the functionality on WebSphere, refer to the *Install Guide*, chapter *Preparing JMX Monitoring*.

The difference between the "<AppServer> via webservice" and the "Webservice" item in the combobox is, that the "<AppServer> via webservice" items support further functionality like the "View AE Status" task. If the JMX webapplication is deployed on a server, which is not listed in the combobox explicitly, it can be used the "webservice" item.

- Red Hat JBoss 4
- Red Hat JBoss 4 via JSR160
- Red Hat JBoss 4 via webservice

Service URL (depends on connection type)

For the WebService connection the ServiceUrl must have the following format: http(s)://<ip>: context_root>

The values for host, port and contextroot depend on your configuration, described in the *Install Guide*, chapter *Preparing JMX Support*, section *JMX Support via WebService*.

Defaults for WebSphere are:

- port for HTTP: 9080
- port for HTTPS: 9443
- **context_root**: *jmxmonitor*

Defaults for WebLogic are:

- port for HTTP: 7001
- **context_root**: applicationserver.jmx.monitor

Defaults for JBoss are:

- port for HTTP: 8080
- **context_root**: applicationserver.jmx.monitor

Port (depends on connection type)

This is the JMX port the software connects to. It is used in combination with the host field. (depends on connection type)

- Oracle WebLogic 7, 8, 9, 10, 11
 7001 per default (WebLogic server port) In productive environments the ports may be set to 7010, 7011...
- IBM WebSphere 5, 6 and 6.1 (bootstrap port) 2809 per default
- JBoss 3, 4, 5 1099 per default (RMI Port)

Most times the ports are set manually by the admins choice in productive environments.

JMX User (depends on the application server security settings)

The user name of the user that is defined in the application server, to access MBeans, if security is enabled on the server.

NOTE On WebSphere 6.1.x.x SSL is activated per default. In this case the user and password field have to be left empty and the credentials have to be entered in the sas.client.props file and the ssl.client.props file. For more information about these files please refer to the chapter "Preparing JMX Support - How to create the keystore and truststore files for WebSphere 6.1.x.x" in the install guide.

Password (depends on the application server security settings)

The password for JMX access.

Timeout (Optional)

The timeout defines a time after which the operation shall cancel automatically. The timeout must be given in seconds. If no timeout is defined, 40 seconds are used as default.

Path to Java

As Oracle WebLogic 9, 10, 11 as well as WebSphere 5 and 6 use their own Java to access JMX, the Java path of the server can not be used. Therefor the Java path of the application servers must be entered here.

- WebLogic 7 The default system Java path can be used
- WebLogic 8
 The default system Java path can be used except WebLogic 8 runs with the Oracle own JRockit Java version. The this version can be used.
- WebLogic 9, 10, 11

 .../bea/jdk15x_xx
 .../bea/jrokitxx_xxx_xx
- WebSphere 5, 6, 6.1

<WebSphereHome>/AppServer/java

- IBM WebSphere 7, 8, 8.5 <CENIT_ROOT>/jre
- JBoss 4

The default system Java path path can be used. It is recommended to use the same java which is used by the JBoss.

webservice

The Java of the WebSphere Application Server must not be used. It is recommended to use the Java, which is shipped with the product. Alternatively it is recommended to use a different IBM or Oracle JRE with at least Version 6.

Path to server Libs

This is the path to the libraries which are needed by JMX to get a JMX connection to the application server. The paths can be found as follows.

- Oracle WebLogic 7, 8 and 9
 <WebLogicHome>/server/lib
- IBM WebSphere 5, 6, 6.1 <WebSphereHome>/AppServer
- IBM WebSphere 7, 8, 8.5 Since this server is used in WebService context, use the path to the JRE, which is used in here.

Server Connection Data (depends on connection type)

The MBean Java program needs several parameters to establish the connection to the application server. The instances need the following parameters depending on which application server is chosen:

- Oracle WebLogic 7 <Domain>;<Server>
- Oracle WebLogic 8
 <Domain>;<Server>
- Oracle WebLogic 9, 10, 11
 Java type may be JRockitRuntime if JRockit is used or JVMRuntime if a standard JVM is used.
 WebLogic shows in the startup console output which Java version is used.
- IBM WebSphere 5
 <Server>;<Node>;<Cell>;<Version>
- IBM WebSphere 6
 <Server>;<Node>;<Cell>;<Version>;<MessageListenerThreadPool-ID>;<ORBThreadPool-ID>;<WebcontainerThreadPool-ID>
- IBM WebSphere 6.1
 Server>;<Node>;<Cell>;<Version>;<MessageListenerThreadPool-ID>;<ORBThreadPool-ID>;<WebcontainerThreadPool-ID>;<TCPChannelsThreadPool-ID>

- IBM WebSphere 7, 8, 8.5 <Server>;<Node>
- RedHat JBoss 4

 <a href="https://www.selimation.com/selimation.
 - **CAUTION** <Server> is not the computer name of the machine, where the server is running, but the virtual server inside the application server environment.

Additional Options (Optional)

This parameter can contain several key value pairs. This field is only used if the basic configuration needs special treatment. Several key-value pairs are separated via semicolon. Example: *key1=value1;key2=value2*.

SAS_PATH=<path_to_sas_file> - Is used by WebSphere application servers (5.x, 6.0.x.x, 6.1.x.x) when security is enabled. For further information please check the manuals. The path usually is on \$WAS_ROOT/AppServer/profiles/<profilename>/properties. If no path is given, the monitors will check if there exists a sas.client.props file in \${CENIT_ROOT}/cala/mon-itors/pam/properties.

IP_ADDRESS=<ip_address_to_connect_to> - For cluster environments the hostname is not usually the address to which can be connected with the jmx client. Enter the IP address of the virtual server to which shall be connected here.

CAUTION On WebSphere 6.1 SSL is activated per default. A keystore and truststore must be created. Please check the *Install Guide*, chapter *Preparing JMX Support - How to create the keystore and truststore files for WebSphere 6.1.x.x.*

For more information about how to configure the *sas.client.props* file refer to the *Install Guide*, chapter *Preparing JMX Support - How to Configure sas.client.props for WebSphere*.

The New... button

Clicking on this button will open the New Instance dialog to create a new JMX instance.



Create a new instance

The Copy From... button

Clicking on this button will open the **Copy Instance from** dialog to copy an existing instance configuration of the current server into the currently selected instance. It is not possible to copy instances from other instances.



The Copy Instance From... dialog

The Delete button

Clicking on this button will delete the currently selected instance.

The Listener Tab

Managed Host:	tivsunblade	-	🚯 Copy from
Managing Host:	tivsunblade		-
Description:			
Java Path	/usr		📾 Browse
JMX Liste	ner		
Listener Port	Ok Cancel 🕅 Help		

The Listener Tab in the New Server dialog

The **New Server** dialog also contains a **Listener** Tab, where FileNet Listener specific configuration can be made. The following parameters are available

Listener Port

The FileNet Listener Port. If nothing is entered the default Listener port will be used. In case more than one listener for the same application is running on the server you should read Special port configurations for PCH in case of multiple instances of the same application

Hosts Edit... button

The hosts edit button will also open the **New Server** dialog with the configuration of the server currently selected in the tree. The first instance of the data list will be pre selected. If an instance was selected in the tree when clicking the button, the dialog will open with the server and the instance pre selected. If the system (root element) is chosen when clicking the edit button, nothing will happen.

Hosts Delete... button

If a server is selected, the server and all its instances will be deleted. Also all associated web environments and products are affected by this. A confirmation dialog with an appropriate warning will be shown before the host is deleted. If an instance is selected when pressing the delete button, only the instance will be removed. Again web environment and products will be affected by this. If the last instance of a server is deleted, the server will also be deleted automatically because a server without instance is forbidden.

The New Web Environment dialog - New... environment button

The following image shows the infrastructure tab with the **Environments** tab selected.

System: Tivsunblade		•	🔇 New	🗊 Delete	関 Help
Infrastructure Products					
Hosts Environments					
Tivsunblade				6) New
🥐 🎯 Envi – 🥏 tivsunbladeInstance				D)	Edit
				1	Delete
					Help
	🗗 Ok 🥘 Cancel				

The Environments tab in the main config window

Pressing the New... button in the Web Environment tab will open the New Web Environment dialog.

Name:	Env1
instances:	tivsunbladeInstance on tivsunblade
Admin Server	tivsunblade 🔹
	Ok Cancel 🛛 Help

The New Web Environment dialog

In this dialog the following parameters can be defined and actions can be performed:

Name

Define the name of the web environment. It is not allowed enter an already used name. In edit mode it is possible to rename the web environment by entering another name.

Instances

In this selection box one or several instances must be chosen. It is not allowed to chose no Instance at all. It is allowed to define one instance in two different web environments.

To choose several elements hold down the Ctrl key on the keyboard and select several elements by clicking them. Release the Ctrl key after selecting the needed instances.

Admin Server

This combo box shows all servers which are associated with the displayed instance. Out of these, an admin server can be defined which is the master host (the host which does the load balancing) in a cluster environment.

ΟΚ

Clicking the OK button will close this dialog and store the made changes to the system.

Cancel

Clicking the Cancel button will close the dialog without saving the changes to the system.

After a web environment was defined, the products tabs are enabled and can be edited now.

Environments Edit... button

The Edit button will also call the New Web Environment dialog and load the environment currently selected in the tree.

Environments Delete... button

The **Delete** button will delete the environment which is selected in the hierarchy tree. This environment will be lost for all products. A warning dialog will ask for confirmation before the environment is deleted. If an instance is selected and deleted, this instance also will be lost for all products which use the environment. If the last instance from an environment is deleted, the environment will automatically be deleted too.

The Products Tab

In the **Products** tab the configuration for the IBM FileNet P8 applications / products is made. Every product or component has its own tab, just as Content Engine, Application Engine, Process Engine, Component Manager and Process Analyzer.

NOTE Even though the PE and CE have been merged in CPE 5.2, ECM SM still monitors these components independently. For this reason, the PE and CE components of CPE 5.2 must be configured on different product tabs..

Product Tab	CPE 5.2 - CE part	CPE 5.2 - PE part	P8 5.0 / 5.1 CE	P8 5.0 / 5.1 PE	P8 4.5 CE	P8 4.5 PE
→ Sub Tab	•					
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part)	1	-	✓	-	✓	-
→ FileNet						
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part)	1	-	1	-	1	-
→ Listener						
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part)	1	-	1	-	1	-
→ JMX						
PE 4.x / Listener for PE 5.x	-	-	-	-	-	1
→ FileNet						
PE 4.x / Listener for PE 5.x	-	1	-	1	-	1

Product Tab	CPE 5.2 - CE part	CPE 5.2 - PE part	P8 5.0 / 5.1 CE	P8 5.0 / 5.1 PE	P8 4.5 CE	P8 4.5 PE
→ Sub Tab	on part	i i part	011 02	0	02	
→ Listener						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	✓	-	1	-	-
→ General						
PE 5.0, 5.1, CPE 5.2 (PE part)	✓	✓	1	1	-	-
→ Security						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	✓	-	1	-	-
→ Database						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	-	-	-	-	-
→ Server Connections						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	✓	-	1	-	-
→ Advanced						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	1	-	1	-	-
→ Server						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	-	-	-	-	-
→ Listener						
PE 5.0, 5.1, CPE 5.2 (PE part)	-	1	-	-	-	-
→ Region						

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) Product Tab

Tools					
System: P8_52		-	🔕 New	💥 Delete	🕜 Help
Infrastructure Products					
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) pplication Engine	PE 4.x / Listener for PE 5.x	PE 5.0, 5.1, CPE 5.2 (PE part)	Component Man	ager Proces	s Analyzer
Name: Engine-wi					🕐 Help

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) Product Tab

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) tab is used to configure the parameters of the Content Engine as well as the Web Application Server part of the Content Process Engine (CPE). It is only possible to define one single Content Engine per system. This Content Engine is running in one WebEnvironment with possibly several servers and several instances. The following parameters can be defined:

Name

Enter the name of the Content Engine here. The name can be chosen arbitrarily.

Web Environment

The WebEnvironment where the Content Engine is running in can be chosen here. Only one WebEnvironment can be defined for the Content Engine. If another one is chosen, the settings of the current one are discarded.

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) FileNet Tab

Name:	Engine-wl	関 Help
Web Environment:	Env1	-
FileNet Lister	er JMX	
Server:	ti muhlada	
CE Install Dath		
CE Ilistali Patri.	/disk2/opt/FileNet/ContentEngine	📾 Browse
FileNet Common Ir	stall Directory: //disk2/opt/FileNet/AE/CommonFiles	📾 Browse
CE User:	Administrator	
CE Password:	•••••	
<u>['</u>	D Ok Ocancel	

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) FileNet Tab

Server

There can be several servers defined for the Content Engine. Every server has its own set of parameters.

CE Install Path

The path were the Content Engine is installed on the server.

FileNet Common Install Directory

The directory of the common FileNet resources.

CE User

Enter the user name for the Content Engine here. The user specified here must have permission to log in to the FileNet Enterprise Manager with read access.

CE Password

Enter the password for the Content Engine user here. The password will be encrypted. If no user is given, the password won't be stored.



Name:	En	gine-wl							🕗 Help
Web Enviro	nment: En	/1						-	
FileNet	Listener	JMX							
Server:		tivsunb	lade		 			 	
Application	Name:	CEMP	Daphne	Server1					
Application	Instance:	CEMPI	nstance	1					
					 		1	 	
					🚺 Ok	🔤 Cancel			

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) Listener Tab

Server

This product can have several servers on which the FileNet Listener can be requested. Please select the server which you want to configure. It is possible to configure several servers.

Application Name

Please enter the application name whose data shall be requested via the FileNet Listener.

Application Instance

Please enter the application instance whose data shall be requested via the FileNet Listener.

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) JMX Tab

Content Engine	Application Engine	Process Engine	Component Manager	Process Analyzer	
Name:	Engine-wl				😰 Help
Web Environment:	Env1				
FileNet Listen	er JMX				
Instance:	tivsunbladeInstance				 -
Instance: Application Name:	tivsunbladeInstance Engine-wl				
Instance: Application Name: Application War Fil	tivsunbladelnstance Engine-wl				
Instance: Application Name: Application War Fil	tivsunbladelnstance Engine-wl e:				
Instance: Application Name: Application War Fil	tivsunbladelnstance Engine-wl e:				•
Instance: Application Name: Application War Fil	tivsunbladeInstance Engine-wi e:				•
Instance: Application Name: Application War Fil	tivsunbladelnstance Engine-wl e:				.
Instance: Application Name: Application War Fil	tivsunbladelnstance Engine-wl e:				
Instance: Application Name: Application War Fil	tivsunbladelnstance Engine-wl e:				•
Instance: Application Name: Application War Fil	tivsunbladeInstance Engine-wl e:				

The CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) JMX Tab

Instance

This product can have several instances on which JMX can be requested. Please select the instance which you want to configure. It is possible to configure several instances.

Application Name

Enter the Application whose status shall be monitored in this field. The default application name is *FileNetEngine*.

Application War File

WebSphere only: The JMX program also needs the war file name of the application. The Content Engine default war file names are *Engine-init.war* and *wsi-ws.war*. Some applications also have several war file names. In this case, the war files are separated via semi colon.

The Application Engine Product Tab

Tools									
System:	P8_52					•	🕘 New	💢 Delete	🕜 Help
Infrast	tructure	Products							
CE 4.x	, 5.0 , 5.1, C	PE 5.2 (CE part) 🤇	Application Engine	PE 4.x / Listener for PE 5.x	PE 5.0, 5.1, CPE 5.2 (PE part)	1	Component Man	ager Proces	s Analyzer
Name:		Workplace	\sim			-	🥂 New	💥 Delete	😢 Help

The Application Engine Product Tab

Name

It is possible to create several Application Engines. Click the **New...** button to open the **New System** dialog. It contains a field to enter the Application Engine name and a combo box to select the Application Engine's web environment. If there are already any Application Engines defined in the current system the **Copy From...** combo box is filled with the Application Engine configurations which can be copied.

NOTE The name of the Application Engine MUST BE the real name of the Application Engine, under which the application will be requested in the web browser, For example *Workplace*.

System:	
Web Environment:	: fwef 🔹 💌
Copy From	
(Ok Cancel

Create a new Application Engine system

Web Environment

This field is read only. If another web environment shall be used, a new Application Engine must be defined by pressing the **New...** button.

The Application Engine FileNet Tab

Name:	Workplace		-	🕻 New	🗊 Delete		🛿 Help
Web Environment:	Env1						
FileNet Lister	ier JMX						
Server:		tivsunblade					-
AE Install Path:		/disk2/opt/FileNet/AE				🖼 E	Browse
FileNet Common Ir	istall Directory	/disk2/opt/FileNet/AE/CommonFiles				📾 E	Browse
AE User:		Administrator					
AE Password:		•••••					
<u> </u>		🗘 Ok 🛛 🙆 Cancel					

The Application Engine FileNet Tab

Server

There can be several servers defined for the Application Engine. Every server has its own set of parameters.

AE Install Path

The path where the Application Engine is stored on the application server

FileNet Common Install Directory

The directory of the common FileNet resources.

AE User

Enter the user name for the Application Engine here.

AE Password

Enter the password for the Application Engine user here. The password will be encrypted. If no user is given, the password won't be stored.

The Application Engine Listener Tab

Name: V	Vorkplace		-	New	💥 Delete	🙆 Help
Web Environment: E	inv1					
FileNet Listene	er JMX					
Server:	tiveunblado					
Application Name	Workplace					
Application Instance	e:					
		🕄 Ok 💿 Cancel				

The Application Engine Listener Tab

Server

This product can have several servers on which the FileNet Listener can be requested. Please select the server which you want to configure. It is possible to configure several servers.

Application Name

Please enter the application name whose data shall be requested via the FileNet Listener.

Application Instance

Please enter the application instance whose data shall be requested via the FileNet Listener.

The Application Engine JMX Tab

Name:	Workplace		-	👫 New	🗊 Delete	🛿 Help
Web Environment:	Env1					
FileNet Listen	er JMX					
Instance:	tivsunbladeInstance					-
Application Name:	Workplace					
Application War Fil	e:					
		🕞 Ok 🔘 Cancel				

The Application Engine JMX Tab

Instance

This product can have several instances on which JMX can be requested. Please select the instance which you want to configure. It is possible to configure several instances.

Application Name

Enter the Application whose status shall be monitored in this field. The default application name is *Workplace*.

Application War File

WebSphere only: The JMX program also needs the war file name of the application. The default war file name is *Workplace.war*. Some applications also have several war file names. In this case, the war files are separated via semi colon.

The PE 4.x / Listener for PE 5.x Product Tab

Tools				
System: P8_52	•	New	💥 Delete	🕜 Help
Infrastructure Products				
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) Application Engine PE 4.x / Listener for PE 5.x PE 5.0, 5.1, CPE 5.2 (PE part)	1	Component Man	ager Proces	s Analyzer
Name: PE1	•	े New	💥 Delete	🕜 Help

The PE 4.x / Listener for PE 5.x Product Tab

Name

It is possible to define several Process Engines. Click the **New...** button to open the **New System** dialog. There is only a field to input the Process Engines name. Clicking **OK** will create the Process Engine. The **Cancel** button closes the dialog without creating a new configuration entry.

-			
Name:			
			1
	Ok	Cancel	

Dialog to create a new PE System

Server

A Process Engine can have several servers. Click the New..." button to open the Add New Server To System dialog. Choose one of the available servers. The Copy From... combo box provides already existing servers. Chose the server from which the configuration shall be copied from. Clicking OK will quit the dialog and save the server. The Cancel button closes the dialog without creating a new configuration entry..



Dialog to choose a server for the Process Engine

The PE 4.x / Listener for PE 5.x FileNet Tab

Name: PE 1		-	👫 New	🗊 Delete	🛿 Help
Server: tivhp11i.dud.cenit.de		-	🕵 New	🗊 Delete	
FileNet Listener					_
IS Domain:	tivhp11i:FileNet				-
FileNet Common Install Directory	/opt/FileNet/CommonFiles				Browse
PE User:	Administrator				
PE Password:	•••••				
PE Communication Port:	32776				
PE Broker Port:	32777				
Locale:	en				
Debug:	On / Off:				
CE Connection Point:	tivhp11i				
Component Manager Host:	tivsunblade				
Component Manager Event Port:	32773				
Rules Host Name:					
Rules Port:					
Full Workflow Functionality:	🖌 On / Off:				
Number of VWKS Processes:	10				
PE Registry Port:	32771				
1	Concel				

The PE 4.x / Listener for PE 5.x FileNet Tab

IS Domain

Select one of the previously configured IS Domains from the list.

FileNet Common Install Directory

Define the PE common installation directory, for instance /opt/FileNet/CommonFiles on UNIX systems of C:/Program Files/FileNet/CommonFiles for WIndows systems.

PE User

Enter the user name for the Process Engine here. This user requires access to tools like vwtool or vwspy and must have permission to log in to the Process Engine..

PE Password

Enter the password for the Process Engine user here. The password will be encrypted. If no user is given, the password won't be stored.

PE Communication Port

Enter the Process Engine Communication port here. Default value is 32776.

PE Broker Port

Enter the Process Engine Broker port here. Default value is 32777.

Default Locale

Specify the default locale of the Process Engine system. See IBM FileNet Process Engine documentation for more details.

Debug

Enables (checked) / disables (not checked) the debugging of the Process Engine.

CE Connection Point

Specify the CE Connection points separated by semicolon (;).

Component Manager Host

Enter the name of the system running the connected Component Manager.

Component Manager Event Port

Enter the Component Manager Event port here. Default value is 32773.

Rules Host

Enter the name of the Rules Engine host here.

Rules Port

Enter the Component Manager Event port here. Default value is 32774

Full Workflow Functionality

Specify whether the Process Engine runs in full Workflow mode or not.

Number of VWKS Processes

The number of VWKS processes.

PE Registry Port

Enter the Process Engine Registry port here. Default value is 32771.

The PE 4.x / Listener for PE 5.x Listener Tab

Name: Process Engine		-	🤗 New	💥 Delete	🕐 Help
Server: tivsunblade		-	謽 New	💥 Delete	
FileNet Listener					
Application Instance:					
	🕄 Ok 📾 Cancel				

The PE 4.x / Listener for PE 5.x Listener Tab

The following parameters are available for the Process Engine Listener configuration.

Application Name

Enter the application name whose data shall be requested via the FileNet Listener here. As the Process Engine has servers itself, there is no additional combo box to select the server

Application Instance

Please enter the application instance whose data shall be requested via the FileNet Listener.

The PE 5.0, 5.1, CPE 5.2 (PE part) Product Tab

Tools						
System: P8_52			•	▼ 🥥 New	💥 Delete	🕜 Help
Infrastructure Products						
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part)	Application Engine	PE 4.x / Listener for PE 5.x	PE 5.0, 5.1, CPE 5.2 (PE part)	Component Ma	nager Proces	s Analyzer
Name: DE01-Stgt				' 🤮 New	💥 Delete	😢 Help



Name

It is possible to define several Process Engines or the Process Egine side of the Content Process ENgine (CPE). Click the **New...**" button to open the **New System** dialog. There is only a field to input the Process Engine's name. Clicking **OK** will create the Process Engine. The **Cancel** button closes the dialog without creating a new configuration entry.

Name:			
	Ok	Cancel	

Dialog to create a new PE System.

The PE 5.0	, 5.1	CPE 5.2	(PE	part)) Main	Settings	Tabs

Name: DE01-Stgt				-	🤗 New	💥 Delete	🕜 Help
General Securi	ty Database	Server Connections	Advanced				
Virtual Server Name	default						
Main Port:	32777						
Naming Service Port	32776						
Server Virtual Host:	w2k8x64r2pe50.	filenet50.de					
Date/Time Mask:	mm/dd/yyyy hh:tt:	SS					
Default Locale:	en_US						-
Server Regions							
Server Instance: w2	k8x64r2pe50.filer	net50.de		•	謽 New	💥 Delete	🕗 Help
Server Listene	r						
CALA_REX Client: OS User: PE Installation Direc PE CE-Client API Ins JDBC Driver Path: Set As Primary Serv Thread Pool Size: Advanced Settings:	tory: tallation Directory ver?	w2k8x64r2pe50.filen F:/FileNet/ProcessEng F:/Filenet/Common Fil F:/FileNet/ProcessEng	et50.de iine es iine/lib/JDBC				
		[7]	Ok 📾 Ca	ncel			

The PE 5.0, 5.1, CPE 5.2 (PE part) Main Settings Tabs

The General Settings Tab

Name: DE01-Stgt	lame: DE01-Stgt 🔹 🔮 New 💥 Delete 🔞 Help								
General Secu	rity Database	Server Connections	Advanced						
Virtual Server Nam	e: default								
Main Port:	32777								
Naming Service Po	rt: 32776								
Server Virtual Hos	* w2k8x64r2pe5).filenet50.de							
Date/Time Mask:	mm/dd/yyyy hh:	ttiss							
Default Locale:	en_US							-	

The Process Engine 5.x General Settings Tab

The following parameters are available for the Process Engine General settings. All parameters can be taken from the IBM 'Process Task Manager' GUI installed on each PE system.

Virtual Server Name

Add the Virtual Server name.

NOTE The PE default value of the first PE is normally *default*.

Main Port

Optional; reserved for future usage.

Specify the PE main port. The default value is 32777

Naming Service Port

Specify the PE Naming Service port. The default value is 32776

Server Virtual Host

Add the hostname of the system the PE runs on

Date / Time Mask

Optional; reserved for future usage.

Specify the value from the corresponding 'Process Task Manager' GUI field.

Default Locale

Optional; reserved for future usage.

Here you will see a selection of locales. Select the default locale of the Process Engine system. Specify the default locale of the Process Engine system. See FileNet P8 Process Engine documentation for more details.

The Security Settings Tab

Name: DE01-Stgt					-	📑 New	💥 Delete	🕗 Help
General Secu	rity Database	Server Connections	Advanced					
Content Engine UR	l: https://w2k8x64r	2aece.filenet50.de:9443	/wsi/FNCEWS	40MTOM/				
Service Username	p8admin							
Service Password								
Administrator Gro	.ip: p8admins							
Configuration Grou	ıp:							

The Process Engine 5.x Security Settings Tab

The following parameters are available for the Process Engine Security settings.

Content Engine URL

Enter the URL of the IBM Content Engine connected to your PE.

Service Username

Enter the user name used to start the PE component.

Service Password

Specify the password of the Service user.

Administrator Group

Optional; reserved for future usage.

Specify the PE Administrative group name.

Configuration Group

Optional; reserved for future usage.

Enter the Configuration group name, if configured in the 'Process Task Manager' GUI.

The Database Settings Tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Name: DE01-Stgt				•	📑 New	💥 Delete	🕗 Help
General Security	Database	Server Connections	Advanced				
Database Type:	DB2						-
Database Version:	DB2LUW						-
Database Name:	PEDB						
Data Tablespace:	PEDB_TS						
Index Tablespace:							
Blob Tablespace:							
Database User Name:	db2admin						
Database Password:	•••••						
Database Host:	w2k8x64r2pe5().filenet50.de					
Database Port:	50000						
JDBC Driver URL:							

The Process Engine 5.x Database Settings Tab

The following parameters are available for the Process Engine Database settings.

Database Type

Here you will see a selection of supported database types. Select the one used by the Process Engine. The selection made will have an effect on the other fields of this tab.

Database Version (DB2 only)

Optional; reserved for future usage.

Here you will see a selection of DB2 database types. Select the one appropriate for the Process Engine's DB2 database (*DB2LUW* for UNIX, Linux and Windows based DB2 server, otherwise select *DB2zOS*).

Database Name

Specify the name of the PE database.

Data Tablespace (DB2, Oracle)

Optional; reserved for future usage.

Specify the tablespace used for the PE.

Data File Group (MSSQL)

Optional; reserved for future usage.

Specify the configured MSSQL data file group for the PE.

Index Tablespace (DB2, Oracle)

Optional; reserved for future usage.

Enter the DB2 or Oracle index tablespace.

Index File Group (MSSQL)

Optional; reserved for future usage.

Enter the MSSQL Index file group name for the PE (if used).

Blob Tablespace (DB2 only)

Optional; reserved for future usage.

Specify the DB2 Blob tablespace.

Database User Name

Specify the Database user name which is used by the Process Engine

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Database Password

Specify the Database users password for PE

Database Host

Specify the database host that runs the PE database

Database Port

Define the database port used for the connection

JDBC Driver URL

Specify the JDBC Driver URL for the configured PE

The Server Connections Settings Tab

Name: DE01	Stgt				•	謷 New	💥 Delete	🕜 Help
General	Security	Database	Server Connections	Advanced				
		. —			 			
Component	Manager Ho	ist: w2k	8x64r2aece.filenet50.d	e				-
Component	Manager Ev	ent Port: 327	73					

The Process Engine 5.x Server Connections Settings Tab

The following parameters are available for the Process Engine Server Connections settings.

Component Manager Host

Optional; reserved for future usage.

Here you will see a selection of hosts. Select the one, the Component Manager used by the Process Engine is installed at.

Component Manager Event Port

Optional; reserved for future usage.

Specify the Component Manager Event port. The default value is 32773.

The Advanced Settings Tab

Name: DE01-Stgt	-	New	💥 Delete	🔞 Help
General Security Database Server Connections Advanced				
Cluster Configuration:				
PE Server to Server Communication Port:				
Advanced Settings:				

The Process Engine 5.x Server Connections Settings Tab

The following parameters are available for the Process Engine Advanced settings.

Cluster Configuration

Checkbox to activate/deactivate cluster configuration.

PE Server to Server Communication Port

Optional; reserved for future usage.

Specify the PE server to server port

Advanced Settings

Optional; reserved for future usage.

Textfield to enter advanced configuration settings. The settings must be entered line by line as key-value-pairs separated by an equal sign (<key>=<value>).

The PE 5.0, 5.1, CPE 5.2 (PE part) Server Settings Tabs

Here you define the specific settings for each Process Engine installation on a dedicated server.

Each server to configure must be added to the PE system as a Server Instance:

Server Instance

It is possible to define several servers a Process Engine is installed at. Click the New... button to open the New Server dialog.

That dialog shows two selections: **Available Server** to select a server, and **Copy configuration from...** The latter contains already defined servers whose configurations can be used as a template to fill the server's settings in the configuration. Exactly one server can be used as a template. Clicking **Ok** will create the new server using the selected one from **Copy configuration from...** for default values of the new server. Clicking **Cancel** will close the dialog without creating a new server.

The **Delete...** button will remove the currently selected server. The **Help** button will open the help dialog.

The Process Engine 5.x Servers Server Configuration Tab

Server Regions				
Server Instance: w2k8x64r2pe50.	ilenet50.de	🔻 📑 New	💥 Delete	🕜 Help
Server Listener				
CALA_REX Client:	w2k8x64r2pe50.filenet50.de			-
OS User:				
PE Installation Directory:	F:/FileNet/ProcessEngine			
PE CE-Client API Installation Direct	F:/Filenet/Common Files			
JDBC Driver Path:	F:/FileNet/ProcessEngine/lib/JDBC			
Set As Primary Server?	Yes			
Thread Pool Size:				
Advanced Settings:				
1				

The Process Engine 5.x Servers Server Configuration Tab

The following parameters are available for the Process Engine Server configuration.

CALA_REX Client

Here you will see a selection of CALA_REX hosts.

OS User (Unix only)

Specify the Process Engine operating system user that is used to start the PE processes.

PE Installation Directory

Specify the Process Engine installation directory.

PE CE-Client API Installation Directory

Specify the Process Engine related CE API directory. This is normally the CE_API directory located below the PE installation directory.

JDBC Driver Path

Specify the installation directory of the JDBC drivers to be used for PE.

Set As Primary Server?

Optional; reserved for future usage.

Here you define the current server as the primary server of the Process Engine. There can only be exactly one primary server. Selecting a server as a primary server while there already is a different primary server defined will remove this flag from the definition of that other server. De-selecting this checkbox will not lead to any changes of any other servers.

Thread Pool Size

Optional; reserved for future usage.

Specify the value of defined in the 'Process Task Manager' GUI.

Advanced Settings

Optional; reserved for future usage.

Textfield to enter advanced configuration settings. The settings must be entered line by line as key-value-pairs separated by an equal sign (<key>=<value>).

The Process Engine 5.x Servers Listener Tab

Server Regions		
Server Instance: w2k8x64r2pe50.filenet50.de	🔻 📑 New 🗱 🕻	Delete 🛛 📀 Help
Server Listener		
Application Name:		
Application Instance:		

The Process Engine 5.x Servers Listener Tab

The following parameters are available for the Process Engine Listener configuration.

Application Name

Enter the application name whose data shall be requested via the FileNet Listener here. As the Process Engine has servers itself, there is no additional combo box to select the server.

Application Instance

Please enter the application instance whose data shall be requested via the FileNet Listener.

The PE 5.0, 5.1, CPE 5.2 (PE part) Regions Settings Tab

Here you can define the regions of the Process Engine.

Server Regio	ns					
Region number: 2			•	🥂 New	💥 Delete	🕗 Help
CE Composition Do	inte a c					
CE Connection Po	Int: wfcn01					
Tablespace:	Default					
	Custom					

The PE 5.0, 5.1, CPE 5.2 (PE part) Regions Settings Tab

The following parameters are available for the Process Engine Regions configuration.

Region number

It is possible to define several regions for a Process Engine. Click the New... button to open the New Region dialog.

That dialog contains an input field to enter the region number. Clicking **Ok** will create a new region for the Process Engine. Clicking **Cancel** will close the dialog without creating a new region. If the user has entered an already existing region number, clicking **Ok** will do no changes to the system, leaving the already defined region unaltered.

The **Delete** button will remove the currently selected region. The **Help** button will open the help dialog.

CE Connection Point

Enter the name of the Content Engine Connection Point associated with this region.

Tablespace

Optional; reserved for future usage.

Allows the definition of the tablespace to be used by the region. The user can select **Default** which is also the default after creating a new region or **Custom**. When selecting **Custom**, the user must enter the name of the custom tablespace. Entering the special tablespace name default in the custom tablespace field is identical to selecting the **Default** tablespace checkbox.

The Component Manager Product Tab

Tools								
System: P8_52				🕘 New	💥 Delete	🕗 Help		
Infrastructure Products								
CE 4.x, 5.0, 5.1, CPE 5.2 (CE part) Application Engine PE 4.x / Listener for PE 5.x PE 5.0, 5.1, CPE 5.2 (PE part) Component Manager Process Analyzer								
Name: tivhp11i.CE_Operations			▼ [New	Delete	🕜 Help		

The Component Manager Product Tab

Name

It is possible to create several Component Manager systems. Click the **New...** button to open the **New System** dialog. It contains a field to enter the Component Manager name and a combo box to select the Component Manager's server. If there are already any Component Managers defined in the current system, the **Copy From...** combo box is filled with the Component Manager configurations which can be copied. The **Cancel** button closes the dialog without creating a new configuration entry.

Create a new Component Manager name:	
Server:	tivsunblade 🔹
Copy Server Configuration From:	
	tivhp11i.CE_Operations
Oli Canad	tivhp11i.WSRequest
OK Cance	

The New Component Manager Dialog

Server

The field is disabled. The server can only be changed via the **Change...** button. The change dialog has also the option to copy an already existing server configuration. After selecting a new server, click **OK** to leave the change dialog. There can be only one Server per Component Manager at one time.

The Component Manager FileNet Tab

Name: tivhp11i.CE_Operations		-	👫 New	🗊 Delete		🖹 Help	
Server: tivsunblade			🐵 Change				
FileNet							
Component Manager Install Path:	/disk2/opt/FileNet/AE/Router					Browse	
FileNet Common Install Path (Component Manager): /disk2/opt/FileNet/AE/CommonFiles					📾 Browse		
Component Manager Name:	tivhp11i.CE_Operations						
Component Manager OS User:							
Component Manager User:	Administrator						
Component Manager Password:	•••••						
Connection Point:	tivhp11i						
<u>[[</u>	🕞 Ok 🛛 🖲 Cancel						

The Component Manager FileNet Tab

Component Manager Install Path

The full path to the configuration file *vwtaskman.xml* of the Component Manager to manage.

Common values are:

Installation type	Installation directory
Workplace XT on Windows	C:/FileNet/WebClient/Router
Workplace on Win- dows	C:/FileNet/AE/Router
Workplace XT on UNIX	/opt/FileNet/WebClient/Router
Workplace on UNIX	/opt/FileNet/AE/Router

NOTE For backward compatibility, the Component Manager tasks and monitors check the subdirectories *AE/Router* and *Router* automatically for *vwtaskman.xml* if the file cannot be found in the specified directory.

FileNet Common Install Path (Component Manager)

Specify the Component Manager Common Install Path here. Default value on UNIX systems is / opt/FileNet/CommonFiles and C:/Program Files/FileNet/CommonFiles on Windows systems.

Component Manager Name

Enter the name of the Component Manager here.

NOTE Please enter the characters case sensitive.

Component Manager OS User (Unix only)

Specify the operating user that runs Component Manager software

Component Manager User

Enter the user name for the Component Manager here. Specify -1 if the user credentials defined within the P8 Process Task Manager should be used.

Component Manager Password

Enter the password for the Component Manager user here. The password will be encrypted. If no user is given, the password won't be stored. If -1 is defined for the user account this parameter is inactive.

Connection Point

Enter the name of the Connection Point here.

NOTE Please enter the characters case sensitive.

The Process Analyzer Product Tab

Tools					
System:	P8_52	•	🔕 New	💥 Delete	🕜 Help
Infras	ructure Products				
CE 4.)	, 5.0, 5.1, CPE 5.2 (CE part) Application Engine PE 4.x / Listener for PE 5.x PE 5.0, 5.1, CPE 5.2 (PE part	r	Component Man	ager Process	s Analyzer
Name:	PA Sys1 🗸		PNew	💥 Delete	🕐 Help

The Process Analyzer Product Tab

Name

It is possible to create several Process Analyzer systems. Click the New... button to open the New **System** dialog. It contains a field to enter the Process Analyzer name and a combo box to select the Process Analyzer's server. If there are already any Process Analyzers defined in the current system, the **Copy From...** combo box is filled with the Process Analyzer configurations which can be copied. The **Cancel** button closes the dialog without creating a new configuration entry.


The "New Process Analyzer" dialog

Server

The filed is disabled. The server can only be changed via the **Change...** button. The change dialog has also the option to copy an already existing server configuration. After selecting a new server, click **OK** to leave the change dialog. There can be only one Server per Process Analyzer at one time.

The Process Analyzer FileNet Tab

Name: PA Sys1		· · · · ·				-	🕞 New	🗊 Delete	ə	🛿 Help
server: w2kfsmen							🚸 Change			
FileNet PA Data	abase	PE Database								
Då Java Bathi										
PA Java Patr:	C:/Program Files/FileNet/Process Analyzer Engine/jpa									
PA Install Path:	C:/Prog	ıram Files/FileNe	et/Process An	alyzer Engir	ne/jre					Browse
FileNet User:	Admini	strator								
Password:	•••••	••••								
Content Engine URL	http://tiv	sunblade:7001A	vsi/FNCEW8	40DIME/						
1				⊡> Ok	Cancel	1				

The Process Analyzer FileNet Tab

PA Java Path

This is the path of the Process Analyzer's Java.

PA Install Path

Enter the path where the Process Analyzer is installed here.

FileNet User

Enter the user name for the Process Analyzer here.

Password

Enter the password for the Process Analyzer user here. The password will be encrypted. If no user is given, the password won't be stored.

Content Engine URL

Enter the Content Engine URL of the associated Content Engine here.

The PA Database Tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication see chapter "How to configure and use the UnifiedDatabaseClient (UDC)" in the Installation Guide.

Name: PA Sys1		-	👫 New	🗊 Delete	📓 Help
server: w2kfsmen			🚸 Change		
FileNet PA Databa	se PE Database				
Database Host:	w2kfsmen				
Database Port:	1433				
Database Instance:					
DB User Name:	pe_mssql_user				
DB User Password:					
JDBC Driver Classnath	Com.microsoft.jabc.sqlserver.SQLServer.2000 Driver for IDBC	lihim	ecoleoworiar C (Pr	ogram Files/Micros	off SOL Serve
obbo biiler elecepati		/10/11	issqiserver.jar,osr n	ogrammines/micros	
	🕞 Ok 🛛 🖲 Cancel				

The PA Database Tab

Database Host

Specify the name of the Process Analyzer database

Database Port

Specify the port of the PA database connection here.

Database Instance

Specify the PA Database Instance name here.

DB User Name

Enter the user name for the PA database user here.

DB User Password

Enter the password for the PA database user here. The password will be encrypted. If no user is given, the password won't be stored.

JDBC Driver Name

Enter the Process Analyzer JDBC Driver Name (Class) here. See FileNet P8 PA Documentation for further details. Copy the appropriate value from the PA task manager.

JDBC Driver Classpath

Enter the Process Analyzer JDBC Driver CLASSPATH settings here. See FileNet P8 PA Documentation for further details. Copy the appropriate value from the PA task manager.

The PE Database Tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Name: PA Sys1		-	📑 New	🗊 Delete	関 Help				
server: w2kfsmen			🕸 Change						
FileNet PA Databa	ise PE Database								
Databaga Tumar									
Database Type:	Oracle								
Database Host:	tivsun60								
Database Port:	1503								
Database Name:	VWdb								
DB User Name:	pe_db_user								
DB User Password:	•••••								
JDBC Driver Name:	oracle.jdbc.driver.OracleDriver								
JDBC Driver Classpath	C:\Program Files\FileNet\Process Analyzer Engine\jpa\ojdbc	14.ja	r						
		_							
	🕞 Ok 🥥 Cancel								

The PE Database Tab

Database Type

Choose one of the databases which are supported: (MSSQL, DB2 and Oracle)

Database Host

Specify the name of the Process Engine database host here.

Database Port

Specify the port of the Process Engine connection here.

Database Name

Enter the PE Database name here (default value is VWdb)

DB User Name

Enter the user name for the PE database user for the PA connection here.

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

DB User Password

Enter the password for the PE database user here. The password will be encrypted. If no user is given, the password won't be stored.

JDBC Driver Name

Enter the Process Engine JDBC Driver Name (Class) here. See FileNet P8 PA Documentation for further details. Copy the appropriate value from the PA task manager.

JDBC Driver Classpath

Enter the Process Engine JDBC Driver CLASSPATH settings here. See FileNet P8 PA Documentation for further details. Copy the appropriate value from the PA task manager.

Special port configurations for PCH in case of multiple instances of the same application

The following applies to the situation more than one PCH listener for the same product, but different instances, is up and running on the same machine. E.g. more than one CE or PE of the same version.

In case of that, the listener monitors and tasks cannot distinguish the different paths for the different instances of the same product version. To distinguish these, the configuration of the PCH ports of these instances must be changed to not use the default ports, like it is described in the following.

For PE and IS - both P8 4.5 and below (non-application server products)

If not already done, enable PCH with these steps:

- Go the sd directory to see if a perf_mon.script file exists. UNIX: /fnsw/local/sd. Microsoft Windows: <drive:>\fnsw_loc\sd (Windows).
- If a perf_mon_script already exists, skip the next step.

- If a perf_mon_script does not exists, create one by copying it from the lib/perf directory. UNIX: cp /fnsw/lib/perf/perf_mon.script /fnsw/local/ sd/perf_mon.script. Microsoft Windows: copy <drive>:\fnsw_loc\sd \perf_mon.script <drive>:\fnsw_loc\sd\perf_mon.script.
- From the sd directory edit the perf_mon_script file to make the first command line of the script file to be "set listener true". Your edited file might look similar to this example:

```
0001 # stamp
0002 #
0003 set listener true
0004 schedule 0 0:00:00 2:00:00
0005 schedule 0 6:00:00 0:15:00
0006 schedule 0 19:00:00 2:00:00
0007 schedule 1 0:00:00 2:00:00
0008 link 0 1
0009 link 1 0
0010 link 2 0
0011 link 3 0
0012 link 4 0
0013 link 5 0
0014 link 6 1
0015 poll /fnsw/local/sd/1/perflog
0016 echo done
0017 # stamp d;lkfjpojr;wohf
```

Save and Exit the file.

Change the primary port:

Setting the environment variable called PCHPORT to the desired port.

Restart the Image Services / PE software.

The Listener will start automatically and will use the defined port.

For CE and AE on IBM WebSphere

How to change the default listener port (32775) on CE and AE (and any other) JVMs.

P8 applications (CE, PE, Workplace, WorkplaceXT, etc) and Image Services have the ability to output certain performance metric data. The P8 System Manager and ECM SM products both use the PCH Listener metrics to gather data and report this data. An example of a single metrics is:

/P8 Content Engine/USER/BusinessInsurance/Security Descriptor Cache/Cache Hit Count,1667,4,Apr 15, 2009 10:17:56 AM,1239805076695

For instance, "1239805076695" corresponds to April 15, 2009 10:17:56.695, the timestamp since the application was started. You will also note the number "4" after the value of "1667". This number is used by the System Manager Dashboard to determine what category the counter belongs to. The categories are RPC, DISK, NETWORK, CPU, and USER.

```
0001 RPC=0
0002 DISK=1
0003 NETWORK=2
0004 CPU=3
```

0005 USER=4

There is nothing else in the task output that identifies what JVM the counter belongs to when multiple JVM's are running on the same physical node using the same IP address. This presents a problem when setting up monitors for systems with multiple of the same type of JVM running on the same OS. If the customer has 4 CEs running on the same server, the Listener task and monitors will return 4 values for each counter. This is due to the fact that all 4 CEs are using the same default listener port (32775). At this time, there is no way to filter out which counter values belong to which JVM.

To work around this issue, each JVM needs to be configured to use a unique port number for the PCH Listener. Use the following procedure to change the listener port for a CE JVM instance:

• Create a new custom property in WAS called "filenet.pchconfig" that points to a file called "PchConfig.properties". You have to manually create this file and you can place it anywhere on the Content Engine Server. *Process Definition may be under the Java and Process Management group.*

i configuration properties.	
└─── <i>\</i> }	
operties	
n	
OK Reset Cancel	
io	oK Reset Cancel

WebSphere: New JVM Custom Properties

Applicatio Custom Pr Opecifies a	<u>n servers</u> > <u>server1</u> > <u>Process Definition</u> > <u>Java Virtual Machine</u> > <u>operties</u> > filenet.pchconfig Irbitrary name and value pairs of data. The value is a string that can set
nternal sy	stem configuration properties.
Configura	tion
-	
C	I Duran a Mara
Genera	il Properties
* Nam	e
filer	et.pchconfig
* × - 1	
* Valu	
teng	ine (PchConfig, properties
Desc	ription
CEF	PCH Listener Config
Appl	y OK Reset Cancel

WebSphere: New JVM Custom Properties, cntd.

Applica Proper	n servers ation servers > se ties	rver1 > Process Definition > Java Virtual Machine	> Custom				
Specifi system	es arbitrary name configuration pro	and value pairs of data. The value is a string that perties.	can set interna				
🕀 Pref	erences						
New	New Delete						
D	6 👯 📽						
Select	Name 🛟	Value 🗘	Description 🗘				
	filenet.pchconfig	C:\Program Files\FileNet\ContentEngine\PchConfig.properties	CE PCH Listener Config				

WebSphere: Server Process Definition, JVM Custom Properites

• Create the "PchConfig.properties" file with one line specifying the desired new listener port number: port_number=32885

PchConfig.properties: Port Number Definition

- Restart the JVM restarting the cluster is OK
- Ensure that you can telnet to the physical server across the new port number. E.g. calling telnet localhost 32885 on a Microsoft Windows based IBM WebSphere installation you should see an output similar to the following screenshot.



Telnet Check of Defined PCH Port.

For CE and AE on Oracle Weblogic

Similar to the procedure on IBM WebSphere, we have to create a custom property for the ORacle Weblogic JVM running the application. Depending on the way the application server is started (start script or using the node manager or admin server), there are two options. Option number one works for both ways, so we prefer this one. If a customer wants to use the node manager option, fine.

Option 1

• When the server (instance) is started, the environment file setDomainEnv.cmd or setDomainEnv.sh is called, no matter which start option is used. The file can be found in the %domain_home%/bin/ (e.g. G:\BEA\user_projects\domains\WebLogicDomain\bin). Edit the file and search for EXTRA_JAVA_PROPERTIES. You should at least find a line JAVA_PROPERTIES="\${JAVA_PROPERTIES} \${EXTRA_JAVA_PROPERTIES}" or set JAVA_PROPERTIES=%JAVA_PROPERTIES% %EXTRA_JAVA_PROPERTIES}" or set operating system. If the variable EXTRA_JAVA_PROPERTIES is not set anywhere else in the file, add a line just above the line JAVA_PROPERTIES=... Create a new custom property called "filenet.pchconfig" that points to a file called "PchConfig.properties". You have to manually create this file and you can place it anywhere on the Content Engine Server. Example: set EXTRA_JAVA_PROPERTIES=-Dfilenet.pchconfig=F:\FilenetCE\PchConfig.properties

set	JAVA_PROPERTIES=-Dplatform.home= <mark>%WL_HOME</mark> % -Dwls.home= <mark>%WLS_HOME</mark> % -Dweblogic.home= <mark>%WLS_HOME</mark> %
8 REI	M To use Java Authorization Contract for Containers (JACC) in this domain,
REI	I please uncomment the following section. If there are multiple machines in
REI	1 your domain, be sure to edit the setDomainEnv in the associated domain on
REI	1 each machine.
REI	1
REI	1 -Djava.security.manager
REI	1 -Djava.security.policy=location of weblogic.policy
REI	1-D javax.security.jacc.policy.provider=weblogic.security.jacc.simpleprovider.SimpleJ&CCPolicy
REI	4 -Djavax.security.jacc.PolicyConfigurationFactory.provider=weblogic.security.jacc.simpleprovider.PolicyConfigurationFactoryImpl
REI	∬ -Dweblogic.security.jacc.RoleMapperFactory.provider=weblogic.security.jacc.simpleprovider.RoleMapperFactoryImpl
set	EXTRA_JAVA_PROPERTIES=-Dfilenet.pchconfig=F:\FilenetCE\PchConfig.properties
set	JAVA_PROPERTIES=%JAVA_PROPERTIES% %EXTRA_JAVA_PROPERTIES%
set	ARDIR=%HL_HOME%\server\lib

setDomainEnv: Java Properties Definition

• Create the "PchConfig.properties" file with one line specifying the desired new listener port number: port_number=32885

📕 PchConfig.properties - Notepad								
Eile	Edit	Farmat	⊻iew	Help				
port	t_nu	mber=3	32885					

PchConfig.properties: Port Number Definition

• Restart the JVM and test the port as described above.

Option 2

• When the managed server (instance) is started using the Node Manager or Admin Server, the custom property can be added using the administration console. Login to AdminConsole->Environments-Servers->YourManagedServer->Configuration (TAB)->ServerStart (SubTab)-> Arguments: (TextArea) Add the custom property to the "Arguments" area:

Change Center	er® Administration C	onsole	
Change Center			
	elcome, weblogic Connected to: We	bLogicDomain	
View changes and restarts	🔓 Home Log Out Preferences 🖟	Record Help	
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Search Home >Simmary of Sensers >VA+b Logic Serve	2	
	Settings for WebLogicSe	IVEF	
Domain Structure	Configuration Protocols L	ogging Debug Monitoring Control Deployments Services Securit	y Notes
WebLogicDomain	General Cluster Services	Keystores SSL Federation Services Deployment Migration Tuni	g Overload Health Monitoring Server Start
B-Interoperability			
LET-Diagnostics	Node Manager is a WebLogic Node Manager will use to start	Server utility that you can use to start, suspend, shut down, and restart servers in nor this server on a remote machine.	mal or unexpected conditions. Use this page to configure the startup settings that
	👍 Java Home:		The Java home directory (path on the machine running Node Manager) to use when starting this server. More Info
	🎼 Java Vendor:		The Java Vendor value to use when starting this server For example, BEA, Sun, HP eto More Info
How do I Configure startup arguments for Managed	街 BEA Home:		The BEA home directory (path on the machine running Node Manager) to use when starting this server. More Info
Servers Start Managed Servers from the Administration Console Shut down a server instance	E Root Directory:		The directory that this server uses as its root directory. This directory must be on the computer that hosts the Node Manager. If you do not specify a Root Directory value, the domain directory is used by default. More Info
	街 Class Path:		The classpath (path on the machine running Node Manager) to use when starting this server. More Info
System Status			
Health of Running Servers			
Failed (0) Critical (0)			
Overloaded (0)	街 Arguments:		The arguments to use when starting this server. More Info
Warning (0) OK (1)	-Dfilenet.pchconfi	g=F:\FilenetCE\PchConfig.properties	

WebLogic Server Administration Console: Adding Arguments.

• Create the "PchConfig.properties" file with one line specifying the desired new listener port number: port_number=32885

📕 PchConfig.properties - Notepad								
Eile	Edit	Farmat	⊻iew	Help				
por	t_nu	mber=3	32885					
0								

PchConfig.properties: Port Number Definition:

• Restart the JVM and test the port as described above.

Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)

ECM SM IBM Content Management (CM8, OnDemand, Common Store) configuration principles



Structure of the IBM CM IM hierarchy structure

The root element of the ECM SM IBM Content Management (CM8, OnDemand, Common Store) (short: IBM CM IM) structure is the so called "Release". It is only an abstract element which is a virtual container of several "Systems". The configuration can consist of several different configured "Systems", which are all stored in the "Release". A system is a whole configuration for a complete environment of several different servers, farms, clusters and products, just as II CE or ContentManager running on these machines. Every

system has a set of different "Servers" which contain the connection information of a physical machine. One server can have several "Instances" which contain common installation, e.g. path to a Java installation, and JMX specific configuration parameters.

Defined instances of different physical servers can be grouped into a kind of virtual servers. Such a group is called a web environment, because it is used to store the JMX specific configurations of the products.

The servers, web environments, and instances, which are defined in the infrastructure, finally are used in the definitions of the products (II CE, CommonStore, ContentManager, ...).

Release

The release is the top level root element. The user will never see the release as an element in the GUI, but since there should not be several root elements (in this case this would be the systems) there is one virtual root element (the release).

System

The system is a collection of all computers and resources of a installation, including the servers and the configuration for the installed products like Process Engine or content Engine. The system includes the whole settings for a ECM SM for IBM CM IM products configuration. It is possible to define several systems.

Infrastructure

The infrastructure contains all servers of the system which shall be configured. It is only a logical element, like the release element. The collection of all servers and web environments is called the infrastructure, because these elements model the server infrastructure of the system.

Server

The server element contains several server specific parameters like the host name or the Java path. A server also contains several instances. The idea is to store as much information in the server as possible so that this parameters are available for all products, when needed, and not every of these parameters must be entered every time a new product has to be configured.

Instance

An instance is the configuration of the JMX specific and Java parameters. The Java parameters (e.g. path to the Java installation) must be set to allow monitors to execute Java programs. If the instance does not have any relation to an application server, e.g. an instance of a CommonStore installation, the application server type must be set to *NONE*.

Configuring and installing ECM SM clients 373 Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)

For application server instances, the JMX port is stored in the instance as well as the application server type. Also other basic connection data like the user, password and timeout are part of an instance. One of the most important JMX parameters is the server connection data, which contains the most important structure information of the application server internals. The following picture shows how an application server is structured and which information must be contained in the infrastructure.



Structure of application servers.

The picture shows one server which has two different application servers running which have several applications deployed. The yellow fields are parameters which are stored in the "server connection data" parameter of the instance parameters. The other fields (Java path, port, user, password...) will be the same for every instance. The following example shows how many instances must be created to monitor all applications.

- Instance 1: [WebSphere Cell Node1 Server 1] will be used for "Application 1" and "Application 2"
- Instance 2: [WebSphere Cell Node1 Server 2], Instance 3: [WebSphere Cell Node2 Server 3], Instance 4: [WebSphere Cell Node2 Server 4], Instance 5: [WebSphere Cell Node2 Serv-

er 5], Instance 6: [WebSphere - Cell - Node2 - Server 5], Instance 7: [WebSphere - Cell - Node2 - Server 6] will be used for the clustered "Application 3".

Instance 8: [Weblogic - Domain - Server1] is used for "Application 4" and "Application 5"

Web Environment

The Web Environments contain several instances which belong to a logical group. The following Web Environments would be used in the example above:

- WebEnv1: Instance1
- WebEnv2: Instance2, Instance3, Instance4, Instance5, Intsance6, Instance7
- WebEnv3: Instance7

In this example the unusual case is used, that there is only one (physical) server which contains all the instances.

Each web environment contains one or more instances. The defined web environments create logical groups. These groups can be seen as virtual servers. Such a group stores JMX specific configuration data per product configuration.

Products

The products contain the configuration of the II CE, the ContentManager and the other IBM Content Management (CM8, OnDemand, Common Store) products. There are products which do have components running as a deployed application in an application server, e.g. the II CE Server, and some which are standalone installations, e.g. CommonStore.

The products with application server deployments do all have an JMX panel for entering the JMX specific configuration parameters of the deployed product instance.

Some products also need database configuration parameters. These can be entered into the appropriate fields of the product panels.

Differences to the other installer plug-ins of the ECM SM

The ECM SM IBM CM IM installer stores its configuration in a binary only format in the same directory where the environment files are stored. This file is created or updated by clicking at the OK button of the IBM CM IM installer plug-in.

At this stage, the system environment files of the configuration are not changed in any way.

The side effect is, the IBM CM IM installer plug-in will never read the ECM SM IBM CM IM system environment file. That file and the server environment files, are *only written* by the installer, but *never read*.

So any manual changes in these files will never show up in the installer plug-in, and they will be overwritten without any further notice later on.

Configure ECM SM IBM Content Management (CM8, OnDemand, Common Store)

To configure ECM SM IBM CM IM properties, press the Configure IBM Content Management (CM8, OnDemand, Common Store) Products ... button.



The ECM SM IBM CM IM Installer Plug-in

The configuration dialog opens.

Configuring and installing ECM SM clients 376 Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)

Infrastructure Products Configuration Hosts WebEnvironments System 1 W2Krsmtest stgt.cenit.de I CE Instance C SI Instance C MOD Instance C MI Instance I CE Instance Local I Delete	ystem: Systen	n 1		-	🔇 New	🗊 Delete	🔞 Help
WebErwironments System 1 ILCE Instance CS Instance CMOD Instance CM Instance ILCE Instance Local	Infrastructure	Products Confi	guration				
 System 1 W2kfsmtest.stgl.cenit.de I CE Instance CS Instance CMOD Instance CM Instance II CE Instance Local 	Hosts We	bEnvironments					
	System 1 P P v2kfsm CS I C CM CM CM CM I CE	test.stgt.cenit.de E Instance nstance DD Instance Instance E Instance Local					New Image: Constraint of the section of the sec

The installer's dialog with expanded tree view

It consists of several tabs which represent the hierarchical structure of the image above.

Create a new system by clicking on the New... button. The New System Dialog will be displayed.

system:	System 1
	Ok Cancel

Dialog to create a new system

The New System Dialog has one input field to enter the new system's name and an OK button to create the system and a Cancel button to leave the dialog without creating the system.

The Infrastructure Tab

The infrastructure tab is used to define the environment in which the system is running. So hosts/servers can be created which contain instances. After creating the servers, the instances can be grouped in web environments.

The infrastructure tab itself contains two other tabs. The **Hosts** tab to define the server and the **WebEnvironments** tab to define the web environments. Both tabs consist of a hierarchical tree of the system, the defined servers and instances in the hosts tab. The web environment tab also has a hierarchical tree view with the system, the defined web environments and the instances associated with the web environments. Both tabs have four buttons. New..., Edit..., Delete, and Help.

The New Server dialog - Hosts New... button

Server:	w2kfsmtest.stgt.cenit.de	-	🚯 Copy From									
Managing Server:	(itself)		-									
Description:	Description: Machine on which the II CE is running											
Instance Settings												
Instance:	🔻 🥔 New 🗈 C	ору From	📋 Delete									
Application Serve	er Type: None		-									
[Service URL]:												
[Port]:												
[JMX User]:												
[JMX User's Pase	sword]:											
[Timeout]:												
Java Path:			📾 Browse									
Server Libs:			📾 Browse									
Server Connectio	n Data:											
Additional Option	s:											
	Ok Cancel] Help										

Dialog to create a new server . The instances tab.

The New Server Dialog is called, when the "New..." button is pressed in the "Hosts" tab. The New Server Dialog consists of several input fields which are explained in the following list.

Server

This is the host which shall be defined in this dialog. The combo box contains all available CALA_REX servers. The field also is editable to enter other servers which are not contained in the combo box.

Managing Server

The Managing Server needs further introduction:

As the ECM SM IBM CM IM configuration also must support server farms and clusters, the Managing Server is used. Farms and clusters are a collection of several servers which appear as only one machine to the other servers and clients in the network. So it may not be possible to request information of these machines directly in some cases. The only interfaces to these machines are JMX, and RMI technology. The JMX requests are executed by the server which is accessible in the network. This server is called the Managing Host and requests the JMX and FileNet Listener parameters.

If a host is Managing Host itself and is not managed by another machine, the Managed Host and the Managing Host are the same machine. The combo box contains all servers which are already defined.

Description

In the description field it is possible to enter some comments about the server. (If it is part of a cluster or what the name of the cluster is)

Copy from... Button

This button opens the "Copy Server From..." Dialog which makes it possible to copy a whole server configuration of an already existing server.

Instances Tab

The Instances tab is used to define several instances at the server.

The Instances Tab

A server can have several (JMX) instances. These instances are defined in the JMX tab of the "New Server Dialog". The following fields can be configured and the following buttons are available to configure the instances:

Instance

The combo box contains all already defined instances of this server. When creating a new server this combo box will be empty. To create a new instance, the "New..." button has to be pressed. The instances can be switched via the combo box. All instances in this combo box are defined for the server (not only the selected instance).

Application Server Type

The following application servers are supported:

- IBM WebSphere 5
- IBM WebSphere 6
- IBM WebSphere 6 via webservice
- IBM WebSphere 6.1
- IBM WebSphere 6.1 via webservice
- IBM WebSphere 7 via webservice
- IBM WebSphere 8, 8.5 via webservice

A WebService based connection to a application server, which has the

applicationserver.jmx.monitor.war/~.ear application running. In this case the **ServiceUrl** has to be used instead of **host** and **port**. For further information about how to install the functionality on WebSphere, refer to the *Install Guide*, chapter *Preparing JMX Monitoring*.

The difference between the "<AppServer> via webservice" and the "Webservice" item in the combo box is, that the "<AppServer> via webservice" items support further functionality like the "View AE Status" task. If the JMX webapplication is deployed on a server, which is not listed in the combo box explicitly, it can be used the "webservice" item.

Service URL (depends on connection type)

For the webservice connection the ServuceUrl must have the following format: http(s)://<ip>: <port>/<context_root>

The values for host, port and contextroot depend on your configuration, described in the "Preparing JMX Support > JMX Support via WebService" chapter of the Install Guide.

Defaults for WebSphere are:

- port for HTTP: 9080
- port for HTTPS: 9443
- context_root: jmxmonitor

Port (depends on connection type)

This is the JMX port to which the software shall connect. Default values are as follows:

- IBM WebSphere 5 2809 per default
- IBM WebSphere 6
 2809 (most likely) per default
- IBM WebSphere 6.1 2809 (most likely) per default
- IBM WebSphere 7, 8, 8.5 The port is not used here, because this server is only used via webservice connection

Most times the ports are set manually by the administrator's choice in productive environments.

JMX User (depends on the application server security settings)

Context sensitive. The password for JMX access.

NOTE On WebSphere 6.1.x.x SSL is activated per default. In this case the user and password field have to be left empty and the credentials have to be entered in the sas.client.props file and the ssl.client.props file. For more information about these files please refer to the chapter "Preparing JMX Support - How to create the keystore and truststore files for WebSphere 6.1.x.x" in the install guide.

Password (depends on the application server security settings)

Context sensitive. The password for JMX access.

Timeout (Optional)

The timeout defines a time, after which the operation shall cancel automatically. The timeout must be given in seconds. If no timeout is defined, 40 seconds are used as default.

Path to Java

As Oracle BEA Weblogic 9 as well as WebSphere 5, 6, and 6.1 use their own Java to access JMX, the Java path of the server can not be used. Therefor the Java path of the application servers must be entered here.

- WebSphere 5 <WebSphereHome>/AppServer/java
- WebSphere 6
 <WebSphereHome>/AppServer/java
- WebSphere 6.1 <WebSphereHome>/AppServer/java
- IBM WebSphere 7, 8, 8.5 <CENIT_ROOT>/jre
 - webservice The Java of the WebSphere Application Server must not be used. It is recommended to use the Java, which is shipped with the product. Alternatively it is recommended to use a different IBM or Oracle JRE with at least Version 6.

Path to server Libs

This is the path to the libraries which are needed by JMX to get a JMX connection to the application server. The paths can be found as follows.

- IBM WebSphere 5, 6, and 6.1 <WebSphereHome>/AppServer
- IBM WebSphere 7, 8, 8.5 <Server>;<Node>

Server Connection Data

The MBean Java program needs several parameters to establish the connection to the application server. The instances need the following parameters depending on which application server is chosen:

- IBM WebSphere 5
 <Server>;<Node>;<Cell>;<Version>
- IBM WebSphere 6
- IBM WebSphere 6.1

<Server>;<Node>;<Cell>;<Version>;<MessageListenerThreadPool-ID>;<ORBThreadPool-ID>;<WebcontainerThreadPool-ID>;<TCPThreadPool-ID>

Additional Options (Optional)

This parameter can contain several key value pairs. This field is only used if the basic configuration needs special treatment. Several key-value pairs are separated via semicolon. Example: key1=value1;key2=value2.

SAS_PATH=<path_to_sas_file> - Is used by WebSphere application servers when security is enabled. For further information please check the manuals. The path usually is on \$WAS_ROOT/ AppServer/profiles/cprofilename>/properties. If no SAS_PATH is defined in the additional options, it uses the path \${CENIT_ROOT}/cala/monitors/pam/properties/sas.client.props if it exists.

IP_ADDRESS=<ip_address_to_connect_to> - For cluster environments the hostname is not usually the address to which can be connected with the JMX client. Enter the IP address of the virtual server to which shall be connected here.

For more information about how to configure the sas.client.props file refer to the chapter "Preparing JMX Support - How to Configure sas.client.props for WebSphere".

The "New..." button

Clicking on this button will open the "New Instance Dialog" to create a new JMX instance.

Instance:	II CE Instance
	Ok Cancel

Create a new instance

The "Copy From..." button

Clicking on this button will open the "Copy Instance from Dialog" to copy an already instance configuration of the actual server into the actual selected instance. It is not possible to copy instances from other instances.



The "Copy Instance From..." dialog

The "Delete" button

Clicking on this button will delete the actually selected instance.

Hosts "Edit..." button

The hosts edit button will also call the "New Server Dialog", with the configuration of the server which was selected in the tree when clicking the button. The first instance of the data list will be pre selected. If an instance was selected in the tree when clicking the button, the dialog will open with the server and the instance pre selected. If the system (root element) is chosen when clicking the edit button, nothing will happen.

Hosts "Delete" button

If a server is selected, the server and all it's instances will be deleted. Also all associated web environments and products are affected by this. A warn dialog advices on that. If an instance is selected, when pressing the delete button, only the instance will be removed. Again web environment and products will be affected by this. If the last instance of a server is deleted, the server will also be deleted automatically, because a server without instance is forbidden.

The "New Web Environment Dialog", "New..." environment button

The following image shows the infrastructure tab with the "WebEnvironments" tab selected.

Configuring and installing ECM SM clients 384 Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)

/stem: S	ystem 1				-	🔇 New	🗊 Delete	🛛 🛛 Help	
Infrastru	icture	Products Co	nfiguration						
Hosts	WebE	nvironments							
Syster	m 1 ab Enviro	nmont 1						🗟 New	
┍≝┉) II CE Ir	nment i istance on w2k	fsmtest.stgt.(cenit.de				🗊 Edit	
- CS Instance on w2kfsmtest.stgt.cenit.de									
-0		Instance on w2	2kfsmtest.stg	it.cenit.de				関 Help	
	ILCE Ir	stance on w2kts Stance Local o	miesi.sigi.ce n w2kfsmtes	:nit.de :t.stat.cenit.di	9				
				loigheenna	-				

The "WebEnvironments" tab in the main config window

Pressing the "New..." button in the "Web Environment" tab will open the "New Web Environment Dialog".

WebEnvironment:	WebEnvironment 1							
Instance:	E Instance on w2kfsmtest.stgt.cenit.de							
Administrative Server: w2kfsmtest.stgt.cenit.de								
	Ok Cancel 🛛 Help							

The "New Environments" dialog

In this dialog the following parameters can be defined and actions can be performed:

Name

Define the name of the web environment. It is not allowed enter an already used name. In edit mode it is possible to rename the web environment with entering another name.

Instance

In this selection list one or several instances must be chosen. It is not allowed to chose no Instance at all. It is allowed to define one instance in two different web environments.

To choose several elements hold down the Ctrl key on the keyboard and select several elements by clicking them. Release the Ctrl key after selecting the needed instances.

Administrative Server

This combo box shows all servers which are associated with the displayed instance. Out of these an admin server can be defined, which server is the master host (the host which does the load balancing) in a cluster environment.

OK button

Clicking the OK button will close this dialog and store the made changes to the system.

Cancel button

Clicking the Cancel button will close the dialog without saving the changes to the system.

After a web environment was defined, the products tabs are enabled and can be edited now.

WebEnvironments "Edit..." button

The environments edit button will also call the "New Web Environment Dialog", with the environment loaded, which is selected in the tree, when pressing the edit button.

WebEnvironments "Delete" button

The environments delete button will delete the environment which is selected in the hierarchy tree. This environment will be lost for all products. A warning dialog will ask for confirmation before the environment is deleted. If an instance is selected and deleted, this instance also will be lost for all products which use the environment. If the last instance from an environment is deleted, the environment will automatically be deleted too.

The Products Tab

In the products tab the configuration for the IBM CM IM applications/products is made. Every product has its own tab.

The "II CE" Product Tab

Name

It is possible to create several II CE configurations. To create a new configuration press the "New..." button. A dialog will open, that contains a field to enter the name and a combo box to select the II CE's web environment. If there are already any II CE configurations defined in the actual system, the "Copy From..." combo box is filled with the II CE configurations which can be copied. The "Delete" button will remove the II CE configuration from the system.

System: Systen	11	•	🔘 New	l	<u>व</u> Del	lete	関 Help				
Infrastructure	Infrastructure Products Configuration										
Name:	II CE System 💌	[*	New	Ì	Delete		🛛 Help				
WebEnvironme	WebEnvironment: WebEnvironment 1 🏾 🖗 Change										
RMI Settings	RMI Settings JMX Settings										
Instance:	II CE Instance										
Install Path:	e:/WebSphereIICE					🗐 E	Browse				
RMI Port:	RMI Port: 1250										
RMI Java Path:	e://VebSphere61/AppServer/java					a E	Browse				
RMI Log-File:	e:/WebSpherelICE//br.log					🚭 Browse					
Server:	w2kfsmtest.stgt.cenit.de						-				
Instance:	II CE Instance Local						-				
Install Path:	e:/WebSpherelICE					🖼 E	Browse				
RMI Port:	1251										
RMI Java Path:	e://VebSphere61/AppServer/java					🖨 E	Browse				
RMI Log-File:	e:/WebSpherelICE/vbr.log 🚭 Browse										
	🕞 Ok 🛛 🔘 Ca	incel									

The II CE dialog

WebEnvironment

The field is disabled. The web environment can only be changed via the "Change..." button. The change dialog also has the option to copy an already existing configuration for a specific web environment. After selecting a new web environment, click OK to leave the change dialog. There can be only one web environment per II CE at one time.

The II CE RMI Settings Tab

System: Systen	n 1	💌 🔘 Nev	w	🗊 Delete	😰 Help					
Infrastructure Products Configuration										
Name:	II CE System	🕻 New	🗊 Dele	ete	🛿 Help					
WebEnvironment: WebEnvironment 1 🏾 🔗 Change										
RMI Settings	JMX Settings									
Instance:	II CE Instance									
Install Path:	e:///ebSphereIICE			<u></u>	Browse					
RMI Port:	1250									
RMI Java Path:	RMI Java Path: e:/WebSphere61/AppServer/java									
RMI Log-File:	e:/WebSphereIICE//br.log			🗠 🗌	Browse					
Server:	w2kfsmtest.stgt.cenit.de				-					
Instance:	II CE Instance Local				-					
Install Path:	e:/WebSphereIICE			<u></u>	Browse					
RMI Port:	1251									
RMI Java Path:	e://VebSphere61/AppServer/java			<u> </u>	Browse					
RMI Log-File:	e:/WebSphereIICE//br.log			🗠 🗌	Browse					
	📑 Ok 🛛 🖲 Ca	ncel								

The II CE Products tab with selected RMI Settings configuration tab

The RMI settings tab is divided in two parts. The upper part contains fields for the RMI settings related with the II CE application server installation.

Instance

Select an instance from the web environment of the II CE. This must be an instance, where the II CE server application is deployed, and running.

Install Path

Enter the path where the II CE Server product is installed.

RMI Port

Enter the RMI port of the configuration service of the II CE here (aka VeniceBridge services). The standard port is 1250.

RMI Java Path

Enter the Java path of the II CE installation here. This can be any Java installed at the server the instance is defined at, if the JVM is capable to run the II CE components.

RMI Log File

Optional field for the RMI logfiles of the II CE server.

The second part contains fields for II CE connectors only installations. These are standalone Java application installations, that are also known as II CE RMI Proxy Connector Servers. Every installation at one server is referenced as an II CE instance of that server.

Server

Select a server an II CE RMI Proxy Connector Server product (aka connectors only installation) was installed at.

Instance

Select an II CE connectors only installation instance from the above server.

Install Path

Enter the path of the directory the RMI bridge start script is located at.

RMI Port

Enter the RMI port the RMI bridge uses. The default is 1251. Normally this is incremented by one for each separate RMI bridge running at a single server.

RMI Java Path

Enter the Java path of the II CE installation here. This can be any Java installed at the server the instance is defined at, if the JVM is capable to run the II CE components. This can be equal for all instances of a server.

RMI Log File

Optional field for the RMI logfiles of the RMI bridge.

The II CE JMX Settings Tab

System: System 1			-	🔘 Nei	N	🗊 Del	ete	🔞 Help
Infrastructure	Products Configuratio	n						
	M CMOD							
Name:	II CE System		▼ □ [*]	New	Ì	Delete	[🛿 Help
WebEnvironment:	WebEnvironment 1						Ŷ	Change
RMI Settings	JMX Settings							
Instanco	II CE Instanco							-
Application Name	VeniceBridge							
WAR File Name:	VeniceBridge.war							
L		[]≱ Ok	🔘 Ca	ncel				

The II CE Product tab with selected JMX Settings configuration tab

Instance

This product can have several instances on which JMX can be requested. Please select the instance which you want to configure. It is possible to configure several instances. You can only select an instance, that is part of the web environment the product is related with (see above).

Application Name

Enter the Application whose status shall be monitored in this field. The default is application name for II CE is "VeniceBridge".

Application War File

WebSphere only: The JMX program also needs the war file name of the application. The default war file name for II CE is "VeniceBridge.war". Some applications also have several war file names. In that case, the war files are separated with semi colons.

The "CS" Product Tab - IBM Common Store

Name

It is possible to create several CS configurations. To create a new configuration press the "New..." button. A dialog will open, that contains a field to enter the name and a combo box to select the CS's web environment. If there are already any CS configurations defined in the actual system, the "Copy From..." combo box is filled with the CS configurations which can be copied. The "Delete" button will remove the CS configuration from the system.

System: System 1 🔹 🖉 New 📋 De								🛅 De	lete	関 Help		
Infras	tructur	e	Products Co	onfiguration								
II CE	CS	CM	CMOD									
Name:	Comm	on St	ore 1			-	[≱	New	Î	Delete	[🛿 Help
Server:	Server: w2kfsmtest.stgt.cenit.de 🏾 🖗 Change											
Gene	ral Sett	ings										
Instanc	:e:		CS Instanc	e.								-
Server	Type:		CS For Lot	us Domino								-
BIN Pat	h:		e:/CSLD/bi	n							a I	Browse
Path To	archir	rt.ini:	e:/CSLD/se	erver/instance	1/archi	int.in	i				🖼 I	Browse
Archive	e Task I	Path:	e:/CSLD/se	erver/instance	1/bin/n	ny_a	irchive	_task.bat			a 1	Browse
Retriev	e Task	Path	e:/CSLD/se	erver/instance	1/bin/n	ny_r	etrieve	_task.bat			a I	Browse
				B	Ok		🖲 Ca	ncel				

The CS dialog

Server

The field is disabled. The server can only be changed via the "Change..." button. The change dialog also has the option to copy an already existing configuration from a specific server. After selecting a new server, click OK to leave the change dialog. There can be only one server per CS at one time.

The CS General Settings Tab

System: System 1			•	🔇 Nev	N	🗊 Del	lete	関 Help		
Infrastructure Products Configuration										
II CE CS CM CMOD										
Name: Common St	ore 1	-	[* N	lew	Ì	Delete	[🛿 Help		
Server: w2kfsmtest.stgt.cenit.de										
General Settings										
Instanco	CS Instanco									
Somor Tuno	CS For Latue Domino									
DIN Dath	c:/CSLD/bin						a			
Doth To prohint init	e:/CSLD/bill	intini						Drowoo		
	e./CSLD/server/instance/harchi	ITIL.ITII		4				Browse		
Archive Task Path:	e:/CSLD/server/instance1/bin/n	ny_arch	iive_	task.bat				Browse		
Retrieve Task Path:	e:/CSLD/server/instance1/bin/n	ny_retri	eve_	_task.bat				Browse		
	🗅 🗘 Ok		Can	cel						

The CS Product tab with selected General Settings configuration tab

Instance

Select an CS instance. Only instances that are members of the selected CS server are listed here.

Server Type

Select the correct CS type. CSLD (Lotus Domino) and CSX (Microsoft Exchange) are possible.

BIN Path

Enter the full path to the **bin** directory of the CS installation here.

Path To archint.ini

Enter the full path to the archint.ini file of the CS instance. This file is the central configuration file of a specific CS installation.

Archive Task Path

If later you want to be able to start and stop an archiving task, enter the full path to the task script here.

Retrieve Task Path

If later you want to be able to start and stop an retrieving task, enter the full path to the task script here.

The "CM" Product Tab - IBM Content Manager

Name

It is possible to create several CM configurations. To create a new configuration press the "New..." button. A dialog will open, that contains a field to enter the name and a combo box to select the CM's web environment. If there are already any CM configurations defined in the actual system, the "Copy From..." combo box is filled with the CM configurations which can be copied. The "Delete" button will remove the CM configuration from the system.

To configure different instances of a CM installation, create a new CM configuration per instance. At the moment, there is no "Copy from..." button to copy data from an already defined configuration to the new one.

Configuring and installing ECM SM clients 393 Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)

ystem: System 1			-	🛛 🔘 Nei	N	💥 Del	ete	🕜 Help	
Infrastructure	Products	Configuratio	n	_					
II CE CS CI	м смо	D							
Name:	Content N	lanager 🔹	- 3	New	- 22	Delete	(🕐 Help	
WebEnvironment:	WebEnviro	onment 1	_					Change	
Library Server	Ressou	rce Manager	7						
Server:		N7P0090264	BIT.de.	cenit-group	o.com			-	
Install Path:		c:/Program F	iles/IBM	/db2cmv8			- 🕥 E	Browse	
Database Type:		DB2							
Library Server on	zOS:								
Database Path:		c:/Program F	iles/db2	/databases	5				
Database Name:		icmnlsdb							
Database Instanc	e Name:								
Database User:									
Database User's I	Password:								
Database Schema	a Name:								
Text Search Sche	ma:								
Database Runtime	e User:								
Database US Use	l: blo:	icmadmin							
Remote System N	ame								
Remote System I)								
Sector System									
					_				



WebEnvironment

The field is disabled. The web environment can only be changed via the "Change..." button. The change dialog also has the option to copy an already existing configuration for a specific web environment. After selecting a new web environment, click OK to leave the change dialog. There can be only one web environment per CM at a time.

The CM Library Server Settings Tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication see chapter "How to configure and use the UnifiedDatabaseClient (UDC)" in the Installation Guide.

Note: The CM8 Library Server configuration tab contains parameters to configure remote monitoring of zOS based CM8 components. Since ECM SM doesn't provide agents for zOS a 'virtual' agent based on Windows, Linux or UNIX has to used to realize remote monitoring.

Tools								
System: System 1			🔻 🥥 Nev	v	🛛 💢 Del	ete	🕜 Help	
Infrastructure Products	Configuratio	on						
I CE CS CM CMO	D							
Name: Content N	lanager	•	謷 New	- 💥 I	Delete	(🕗 Help	
WebEnvironment: WebEnviro	onment 1					8	Change	
Library Server Ressou	rce Manager							
Server:	N7P0090264	4BIT.d	e.cenit-group	.com			_	
Install Path:	c:/Program F	iles/IE	3M/db2cmv8			- 🕤 E	Browse	
Database Type:	DB2						-	
Library Server on zOS:								
Database Path:	c:/Program Files/db2/databases							
Database Name:	icmnlsdb							
Database Instance Name:								
Database User:								
Database User's Password:								
Database Schema Name:								
Text Search Schema:								
Database OS User	icmadmin							
TWO TASK Variable:	Terriadinin							
Remote System Name								
Remote System IP								
	I 0	k	🔤 Cancel					

The CM Products tab with selected Library Server configuration tab

Server

Select the server on which at least one CM instance is installed.

Install Path

Enter the path where the CM product is installed at the server. In the case of a remote monitored Content Manager Library server (for instance a zOS based system) specify the Java JRE path here (without /bin at the end).
Database Type

Select the correct type of the CM database. IBM DB2 and Oracle are supported.

Library Server on zOS

Active this checkbox in the case a remote zOS based CM8 Library server has to be monitored.

Note: Only DB2-based CM8 Library Servers can be monitored.

Database Path

Enter the path to your RDBMS installation. The correct value depends upon the selected database type.

JDBC (UDC) client

If the JDBC based UDC communication to the DB should be used, specify the Java install path here (without /bin at the end) instead of the DB installation path. UDC supports Java version 7 and newer.

Database Name

Enter the name of the database here.

For Oracle this field corresponds to the setting of *ORACLE_SID*. You can specify an Oracle service name in the format /<*dbname*> as well.

Remote Database Name

This field changes its label depending on the selected database type. If the type is *NONE*, the label changes to *Remote Database Name*.

For DB2 the label is Database Instance name. The value is required. Enter the name of the DB2 instance here. If the JDBC based UDC communication to the DB2 database should be used the configuration for a DB2 instance/database looks like: <DB2 server name>,<path to the DB2 JDBC driver location>,[optional DB2 port]. The default port number is 50000. Example: db2Serv1,C:/Program Files/db2jdbc,50000.

For Oracle the label is *Remote Oracle DB name*. The value is optional. If your database is configured for remote access, enter the TNS name (Service name) of the database. If the JDBC based UDC communication to the Oracle DB should be used the configuration for an ORACLE DB server looks like: <Oracle server name>,<path to the Oracle JDBC driver location>,[optional Oracle port]. The default port number is 1521. Example: oracleServ1,C:/Program Files/oraclejdbc,1521.

Database User

Enter the user who can connect to the database.

Database User's Password

Enter the password of the database user.

Database Schema Name

The name of the database schema where the CM8 objects are created.

Text Search Schema Name

The name of the Text search schema, if it's different to the default Text search schema name. DB2 on UNIX, Linux and UNIX uses DB2 NetSearch for text search. The default schema name is 'DB2EXT'. DB2 on zOS uses Omnifind for text search. The default schema name is 'SYSIBMTS'. In the case Text search uses the default values this parameter can be unsed, otherwise specify the correct DB2 text search schema name.

Database Runtime User

Enter the runtime user for the database here.

Database OS User

The operating system user who is used to startup the database. If the JDBC based UDC communication to the DB is configured this parameter is ignored.

TWO_TASK Variable (Oracle only)

Optional: This variable is only used for Oracle databases. Specify the value of the Oracle TWO_TASK variable, if SQLNet access without Oracle service name is required. If the JDBC based UDC communication to the DB is configured this parameter is ignored.

Remote System Name (optional)

In case the Library Server runs on a remote system, fill in its host name, here.

Remote System IP (optional)

In case the Library Server runs on a remote system, fill in its IP address, here.

The CM Resource Manager Settings Tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication see chapter "How to configure and use the UnifiedDatabaseClient (UDC)" in the Installation Guide.

Note: The CM8 Resource Manager configuration tab contains parameters to configure remote monitoring of zOS based CM8 components. Since ECM SM doesn't provide agents for zOS a 'virtual' agent based on Windows, Linux or UNIX has to used to realize remote monitoring.

Configuring and installing ECM SM clients 397 Configuring ECM SM clients for IBM Content Management (CM8, OnDemand, Common Store)

10015			-					
System: System 1			•	🕘 Nei	w	🛛 💢 Del	ete	🕜 Help
Infrastructure	Products (Configuration						
II CE CS CI	M CMOD							
Name:	Content Ma	nager 💌	2	New	- 💥	Delete	(🗿 Help
WebEnvironment:	WebEnviror	ment 1					8	Change
Library Server	Ressourc	e Manager						
Instance		Minstance						
		in instance						
Application Name	:							
WAR Flie Name:	I_							
Server:	h	7P0090264B	T.de.	cenit-group	o.com			-
Database Type:	C	B2						-
Resource Manage	er on zOS:							
Database Path:	с	:/Program File	s/db2	/databases	5			
Database Name:	r	mdb						
Database Instanc	e Name:							
Database User:								
Database User's I	Password:							
Database Schema	a Name:							
Database Runtime	e User:							
Database OS Use	r: r	madmin						
TWO_TASK Varia	ble:							
Remote System N	lame							
Remote System IF	0							
		C Ok	1	Cancel				

The CM Product tab with selected Resource Manager configuration tab

The Resource Manager settings tab is divided in two parts. The upper part contains fields for the JMX settings related with the Resource Managers application server parts of the installation.

Instance

This product can have several instances on which JMX can be requested. Please select the instance which you want to configure. It is possible to configure several instances. You can only select an instance, that is part of the web environment the product is related with (see above).

Application Name

Enter the Application whose status shall be monitored in this field.

Application War File

WebSphere only: The JMX program also needs the war file name of the application. Some applications also have several war file names. In that case, the war files are separated with semicolons.

The second part contains fields for the database parts of the Resource Manager.

Server

Select the server on which at least one CM instance is installed.

Database Type

Select the correct type of the CM database. IBM DB2 and Oracle are supported.

Resource Manager on zOS

Active this checkbox in the case a remote zOS based CM8 Resource Manager has to be monitored.

Note: Only DB2-based CM8 Resource Managers can be monitored.

Database Path

Enter the path to your RDBMS installation. The correct value depends upon the selected database type.

JDBC (UDC) client

If the JDBC based UDC communication to the DB should be used, specify the Java install path here (without /bin at the end) instead of the DB installation path. UDC supports Java version 7 and newer.

Database Name

Enter the name of the database here.

For Oracle this field corresponds to the setting of *ORACLE_SID*. You can specify an Oracle service name in the format /<*dbname*> as well.

Remote Database Name

This field changes its label depending on the selected database type. If the type is *NONE*, the label changes to *Remote Database Name*.

For DB2 the label is Database Instance name. The value is required. Enter the name of the DB2 instance here. If the JDBC based UDC communication to the DB2 database should be used the configuration for a DB2 instance/database looks like: <DB2 server name>,<path to the DB2 JDBC driver location>,[optional DB2 port]. The default port number is 50000. Example: db2Serv1,C:/Program Files/db2jdbc,50000.

For Oracle the label is *Remote Oracle DB name*. The value is optional. If your database is configured for remote access, enter the TNS name (Service name) of the database. If the JDBC based UDC communication to the Oracle DB should be used the configuration for an ORACLE DB server looks like: <Oracle server name>,<path to the Oracle JDBC driver location>,[optional Oracle port]. The default port number is 1521. Example: oracleServ1,C:/Program Files/oraclejdbc,1521.

Database User

Enter the user who can connect to the database.

Database User's Password

Enter the password of the database user.

Database Runtime User

Enter the runtime user for the database here.

Database OS User

The operating system user who is used to startup the database. If the JDBC based UDC communication to the DB is configured this parameter is ignored.

TWO_TASK Variable

Optional: This variable is only used for Oracle databases. Specify the value of the Oracle TWO_TASK variable, if SQLNet access without Oracle service name is required. If the JDBC based UDC communication to the DB is configured this parameter is ignored.

Remote System Name (optional)

In case the Ressource Manager runs on a remote system, fill in its host name, here.

Remote System IP (optional)

In case the Ressource Manager runs on a remote system, fill in its IP address, here.

The "CMOD" Product Tab

Archive Name

It is possible to create several CMOD configurations. To create a new configuration press the "New..." button. A dialog will open, that contains a field to enter the CMOD archive name and a combo box to select the CMOD's web environment. The "Delete" button will remove the CMOD configuration from the system.

To configure different instances of a CMOD installation, create a new CMOD configuration per instance. At the moment, there is no "Copy from..." button to copy data from an already defined configuration to the new one.

WebEnvironment

The field is disabled. The web environment can only be changed via the "Change..." button. After selecting a new web environment, click OK to leave the change dialog. There can be only one web environment per CMOD at a time.

The CMOD General Settings Tab

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Note: The Content Manager OnDemand configuration tab contains parameters to configure remote monitoring of zOS based CMoD components. Since ECM SM doesn't provide agents for zOS a 'virtual' agent based on Windows, Linux or UNIX has to used to realize remote monitoring.

Tools							
System: System 1			-	Nev	v 💥	Delete	🕜 Help
Infrastructure Products Configuration							
Archive Name: ARCHIVE		-	P I	New	💥 Delete		😢 Help
WebEnvironment: WebEnvironment1							Change
General Settings JMX Settings							
Server:	w2kfsmtest.stgt.c	enit.d	le				•
OnDemand Install Path:	C:/Program Files/IE	3M/On	Dema	and32		5	Browse
OnDemand OS user:							
OnDemand Logon Account: odadmin							
Password of OnDemand Account:							
Database Type: DB2							-
OnDemand on zOS:	OnDemand on zOS:						
Database Path: C:/Program Files/IBM/DB2							
Database Library Path:							
Database Name:	ARCHIVE1						
Database Instance Name:	INST01						
Database User:	admin						
Database User's Password:	•••••						
Database OS User:	odadmin						
Java Install Path:	C:/Program Files/IE	BM/SG	LLIB/j	ava/jdk			
Jar Files:	C:/Program Files/IE	8M/SC	(LLIB	ava			
JUBL URL:							
Remote System Name							
Remote System IP							
TSM:	Enable TSM						
TSM Install Path							
ODWEK Path:	C:/Program Files/IE	3M/On	Dema	and Web E	- nablement K	Git	
ODWEK Port: 1445							
Listener Name:	IBM Content Manag	ler Or	n Dem	and			
Listener Port: 32775							
Full Text Search (FTS) Server Installation Directory:	C:/Program Files/IE	8M/On	Dema	and FTS S	erver/V9.0		
	👔 Ok 🛛 💿 Ca	ncel					

The CMOD General Settings tab

Server

Select the server on which the CMOD is installed.

NOTE For CMoD on zOS, this is the "virtual" server which is used for remote monitoring.

OnDemand Install Path

Enter the path where the CMOD product is installed at the server.

Note: Leave this parameter unset in the case a remote zOS based CMoD system should be monitored.

OnDemand OS User

This is the operating system user which is allowed to startup and shutdown the database.

- **NOTE** This user name additionally defines the name of the Database schema, where the CMOD instance tables (including the SL2 table) are stored.
- **NOTE** For CMoD on zOS, the OS user parameter is not required (even if the "virtual" server is a UNIX or Linux system).

OnDemand Logon Account

This account is used by monitors to logon to OnDemand through ODWEK API.

Password of OnDemand Logon Account

Password of the OnDemand logon account.

Database Type

Select the correct type of the CMOD database. IBM DB2, MSSQL and Oracle are supported.

OnDemand on zOS

Select this checkbox in the case the OnDemand runs on zOS.

NOTE Only DB2-based OnDemand servers can be monitored.

Database Path

Enter the path to your RDBMS installation. The correct value depends upon the selected database type.

JDBC (UDC) client

If the JDBC based UDC communication to the DB should be used, specify the Java install path here (without /bin at the end) instead of the DB installation path. UDC supports Java version 7 and newer.

NOTE For CMoD on zOS, this parameter should contain the path to the Java installation to be used. It is recommended to use the JRE installation the ECM_SM agent provides. In this case the Database Library path is not required.

Database Library Path

UNIX only. Enter the path to the shared libraries for your RDBMS installation. The correct value depends upon the selected database type. Depending on the OS version (32Bit or 64Bit) you may need to specify the 64 Bit or 32 Bit version of the database libraries here.

NOTE For CMoD on zOS, the Database Library path is not required if the ECM_SM agent JRE installation is used.

Database Name

Enter the name of the database here.

- **NOTE** The Database name often corresponds with the CMoD archive name you specified above.
- **NOTE** For Oracle this field corresponds to the setting of *ORACLE_SID*. You can specify an Oracle service name in the format /<*dbname*> as well.
- **NOTE** For CMoD on zOS, this is the name of the OnDemand database, default ARSDBASE

Database Instance name (DB2), Remote Oracle DB name (Oracle), Server/Instance name (MSSQL) This field changes its label depending on the selected database type.

For DB2 the label is Database Instance name.

DB2 via DB2 client access

DB2 instance name (required).

DB2 via JDBC (UDC) access

If the JDBC based UDC communication to the DB2 database should be used the configuration for a DB2 instance/database looks like: <DB2 server name>,<path to the DB2 JDBC driver location>,[optional DB2 port]. The default port number is 50000.

Example: db2Serv1,C:/Program Files/db2jdbc,50000

DB2 via JDBC (UDC) access for CMoD on zOS

This parameter is used by the DB2 database monitors to connect to the remote DB2 on zOS using JDBC.

Specify the parameter using this syntax:

<DB2 server name>,<path to the DB2 JDBC driver location>,<DB2 port>,<JDBC</pre> driver class>,<JDBC URL>

Example:

```
10.0.8.227,E:/
jdbc zos,50000,com.ibm.db2.jcc.DB2Driver,jdbc:db2://10.0.8.227:50000/
DBA3
```

For MSSQL the label is Server/Instance name.

MSSQL via MSSQL client access

Specify the Server/Instance name. The value is optional.

The following combinations are possible:

- Leave this parameter unset, if the local Default MSSQL instance should be monitored.
- Specify the remote MSSQL server name, if the Default instance should be monitored on a remote server.
- Specify MSSQL Server name/Instance name, if a custom MSSQL instance on the local or remote server should be monitored.
 - NOTE Use / instead of \ between MSSQL Server and Instance name!

MSSQL via JDBC (UDC) access

If the JDBC based UDC communication to the MSSQL DB should be used the configuration for a Default MSSQL instance looks like: <MSSQL server name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port]. The default port number is 1433.

Example: mssqlServ1,C:/Program Files/sqljdbc11/enu,1433

An MSSQL custom instance UDC configuration looks like; <MSSQL server name>/<Instance name>,<path to the MSSQL JDBC driver location>,[optional MSSQL port].

Example: mssqlServ1/INSTANCE1,C:/Program Files/sqljdbc11/enu,1433

NOTE For information on how to connect to an SSL secured MSSQL Server see Chapter How to configure and use the UnifiedDatabaseClient in the ECM SM Install Guide.

For Oracle the label is Remote Oracle DB name.

Oracle via Oracle Client access

If your database is configured for remote access, enter the TNS name (Service name) of the database (otherwise not required).

Oracle via JDBC (UDC) access

If the JDBC based UDC communication to the Oracle DB should be used the configuration for an ORACLE DB server looks like: <Oracle server name>,<path to the Oracle JDBC driver location>,[optional Oracle port]. The default port number is 1521.

Example: oracleServ1,C:/Program Files/oraclejdbc,1521

Database User

Enter the user who can connect to the database.

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Database User's Password

Enter the password of the database user.

For MSSQL, leave empty if no user is specified.

Database OS User

The operating system user who is used to executing the database tools. If the JDBC based UDC communication to the DB is configured this parameter is ignored.

NOTE For CMoD on zOS, this parameter is ignored, it can be left empty.

Java Install Path

Enter the path to a Java installation at the CMOD server, which is compatible to the CMOD installation. In the case of remote monitoring you may use the JRE packaged with the ECM SM agent.

Jar Files

Several full qualified jar files names which are needed to set up a connection to the database including the Database specific JDBC driver jar file(s). The full qualified jar file names can be given relative (to installation directory) and absolute paths. Only a colon (UNIX/Linux) or a semicolon (Windows) can be used as separator.

Note: In the case of remote zOS based DB2 the DB2 license file is called db2jcc_license_cisuz.jar.

JDBC URL

Optional. The JDBC URL is used for Linux/UNIX/Windows based systems only to monitor the CMoD system log table (usually SL2), on zOS the ODWEK API is used.

In most cases, the default value can be used which is created automatically during client configuration. These are the generated default values if the field is left empty:

DB2

com.ibm.db2.jcc.DB2Driver:↓
jdbc:db2://localhost:50000/↓
<database_name>

MSSQL

com.microsoft.sqlserver.jdbc.↓ SQLServerDriver:jdbc:sqlserver://↓

<hostname>:<port>;instanceName=<Named-instand</pre>

ce-name> if a value was specified in the field **server/instance name**. Don't specify the part ;*instanceName=<Named-instance-name>*, if the Default MSSQL instance is used.

Oracle

oracle.jdbc.driver.OracleDriver:↓ jdbc:oracle:thin:@localhost:↓ 1521:<database_name> oracle.jdbc.driver.OracleDriver:jdbc:oracle:thin:@<remote_↓ oracle_db_name> if a value was specified in the field Remote Oracle DB name

TWO_TASK Variable

Optional: This variable is only used for Oracle databases. Specify the value of the Oracle TWO_TASK variable, if SQLNet access without Oracle service name is required. If the JDBC based UDC communication to the DB is configured this parameter is ignored.

Remote System Name

In case the OnDemand runs on a remote system (e.g. remote zOS), fill in its host name, here.

If the parameter is specified, events will be shown under this hostname in the event console.

Remote System IP

In case the OnDemand runs on a remote system (e.g. remote zOS), fill in its IP address, here.

If the parameter is specified, events will be shown under this hostname in the event console.

TSM

Enable/disable the Tivoli Storage Manager support.

TSM Install Path

The installation path to the IBM Tivoli Storage Manager. If the TSM checkbox is unchecked, this field is not editable. The path still will be stored in the configuration of the installer, but will not be written out to the environment files.

ODWEK Path

Enter the path where the OnDemand Web Enablement Kit product is installed at the server.

or

In the case of remote CMoD server monitoring the ODWEK API files have to be installed on the system running the monitors ('virtual' CMoD system).

ODWEK Port

Enter the port for the OnDemand Web Enablement Kit, usually 1445.

Listener Name

Enter the name of the PCH Listener, usually IBM Content Manager OnDemand.

NOTE The PCH Listener monitoring requires at least Java(TM) 7. The PCH Listener monitors will not work with older Java(TM) versions. You may use the JRE shipped with the agent.

Listener Port

Enter the port of the PCH Listener, usually 32775.

Full Text Search (FTS) Server Installation Directory

Enter the path to the installation of Full Text Search, usually C:/Program Files/IBM/OnDemand FTS Server/V9.0.

The CMOD JMX Settings Tab

System: System 1		-	🔇 New	🗊 Dele	te 🛛 🕅 Help		
Infrastructure	Products Configuration		4				
II CE CS CM CMOD							
Name:	Content Manager on Demand 1	- 🖡	New 📋	Delete	😰 Help		
WebEnvironment: WebEnvironment 1 🔗 Change							
General Settings	s JMX Settings						
Instance:	CMOD Instance				<u> </u>		
Application Name	ODWA						
WAR File Name:	ODWA.war						
<u>[</u>	🕞 Ok 🛛 🖲 Car	ncel					

The CMOD Product tab with selected JMX Settings configuration tab

Instance

This product can have several instances on which JMX can be requested. Please select the instance which you want to configure. It is possible to configure several instances. You can only select an instance, that is part of the web environment the product is related with (see above).

Application Name

Enter the Application whose status shall be monitored in this field.

Application War File

WebSphere only: The JMX program also needs the war file name of the application. Some applications also have several war file names. In that case, the war files are separated with semi colons.

Default: ODWA.war

Installing ECM SM clients

Saving the FileNet configuration

After configuring all FileNet servers, press the **OK** button in the main configuration window to go on with installation.

Back in the main dialog, press the **Save Configuration** button to save the configuration to the directory selected in the **Configuration directory** field.



Save configuration

Installing ECM SM client software

To install the client software on an ECM SM client, press the Install client ... button in the main dialog.



Install client

This opens a new dialog showing a list of configured hosts.

Hostname	Agent Id	Status					
W2K3CM8DB2	w2k3cm8db2_agent	online					
hqdemo	hqdemo_agent	offline					
tivhpcl	tivhpcl_base_agent	online	=				
tivhpcl	tivhpcl_p8_agent	online					
w2keworksfndn.eworks.fndn	w2keworksfndn_agent	offline	-				
Ok Cancel							

Select client

Choose the host to install and press Ok to start the installation program.

Note that you can only select hosts with status online.

File Help							
Install information		Install method					
			O Local machine				
Product:	cala 💌		Remote machine				
Hostname:	W2K3CM8DB2	File transfer:	cala_rex	-			
Operating system:	Windows NT/2000/XP	Remote execution:	cala rex	•			
oper cang opercan		Temole excellent	Comufiles only				
			Copy mes only				
Install directories							
Source directory:	cn://repos/install						
Target directory:	c:\opt\cenit\cala						
JDK path	D:\eclipse\jre1.6.0_07						
Install options							
🔲 Keep monitor se	ettings Au	tostart mode: After	install and at boot tim	ie 💌			
🗌 Reconfigure only	y						
🗹 Create environm	nent file						
🗌 Uninstall							
Selected configurat	tion						
Configuration: FSN	I CLIENT WINDOWS			-			
This is a FileNet System Monitor client configuration for Microsoft Windows operating systems.							
Set configuration variables Copy configuration from							
	Install and configur	e Close	Help				

Installer main window

A further description of the installation program can be found in the *ECM SM CALA Users Guide*. Please refer to this document for more information about client installation.

If the client installation has been completed, press the **Close** button to get back to the configuration main dialog.

After installing CALA on a server or client system, the server must be added to the ECM SM web interface GUI.

Select Host Administration from the sidebar menu and then click on the Hosts link in the central frame, click at the Insert new host button. A new input form appears. Insert the hostname or its IP address into the input field, and select a department from the listbox where to add the new client. Press Apply to commit the data.

After a few minutes you should see events arriving from the new installed system.

Additional Configuration Tasks

The tasks described in this chapter provide additional optional configuration steps after installing the ECM SM client.

Configure ESX Settings

Description

This task can be used to configure the required settings to monitor the virtual machine.

NOTE To access secure (https based) VMware ESX/ESXi server, you must configure keystore settings using the task **Configure Keystore Settings**.

Parameters

File Tools	Help						
Global Settings							
Product:	Configura	ation				•	
Task:	Configure	e ESX Settings				•	
Task Spec	ific Settin	gs —					
Serve	ers: n7p0	2471c64bit_agent	•				
VM Na	VM Name: Win2K3			Remove	Reload list		
ESX	Version:	4.x	-				
E	ESX URL:	https://10.1.14.64/sdk					
E	SX User:	root					
ESX Pa	assword:	•••••					
Store as	task defi	nition		Run task	About this tas	k	
Connected to	0 192.168.2	40.9:23802 as admin					

Configure ESX Settings

Servers

Required. The parameters will be stored on the selected server.

VM Name

Required. Specify the name of the virtual machine from the VMware ESX/ESXi server. This name is case-sensitive and may contain blanks.

ESX/ESXi Version

The version of the VMware ESX/ESXi API (vim25.jar) which should be used to establish the connection.

ESX/ESXi URL

Required. Specify the VMware ESX/ESXi server URL. Use the Fully Qualified Domain Name (FQDN) instead of its IP address.

ESX/ESXi User

Required. Specify the user to use for connection to the VMware ESX/ESXi server.

ESX/ESXi Password

Required. Specify the password to use for connection to the VMware ESX/ESXi server.

Sample Output

```
-----Standard Output-----
Successfully configured ESX settings for VM VirtualMachine
```

Configure JMX Classpath and CLI Settings

Description

This task can be used to edit the JMX standard settings for the JMX status monitors and the JPS monitors. This task must be used, when the program needs additional classpath information to run correctly.

Parameters

File Tools	Help
-Global Set	tings
Product:	Configuration 💌
Task:	Configure JMX Classpath and CLI Settings
Task Spec	ific Settings
	Separate
	n7p0090264bit -
	AppServer Types: WEBLOGIC
	JMX Classpath: IBM_LIB_PATH}/org.apache/xml-apis.jar
	Additional parameters: -Xmx1024m -m 500000
Store as	task definition Run task About this task

Configure JMX Classpath and CLI Settings

Servers

Required. Select the server for which the JMX classpath must be edited. The list shows all available CALA_REX clients.

AppServer Type

The classpath config file contains the classpaths for all supported connection types. Select the type of your application server.

JMX Classpath

This is the classpath, which is used in the monitoring script. Use the variables, which are used in the predefined classpath, instead of the full qualified name to avoid errors from spaces in the path name or something similar. Also do never use double quotes.

Additional parameters

This parameter can be used to add Application Server specific parameters to the Java commands that are executed by monitors and tasks against the Application Server.

Possible parameters look like

-Xmx1024m (interpreted by all Java command, increases the Java Heap size to 1024 MB)

Or

-Dweblogic.MaxMessageSize=150000000 (increases Weblogic Max Message Size parameter to 150MB)

Or

-m 500000 (sets the timeout of the Java call to 500 seconds).

Single parameters containing blanks require masking with " before and after the value, e.g. "-Dmyparameter=This Path contains blanks<math>".

Note: you can specify more than one parameter, e.g. -Xmx1024m -m 500

Sample Output

-----Standard Output-----The new file was written to the following path: /opt/IBM/ECMSM/cala/monitors/pam/jmx_J classpaths.prop

Configure JMX Parameters

Description

This task can be used to edit the JMX standard settings for the JMX Status Monitors. The JMX Status Monitors request several pre defined MBeans and their attributes. This task must be used when the parameters differ from the default templates, which are defined in the monitor and several MBeans must be enabled or disabled.

You can edit the settings for all servers, monitors and MBeans in succession. The settings will be cached locally on the server. When you click the "Run task" button, all changes will be copied to the clients.

Parameters

File Tools	Help					
Global Settings						
Product:	Configuration 💌					
Task:	sk: Configure JMX Parameters					
-Task Spec	ific Settings					
	Servers: N	7P0090264BIT.de.cenit-group.com	-			
	Monitors: N	websphere61	-			
	MBeans: N	lemory	-			
	MBean Stat	tus: 🔽 enabled				
	name:	J∨M				
	platform:	proxy				
	j2eeType:	JVM				
	type:	J∨M				
	mbeaniden	tifier: J∨M				
	spec:	1.0				
Store as	task definition	Run task	About this task			

Configure JMX Parameters

Servers

Required. Select the server for which the JMX parameters must be edited. The list shows all clients where the JMX settings file mbeantemplates.xml can be found.

Monitors

Required. Select the monitor for which the JMX settings must be edited.

MBeans

Required. Select the MBean for which the JMX settings must be edited.

MBean Status

Optional. With this checkbox, MBeans can be enabled or disabled. If an MBean is disabled, it will not be checked by the corresponding monitor.

Note: At least one MBean needs to be enabled.

Entry fields

The number and labels of the entry fields depends on the selected MBean.

Sample Output

Successfully updated JMX settings on 10.0.114.204 Successfully updated JMX settings on 10.0.114.216

Configure Keystore Settings

Description

This task is used to specify the keystore that https-based CE-URL communication of P8 4.x ObjectStore monitors require.

NOTE Before you use this task, perform the required steps, which are described in Keystore certificate import for use with Java based monitors.

Note: This task doesn't create a keystore, it only stores settings of an already created keystore for ECM SM use. For further information on how to create a keystore see information on the Web regarding the Java keytool, for instance at http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

Parameters

File Tools	; Help				
Global Set	tings				
Product:	Configuration			-	
Task:	Configure Keystore Settings			-	
Task Specific Settings					
	Servers:	n7p0090264bit			
	Keystore Filename incl. Path:	/home/usre/truststo	re.jks		
	Keystore Type:	jks			
	Keystore Password:	•••••			
Store as	s task definition		Runtask	About this task	
Store da	o tuon uoninition		nuntuan	About this task	

Configure Keystore Settings

Server (required)

Required. The parameters will be stored on all selected servers.

Keystore File name

Required. Specify the filename that contains the keystore including full path.

Keystore Type

Required. Specify the type of the given keystore. The value that must be specified depends on the JDK. Possible values are jks (default for SUN JDKs) and pkcs12

Keystore Password

Required. Specify the password for the given keystore.

Sample Output

Successfully configured keystore settings

Configure LDAP settings on clients

Description

This task creates a login.conf and (if MS ADS is selected) a krb5.conf file on the specified client. Additionally it downloads the file jaas_test.zip to clients and extracts the zip archive on the client into the directory <install-dir>/tools/jaas_test.

In the case this task is executed from a ECM SM Server version 4.5.0+ the server side configured login.conf and krb5.conf file (MS ADS only) can be used.

Background

The settings for the LDAP authentication are all based on the same principles regardless of the concrete LDAP server used. These principles are described here to give a better understanding about the input parameters described in the following sub-sections.

NOTE In the following the placeholders $\{0\}$ and $\{1\}$ will be replaced with the username and the password during runtime. So you should not enter these values directly in your configuration, but use the shown placeholders.

Server Name and Port

These parameters are necessary to establish a network connection to the LDAP server. As server name specify the hostname (without domain) of an LDAP server and the corresponding LDAP port.

Group (Provider) URL

This defines the entry point in the LDAP tree where the search should be done. Depending on the LDAP type (e.g. MS ADS, Novell, etc.) the elements can be either users, that hold the information to which groups it belongs to, or it can be groups, where the user is a member.

Group Attribute

This is the name of the attribute used to identify the groups for the user that was searched for (e.g. memberOf, member).

Group Query

This LDAP pattern is the name of the attribute, that normally contains the login name of a user. It is used to retrieve the belonging groups for the specified account (e.g. sAMAccountName= $\{0\}$, where $\{0\}$ is a place holder for the login name).

Group Name Pattern

This is a filter (regular expression) to match distinctive group entries from the LDAP tree. (e.g. group.name.pattern=" $CN=([^{,}]^{*}), *$ ")

Group Name Index

The result of the regular expression in the "Group Name Pattern" is indexed into groups. The group name index refers to the indexed group. Counting starts by 1 (one).

User URL

This is the LDAP search pattern (aka filter) used to get the elements from the LDAP tree, which contain the user.

Parameters

File Tools Help						
Global Settings						
Product: Configuration	ı 🔽					
Task: Configure LDAP Settings on Clients						
Task Specific Settings						
Servers: N7P0090	264BIT.de.cenit-group.com					
	ngin conf and (if exists krb5 conf) from the server					
LUAP Type: MS ADS ((with SASL/GSSAPI authentication)					
Secur	re LDAP					
ADS Server Name:	adssrv.fsm.com					
ADS Server Port:	389					
Domain Name:	fsm					
Group Provider URL:	CN=Users,*					
Group Query:	sAMAccountName={0}					
Group Attribute:	memberOf					
Group Name Pattern:	CN=([^,]*),.*					
Group Name Index:	1					
Store as task definition	n Run task About this task					

Configure LDAP settings on clients

Servers

Required. Select the server(s) where the LDAP settings should be created.

Use existing configuration files

Check this box, if the existing login.conf and (if available krb5.conf) should be downloaded

In the case this check box is selected all other parameters except the list box 'Supported LDAP types' can be left unset.

Supported LDAP types

Select one of the following supported LDAP types: MS AD LDS, MS ADS using GSSAPI, MS ADS without GSSAPI, SUN Directory Server, IBM Tivoli Directory Server, Novell eDirectory Server

Select secure or unsecure LDAP

Select whether secured (Idaps) or unsecure (Idap) should be used

All other settings depend on the selection of LDAP Type.

Settings for MS AD LDS based LDAP server

Server Name

Specify the full qualified MS AD LDS LDAP server name

Server Port

Specify the MS AD LDS LDAP server port (default unsecure port: 389, secured: 636)

Group URL

Specify the Group URL pattern to search for groups

Example: OU=User, O=fsm, C=com

NOTE Do NOT add $CN = \{ 0 \}$ to this parameter

Group Attribute

Specify the Group attribute that contains group information.

Default: memberOf

Group Query

Specify the LDAP query to determine the groups of a specific user. $\{0\}$ will be replaced by the user name.

Default value is distinguishedName=CN={0},OU=Users,O=<domain>,C=<domain-suffix> If the MS AD LDS server is configured to use the LDAP displayName instead of the distinguished-Name please use the following value without any extension: $displayName = \{ 0 \}$

User URL

Specify the User URL pattern to search for users

Example: CN={0},OU=User,O=FSM,C=COM

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: CN=([^ ,] *) , . *

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Settings for MS ADS based LDAP server

Server Name

Specify the MS ADS server name without DNS suffix (for instance adsserv1)

Server Port Specify the MS ADS server port (default port: 389)

Domain Name

Specify the ADS Domain name in lowercase letter

Group Provider URL

Specify the Group provider URL pattern to search for groups

Group Query

Specify the LDAP query to determine the groups of a specific user. $\{o\}$ will be replaced by the user name.

Default: *sAMAccountName=*{0}

Group Attribute

Specify the Group attribute that contains group information.

Default: memberOf

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: *CN*=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

LDAP Security principal (non GSSAPI-authentication only)

Default value. { 0 } or { 0 }@<domain-name>

Use { 0 }@<domain-name> in the case the ADS server requires 'Bind with Credentials', otherwise use { 0 }

Settings for SUN Java System Directory Server

Server Name Specify the full qualified SUN Directory server name

Server Port

Specify the SUN Directory LDAP server port (default: 389)

Group URL

Specify the Group URL pattern to search for groups

Group Query

Specify the LDAP query to determine the groups of a specific user. $\{0\}$ will be replaced by the user name.

Default: (&(objectClass=groupOfUniqueNames)(uniqueMember=uid={0},*))

Group Attribute

Specify the Group attribute that contains group information.

Default: cn

User URL

Specify the User URL pattern to search for users

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: *ou=([^,]*),.**

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Settings for IBM Tivoli Directory Server

Server Name

Specify the full qualified IBM Tivoli Directory server name

Server Port

Specify the IBM Tivoli Directory LDAP server port (default: 389)

Group URL

Specify the Group URL pattern to search for groups

Ex.: ldap[s]://<ldap-server-name>>:<ldap-port>

Group Query

Specify the LDAP query to determine the groups of a specific user. $\{o\}$ will be replaced by the user name.

Default: (&(objectClass=accessGroup)(member=cn={0}*))

Group Attribute

Specify the Group attribute that contains group information.

Default: cn

User URL

Specify the User URL pattern to search for users

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: cn=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Settings for Novell eDirectory LDAP server

Server Name

Specify the full qualified Novell eDirectory server name

Server Port

Specify the Novell eDirectory LDAP server port (default: 389)

Group URL

Specify the Group URL pattern to search for groups

Ex.: ldap[s]://<ldap-server-name>:<ldap-port>... /T=<Novell-Tree-Name>

Group Query

Specify the LDAP query to determine the groups of a specific user. $\{o\}$ will be replaced by the user name.

Default: (member=cn={0},OU=<ou name>,O=<Organization/domain name>)

Group Attribute

Specify the Group attribute that contains group information.

Default: none (unset)

User URL

Specify the User URL pattern to search for users

Group Name Pattern

Adjust the Group name pattern settings, if required

Default: cn=([^,]*),.*

Group Name Index

Specify the Group name index that contains group information.

Default: 1

Configure TSM Settings

Description

This task creates the configuration file required by the monitors in the TSM monitor archive.

Parameters

File Tools	File Tools Help						
Global Settings							
Product:	Configuration 💌						
Task:	Configure TSM Settings 🔹						
Task Specif	fic Setti	ings –					
-		_					
Serv	vers: N7	7P009	0264BIT.de.cenit-group.com	•			
TSM Syst	tem: Te	stSys	tem	•	Remove	Reload list	
TS	SM Ver	sion:	5.x	•			
	TSM A	lias:	test_001				
1	ISM Se	rver:					
	TSM	Port:					
		User:	analyst				
	Passw	vord:	•••••				
	05	User:	fsmusr				
Installatio	on Direc	ctory:					
Additio	Additional Options:						
Store as t	Store as task definition Run task About this task						

Configure TSM Settings

Servers

Required. The parameters will be stored on the selected server.

TSM System

Required. Specify a system name for the TSM configuration (logical name).

TSM Version

Required. Select the version of the TSM system from the list.

TSM Alias

Optional, UNIX / Linux only.

Alias as defined in dsm.sys. If no alias is specified, dsmadmc uses the first server defined in the dsm.sys configuration file. If multiple server nodes are configured for the dsmadmc, the specific alias name has to be set to ensure that the monitor uses the correct server node

TSM Server

Optional, Windows only.

Specify the TSM server for **dsmadmc**. If no server name is specified, **dsmadmc** tries to connect to the local host.

TSM Port

Optional, Windows only.

Specify the TSM port for **dsmadmc**. If no port number is specified, **dsmadmc** tries to connect using the default port 1500.

User

Required. Specify the user to use for connection to TSM.

The user specified here must be a user of class *analyst*. This class can be added for a user with the following command:

dsmadmc grant authority <USERNAME> classes=analyst

Password

Required. Specify the password to use for connection to TSM.

OS User

Optional, UNIX; Linux only. Specify the operating system user to use for calling the **dsmadmc** tool. This user is required, if the dsmadmc shall be executed with another user, than the CALA_REX user.

Installation Directory

Optional. Specify the path to the dsmadmc binary if the binary cannot be found in the PATH.

Additional Options

Optional. Specify any required additional options for the dsmadmc tool.

Configure WMI Java Path

Description

This task can be used to set the Java path for applications (in this case the Java path for WMI). Some monitors use this Java path. If a monitor uses the path, it is mentioned in the monitor description. The path should be valid and without the "bin" directory. It is added automatically.
Parameters

File Tools	; Help								
Global Settings									
Product:	Configuration								
Task:	Configure WMI Java Path								
-Task Spec	cific Settings								
Servers:	n7p0090264bit 👻								
Java Insta	II Path: C:/Program Files/Java/jre6								
Store as	s task definition Run task About this task								

Configure WMI Parameters

Servers

Required. Select the server for which the Java installation path for WMI monitoring shall be configured.

Java Install Path

The Java Home of this client.

Sample Output

The settings file "C:/opt/ia_stuff/ia_fp2/cala/monitors/pam/standard_env.prop" was updated (key: "JAVA_HOME", value: "c:/opt/ia_stuff/ia_fp2/jre")

Additional ECM SM specific Configuration Tasks

The tasks described in this chapter provide additional optional configuration steps after installing the ECM SM client.

Configure Datacap Database Settings

Description

This task stores the database settings of a Datacap application in a file for later usage.

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Parameters

File Tools Help								
Global Settings								
Product: Configurati	Configuration							
Task: Configure [Configure Datacap Database Settings							
Task Specific Settings								
Ser	vers: n7p0(090264bit	-					
Datacap Application N	ame: 1040e	Z	-	Remove	e Reload lis	st		
Datacap Installation	Dir: C:/DATA	CAP			-			
Database Parameter 9	Set: 1040ez/	ADM	-					
Database Cla	ss: ADM		-					
Database Type:	MSSQL							
Database Name:	1040ezADM							
Database Schema:								
Database Username:	datacap							
Database Password:	•••••							
Database DriverPath:	/tmp							
Database Server:	DATACAPSI	RV						
Database Port:	1433							
Database JDBC URL:								
Store as task definit	ion		Rı	in task	About this ta	sk		

Configure Datacap Database Settings

Server

Required. Select a server from the listbox. The Datacap settings file will be created on the selected server.

Datacap Application Name

Required. Enter the name of a new Datacap application to configure or select an existing Datacap application for editing or removal.

Datacap Installation Dir

Required. Enter the installation directory of the Datacap application.

Database Parameter Set

Required. Enter a descriptive name for the database parameter set related to this Datacap application or select an existing set from the list.

Database Class

Required. Select a Datacap database class from the list. Possible types are *ADM*, *ENGINE*, *EXPORT* and *FINGERPRINT*.

Database Type

Required. Select the database type of the Datacap application from the list.

Database Name

Required. Enter the database name.

 Oracle: in the case Oracle naming service is used the following format is required: /ServiceName

Database Schema

Required for DB2, optional for Oracle and MSSQL based Datacap applications. Enter the database schema name.

Database Username

Required for DB2 and Oracle, optional for MSSQL. Enter the name of the user to use for database connection.

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Database Password

Required for DB2 and Oracle, optional for MSSQL. Enter the password of the database user.

Database Driver Path

Required. Enter the full qualified path to the JDBC driver files.

Database Server

Required. Enter the DB server name. In the case the Custom Database JDBC URL is specified with this task this parameter is not required.

- DB2: Database server name or IP address.
- MSSQL with Default instance: Server name.
- MSSQL with Custom Instance: serverName/InstanceName.

• Oracle: Oracle server name or IP address

Database Port

Required. Enter the port number of the database. In the case the Custom Database JDBC URL is specified with this task this parameter is not required.

Database JDBC URL

Optional. Enter the JDBC URL to connect to the database.

The format of the URL depends on the database and driver. Common formats are:

DB2

jdbc:db2://localhost:50000/<database_name>

MSSQL

jdbc:sqlserver://<hostname>:<port>;instanceName=<Named-instance-name>

Oracle

- Oracle database with ORACLE_SID / Database name configuration: jdbc:oracle:thin: @localhost:1521:<database_name>
- Oracle database with service name configuration: jdbc:oracle:thin:@localhost:1521/<service-name>
- jdbc:oracle:thin:<remote_oracle_db_name>
- jdbc:oracle:thin:@(DESCRIPTION=(load_balance=yes)(ADDRESS_ LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=oraserv1)(PORT=1521)) (ADDRESS=(PROTOCOL=TCP)(HOST=oraserv2)(PORT=1521))) (CONNECT_ DATA=(SERVICE_NAME=myoradb)(failover_mode=(type=select)(method=basic) (retries=32)(delay=4))))

Either server and port or the JDBC URL must be given.

Configure IBM Case Manager Settings

Description

This task creates the file icm_conf.prop on the selected server. This configuration file is required for IBM Case Manager monitoring.

Parameters

File Tools	Help							
Global Setting	gs —							
Product: Co	Configuration 🗸							
Task: Co	onfigure	IBM Case Manag	jer	Settings			•	
Task Specific	Task Specific Settings							
	рГ				_	1		
3	servers:	n7p0090264bit_	j		•			
Configuration	n Name: i	icm vm			-	Remove	Reload list	
	P8 Syst	tem: P8_52			-			
	P8 Prod	luct: CPE 5.2			-			
		CE UF	RL:	http://svwap002di:9081/wsi/FNCEWS40MTOM/				
		CE Us	er:	dev-icc4sap-ceadmin				
		CE Passwo	rd:	•••••				
ICM Installati	ion Direct	tory: c:/temp						
ICM Lis	stener Na	ime: IBM Case N	lan	ager				
ICM L	Listener F	Port: 32775						
Store as ta	ask defini	ition			Ru	in task	About this task	
Connected to lo	ocalhost:23	3802 as admin						

Configure IBM Case Manager Settings

Servers

Required. The parameters will be stored on the selected server.

Configuration Name

Required. Specify a user defined name to create a new configuration or select an existing configuration.

P8 System

Required. Select the P8 5.x system that contains the CE connection settings corresponding to the ICM installation.

P8 Product

Required. Specify the P8 5.x product that contains the CE connection settings corresponding to the ICM installation.

Selecting the P8 System and Product will fill the following fields:

CE URL

The CE connection URL for the selected P8 System. This URL will be used by the ICM monitors CaseStatus, SolutionStatus and TaskStatus to connect to the CE to gather data.

CE User

The CE user for the selected P8 System. This user will be used by the ICM monitors CaseStatus, SolutionStatus and TaskStatus to connect to the CE to gather data.

CE Password

The CE password for the selected P8 System. This password will be used by the ICM monitors CaseStatus, SolutionStatus and TaskStatus to connect to the CE to gather data.

These values are taken from the Core Agent Installer, plugin **Configure IBM FileNet 4.x / 5.x**, tab **PE 5.0, 5.1, CPE 5.2 (PE part)**, sub tab **Security** because the Java-based ICM monitors require the same connection data to the CE as the Java-based PE monitors.

Note that these fields cannot be changed by this configuration task. If the CE URL or the credentials change, first reconfigure the CE connection settings in the Core Agent Installer, then rerun this task to update the data on the selected ICM server.

ICM Installation Directory

Required. Specify the installation path of the Case Manager software.

The JAR files required to connect to the Case Manager will be searched in the subdirectories CaseAPI/lib and CaseAPI/lib_cm8 of the given directory.

ICM Listener Name

Optional. Specify the name of the PCH listener for IBM Case Manager.

Default: IBM Case Manager

ICM Listener Port

Optional. Specify the port of the PCH listener for IBM Case Manager.

Default: 32775

Configure IBM Content Navigator Settings

Description

This task creates the file **cont_nav_conf.prop** on the selected server. This configuration file is required for IBM Content Navigator monitoring.

Parameters

File Tools	Help							
Global Sett	tings —							
Product:	Configurat	Configuration 🗸						
Task:	Configure	BM Content Navigator Settings		-				
Task Spec	ific Setting:	j						
s	ervers: loc	alhost_	•					
Application Name: navigator		•	Remove					
Co	ntext Root:							
Communic	ation Type:	http	•					
Sei	rver Name:							
Web Applic	ation Port:							
	ICN User:							
ICN	Password:							
Store as task definition Run task About this task								

Configure IBM Content Navigator Settings

Servers

Required. Select the server(s) where the IBM Content Navigator settings should be created.

Application Name

Required. Enter the name of the IBM Content Navigator web application.

Communication Protocol

Required. Select either *https* or *http* as communication protocol.

Server Name

Optional. Specify the name of the server where IBM Content Navigator is running.

Default: local hostname

Web Application Port

Required. Specify the port number of the IBM Content Navigator web application.

ICN User

Optional. Specify the name of the user to use to login to the ICN system.

ICN Password

Optional. Specify the password of the user to use to login to the ICN system.

Configure ICC4SAP Settings

Description

This task creates the file **icc4sap_conf.prop** on the selected server. This configuration file is required for ICC4SAP monitoring.

Parameters

File Tools	Help								
Global Set	tings —								
Product:	Configur	ation				-			
Task:	Configur	Configure ICC4SAP Settings							
Task Spec	ific Settir	ngs							
5	ervers.	-l'02250			_				
	crecis.	1111102259			•				
ICC4SAP In	stance:	nyinstance				Remove			
Inst	all path:								
Path to are	chint.ini:								
	OS User:								
	Sumx:								
•						•			
Store as task definition Run task About this task									

Configure ICC4SAP Settings

Servers

Required. Select the server(s) where the ICC4SAP settings should be created.

ICC4SAP Instance

Required. Specify an instance name for the ICC4SAP configuration.

Install path

Required. Enter the path where ICC4SAP is installed.

Path to archint.ini

Required. Enter the path to the archint.ini of the ICC4SAP instance.

OS User

Optional. UNIX, Linux only. Specify the operating system user to be used for calling the ICC4SAP tools. This user is required, if the ICC4SAP tools shall be executed with a user other than the CALA_REX User.

Default: The standard monitoring user on the system.

Suffix

Optional. Service suffix used to identify service and process names if several instances of ICC4SAP are installed.

Configure CEBI Tool Settings

Description

This task creates the file **cebit_conf.prop** on the selected server. This configuration file is required for IBM CE Bulk Import Tool monitoring.

Parameters

File Tools	Help							
Global Settings								
Product:	Configuration	Configuration 🗸						
Task:	Configure CEB	Tool Settings			-			
Task Spec	ific Settings							
	Servers: N7	20090264RIT de cenit-group com	-					
CEBI T	ool System: CE	BI on Windows	-	Remove	Reload list			
C	E Library Path:	C:/Program Files (x86)/IBM/FileNet/CE	ECI					
	Java Path:							
In	stallation Path:	C:/Program Files (x86)/IBM/FileNet/Co	onte					
	OS User:							
We	ebSphere Path:							
WebS	phere Options:							
Store as	s task definition			Run task	About this task			

Configure CEBI Tool Settings

Servers

Required. Select the server(s) where the IBM CE Bulk Import Tool settings should be created.

CEBI Tool System

Required. Select or enter the name of the CEBI Tool System to be configured.

CE Library Path

Required. Enter the path to the IBM Content Engine's libraries.

Example: C:\Program Files (x86)\IBM\FileNet\CEClient\

Java Path

Optional. Enter the path to the preferred Java Runtime Environment to run the monitors.

Default: The ECM SM standard JRE

Installation Path

Required. Enter the installation path of the CEBI Tool System.

Example: C:\Program Files (x86)\IBM\FileNet\ContentEngine\tools\CEBI\

OS User

Optional. Enter the user to run the monitors. That must be a valid user on the system the monitor runs and must have access to the CEBI Tool directories and services.

Default: The standard monitoring user on the system.

WebSphere Path

Optional. In case of running CEBI Tool on WebSphere Application Server enter its installation path here.

WebSphere Options

Optional. In case of running CEBI Tool on WebSphere Application Server enter additional options here.

Default: None.

Configure ObjectStore Database Settings

Description

This task stores the database settings of an ObjectStore in a file for later usage.

This component can be configured to use either native or JDBC-based communication. For details about JDBC-based communication refer to the Installation Guide, chapter "How to configure and use the Unified-DatabaseClient (UDC)", section "Usage" > *<DatabaseType*>.

Parameters

File Tools	Help								
-Global Sett	tings								
Product:	Configurati	Configuration							
Task:	Configure (Configure Objectstore Database Settings							
-Task Spec	ific Settings	;							
:	Servers: n7	p0090264bit	-						
Objectstor	e name: Ot	jectstore 1	-	Remove	Reload list				
CSS	Installation	Dir:							
Database	Parameter 9	Set: Objectstore 1	-						
Data	base Type:	DB2							
Datab	ase Name:	CE							
Databas	e Schema:	CE							
Database	Username:	dbadmin							
Database	Password:	•••••							
Database	DriverPath:	C:/Program Files/IBM/DB2/JDBC Drivers							
Databa	ase Server:								
Data	abase Port:								
Database	JDBC URL:	com.ibm.db2jcc.DB2Driver.jdbc:db2://loc							
Store as	task defini	tion	Ru	n task	About this task				

Configure ObjectStore Database Settings

Server

Required. Select a server from the listbox. The ObjectStore settings file will be created on the selected server.

ObjectStore name

Required. Enter the name of a new ObjectStore to configure or select an existing ObjectStore for editing or removal.

CSS Main Installation Dir

Optional. Enter the main installation directory of the Content Search Services software, if applicable. Note: this is not the subdirectory of the CSS server configuration. Help: specify the directory that contains the *css-servers.xml* file.

CSS Server name

Optional. Enter the real CSS server name. Verify the server name, check the file *css-servers*. *xm*1.

Database Parameter Set

Required. Enter a descriptive name for the database parameter set related to this ObjectStore or select an existing set from the list.

NOTE It is currently not possible to share a Database Parameter Set between multiple ObjectStores.

Database Type

Required. Select the database type of the ObjectStore from the list.

Database Name

Required. Enter the database name.

 Oracle: in the case Oracle naming service is used, the following format is required: /ServiceName

Database Schema

Required for DB2, optional for Oracle and MSSQL based ObjectStores. Enter the database schema name.

Database Username

Required for DB2 and Oracle, optional for MSSQL. Enter the name of the user to use for database connection.

MSSQL

Leave field empty to connect using Windows authentication with the credentials of the CALA service user. For details about JDBC-based Windows authentication refer to the Installation Guide, chapter "How to configure and use the UnifiedDatabaseClient (UDC)", section "Usage" > "MSSQL" > "Windows authentication over JDBC driver".

Database Password

Required for DB2 and Oracle, optional for MSSQL. Enter the password of the database user.

Database Driver Path

Required. Enter the full qualified path to the JDBC driver files.

Database Server

Required. Enter the DB server name. In the case the Custom Database JDBC URL is specified with this task this parameter is not required.

- DB2: Database server name or IP address.
- MSSQL with Default instance: Server name.
- MSSQL with Custom Instance: serverName/InstanceName.
- Oracle: Oracle server name or IP address

Database Port

Required. Enter the port number of the database. In the case the Custom Database JDBC URL is specified with this task this parameter is not required.

Database JDBC URL

Optional. Enter the JDBC URL to connect to the database.

The format of the URL depends on the database and driver. Common formats are:

DB2

jdbc:db2://localhost:50000/<database_name>

MSSQL

jdbc:sqlserver://<hostname>:<port>;instanceName=<Named-instance-name>

Oracle

- Oracle database with ORACLE_SID / Database name configuration: jdbc:oracle:thin: @localhost:1521:<database_name>
- Oracle database with service name configuration: jdbc:oracle:thin:@localhost:1521/<service-name>
- jdbc:oracle:thin:<remote_oracle_db_name>
- jdbc:oracle:thin:@(DESCRIPTION=(load_balance=yes)(ADDRESS_ LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=oraserv1)(PORT=1521)) (ADDRESS=(PROTOCOL=TCP)(HOST=oraserv2)(PORT=1521))) (CONNECT_ DATA=(SERVICE_NAME=myoradb)(failover_mode=(type=select)(method=basic) (retries=32)(delay=4))))

Either server and port or the JDBC URL must be given.

ECM SM Mobile app installation and configuration

Installation Prerequisites

Ensure you have access to a supported iOS or Android device. Ensure you have access to a current ECM SM server.

IBM Enterprise Content Management System Monitor Mobile Installation and configuration routine

- Install the App from the Apple App Store or Google Play Store.
- Start the IBM IBM Enterprise Content Management System Monitor Mobile app
- Select the 'plus' icon and add one or more ECM SM server. Specify a logical name, the real server name, the port of the ECM SM UI and select whether http or https based communication is required. Press the Save button.
- Once at least one server is configured you can specify username and password to connect to the ECM SM system.

ECM SM HA and DR support

General ECM SM HA and DR support

ECM SM server and client agents support OS generic startup and shutdown methods. This allows the installation of more than one agent of each kind (ECM SM CALA_REX and ECM SM CALA) on one system.

The following OS specific agent registration methods (responsible for the control of the agent) are supported:

- Windows based systems: Windows Services registration
- AIX /etc/inittab registration
- SUN Solaris, HP-UX and SuSE/Redhat Linux /etc/rc.* registration

In general ECM SM agents can be installed using other, none OS specific, startup and shutdown methods. Therefore the installation GUI and the Command Line install scripts provide checkboxes / CLI parameters to disable the OS specific startup registration method. An independent ECM SM startup script is created during the agent installation anyway. This ECM SM Control-Script can be integrated into HA scenarios.

ECM SM Server HA and DR support

ECM SM server agents can be installed on active / passive cluster systems, where the name and IP address of the system stays the same after takeover.

The following components need to be started / stopped / taken over on a ECM SM server:

- ECM SM Database system with the database
- ECM SM webserver
- ECM SM CALA_REX Server agent
- ECM SM CALA Server (Monitoring) agent

ECM SM Agent HA and DR support

The ECM SM agents can be installed on active / passive cluster systems, where the name and IP address of the system stays the same after takeover.

The following components need to be started / stopped / taken over on a ECM SM agent:

- ECM SM CALA_REX agent
- ECM SM CALA (Monitoring) agent

Both agents should be installed on the file system / disk / nfs mount that is accessible from both nodes. The start/stop scripts for the agents have to be manually included into the HA takeover configuration.

The configuration for CALA_REX and CALA agents to use the virtual address of the HA package is done while installing the CALA_REX agent. The graphical installer offers a parameter "CALA_REX Agent IP-address" for the IP address used with the hostname specified in parameter "CALA_REX Agent IP name". If the CALA_REX agent should technically use the virtual network interface to connect to the ECM SM server instead of the primary network interface, the additional parameter "localport=<virtual ip address>:*" needs to be set in the field "Additional CALA_REX parameters".

值 IBM Enterprise Content Manage	ement System Monitor CALA_REX Agent 📃 🔀
	Specify the IBM ECM SM CALA_REX Agent settings
IBM.	Specify the IBM ECM SM CALA_REX Agent settings here
System Monitor	Anont softings
	CALA_REX Agent IP name vip-w2k8x64r2.p8demo.com
	Additional CALA_REX parameters - for instance CALA_REX agent port settings listenport=127.0.0.1:23704;localport=192.168.240.234
	Agent ID Service Postfix (AIX: max 8 characters) agent-vip
	Agent description Agent using vircual iP address
	Windows only: Password of CALA_REX user *********
	Optional: CALA_REX Agent IP-address, required for HA environments 192.168.240.234
	Optional: CALA_REX libpathadd variable
	Enable installer debugging
InstallAnywhere Cancel Help	Previous Next



This hostname and IP address will be used in subsequent CALA agent installations or updates. It can be manually changed in the "Set configuration variables" menu of the CALA installer. The parameter is named "IP address to use as origin for events".

IBM ECI	۲ SM Non Core Client Installation 📃 🗉 🛽 ک	3			
File Help					
0					
	Set configuration variables				×
	Global settings:				1
	DO NOT CHANGE the Installation Type SETTING - This is a agent configuration	CLIENT	Default	?	=
	IBM ECM SM CALA Monitoring Agent Service name	IBM ECM SM CALA Monitoring Agent	Default	?	
Install info	List of ECM SM Event Servers	w2k8x64r2	Default	?	
	Remote ECM SM Event Server port	23840	Default	?	
Product:	IP address to use as origin for events	192.168.240.234	Default	?	
Hostname	Local port for Monitoring Agent to server communication		Default	?	
Operating	Encryption level for server communication		Default	?	
- Install diro	Minimum port for internal Monitoring Agent communication	44001	Default	?	
Source dir	Maximum port for internal Monitoring Agent communication	45000	Default	?	
Target dire	Start port for Monitoring Agent components	23831	Default	?	
JDK path					
Instan opti	▶ Base system womoning				
✓ Reconfi	✓ Windows Eventlogs				
Create	Windows Eventlogs system, application		Default	?	
Uninsta	P		D-614	2	
- Selected c					
This is an I	Ok	Cancel			
	Install and configure Exit Help				
	Hatan and configure LAR help				

Set configuration variables: IP Address of agent

ECM SM Agent multi agent / multi destination CALA_REX and CALA installation

ECM SM agents are installed with so called Instance ID's. With this functionality more than one CALA_REX and CALA agent can be installed on one single system. For more details about CALA_REX installation parameters see chapter CALA_REX Installation.

Additionally the ECM SM CALA agent supports multi-server configuration. This means that events from one CALA agent can be forwarded to more than one ECM SM server in parallel.

CALA configuration settings

Configuration variables for ECM SM Client Unix

Global Settings

Select the checkbox "Global Settings" to activate this section.

IBM ECM SM Monitoring Agent name

Optional:Specifies the displayed daemon name. If unset "IBM ECM SM CALA Monitoring Agent" will be used.

Do NOT add non-ASCII characters, "#", ";" or "\$"!

List of ECM SM Event Servers

Required. Specify a list of ECM SM Event Servers.

If the list is separated by semicolon, the agent will send its events to the first server where connection is successful. The order describes the order the Monitoring Agent tries to connect to the Event Servers.

If the list is separated by comma, the agent will send its events to all given event servers.

Note: In the case more than one Event Server is installed you should specify all installed Event Server hostnames here to allow the agent to find the active Event Server itself without reconfiguration.

Note: In the case you already specified the list of Event Servers during the installation of the CALA_ REX Agent specify 'ALL_EVENT_SERVERS' as value.

Remote ECM SM Event Server port

Required. Specify the port on which the Event Server component on the ECM SM server is running.

Default setting is 23840.

IP address to use as origin for events

Optional. Specify the IP address that must be set as origin for events sent from this agent. Default value is the IP address specified in the ip-address parameter for CalaRex. If you leave this field empty, the IP address determined by nslookup will be used (this may lead to unexpected results on agents with multiple IP addresses).

Local port for Monitoring Agent to server communication

Optional. Specify the port that must be used locally for communication with the server. All outgoing data from the agent will be sent through this port. If you leave this field empty, each sending component will open a random port for itself.

Encryption level for server communication

Optional. Specify the encryption level (1-3) to use for communication with the server. If you leave this field empty, the encryption level will be set to "1".

Minimum port for internal Monitoring Agent communication

Optional. Specify the minimum port number to use for internal CALA communication. If you do not specify a port number range, random ports will be used for internal communication.

Default setting is 44001.

Maximum port for internal Monitoring Agent communication

Optional. Specify the maximum port number to use for internal CALA communication. If you do not specify a port number range, random ports will be used for internal communication.

Default setting is 45000.

Start port for Monitoring Agent components

Required. Specify the start port for CALA components. In the configuration file, each component will have a different port starting from this base port number.

Default setting is "23831".

Custom su program

Specify the name of a custom su program (Substitute user), which should be used instead of su. Note: Filename including path is required.

su parameters

Specify parameters that follow the custom 'su' program at the CLI before the user name is specified (example: If /opt/my_sy/my_su_proc is the custom su program and of this program requires the parameter -u to specify the username than enter '-u' here. Note: If 'sudo' is used specify '-H -u ' here.)

Additional su parameters

Specify required execution parameters that follow the username (example: If /opt/my_sy/my_su_proc is the custom su program and of this program requires the parameter -c to specify the command than enter '-c' here.) Note: the normal 'su' program would require '-c' here, too. Note: If 'sudo' is used leave this parameter unset.

Custom shell Binary

Due to issues with some shell implementations it is possible to specify a custom shell for tasks and monitors. Note: Filename including path is required, e.g. /opt/freeware/bin/bash.

Custom AWK Binary

Due to limilations with some awk / nawk implementations (AIX and HP-UX) it is possible to specify a custom awk for tasks and monitors. Note: Filename including path is required, e.g. /opt/local/bin/ gawk

Base System Monitoring

Select the checkbox "Base System Monitoring" to activate this section.

System Log

Select the checkbox "System Log" to activate this section.

Syslog settings

Optional. Specify a list of syslog settings separated by ";". Example is *.emerg;*.alert;*.crit;*.err. If you use 'USE_EXISTING_SETTINGS' the current settings will be used and Syslog monitoring will be activated.

To deactivate Syslog monitoring, proceed as follows:

- 1. Open the "Set Configuration Variables" dialog.
- 2. Uncheck the "System Log" entry.

3. Select any other logfile. This can be a valid logfile or a non-existing one (e.g. "Oracle Alert Log"). Do not specify a valid directory, if the logfile does not exist on the system or should not be monitored (you may leave the default value). Be sure, that at least one logfile is selected. Otherwise the installation will fail.

4. Reinstall the agent with the new settings.

The System Log will now be monitored no longer.

AIX Error Report

Select the checkbox "AIX Error Report" to activate this section.

Configure Error Report hardware check (AIX only)

Required. Specify "Yes" to enable the Error Report hardware check. If Error Report hardware check is already configured, this setting will be ignored.

Oracle Alert Logfiles

Select the checkbox "Oracle Alert Logfiles" to activate this section.

Oracle Alertlog Logfile directory

Required. To specify the directory where the Oracle Alert logfiles are located, replace <ORACLE_HOME> by your current installation setting, e.g. "/usr/ora920".

Oracle Listener Logfiles

Select the checkbox "Oracle Listener Logfiles" to activate this section.

Oracle Listener Logfile directory

Required. To specify the directory where the Oracle Listener logfiles are located, replace <ORACLE_HOME> by your current installation setting, e.g. "/usr/ora920".

Monitors for Oracle

Select the checkbox "Monitors for Oracle" to activate this section.

ORACLE_HOME directory

Required. Specify the setting of ORACLE_HOME, e.g. "/usr/ora920".

Oracle SID

Required. Specify the Oracle SID that you want to monitor.

Default setting is "orc1".

Oracle OS user

Required. Specify the OS user that must be used to execute Oracle commands.

Default setting is "oracle".

IBM FileNet Image Manager Logfiles

Select the checkbox "IBM FileNet Image Manager Logfiles" to activate this section.

Monitors for IBM FileNet Image Manager

Select the checkbox "Monitors for IBM FileNet Image Manager" to activate this section.

ServerLink Logfiles

Select the checkbox "ServerLink Logfiles" to activate this section.

CSAR, SSAR and ISAR (NLS) Logfiles

Select the checkbox "CSAR, SSAR and ISAR (NLS) Logfiles" to activate this section.

ISCE Logfiles

Select the checkbox "ISCE Logfiles" to activate this section.

ISCE Logfile name

Required. Specify the name of the ISCE logfile.

ISCE Logfile directory

Required. To specify the directory where the ISCE logfiles are located, replace <ISCE_Logging_ Directory> by your current installation setting.

Note: Use "/" instead of "\".

ACSAP Logfiles

Select the checkbox "ACSAP Logfiles" to activate this section.

ACSAP Logfile directory

Required. Specify the directory where the ACSAP logfiles are located, e.g "C:/ACSAP/logs".

Note: Use "/" instead of "\".

Apache Error Logfile

Required. Specify the name of the Apache error logfile, e.g. "ACSAP_J2EEDD_MM_YYYY*.txt".

You can use wildcards to monitor more than one logfile at once or placeholder for the actual date (DD, MM, YYYY).

BP8 Logfiles

Select the checkbox "BP8 Logfiles" to activate this section.

BP8 Logfile name

Required. Specify the name of the BP8 logfile.

BP8 Logfile directory

Required. To specify the directory where the BP8 logfile is located, replace <PB8_Logging_Directory> by your current installation setting.

Note: Use "/" instead of "\".

BP8 Logfile name

Required. Specify the name of the BP8 logfile.

BP8 Logfile directory

Required. To specify the directory where the BP8 logfile is located, replace <PB8_Operations_ Logging_Directory> by your current installation setting.

Note: Use "/" instead of "\".

ISRA Logfiles

Select the checkbox "ISRA Logfiles" to activate this section.

ISRA Logfile name

Required. Specify the name of the ISRA logfile. In most cases, this file is called "ISRA.log".

You can use wildcards to monitor more than one logfile at once (e.g. "ISRA*.log").

ISRA Logfile directory

Required. To specify the directory where the ISRA logfiles are located, replace <ISRA_Logging_Directory> by your current installation setting.

IBM P8 Process Engine Log files

Select the checkbox "IBM P8 Process Engine Log files" to activate this section.

P8 PE 5.0 Manager system Logfile name

Required. Specify the name of the P8 PE 5.0 Manager system logfile name. Default value: pemgr_system.log

P8 PE 5.0 Manager Log directory

Required. To specify the directory where the P8 PE Manager system logfile is located, replace <P8_5.0_Manager_Log_Directory> by the PE 5.0 Manager logfile path.

Example: /opt/IBM/ProcessEngine/data/logs

P8 PE 5.0 Server Logfile name

Required. Specify the name of the P8 PE 5.0 Server logfile name. Default value: pesvr_system.log

P8 PE 5.0 Server Log directory

Required. To specify the directory where the P8 PE 5.0 Server logfile is located, replace <P8_5.0_ Server_Log_Directory> by the PE 5.0 Manager logfile path.

Example for the virtual PE server called 'default': /opt/IBM/ProcessEngine/data/pesrv.default/logs

P8 Server Error Log

Select the checkbox "P8 Server Error Log" to activate this section.

P8 Server Error Logfile name

Required. Specify the name of the P8 Server Error logfile. Default value: p8_server_error.log

P8 Logfile directory

Required. To specify the directory where the P8 Server Error logfile is located, replace <P8_Logging_Directory> by your current installation setting.

Example for an IBM WebSphere based P8 server is: /opt/IBM/WebSphere/AppServer/profiles/default/FileNet/server1

PPM Tracefiles

Select the checkbox "PPM Tracefiles" to activate this section.

RMI Logfiles

Select the checkbox "RMI Logfiles" to activate this section.

Router Tracefiles

Select the checkbox "Router Tracefiles" to activate this section.

FileNet Listener

Select the checkbox "FileNet Listener" to activate this section.

Configuration file for FileNet Listener

Required. Specify the name of the FileNet Listener configuration file. The file must be located in the subdirectory "repos/install/custom" of the WebConsole server installation.

FileNet Content Services Logfiles

Select the checkbox "FileNet Content Services Logfiles" to activate this section.

FileNet Content Services Auditlog

Select the checkbox "FileNet Content Services Auditlog" to activate this section.

Verity Logfiles

Select the checkbox "Verity Logfiles" to activate this section.

Monitors for FileNet Content Services

Select the checkbox "Monitors for FileNet Content Services" to activate this section.

IBM Content Manager Version 8 Eventlog

Select the checkbox "IBM Content Manager Version 8 Eventlog" to activate this section.

Prefilter for incoming events from table ICMSTITEMEVENTS

Optional. Define a prefilter for incoming events from table ICMSTITEMEVENTS to process only those events that match this filter.

Prefilter for outgoing events from table ICMSTITEMEVENTS

Optional. Define a prefilter for outgoing events from table ICMSTITEMEVENTS to discard all events that match this filter.

Prefilter for incoming events from table ICMSTSYSADMEVENTS

Optional. Define a prefilter for incoming events from table ICMSTSYSADMEVENTS to process only those events that match this filter.

Prefilter for outgoing events from table ICMSTSYSADMEVENTS

Optional. Define a prefilter for outgoing events from table ICMSTSYSADMEVENTS to discard all events that match this filter.

IBM CM Library Server Logfile

Select the checkbox "IBM CM Library Server Logfile" to activate this section.

IBM CM Library Server Logfile directory

Required. To specify the directory where the Library Server logfile is located, replace <DB2CMV8_ HOME> by your current installation setting, e.g. "C:/Program FilesIBM/db2cmv8".

The logfile name and path can be found in the system administration client,

Library Server Parameters - Configurations - Library Server Configuration - Log and Trace - Trace file name

or with query "select LIBRARYSERVERID, TRACEFILENAME from ICMSTSYSCONTROL"

Note: Use "/" instead of "\".

IBM CM Library Server Logfile

Required. Specify the name of the Library Server logfile, e.g. "icmserver.log".

You can use wildcards to monitor more than one logfile at once (e.g. "icmserver*.log").
The logfile name and path can be found in the system administration client,

Library Server Parameters - Configurations - Library Server Configuration - Log and Trace - Trace file name

or with query "select LIBRARYSERVERID, TRACEFILENAME from ICMSTSYSCONTROL"

IBM Content Manager Version 8 Agent and Common Store Server Error Log

Select the checkbox "IBM Content Manager Version 8 Agent and Common Store Server Error Log" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Content Manager Version 8 Agent and Common Store Server Error Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

IBM Common Store Retrieve Logfile

Select the checkbox "IBM Common Store Retrieve Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Common Store Retrieve Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Common Store Retrieve Logfile.

IBM Common Store Archive Logfile

Select the checkbox "IBM Common Store Archive Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Common Store Archive Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Common Store Archive Logfile.

IBM Content Manager Resource Manager Migrator Logfile

Select the checkbox "IBM Content Manager Resource Manager Migrator Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Content Manager Resource Manager Migrator Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Content Manager Resource Manager Migrator Logfile.

IBM Content Manager Resource Manager Asyncr Logfile

Select the checkbox "IBM Content Manager Resource Manager Asyncr Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Content Manager Resource Manager Asyncr Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Content Manager Resource Manager Asyncr Logfile.

IBM Content Manager Resource Manager Logfile

Select the checkbox "IBM Content Manager Resource Manager Logfile" to activate this section.

IBM CM Resource Manager Logfile directory

Required. To specify the directory where the Resource Manager logfile is located, replace </br><WASHOME> by your current installation setting, e.g. "/usr/WASCMSTU01".

Note: Use "/" instead of "\".

IBM CM Resource Manager Logfile

Required. Specify the name of the Resource Manager logfile, e.g. "icmrm.logfile.413818".

You can use wildcards to monitor more than one logfile at once (e.g. "icmrm.logfile.*").

....

IBM Content Manager On Demand Database Log

Select the checkbox "IBM Content Manager On Demand Database Log" to activate this section.

IBM WebSphere Application Server System out / system error Logfiles

Select the checkbox "IBM WebSphere Application Server System out / system error Logfiles" to activate this section.

WAS system out / system error Logfile directory (first instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (first instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (second instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (second instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (third instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (third instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile.You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (fourth instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (fourth instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile.You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (fifth instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (fifth instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (sixth instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (sixth instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

Apache Access Logfiles

Select the checkbox "Apache Access Logfiles" to activate this section.

Apache Logfile directory

Required. To specify the directory where the Apache logfiles are located, replace <APACHE_HOME> by your current installation setting, e.g "/var/log/httpd".

Apache Access Logfile

Required. Specify the name of the Apache access logfile, e.g. "access_log".

You can use wildcards to monitor more than one logfile at once (e.g. "*access_log").

Apache Error Logfiles

Select the checkbox "Apache Error Logfiles" to activate this section.

Apache Logfile directory

Required. To specify the directory where the Apache logfiles are located, replace <APACHE_HOME> by your current installation setting, e.g "/var/log/httpd".

Apache Error Logfile

Required. Specify the name of the Apache error logfile, e.g. "error_log".

You can use wildcards to monitor more than one logfile at once (e.g. "*error_log").

Tivoli Storage Manager Logfiles

Select the checkbox "Tivoli Storage Manager Logfiles" to activate this section.

TSM dsierror logfile directory

Required. Specify the directory where the TSM logfiles are located.

Note: Use "/" instead of "\".

TSM logfile names to be checked

Required. Specify the name of the TSM logfile. You can use the wildcard "*" to monitor more than one logfile at once.

TSM dsmerror logfile directory

Required. Specify the directory where the TSM logfiles are located.

Note: Use "/" instead of "\".

TSM logfile names to be checked

Required. Specify the name of the TSM logfile. You can use the wildcard "*" to monitor more than one logfile at once.

ICC4SAP Error Logfiles

Select the checkbox "ICC4SAP Error Logfiles" to activate this section.

ICC4SAP Logfile directory

Required. Specify the directory where the ICC4SAP Error logfiles are located, e.g "/opt/IBM/IC-CSAP/Server/instances/RT1".

ICC4SAP Error Logfile

Required. Specify the name of the ICC4SAP Error logfile, e.g. "icc_error.log".

You can use wildcards to monitor more than one logfile at once or placeholder for the actual date (DD, MM, YYYY).

SAPIC Error Logfiles

Select the checkbox "SAPIC Error Logfiles" to activate this section.

SAPIC Logfile directory

Required. Specify the directory where the SAPIC Error logfiles are located, e.g "/opt/CENIT/importmanager-2.8/log".

SAPIC Error Logfile

Required. Specify the name of the SAPIC Error logfile, e.g. "sapic.log".

You can use wildcards to monitor more than one logfile at once or placeholder for the actual date (DD, MM, YYYY).

Agent waits for server to connect

Select the checkbox "Agent waits for server to connect" to activate this section.

Device to listen for server to connect

Required. Specify the local network device (ip address) on which the agent is listening for incoming requests from the server(s). This should be the address of the network card connected to the internal (private) network. Specify * to listen on all network devices.

Port to listen for server to connect

Required. Specify the local port on which the agent must listen for the server(s) to connect.

Default setting is "11030".

Servers ip address

Required. Specify the ip address of the server(s) allowed to connect to this agent. The ip address may contain the wildcard "*" to allow a range of ip addresses to connect (e.g. "10.0.114.*") or just "*" to allow all servers.

Local port on server which is used to connect

Required. Specify the port the server is connecting from or "*" to allow all server ports. If a specific port is given, the agent will only accept connections coming from this port.

Default setting is "11031".

Minimum encryption level to be used

Optional. Specify the encryption level (1-3) to use for communication with the server(s). If you leave this field empty, the encryption level will be set to "1".

Configuration variables for ECM SM Client Windows

Global Settings

Select the checkbox "Global Settings" to activate this section.

IBM ECM SM CALA Monitoring Agent Service name

Optional:Specifies the Windows Service name. If unset "IBM ECM SM CALA Monitoring Agent" will be used.

Do NOT add non-ASCII characters, "#", ";" or "\$"!

List of ECM SM Event Servers

Required. Specify a list of ECM SM Event Servers.

If the list is separated by semicolon, the agent will send its events to the first server where connection is successful. The order describes the order the Monitoring Agent tries to connect to the Event Servers.

If the list is separated by comma, the agent will send its events to all given event servers.

Note: In the case more than one Event Server is installed you should specify all installed Event Server hostnames here to allow the agent to find the active Event Server itself without reconfiguration.

Note: In the case you already specified the list of Event Servers during the installation of the CALA_ REX Agent specify 'ALL_EVENT_SERVERS' as value.

Remote ECM SM Event Server port

Required. Specify the port on which the Event Server component on the ECM SM server is running.

Default setting is 23840.

IP address to use as origin for events

Optional. Specify the IP address that must be set as origin for events sent from this agent. Default value is the IP address specified in the ip-address parameter for CalaRex. If you leave this field empty, the IP address determined by nslookup will be used (this may lead to unexpected results on agents with multiple IP addresses).

Local port for Monitoring Agent to server communication

Optional. Specify the port that must be used locally for communication with the server. All outgoing data from the agent will be sent through this port. If you leave this field empty, each sending component will open a random port for itself.

Encryption level for server communication

Optional. Specify the encryption level (1-3) to use for communication with the server. If you leave this field empty, the encryption level will be set to "1".

Minimum port for internal Monitoring Agent communication

Optional. Specify the minimum port number to use for internal CALA communication. If you do not specify a port number range, random ports will be used for internal communication.

Default setting is 44001.

Maximum port for internal Monitoring Agent communication

Optional. Specify the maximum port number to use for internal CALA communication. If you do not specify a port number range, random ports will be used for internal communication.

Default setting is 45000.

Start port for Monitoring Agent components

Required. Specify the start port for CALA components. In the configuration file, each component will have a different port starting from this base port number.

Default setting is "23831".

Base System Monitoring

Select the checkbox "Base System Monitoring" to activate this section.

Windows Eventlogs

Select the checkbox "Windows Eventlogs" to activate this section.

Windows Eventlogs

Required. Specify a comma-separated list of Windows eventlogs that must be monitored.

Prefilter for incoming events

Optional. Define a prefilter for incoming events to process only those events that match this filter.

A filter definition is structured like this:

* the eventlog names entered in the prefilter fields must match the names entered in the "Windows Eventlog names" field exactly (case-sensitive!)

* the eventlog name and its filters are separated by a colon (:): <eventlog>:<filterdefinition>

* filters for several eventlogs are separated by a percent sign (%): <eventlog1>:<filterdefinition1>%<eventlog2>:<filterdefinition2>

* a filter definition consists of one or more filter assignments

* each filter assignment contains a list of assignments: <key>=<value>

* several possible values for one key can be separated by a comma: <key>=<value1>,<value2>

* if filter assignments are separated by semicolons (;), both assignments must match to make the filter match: <key1>=<value1>;<key2>=<value2>

* if filter assignments are separated by pipe symbols (|), at least one of the assignments must match to make the filter match: <key1>=<value1>|<key2>=<value2>

Possible pre-filter keys are: eventid , eventtype and source. Note that space characters in the source name must be replaced by underscores (see examples below).

Examples:

application:eventtype=Information|source=SceCli;eventid=1202%system:eventtype=Information| source=User_Profile_Service;EventId=1111

This filter will match for:

application log: all events with Event Type "Information", all events with Event Source "SceCli" AND Event ID "1202"

system log: all events with Event Type "Information", all events with Event Source "User Profile Service" AND Event ID "1111"

application:eventtype=Information|source=SceCli;eventid=1202%system:eventtype=Information| source=TermDD;eventid=50|source=W32Time,Print

This filter will match for:

application log: all events with Event Type "Information", all events with Event Source "SceCli" AND Event ID "1202"

system log: all events with Event Type "Information", all events with Event Source "TermDD" AND Event ID "50", all events with Event Source "W32Time" OR "Print"

A useful filter for IBM ECM related Windows event logs is:

application:

source=IMS,VWServices,VWServicesAE,VWServicesPA,VWServicesPE,VWServicesPS,FileNET,Content_ Engine_File_Store_Service,Content_Engine_Object_Store_Service,Content_Engine_Content_ Cache_Service,FileNet_Publishing,FileNET_Content_Engine,VMAE_Publisher_ Service,AEEngine,CSMGR,ftserver,MSSQLSERVER,FileNETPrintService.

Prefilter for outgoing events

Optional. Define a prefilter for outgoing events to discard all events that match this filter.

A filter definition is structured like this:

* the eventlog names entered in the prefilter fields must match the names entered in the "Windows Eventlog names" field exactly (case-sensitive!)

* the eventlog name and its filters are separated by a colon (:): <eventlog>:<filterdefinition>

* filters for several eventlogs are separated by a percent sign (%): <eventlog1>:<filterdefinition1>%<eventlog2>:<filterdefinition2>

* a filter definition consists of one or more filter assignments

* each filter assignment contains a list of assignments: <key>=<value>

* several possible values for one key can be separated by a comma: <key>=<value1>,<value2>

* if filter assignments are separated by semicolons (;), both assignments must match to make the filter match: <key1>=<value1>;<key2>=<value2>

* if filter assignments are separated by pipe symbols (|), at least one of the assignments must match to make the filter match: <key1>=<value1>|<key2>=<value2>

Possible pre-filter keys are: eventid , eventtype and source. Note that space characters in the source name must be replaced by underscores (see examples below).

Examples:

application:eventtype=Information|source=SceCli;eventid=1202%system:eventtype=Information| source= User_Profile_Service;EventId=1111

This filter will match for:

application log: all events with Event Type "Information", all events with Event Source "SceCli" AND Event ID "1202"

system log: all events with Event Type "Information", all events with Event Source "User Profile Service" AND Event ID "1111"

application:eventtype=Information|source=SceCli;eventid=1202%system:eventtype=Information| source=TermDD;eventid=50|source=W32Time,Print

This filter will match for:

application log: all events with Event Type "Information", all events with Event Source "SceCli" AND Event ID "1202"

system log: all events with Event Type "Information", all events with Event Source "TermDD" AND Event ID "50", all events with Event Source "W32Time" OR "Print"

Monitors for MSSQL Server

Select the checkbox "Monitors for MSSQL Server" to activate this section.

Oracle Alert Logfiles

Select the checkbox "Oracle Alert Logfiles" to activate this section.

Oracle Alertlog Logfile directory

Required. To specify the directory where the Oracle Alert logfiles are located, replace <ORACLE_ HOME> by your current installation setting, e.g. "c:/ORANT".

Note: Use "/" instead of "\".

Oracle Listener Logfiles

Select the checkbox "Oracle Listener Logfiles" to activate this section.

Oracle Listener Logfile directory

Required. To specify the directory where the Oracle Listener logfiles are located, replace <ORA-CLE_HOME> by your current installation setting, e.g. "c:/ORANT".

Note: Use "/" instead of "\".

Monitors for Oracle

Select the checkbox "Monitors for Oracle" to activate this section.

ORACLE_HOME directory

Required. Specify the setting of ORACLE_HOME, e.g. "C:/ORANT".

Note: Use "/" instead of "\".

Oracle SID

Required. Specify the Oracle SID that you want to monitor.

Default setting is "orc1".

IBM FileNet Image Manager and WAL Logfiles

Select the checkbox "IBM FileNet Image Manager and WAL Logfiles" to activate this section.

Monitors for IBM FileNet Image Manager

Select the checkbox "Monitors for IBM FileNet Image Manager" to activate this section.

IBM Content Collector, IBM FileNet Email Manager & Records Crawler Logfiles

Select the checkbox "IBM Content Collector, IBM FileNet Email Manager & Records Crawler Logfiles" to activate this section.

ICC, EMM or RC Logfile created by ECM SM LogfileErrors monitor - reduced processing load

Select the checkbox "ICC, EMM or RC Logfile created by ECM SM LogfileErrors monitor - reduced processing load" to activate this section.

Name of Logfile generated by ECM SM Monitor LogfileErrors monitor, which reads errors from ICC, EMM or RC Logfile

Directory where logfile of ECM SM Monitor LogfileErrors is located, which reads errors from ICC, EMM or RC Logfile

Monitors for IBM Content Collector, IBM FileNet Email Manager & Records Crawler

Select the checkbox "Monitors for IBM Content Collector, IBM FileNet Email Manager & Records Crawler" to activate this section.

ServerLink 4 Logfiles

Select the checkbox "ServerLink 4 Logfiles" to activate this section.

CSAR, SSAR and ISAR (NLS) Logfiles

Select the checkbox "CSAR, SSAR and ISAR (NLS) Logfiles" to activate this section.

Capture Trace Logfiles

Select the checkbox "Capture Trace Logfiles" to activate this section.

Capture FaxEntry Logfiles

Select the checkbox "Capture FaxEntry Logfiles" to activate this section.

ISCE Logfiles

Select the checkbox "ISCE Logfiles" to activate this section.

ISCE Logfile name

Required. Specify the name of the ISCE logfile.

ISCE Logfile directory

Required. To specify the directory where the ISCE logfiles are located, replace <ISCE_Logging_ Directory> by your current installation setting.

Note: Use "/" instead of "\".

ACSAP Logfiles

Select the checkbox "ACSAP Logfiles" to activate this section.

ACSAP Logfile directory

Required. Specify the directory where the ACSAP logfiles are located, e.g "C:/ACSAP/logs".

Note: Use "/" instead of "\".

Apache Error Logfile

Required. Specify the name of the Apache error logfile, e.g. "ACSAP_J2EEDD_MM_YYYY*.txt".

You can use wildcards to monitor more than one logfile at once or placeholder for the actual date (DD, MM, YYYY).

IBM P8 Process Engine Log files

Select the checkbox "IBM P8 Process Engine Log files" to activate this section.

P8 PE 5.0 Manager system Logfile name

Required. Specify the name of the P8 PE 5.0 Manager system logfile name. Default value: pemgr_system.log

P8 PE 5.0 Manager Log directory

Required. To specify the directory where the P8 PE Manager system logfile is located, replace <P8_5.0_Manager_Log_Directory> by the PE 5.0 Manager logfile path.

Example: C:/Program Files/IBM/ProcessEngine/data/logs

Note: Use "/" instead of "\".

P8 PE 5.0 Server Logfile name

Required. Specify the name of the P8 PE 5.0 Server logfile name. Default value: pesvr_system.log

P8 PE 5.0 Server Log directory

Required. To specify the directory where the P8 PE 5.0 Server logfile is located, replace <P8_5.0_ Server_Log_Directory> by the PE 5.0 Manager logfile path.

Example for the virtual PE server called 'default': C:/Program Files/IBM/ProcessEngine/data/pesrv. default/logs

Note: Use "/" instead of "\".

BP8 Logfiles

Select the checkbox "BP8 Logfiles" to activate this section.

BP8 Logfile name

Required. Specify the name of the BP8 logfile.

BP8 Logfile directory

Required. To specify the directory where the BP8 logfile is located, replace <PB8_Logging_Directory> by your current installation setting.

Note: Use "/" instead of "\".

BP8 Logfile name

Required. Specify the name of the BP8 logfile.

BP8 Logfile directory

Required. To specify the directory where the BP8 logfile is located, replace <PB8_Operations_ Logging_Directory> by your current installation setting.

Note: Use "/" instead of "\".

ISRA Logfiles

Select the checkbox "ISRA Logfiles" to activate this section.

ISRA Logfile name

Required. Specify the name of the ISRA logfile. In most cases, this file is called "ISRA.log".

You can use wildcards to monitor more than one logfile at once (e.g. "ISRA*.log").

ISRA Logfile directory

Required. To specify the directory where the ISRA logfiles are located, replace <ISRA_Logging_ Directory> by your current installation setting.

Note: Use "/" instead of "\".

P8 Server Error Log

Select the checkbox "P8 Server Error Log" to activate this section.

P8 Server Error Logfile name

Required. Specify the name of the P8 Server Error logfile. Default value: p8_server_error.log

P8 Logfile directory

Required. To specify the directory where the P8 Server Error logfile is located, replace <P8_Logging_Directory> by your current installation setting.

Example for an IBM WebSphere based P8 server is: C:/Program Files/IBM/WebSphere/AppServer/profiles/default/FileNet/server1

Note: Use "/" instead of "\".

PPM Tracefiles

Select the checkbox "PPM Tracefiles" to activate this section.

RMI Logfiles

Select the checkbox "RMI Logfiles" to activate this section.

Router Tracefiles

Select the checkbox "Router Tracefiles" to activate this section.

Process Analyzer Logfiles

Select the checkbox "Process Analyzer Logfiles" to activate this section.

IBM FileNet Listener

Select the checkbox "IBM FileNet Listener" to activate this section.

Configuration file for IBM FileNet Listener

Required. Specify the name of the IBM FileNet Listener configuration file. The file must be located in the subdirectory "repos/install/custom" of the WebConsole server installation.

IBM FileNet Content Services Logfiles

Select the checkbox "IBM FileNet Content Services Logfiles" to activate this section.

IBM FileNet Content Services Auditlog

Select the checkbox "IBM FileNet Content Services Auditlog" to activate this section.

Verity Logfiles

Select the checkbox "Verity Logfiles" to activate this section.

Monitors for IBM FileNet Content Services

Select the checkbox "Monitors for IBM FileNet Content Services" to activate this section.

IBM Content Manager Version 8 Eventlog

Select the checkbox "IBM Content Manager Version 8 Eventlog" to activate this section.

Prefilter for incoming events from table ICMSTITEMEVENTS

Optional. Define a prefilter for incoming events from table ICMSTITEMEVENTS to process only those events that match this filter.

Prefilter for outgoing events from table ICMSTITEMEVENTS

Optional. Define a prefilter for outgoing events from table ICMSTITEMEVENTS to discard all events that match this filter.

Prefilter for incoming events from table ICMSTSYSADMEVENTS

Optional. Define a prefilter for incoming events from table ICMSTSYSADMEVENTS to process only those events that match this filter.

Prefilter for outgoing events from table ICMSTSYSADMEVENTS

Optional. Define a prefilter for outgoing events from table ICMSTSYSADMEVENTS to discard all events that match this filter.

IBM CM Library Server Logfile

Select the checkbox "IBM CM Library Server Logfile" to activate this section.

IBM CM Library Server Logfile directory

Required. To specify the directory where the Library Srever logfile is located, replace <DB2CMV8_ HOME> by your current installation setting, e.g. "C:/Program FilesIBM/db2cmv8".

The logfile name and path can be found in the system administration client,

Library Server Parameters - Configurations - Library Server Configuration - Log and Trace - Trace file name

or with query "select LIBRARYSERVERID, TRACEFILENAME from ICMSTSYSCONTROL"

Note: Use "/" instead of "\".

IBM CM Library Server Logfile

Required. Specify the name of the Library Server logfile, e.g. "icmserver.log".

You can use wildcards to monitor more than one logfile at once (e.g. "icmserver*.log").

The logfile name and path can be found in the system administration client,

Library Server Parameters - Configurations - Library Server Configuration - Log and Trace - Trace file name

or with query "select LIBRARYSERVERID, TRACEFILENAME from ICMSTSYSCONTROL"

IBM Content Manager Version 8 Agent and Common Store Server Error Log

Select the checkbox "IBM Content Manager Version 8 Agent and Common Store Server Error Log" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Content Manager Version 8 Agent and Common Store Server Error Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

IBM Common Store Retrieve Logfile

Select the checkbox "IBM Common Store Retrieve Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Common Store Retrieve Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Common Store Retrieve Logfile.

IBM Common Store Archive Logfile

Select the checkbox "IBM Common Store Archive Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Common Store Archive Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Common Store Archive Logfile.

IBM Content Manager Resource Manager Migrator Logfile

Select the checkbox "IBM Content Manager Resource Manager Migrator Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Content Manager Resource Manager Migrator Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

Required. Specify the name of the IBM Content Manager Resource Manager Migrator Logfile.

IBM Content Manager Resource Manager Asyncr Logfile

Select the checkbox "IBM Content Manager Resource Manager Asyncr Logfile" to activate this section.

Logfile directory

Required. Specify the directory where the IBM Content Manager Resource Manager Asyncr Logfiles are located.

You can use wildcards ("*" and "?") to searchin one than more directory.

Note: Use "/" instead of "\".

Logfile name

.

Required. Specify the name of the IBM Content Manager Resource Manager Asyncr Logfile.

IBM Content Manager Resource Manager Logfile

Select the checkbox "IBM Content Manager Resource Manager Logfile" to activate this section.

IBM CM Resource Manager Logfile directory

Required. To specify the directory where the Resource Manager logfile is located, replace </Replace AMASHOME> by your current installation setting, e.g. "/usr/WASCMSTU01".

Note: Use "/" instead of "\".

IBM CM Resource Manager Logfile

Required. Specify the name of the Resource Manager logfile, e.g. "icmrm.logfile.413818".

You can use wildcards to monitor more than one logfile at once (e.g. "icmrm.logfile.*").

IBM Content Manager On Demand Database Log

Select the checkbox "IBM Content Manager On Demand Database Log" to activate this section.

IBM WebSphere Application Server System out / system error Logfiles

Select the checkbox "IBM WebSphere Application Server System out / system error Logfiles" to activate this section.

WAS system out / system error Logfile directory (first instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (first instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (second instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (second instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (third instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (third instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (fourth instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (fourth instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile.You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (fifth instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (fifth instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile.You can specify comma separated files, if you want to check more than one file in the previously defined directory

WAS system out / system error Logfile directory (sixth instance/server/profile)

Required. To specify the directory where the WAS system output / system error logfiles are located. Leave this parameter unset to ignore this parameter.

Note: Use "/" instead of "\".

WAS system out / system error Logfile name (sixth instance/server/profile)

Required. Specify the name of the WAS system out / system error logfile. You can specify comma separated files, if you want to check more than one file in the previously defined directory

Apache Access Logfiles

Select the checkbox "Apache Access Logfiles" to activate this section.

Apache Logfile directory

Required. To specify the directory where the Apache logfiles are located, replace <APACHE_ HOME> by your current installation setting, e.g. "c:/Program Files/Apache Group/apache2".

Note: Use "/" instead of "\".

Apache Access Logfile

Required. Specify the name of the Apache access logfile, e.g. "access.log".

You can use wildcards to monitor more than one logfile at once (e.g. "*access.log").

Apache Error Logfiles

Select the checkbox "Apache Error Logfiles" to activate this section.

Apache Logfile directory

Required. To specify the directory where the Apache logfiles are located, replace <APACHE_ HOME> by your current installation setting, e.g. "c:/Program Files/Apache Group/apache2".

Note: Use "/" instead of "\".

Apache Error Logfile

Required. Specify the name of the Apache error logfile, e.g. "error.log".

You can use wildcards to monitor more than one logfile at once (e.g. "*error.log").

Tivoli Storage Manager Logfiles

Select the checkbox "Tivoli Storage Manager Logfiles" to activate this section.

TSM dsierror logfile directory

Required. Specify the directory where the TSM logfiles are located.

Note: Use "/" instead of "\".

TSM logfile names to be checked

Required. Specify the name of the TSM logfile. You can use the wildcard "*" to monitor more than one logfile at once.

TSM dsmerror logfile directory

Required. Specify the directory where the TSM logfiles are located.

Note: Use "/" instead of "\".

TSM logfile names to be checked

Required. Specify the name of the TSM logfile. You can use the wildcard "*" to monitor more than one logfile at once.

ICC4SAP Error Logfiles

Select the checkbox "ICC4SAP Error Logfiles" to activate this section.

ICC4SAP Logfile directory

Required. Specify the directory where the ICC4SAP Error logfiles are located, e.g "C:/IBM/IC-CSAP/Server/instances/RT1".

Note: Use "/" instead of "\".

ICC4SAP Error Logfile

Required. Specify the name of the ICC4SAP Error logfile, e.g. "icc_error.log".

You can use wildcards to monitor more than one logfile at once or placeholder for the actual date (DD, MM, YYYY).

SAPIC Error Logfiles

Select the checkbox "SAPIC Error Logfiles" to activate this section.

SAPIC Logfile directory

Required. Specify the directory where the SAPIC Error logfiles are located, e.g "C:/CENIT/import-manager-2.8/log".

Note: Use "/" instead of "\".

SAPIC Error Logfile

Required. Specify the name of the SAPIC Error logfile, e.g. "sapic.log".

You can use wildcards to monitor more than one logfile at once or placeholder for the actual date (DD, MM, YYYY).

Agent waits for server to connect

Select the checkbox "Agent waits for server to connect" to activate this section.

Device to listen for server to connect

Required. Specify the local network device (ip address) on which the agent is listening for incoming requests from the server(s). This should be the address of the network card connected to the internal (private) network. Specify * to listen on all network devices.

Port to listen for server to connect

Required. Specify the local port on which the agent must listen for the server(s) to connect.

Default setting is "11030".

Servers ip address

Required. Specify the ip address of the server(s) allowed to connect to this agent. The ip address may contain the wildcard "*" to allow a range of ip addresses to connect (e.g. "10.0.114.*") or just "*" to allow all servers.

Local port on server which is used to connect

Required. Specify the port the server is connecting from or "*" to allow all server ports. If a specific port is given, the agent will only accept connections coming from this port.

Default setting is "11031".

Minimum encryption level to be used

Optional. Specify the encryption level (1-3) to use for communication with the server(s). If you leave this field empty, the encryption level will be set to "1".

Appendix A. Further CALA_REX installation and configuration options

Installing CALA_REX to run as non-root

If CALA_REX is not installed as user root or administrator, configuring of autostart may fail because of lacking permissions. This can be configured retrospectively by calling the script **cr_cli_cfg.sh** (CALA_REX client) or **cr_srv_cfg.sh** (CALA_REX server).

If CALA_REX is not installed as user root on UNIX / Linux systems the Syslog settings cannot be changed/adjusted by the CALA installation program. If Syslog monitoring is required use 'USE_EXISTING_SETTINGS' (the default value) for the Syslog settings. Note: If changes cannot be done no warning or error message is displayed during CALA installation.

NOTE If the CALA_REX client or server has been installed from root or Administrator, the steps described in this chapter have already been performed and don't need to be executed again.

Running shell scripts on Microsoft Windows

The shell scripts described above need the Windows shell to be in the path. Please set the environment variable CENIT_ROOT to your cenit-root directory and add %CENIT_ROOT%/shell to the PATH environment variable.

The shell scripts are started with the command

```
sh.exe [script-name] [script parameters]
```

Creating the environment scripts

Write access to /etc/cenit is needed for this step.

The environment script is used from ECM SM applications to determine the cenit-root directory. The script is named set_cenit_env.sh and is located in the cenit-root directory. The directory /etc/cenit contains a link to this script.

The script cr_cli_cfg.sh (cr_srv_cfg.sh for CALA_REX server) is used to create and remove the env script and the link in /etc/cenit. Before calling this script, the environment variable CENIT_ROOT needs to be set.

NOTE On UNIX systems, you need root permissions to execute both calls successfully as the calls create links in /etc and entries in /etc/inittab (see section The autostart links below for details).

To create the script and link call:

cr_cli_cfg.sh create-env-script

The both files are removed by calling:

cr_cli_cfg.sh remove-env-script

On Microsoft Windows systems, a copy of the original set_cenit_env.sh script is located in [System-Root]/system32/Drivers/etc/cenit.

Configuring autostart

To configure CALA_REX for autostart call:

cr_cli_cfg.sh autostart

To remove CALA_REX from the startup procedure, call the script with the remove-autostart parameter:

cr_cli_cfg.sh remove-autostart

NOTE You will need administrative permissions to add or remove CALA_REX to/from autostart.

The autostart links

On Microsoft Windows, CALA_REX client and server are registered as service and can therefore be managed via the Windows service manager.

On Unix systems, the script creates links in the **init.d** directories. The location of the init scripts depends on the operating system, refer to the following table for information (for CALA_REX server replace **FileNet-CrxCli** with **FileNetCrxSrv**).

If an installation id is given during install, the links are extended with the installation id as a postfix.

Operating system	path of start/stop script	autostart links
AIX	/etc/rc.FileNetCalaRexCli	entry in /etc/inittab
Linux	/etc/init.d/FileNetCalaRexCli	/etc/init.d/rc3.↓ d/S500FileNetCalaRexCli
		/etc/init.d/rc5.↓ d/S500FileNetCalaRexCli
		/etc/init.d/rc3.↓ d/K500FileNetCalaRexCli
		/etc/init.d/rc5.↓

Operating system	path of start/stop script	autostart links
		d/K500FileNetCalaRexCli
HP-UX	/sbin/init.d/FileNetCalaRex- Cli	/sbin/rc3.d/S500FileNetCalaRex.J Cli /sbin/rc0.d/K500FileNetCalaRex.J Cli
SUN Solaris	/etc/init.d/FileNetCalaRexCli	/etc/rc3.d/S500FileNetCalaRexCli
		/etc/rc0.d/K500FileNetCalaRexCli

The start/stop script is a link to CALA_REX.sh in the CALA_REX installation directory.

Adjusting CALA_REX configuration settings

Note: A administrator requires write access to the configuration file and directory to change the CALA_REX configuration files. Starting the configuration commands (see below) requires the same rights.

After installing the CALA_REX client, you can adjust the settings with the script **cr_cli_cfg.sh**. On the CALA_REX server, the configuration script is called **cr_srv_cfg.sh**. The parameters accepted by these scripts are the same.

Usage:

./cr_srv_cfg.sh configure <option>=<value>

./cr_cli_cfg.sh configure <option>=<value>

The following table shows the available options and their default values, without the transaction log parameters. The latter are described in their own section below.

Option	Description and default value	Note
debugfile	the name of the debugfile	
debuglevel	the debug level (0 - log all 9 - log fatal errors only) Default Value: 0	
listenport	port to accept connections on format: hostname:port Default Value:	
	127.0.0.1:23802 (server) 127.0.0.1: 23804 (client)	
description	machine description	
ip-address	the machines ip address Default Value: automatically detected	
	the CENIT ROOT directory	
cenit-instid	the installation id (if several instances are installed on one machine)	
tempdir	the directory used for temporary files	
pathadd	a string to add to the PATH of child processes	
libpathadd	a string to add to the libpath variable of child processes	
usessl	switch for using SSL possible values: true, false Default Value:	

Option	Description and default value	Note
	true	
pingperiod	the period (in seconds) to check if the server connection is alive Default Value:	
	120	
server	the host and port of the CALA_REX serv- er format: hostname:port	client only
localport	the outgoing port when connection to the server, format: hostname:port Default Value:	client only
	automatically assigned	
java.argument.%d	arguments to be passed to the java vir- tual machine (replace %d with a number starting from 0)	server only
java.libjvm	name, or path an name of the java virtual machine library to be used Default Value:	server only
	jvm on Windows, libjvm on Unix	
hostdb.database	the url of the database holding the hosts table Default Value:	server only
	(see Format of database urls)	
hostdb.databasehost	the host running the database Default Value:	server only, not used in the jdbc context
	127.0.0.1	
hostdb.user	the user for accessing the host table Default Value:	server only
	webtpladmin	
hostdb.passwd	the (encrypted) password for accessing the hosts table Default Value:	server only
	00001204190d081409081e00	
hostdb.table	the name of the hosts table Default Value:	server only
	CALA_REX_hosts	
hostdb.col.hostname	the name of the hostname column Default Value:	server only
	Hostname	
hostdb.col.description	the name of the host description column Default Value:	server only

Option	Description and default value	Note
	Description	
hostdb.col.os	the name of the hosts' operating system column Default Value:	server only
	os	
hostdb.col.cenit_root	the name of the hosts' cenit root column Default Value:	server only
	CENIT_ROOT	
hostdb.col.↓ cala_rex_version	the name of the hosts' CALA_REX ver- sion column Default Value:	server only
	CALA_REX_Version	
hostdb.col.ip_address	the name of the hosts' ip address column Default Value:	server only
	IP_Address	
hostdb.col.status	the name of the hosts' status column Default Value:	server only
	Status	
hostdb.col.ciphers	The database column to receive the cipher algorithms used on the client connection Default Value:	server only
	CSM_CIPHERS	
hostdb.col.cert	The database column to receive the client's certification data Default Value:	server only
	CSM_CERT	
hostdb.status.online	the value for "host is online" Default Value:	server only
	online	
hostdb.status.offline	the value for "host is offline" Default Value:	server only
	offline	
hostdb.col.type	the name of the hosts' type column Default Value:	server only
	Туре	
hostdb.type.server	the value for "host is running CALA_REX server" Default Value:	server only
	SERVER	

Option	Description and default value	Note
hostdb.type.client	the value for "host is running CALA_REX client" Default Value:	server only
	CLIENT	
permdb.database	the url of the database holding the user permissions table Default Value: (see Format of database urls)	server only, not used in the jdbc context
permdb.user	the user for accessing the permissions table Default Value: webtpladmin	server only
permdb.passwd	the (encrypted) password for accessing the permissions table Default Value: 00001204190d081409081e00	server only
permdb.table	the name of the permissions table Default Value: rights	server only
permdb.field.user	the name of the user column Default Value: User	server only
permdb.field.passwd	the name of the password column Default Value: password	server only
permdb.perms.table	the name of the privileges table Default Value: user_priv	server only
permdb.perms.field.user	the name of the user column in the privi- leges table Default Value: User	server only
permdb.perms.field.type	the name of the type column in the privi- leges table Default Value: Type	server only
permdb.perms.field.allow	the name of the allowed column in the privileges table Default Value: allow	server only

Option	Description and default value	Note
permdb.perms.field.deny	the name of the deny column in the privi- leges table Default Value:	server only
	deny	
ssl.allowanoncnx	Specifies for which connection types anonymous connections are allowed. One of the values: none, auto, appli- cation, server, client, client_ and_J application Default Value: client_and_application (srv)	auto allows anony- mous connections only if the file specified in ssl.trustcert.file is not found.
ssl.trustcert.file	Default Value:	
	ROOT/keys/trusted	
	cas.pem	
ssl.trustcert.dir	A directory containing trusted certificates Default Value:	
	NULL	
ssl.cipherlist	The list of ciphers to use (see OpenSSL documentation for details) Default Value:	
	ALL:!LOW:~	
	!EXP:	
	!MD5:↓ @STRENGTH	
ssl.verifydepth	The maximum length of the verify chain. Default Value:	
	3	
ssl.certificatestore	The name of the certificate store file. This file contains the certificates to be send to the peer. It may contain several certificates (e.g. some certificates of the certificate chain) Default Value:	
	\$CENIT	
	ROOT/keys/cala_rex_↓	
	srv_cert.J	
l		I
Option	Description and default value	Note
-----------------------	---	------
	\$CENIT_↓ ROOT/keys/cala_rex_↓ cli_cert.↓ pem (Cli)	
ssl.keystore	The name of the keystore file. This files contains the private key Default Value: \$CENIT_J ROOT/keys/cala_rex_J srv_priv.J pem (srv) \$CENIT_J ROOT/keys/cala_rex_J cli_priv.J pem (Cli)	
ssl.keystore.password	The password for opening the keystore file (pwdcrypt encrypted) Default Value: 11201e1900242a0b1733041d00313 30b0116422a1600 (srv) 11201e1900242a1b3e50171606313 30b0116422a1600 (cli)	

The value may contain reference to environment variables or to other properties defined before.

The syntax for referring environment variables is:

\$(env:[variable_name])

prior defined properties can be accessed using the following syntax:

\$(prop:[property_name])

NOTE The \$ symbol needs to be quoted if passed as a parameter to the cfg script.

Examples

To add the directories /usr/local/bin and /etc/Tivoli/bin to the PATH setting, enter the following command:

./cr_cli_cfg.sh configure 'pathadd=/usr/local/bin:/etc/Tivoli/bin'

NOTE On Windows systems, the existing pathadd entry for the shell (\$(prop:cenit-root)/shell) must not be removed. If you need to add more entries to the path, you must always add the entry for the shell as well, e.g.

./cr_cli_cfg.sh configure 'pathadd=\$(prop:cenit-root)/shell:C:/Tools/perl/bin'

Format of database urls

Database urls must be given in the following format: <ctk-driver class>:<jdbc-driver class>:<jdbc-url>

The CTK Driver class must be *de.cenit.eb.sm.ctk.db.DB2CTKDriver* when accessing a DB2 database or *de.cenit.eb.sm.ctk.db.DefaultCTKDatabaseDriver* for all other databases.

de.cenit.eb.sm.ctk.db.DefaultCTKDatabaseDriver:com.mysql.jdbc.Driver:jdbc:mysql://
localhost/CALA

Example url for accessing the mysql database CALA

Additional configuration settings for authentication for the CALA_REX server (JAAS configuration)

ECM SM uses JAAS for authenticating users. For details about JAAS see the JAAS Homepage at <u>http://</u>docs.oracle.com/javase/7/docs/technotes/guides/security/jaas/JAASRefGuide.html.

On the ECM SM server, there are two additional configuration files for user authentication: \$__envvar_CENIT_ROOT_name__/cala_rex_cala_rex_auth.cfg and \$__envvar_CENIT_ROOT__
name__/cala_rex/cala__J
rex_altauth.cfg.

These files configure the authentication mechanism used for authenticating users. The file cala_rex_auth.cfg configures the authentication mechanism to be used for normal users. A special authentication mechanism can be configured for exactly one user in the file cala_rex_altauth.cfg.

<propertygroup name="alt.authentication"> <property name="alt.user" value="admin"></property> <property name="implementation.class" value="de.cenit.eb.sm.ctk.aal.DefaultAALDriver"></property> <!-- configuration for the kerberos login--> <propertygroup name="loginmodule.0"> <propertygroup name="loginmodule.0"> <property name="class" value="com.sun.security.auth.module.Krb5LoginModule"></property> <property name="controlflag" value="required"></property> <property name="systemproperties"> <property name="java.security.krb5.realm" value="MYFSMDOMAIN"></property> <property name="java.security.krb5.realm" value="MYFSMDOMAIN"></property> <property name="java.security.krb5.kdc" value="dc.myfsmdomain.example"></property> </property></propertygroup> <property name="useTicketCache" value="true"></property> <property name="icketCache" value="fulser_krb5cc\"></property></propertygroup></propertygroup>	
<property name="useTicketCache" value="true"></property> <property name="ticketCache" value="\${user.krb5cc}"></property>	

</propertygroup>

An example cala_rex_altauth.cfg file

The format of both files is nearly identical. The property *alt.user* is only valid in the **cala_rex_altauth. cfg** file.

The name of the outermost property group must be *authentication* in **cala_rex_auth.cfg** and *alt.authentication* in **cala_rex_altauth.cfg**.

The *implementation.class* property is ECM SM internal and should always been set to *de.cenit. eb.sm.ctk.aal.*...*DefaultAALDriver.*

JAAS supports configurations with several login mechanism (implemented in so called login modules) to be chained. Add a property group for each login module to be used. The groups are named loginmodule followed by a period and serial number (starting with 0). For each group the following parameters can be configured:

- *class*: the module implementation class
- controlflag: sets the module's control flag, JAAS supports the following values: required, requisite, sufficient and optional

There are also two property groups to configure the login module. The property group *systemproperties* specifies the java system property settings to be passed to the module, the group *options* specifies the options to be passed to the login module. For the supported system properties and options refer to the documentation of the used login module.

Configuration options of the ECM SM native login module

The ECM SM login module is implemented in the class *de.cenit.eb.sm.ctk.aal.module.CtkWebTemplateLoginModule* and supports the following options (system property settings are not used):

- *database.url*: the database url (see Format of database urls)
- *database.user*: the name of the database user
- *database.passwd*:the (pwdcrypt encrypted) password of the database user
- *sql.getpasswd*: the sql statement for selecting a user's group (the string { 0 } is replaced with the username)
- *sql.getgroups*:the sql statement for getting the groups a user is assigned to (the string { 0 } is replaced with the username

Configuration options of the ECM SM JNDI login module

There is a also a login module for accessing JNDI sources (see the JNDI homepage at <u>http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/index.html</u>). This module can be used to access LDAP directory services and is implemented in the class *de.cenit.eb.sm.ctk.aal.e*

module.CtkAALJndiLoginModule.

The JNDI login module takes the following configuration options:

- initial.context.env.java.naming.↓
 factory.initial: Classname of the factory for creating the JNDI context.
- *initial.context.env.[varname]*: Sets an environment variable [varname] for creating the JNDI context object.
- *initial.context.env.provider.url*: The LDAP URL used for user authentication.
- group.provider.url: The URL used for finding the user's groups.
- group.query: The LDAP query for finding the user's groups.
- group.attribute: The attribute containing a group's name.
- group.name.pattern: A regular expression for post-processing the groupname returned by the query.
- group.name.index: The index of the groupname in the group mask specified.
- *authentication*: One of *internal* or *external*. Use *external* if authentication is done by another module e.g. the kerberos module. The *CtkAALJndiLoginModule* is used only for detecting the user's groups in this case.

These configuration parameters may contain the variables $\{ 0 \}$ (for username) and $\{ 1 \}$ (for password) which are replaced with the corresponding values.

```
<propertygroup name="authentication">
 <!-- To use the default configuration just adjust the two values
    "domain.name.uppercase" and "domain.controller.name".
 -->
 <!-- use the CTK ALL driver -->
 <property name="implementation.class" value="de.cenit.eb.sm.ctk.aal.DefaultAALDriver"/>
 <!-- configuration for the kerberos login -->
 <propertygroup name="loginmodule.0">
   <property name="class" value="com.sun.security.auth.module.Krb5LoginModule"/>
   <property name="controlflag" value="required"/>
   <propertygroup name="systemproperties">
     <!-- realm is the domain in uppercase letters:
         default value: DOMAIN in uppercase letters
      -->
     <property name="java.security.krb5.realm" value="FSMDOMAIN" />
     <!--kdc is the domain controller:
         default value: the name of the domain server
     -->
     <property name="java.security.krb5.kdc" value="dc.fsmdomain.example" />
   </propertygroup>
   <propertygroup name="options">
     <property name="useTicketCache" value="true"/>
     <property name="ticketCache" value="${user.krb5cc}"/>
   </propertygroup>
 </propertygroup>
 <!-- configuration for the group query via Idap -->
 <propertygroup name="loginmodule.1">
   <property name="class" value="de.cenit.eb.sm.ctk.aal.module.CtkAALJndiLoginModule"/>
```



An example configuration using the JNDI login module in combination with the kerberos login module

Additional configuration settings for the transaction log

The following table lists all possible transaction log specific CALA_REX configuration parameters.

NOTE For better visual appearance the prefix 'translog' is removed from every attribute in the following table.

name attribute	Description and allowed value(s) of the value attribute
.actions	Type of transactions to be logged. The values are identical to the values of the $TypeText$ field of the $CSM_DEF_TRANSTYPES$ database table. The default is to log all types of transactions (value = *). A list of values must be separated with spaces or commas. Allowed value(s) of the $value$ attribute:

name attribute	Description and allowed value(s) of the value attribute
	<pre>login, login-reply, get-file, put-file, list-files, list-clients, mkdir, exec, has- permission, status, ping, register, shut- down, *.</pre>
.target	Target of the log: <i>file</i> means a csv logfile, <i>db</i> means the server's database. The default is <i>db</i> . Allowed value(s) of the <i>value</i> attribute:
	file,db
.file.filename	If <i>target</i> is set to <i>file</i> , this property sets the path and filename the log should be written. If <i>target</i> is set to <i>db</i> , this property will be ignored. The filename can contain valid strftime format strings, which are evaluated the very first time, the file is created. The default is crxtlog.log . Allowed value(s) of the <i>value</i> attribute:
	<filename></filename>
.db.host	If target is set to <i>db</i> , this property sets the database table name, the log should be written. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_TRANSACTIONS</i> . Allowed value(s) of the <i>value</i> attribute:
	<database host=""></database>
.db.name	If target is set to <i>db</i> , this property sets the database name, the log should be written. If target is set to <i>file</i> , this prop- erty will be ignored. The default is <i>CALA</i> . But for a pro- ductive environment, it must be something like < <i>com</i> - <i>plete-jdbc-url>/CALA</i> . Allowed value(s) of the <i>value</i> attribute:
	<database name=""></database>
.db.user	If target is set to <i>db</i> , this property sets the user's name to access the database. If target is set to <i>file</i> , this property will be ignored. The default is <i>webadmin</i> . Allowed value(s) of the <i>value</i> attribute:
	<database user=""></database>
.db.passwd	If target is set to <i>db</i> , this property sets the database user's password. If target is set to <i>file</i> , this property will be ignored. The default is the standard password for the above named user. Allowed value(s) of the <i>value</i> attribute:
	<database password="" user's=""></database>
.db.logtable.tablename	If target is set to <i>db</i> , this property sets the data- base table name, the log should be written. If tar- get is set to <i>file</i> , this property will be ignored. The default is <i>CSM_TRANSACTIONS</i> for MySQL and <i>CALA.CSM_TRANSACTIONS</i> for DB2 and MS-SQL. Allowed value(s) of the <i>value</i> attribute:

	Departmention and allowed value(a) of the 3 attribute	
	Control and allowed value(s) of the value attribute Control and allowed value(s) of the value attribute	
	<database harne="" log="" table=""></database>	
.db.logtable.columns.selectid	If target is set to <i>db</i> , this property sets the column name for the select id in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_SELEC-</i> <i>TID</i> . Allowed value(s) of the <i>value</i> attribute:	
	<name column="" for="" in="" log="" selected="" table="" the=""></name>	
dh logtable gelumng ugername	If target is set to db this property sets the column name	
.ub.iogtable.columns.username	for the username in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_USER-NAME</i> .	
	Allowed value(s) of the <i>value</i> attribute:	
	<name column="" for="" in="" log="" table="" the="" username=""></name>	
.db.logtable.columns.clientip	If target is set to db , this property sets the column name for the client IP address in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_CLIENTIP</i> . Allowed value(s) of the <i>walue</i> attribute:	
	Allowed value(3) of the varue attribute.	
	<name client="" column="" for="" in="" ip="" log="" table="" the=""></name>	
.db.logtable.columns.↓ clientname	If target is set to <i>db</i> , this property sets the column name for the client hostname in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_CLIENTHOSTNAME</i> . Allowed value(s) of the <i>value</i> attribute:	
	<name client="" column="" for="" in="" log="" name="" table="" the=""></name>	
.db.logtable.columns.targetip	If target is set to <i>db</i> , this property sets the column name for the destination IP address in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_TARGETIP</i> . Allowed value(s) of the <i>value</i> attribute:	
	<name column="" for="" in="" ip="" log="" table="" target="" the=""></name>	
.db.logtable.columns.↓ targetname	If target is set to <i>db</i> , this property sets the column name for the destination hostname in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_TARGETHOSTNAME</i> . Allowed value(s) of the <i>value</i> attribute:	
	<name column="" for="" in="" log="" name="" table="" target="" the=""></name>	
.db.logtable.columns.type	If target is set to <i>db</i> , this property sets the column name for the transaction type in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_TYPE</i> . Allowed value(s) of the <i>value</i> attribute:	
	<name column="" for="" in="" log="" table="" the="" transaction="" type=""></name>	
.db.logtable.columns.starttime	If target is set to <i>db</i> , this property sets the column name for the start time of the transaction in the log table. If target	

name attribute	Description and allowed value(s) of the <i>value</i> attribute
	is set to <i>file</i> , this property will be ignored. The default is
	Allowed value(s) of the value attribute:
	<name column="" for="" in="" log="" starttime="" table="" the=""></name>
.db.logtable.columns.endtime	If target is set to <i>db</i> , this property sets the column name for the end time of the transaction in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_ENDTIME</i> . Allowed value(s) of the <i>value</i> attribute:
	<name column="" endtime="" for="" in="" log="" table="" the=""></name>
.db.logtable.columns.status	If target is set to <i>db</i> , this property sets the column name for the transaction status in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_STATUS</i> . Allowed value(s) of the <i>value</i> attribute:
	<name column="" for="" id="" in="" log="" status="" table="" the=""></name>
.db.logtable.columns.params	If target is set to <i>db</i> , this property sets the column name for the transaction parameters in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_PARAMETERS</i> . Allowed value(s) of the <i>value</i> attribute:
	<name column="" for="" in="" log="" parameters="" table="" the=""></name>
.db.logtable.columns.output	If target is set to <i>db</i> , this property sets the column name for the transaction output in the log table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_OUTPUT</i> . Allowed value(s) of the <i>value</i> attribute: <name column="" for="" in="" log="" output="" table="" the=""></name>
.db.ttypes.tablename	If target is set to <i>db</i> , this property sets the database table name of the possible transaction types. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_DEF_TRANSTYPES</i> . Allowed value(s) of the <i>value</i> attribute:
dh ttimog golumng id	If target is set to dh this property sets the column name
.ub.ttypes.corumns.ru	for the transaction type id in the types table. If target is set to $file$, this property will be ignored. The default is CSM_TYPEID . Allowed value(s) of the $value$ attribute:
	<name column="" for="" id="" in="" table="" the="" types=""></name>
.db.ttypes.columns.text	If target is set to <i>db</i> , this property sets the column name for the transaction description text in the types table. If tar- get is set to <i>file</i> , this property will be ignored. The de- fault is <i>CSM_TYPETEXT</i> . Allowed value(s) of the <i>value</i> attribute:

name attribute	Description and allowed value(s) of the value attribute
	<name column="" for="" in="" table="" text="" the="" types=""></name>
.db.stats.tabelname	If target is set to <i>db</i> , this property sets the database table name of the possible status values. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_DEF_TRANSSTATS</i> . Allowed value(s) of the <i>value</i> attribute: < <i>database status table name</i> >
.db.stats.columns.id	If target is set to <i>db</i> , this property sets the column name for the status type id in the status table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_STATUSID</i> . Allowed value(s) of the <i>value</i> attribute: < <i>name</i> for <i>id</i> column in the status table>
.db.stats.columns.text	If target is set to <i>db</i> , this property sets the column name for the status description text in the status table. If target is set to <i>file</i> , this property will be ignored. The default is <i>CSM_STATUSTEXT</i> . Allowed value(s) of the <i>value</i> attribute: <name column="" for="" in="" status="" table="" text="" the=""></name>

Most of the time, only the *translog.actions* property will be set to alter the default, which is to log all possible types of transactions.

Beside that, the *translog.target* is also of a broader interest. Through this property, the log can be redirected into a CSV file or a database. If the *translog.target* is set to *file*, the path of the filename must be set with the *translog.file.filename* property. The default is to log into the standard ECM SM database.

NOTE The file based logging should only be used for testing or debugging purposes.

Required adjustments on the server

On the server the supported Java version must be found in the PATH to allow execution of distributed tasks. Make sure that Perl 5 or higher is in the PATH as well. Otherwise, CALA installation will fail.

Required adjustments on the client

Make sure that Perl 5 or higher is in the PATH. Otherwise, CALA installation will fail.

Starting and Stopping CALA_REX daemons manually

Starting and Stopping CALA_REX services on Microsoft Windows

The CALA_REX client and server processes are installed as Windows services and can simply be started and stopped using the Microsoft Windows service manager. For default display and short-name of CALA_REX processes refer to the following table.

process type	display name	shortname
CALA_REX client	IBM CalaRex Client	CALA_REX_cli
CALA_REX server	IBM CalaRex Server	CALA_REX_srv

If an installation id has been given at installation time, the service display- and shortname are extended with this id as a postfix.

The processes can also be started or stopped using the **net** start and **net** stop commands, passing the service's shortname as parameter.

Examples

To start the CALA_REX client, enter at the command prompt:

net start CALA_REX_cli

To stop the CALA_REX server, enter at the command prompt:

net stop CALA_REX_srv

Starting and Stopping CALA_REX daemons in Unix systems

The CALA_REX daemons are started and stopped via the cala_rex.sh script. The scripts are located in the CALA_REX installation dir (\$CENIT_ROOT/CALA_REX) and take the arguments start, stop or restart.

Examples

To start the CALA_REX client or server daemon:

./CALA_REX.sh start

To stop the CALA_REX client or server daemon:

./CALA_REX.sh stop

Appendix B. How To...

Adding a new monitor command table to a configuration archive

The steps how to add a new monitor command table to an existing configuration archive are described in the CALA Monitoring Manager User's Guide, chapter *Adding a command table to a configuration archive*.

Adding a new logfile to a configuration archive

The following steps describe how to add a new logfile to the ECM SM monitoring.

NOTE Changing the configuration archives can result in a corrupt configurations and may lead to unspecified behaviour of the monitoring application. It should therefore only be performed by experienced ECM SM users.

When adding a new logfile configuration, the client configuration archives need adjusting.

The archives are located in the repository directory on the ECM SM server:

- <Installation-Directory>/repos/install/configurations/ on Linux and Unix servers
- <Drive>:<Installation-Directory>/repos/install/configurations/ on Windows servers

First of all, you need a .fmt or .v2s format description for the logfile to be monitored. See the V2SEditor User's Guide for how to create such files.

Adjusting the client archives

The client archives are named ECM <u>SM_CLIENT_<OS>.tar.gz</u>, while <OS> is either WINDOWS (for Microsoft Windows clients) or <u>UNIX</u> (for Linux and Unix clients).

- 1 Locate the archive to be changed and unpack it to a temporary directory. Use the command gzip dc <filename>.tar.gz|tar -xvf to unpack the archive, where <filename> is the path and name of the appropriate archive.
- 2 Choose a datatype for the new logfile. The datatype should be a alphanumerical string without spaces and special characters.
- 3 Copy the new format description file to the fmt/ subdir. Its name should be <datatype>.v2s
- 4 Create a <dataype>.cala in the tmp/<subdir>. An existing .cala (e.g. oraalert.cala) file can be used as a template. Be sure to adjust all paths before saving the new file.
- 5 Edit the file cala_defaults.txt from the package root dir, add a new entry: <datatype>;;SELECTION;;1. Setting SELECTION to 1 means, that the new data type is selected by default, setting it to 0 means that it has to be checked by the user.
- 6 Repack the directory. Call the following command from the temporary directory where the archive has been unpacked. Be sure, that <filename> also contains a path.

```
tar -cvf filename.tar .; gzip filename.tar
```

Change hostname or IP address of ECM SM server

If the hostname or ip address of the ECM SM server changes, some following steps have to be done before the change takes place.

Before you adjust configuration files on the server be aware all connected agents (managed systems) are prepared to connect to the changed server.

Run the 'Update CALA_REX' task on each agent

Run the 'Update CALA_REX# task on each agent. Specify the changed server name and if necessary the server port, too. The CALA_REX and CALA agent on the managed system will be reconfigured to the new server name (and port if specified) and restarted afterwards. Note: unless the Server is adjusted, too, the managed systems can no longer be monitored and managed.

In the case the ECM SM Server components are installed on more than one server be aware to specify the correct server names. The parameter 'CalaRex / Primary Server name' is the name of the server where the CALA_REX Server component is installed, the parameter 'Event Servers' contains the semicolon separated list of available Event Servers (please do not add blanks to the list of Event Servers).

After changing the server name on all connected agents the server have to be adjusted. The following next steps are required:

Shut down the ECM SM Event Server service

Shut down the ECM SM Event Server service. In the case the system runs on WebSphere stop the deployed WAS application.

Shut down the ECM SM GUI Server service

Shut down the ECM SM GUI Server service. In the case the system runs on WebSphere stop the deployed WAS application.

Shut down the ECM SM CALA_REX service

Shut down the ECM SM CALA_REX service.

After shut down of the Server services / agents the adjustment of configuration files is necessary:

\$CENIT_ROOT/cala_rex/cfg/cala_rex_finca.cfg

Verify and adjust the Database server name, if necessary.

\$CENIT_ROOT/cala_rex/cfg/cala_rex_srv.cfg

Verify and adjust the Database server name, if necessary.

\$CENIT_ROOT/.prodinfo/FSM_SERVER.settings

Verify and adjust the ECM SM server name and if necessary the Database server name.

\$CENIT_ROOT/eventserver/cfg/finca-cfg.xml

Verify and adjust the ECM SM server name of the Event Server

\$CENIT_ROOT/eventserver/cfg/db-cfg.xml

Verify and adjust the Database Server name of the Event Server

\$CENIT_ROOT/gui/cfg/finca-cfg.xml

Verify and adjust the ECM SM server name of the GUI Server

\$CENIT_ROOT/gui/cfg/db-cfg.xml

Verify and adjust the Database Server name of the GUI Server

\$CENIT_ROOT/downloadserver/cfg/finca-cfg.xml

Optional Verify and adjust the ECM SM server name of the Download Server service

\$CENIT_ROOT/initdb/cfg/db-cfg.xml

Verify and adjust the Database Server name of the initdb component (Database initialization)

\$CENIT_ROOT/cala/cala_variables.txt

Verify and adjust the ECM SM server name. Note: This file only exists in the case the Monitoring Agent CALA in installed on the ECM SM server

\$CENIT_ROOT/cala/logctlsrv.conf

Verify and adjust the ECM SM server name. Note: This file only exists in the case the Monitoring Agent CALA in installed on the ECM SM server

Now all stopped ECM SM services / agents can be restarted.

Restart the ECM SM Event Server service

Restart the ECM SM Event Server service. In the case the system runs on WebSphere start the deployed WAS application.

Restart the ECM SM GUI Server service

Restart the ECM SM GUI Server service. In the case the system runs on WebSphere start the deployed WAS application.

Restart the ECM SM CALA_REX Server service

Restart the ECM SM CALA_REX Server service.

On all administrative desktops the JAVA Webstart cache of the ECM SM applications need to be cleared before you use the applications again.

Start a Unix-like shell on Microsoft Windows

NOTE

The commands listed below are Unix shell commands. Users of Microsoft Windows need to open a command prompt window and call the following cmd script to open the bash:

```
<windowsDrive>:\<WindowsPath>\system32\drivers\etc\cenit
\start_shell.cmd
Example: c:\windows\system32\drivers\etc\cenit
\start_shell.cmd
```

If the shell has started successfully, the command promt bash\$ is printed. Unix shell commands can now be entered, the shell is left with the command **exit**.

Deinstall the ECM SM agent software

- Uninstall CALA using the CALA installer
- Uninstall the CALA_REX agent:
 - Microsoft Windows: Remove the CALA_REX agent with the Add or Remove Software (Windows) entry in the Administrative tools section or use the InstallAnywhere Uninstall-program (all platforms incl. Windows) to remove both CALA and CALA_REX from the agents.
 - Unix/Linux: Remove the CALA_REX agent by calling the uninstaller. The uninstaller can be found in the directory where the CALA_REX software is installed. There exists a sub-directory named Uninstall_IBM..._CALA_REX_Agent. Change into that directory and execute the uninstaller named Uninstall_IBM..._CALA_REX_Agent.
- The remaining content of the ECM SM client installation directory can be removed.

Deinstall the ECM SM server software

- Uninstall the ECM SM client software on the clients (seeDeinstall the ECM SM agent software).
- Uninstall CALA using the CALA installer
- Uninstall the CALA_REX server Remove the ECM SM Server software with the Add or Remove Software (Windows) entry in the Administrative tools section or use the InstallAnywhere Uninstall-program (all platforms incl. Windows) to remove both ECM SM from the server system.
- The remaining content of the ECM SM server installation directory can be removed. Note: in the directory \$CENIT_ROOT/.prodinfo you'll find several *.settings files. If you keep the .prodinfo directory with the *.settings files the installer can use the previous settings for later installation.
- Delete the database and its content used by ECM SM.

Reinstall CALA_REX agent or server

NOTE The commands listed below are Unix shell commands. The section Start a Unixlike shell on Microsoft Windows describes how to start a Unix-like shell on Microsoft Windows systems.

Reinstall CALA_REX agent

stop CALA_REX agent and remove start scripts/registry entries

```
cd $CENIT_ROOT
. ./set_cenit_env.sh
sh cala_rex/cala_rex.sh stop
sh cala_rex/cr_cli_cfg.sh remove-autostart
sh cala_rex/cr_cli_cfg.sh remove-env-script
```

reinstallCALA_REX agent, configure autostart and start the service

```
cd $CENIT_ROOT
. ./set_cenit_env.sh
sh cala_rex/cr_cli_cfg.sh create-env-script
sh cala_rex/cr_cli_cfg.sh autostart
sh cala_rex/cala_rex.sh start
```

Reinstall CALA_REX server

stop CALA_REX server and remove start scripts/registry entries

```
cd $CENIT_ROOT
. ./set_cenit_env.sh
sh cala_rex/cala_rex.sh stop
sh cala_rex/cr_srv_cfg.sh remove-autostart
sh cala_rex/cr_srv_cfg.sh remove-env-script
```

reinstallCALA_REX agent, configure autostart and start the service

```
cd $CENIT_ROOT
. ./set_cenit_env.sh
sh cala_rex/cr_srv_cfg.sh create-env-script
sh cala_rex/cr_srv_cfg.sh autostart
sh cala_rex/cala_rex.sh start
```

Move a ECM SM agent to another server

Adjust CALA configuration

It is strongly recommended to use the task 'Update CalaRex' from the 'Migration' task archive to connect the CALA_REX and CALA Monitoring agent to a new server.

• Load the file logctlsrv.conf in the cala subdir of your ECM SM into an editor.

NOTE Since the file may use Unix line separators, users of Microsoft Windows should should use WordPad instead of notepad for editing.

• Find the line staring with remote_calmon=. The hostname or ip address of the server is specified in the item starting with ip! and ending with a comma.

remote_calmon=ip!10.0.114.214,port!23840,conf!ip;port

Figure: An example configuration line from logctlsrv.conf

Adjust CALA_REX configuration

It is strongly recommended to use the task 'Update CalaRex' from the 'Migration' task archive to connect the CALA_REX and CALA agent to a new server.

• Load the file cala_rex_cli.cfg in the cala_rex subdir of your ECM SM into an editor.

NOTE

Since the file may use Unix line separators, users of Microsoft Windows should should use WordPad instead of notepad for editing.

• Find the line which configures the *server* property and alter it's value.

<property name="server" value="10.0.14.193:23802"/>

Figure: An example configuration line from cala_rex_cli.cfg

How to install ECM SM on a Windows Cluster

Requirements

- Running Windows Cluster with shared drive
- Working DNS for cluster name

The best way for running ECM SM in a cluster is to use a remote database.

Pre-Steps

First decide if you want to keep the required "3rd Party Software" local on each node, or if you want switch it as well.

Example of a working cluster

On the shared drive:

JDBC Driver

Installation

Begin with the installation on the active node and install everything you want to switch on the shared drive.

- Set your needed environment variables
- Run the graphical InstallAnywhere installeron the system
- Start the "WebConsole" and install the "CALA" part of the ECM SM Server (optional).

Take a look if the ECM SM servers registers with the cluster name in your "WebConsole" and if the events appear correct.

- Stop all the services for the Software you installed on the shared drive and switch the startup method to manual.
- Export the registry entries for "IbmFsmRap" and "IbmFsmSrv" and "CALA" (optional, if exists) and "cala_rex_srv" service to the shared drive. You can find them by executing regedit and browsing to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- Run the cluster administrator and move the active node.

Now the installation on the former active node is finished.

• On the node, that is active right now, please install again the software you wanted to keep local

• Then install again the software you wanted to have on the shared drive (e.g. JDBC driver)

Be sure to use the same installation directory as on the first node again.

- (Optional): Open a command line and switch to your <ECM SM-directory>\cala. Run cala_srv.exe auto to install the "CALA_REX" Service.
- Switch to CALA_REX folder (<ECM SM-directory>\cala_rex) and run cala_rex_srv.exe auto to install "CALA_REX" Service
- Import the previous export Services Entries for "IbmFsmRap" and "IbmFsmSrv" and "CALA" (optional, if exists) and "cala_rex_srv" by simply double clicking. This will overwrite the settings made from the manual service installation.
- Stop again all the services for the software you installed on the shared drive and switch the startup method to manual.
- Restart this node and move the cluster again.

The installation of the software is finished. Now the Cluster Administrator must be adjusted.

Preparing Cluster Administrator

When the second node is up again start the cluster administrator.

- Right click on the Cluster Group and add new Resource
- Give a name and choose "Generic Service" from Resource type.
- Leave the possible owners like it is
- From the dependencies choose the Cluster Name and the Shared drive
- Enter Service name for the application
- There is no need to add a Registry Key. Just click finish.

Repeat these steps for "IbmFsmRap" and "IbmFsmSrv" and "CALA" (optional, if exists) and "cala_rex_srv" Service. Start with "CALA_REX" and use the following dependencies: Cluster Name and Shared Drive.

The ECM SM cluster installation is now completed. Do some test by moving the active node and try the access the "WebConsole" on the clustername.

Switch the node during you have an opened "WebConsole" and see if you can access pages after successful cluster switch.

JVM Properties for an IBM WebSphere Based Installation

It is recommended to set the following environment variables in the IBM WebSphere server the application is running at; simply to avoid tedious repetitions of long paths.

View: All tasks
III Welcome
Guided Activities
Servers
Applications
Services
Resources
Security
Environment
 Virtual hosts Update global Web server plug-in configuration WebSphere variables Shared libraries Replication domains Naming OSGi bundle repositories
Monitoring and Tuning
Troubleshooting
Service integration
⊕ UDDI

Navigate to "Environment" > "WebSphere variables".

	ere Variables		4
ebS	phere Variables		
e th her grea	nis page to define substitution variables. Variables s server, node, cluster, or cell. Values at one scope li ater scope levels. Therefore, server variables overri	pecify a level of indirection for some system-defined values, such as avel can differ from values at other levels. When a variable has confl de node variables, which override cluster variables, which override cel	s file system root directories. Variables have a scope level, which icting scope values, the more granular scope value overrides val I variables.
Sco	pe: Cell=was7suseNode01Cell, Node=was7suseNo	de01, Server=server1	
	Scope specifies the level at which the resource of scope settings help. Node=was7suseNode01, Server=server1	efinition is visible. For detailed information on what scope is and ho	w it works, <u>see the</u>
Pre	ferences		
New	/ Delete		
3			
lect	Name 🗘	Value 🗘	Scope 🗘
ou c	an administer the following resources:		
	DB2UNIVERSAL JDBC DRIVER PATH	/root/db2jdbc	Node=was7suseNode01,Server=server1
			Node=was7suseNode01.Server=server1
-	ECM SM CONSOLE WAR	/opt/IBM/WebSphere/AppServer/ profiles/AppSrv01/installedApps/ was7suseNode01Cell/ECM_SM_SERVER.ear/war/ ECM_SM_SERVER_gui_app.war	
	ECM SM CONSOLE WAR	/opt/IEM/Websphere/AppServer/ profiles/AppSrov[Jinstalledpsrov] was7suseHode0icel/ECM_SM_SERVER.ear/war/ ECM_SM_SERVER_gui_app.war /opt/IEM/WebSphere/AppServer/profiles/ AppSr01/installedps/was7useNode0iCell/ ECM_SM_SERVERSERVER.ear/war/ ECM_SM_SERVER_erver_app.war/	Node=was7suseNode01.Server=server1
	ECM SM CONSOLE WAR	/opt/leM/Websphere/AppServer/ profiles/AppSrov[/installedpsrov] was7suseHode0iCell/ECM_SM_SERVER.ear/war/ ECM_SM_SERVER_gui_app.war /opt/IEM/WebSphere/AppServer/profiles/ AppSrov1/installedps/was7suseNode0iCell/ ECM_SM_SERVER_arver_app.war/ \${LOG_ROOT}/server1	Node=was7suseNode01.Server=server1

Create new "WebSphere variables" via "New". The necessary variables:

\${ECM_SM_CONSOLE_WAR}	/opt/IBM/WebSphere/AppServer/profiles/Ap- pSrv01/installedApps/was7suseNode01Cell/ ECM_SM_SERVER.ear/war/ ECM_SM_SERVER_gui_app.war
\${ECM_SM_SERVER_WAR}	/opt/IBM/WebSphere/AppServer/profiles/Ap- pSrv01/installedApps/was7suseNode01Cell/ ECM_SM_SERVERSERVER.ear/war/ ECM_SM_SERVER_server_app.war/

The following custom properties must be set for the application server's JVM the application is running with/ on.

View: All tasks	Cell=was7suseNo	de01Cell, Profile=AppSrv01			
Welcome	Application serve	ers		? -	
Guided Activities	Application se	rvers			
E Servers	Use this page to yiew a list of the application servers in your equipament and the status of each of these servers. You can also use this page to change the status of a specific application server.				
Server Types	Preferences				
WebSphere MQ servers	100 m	(1) 通			
	Name 🗘	Node 🗘	Host Name 🗘	Version 🗘	
Applications	You can administer the following resources:				
Services	server1	was7suseNode01	was7suse	Express 7.0.0.23	
Resources				JPA 2.0 Feature 1.0.0.7	
Security				OSGi Apps Feature 1.0.0.7	
Environment	Total 1				
Users and Groups					
Monitoring and Tuning					
Troubleshooting					
Service integration					
E DDI					

Navigate to "Servers" > "Server Types" > "WebSphere application servers" and click on your server.

this page to configure an application server. An application server is a server that time Configuration	provides services required to run enterprise applications.	
General Properties	Container Settings	
Name	Session management	
server1	SIP Container Settings	
Node name	Web Container Settings	
was7suseNode01	Portlet Container Settings	
Run in development mode	EJB Container Settings	
	Container Services	
V Parallel start	Business Process Services	
Start components as needed	Applications	
Access to internal server classes	Installed applications	
	Server messaging	
Server-specific Application Settings	Messaging engines	
Classloader policy Multiple	Messaging engine inbound transports	
Class leading mode	WebSphere MQ link inbound transports	
Classes loaded with parent class loader first	SIB service	
	Server Infrastructure	
	Java and Process Management	
Apply OK Reset Cancel	Class loader	

Click on the "Process definition" link under "Java and Process Management".

guadon	
eneral Properties	Additional Properties
Executable name	Java Virtual Machine
Executable arguments	Environment Entries
	Logging and tracing
Start command	
Charle and an annual second se	
Stop command	
Stop command arguments	
Working directory	
\${USER_INSTALL_ROOT}	
Executable target type	
JAVA_CLASS	
Even whether the second	

Click on the "Java Virtual Machine" link.

plication servers > server1 > Process definition > Java	a Virtual Machine	
nfiguration Runtime	hine settings.	
General Properties		Additional Properties
Classpath		Custom properties
Dest Classesth		
Boot Classpath		

Click on the "Custom properties" link.

Applic	plication servers > server1 > Process definition > Java Virtual Machine > Custom properties				
Use th	is page to specify an arbitrary name and value pair. The value that i	s specified for the name and value pair is a string that can set internal system configuration properties.			
E Pre	rerences				
Select	lect Name C Value C Des				
You d	ou can administer the following resources:				
	birt.resource.html	\${ECM_SM_CONSOLE_WAR}/reports/html			
	<u>birt.resource.pdf</u>	\${ECM_SM_CONSOLE_WAR}/reports/pdf			
	birt.root.dir	\${ECM_SM_CONSOLE_WAR}			
	com.ibm.security.igss.debug	off			
	com.ibm.security.krb5.Krb5Debug	off			
	de.cenit.eb.sm.finca.functional.services xml.config.filename	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/cfg/finca-cfg.xml			
	de.cenit.eb.sm.finca.functional.services_xml.config.filename.rap	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/cfg/finca+cfg.xml			
	de.cenit.eb.sm.finca.functional.services_xml.config.filename.server	\${ECM_SM_SERVER_WAR}/WEB-INF/res/cfg/finca-cfg.xml			
	de.cenit.eb.sm.finca.functional.services xml.config.main.path	cfg/			
	de.cenit.eb.sm.finca.functional.services_xml.config.main.pattern	finea-cfg.xml			
	de.cenit.eb.sm.finca.functional.services xml.config.main.root	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/			
	de.cenit.em.sm.pwdcrypt.agentid	mywasserver_primary			
	de.cenit.em.sm.pwdcrypt.keyfilecontent	:AES128:BASE64:wA6t+Vbtaqgda1/d118kloOY2cb6J657Hi9dpDKTr8Oc3M0pPiqkqbeVxrRWanKJLUg7vvtEaSatMl64b51kTK+JKDLj1vmonf7W37hYVw=			
	eclipse.consoleLog	true			
	<u>eclipse.log.level</u>	ALL			
	felix.fileinstall.dir	\${ECM_SM_SERVER_WAR}/WEB-INF/res/cfg/			
	finca.functional.usermgmt.icons	\$(ECM_SM_CONSOLE_WAR)/WEB-INF/res/icons			
	java.security.auth.login.config	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/auth/login.conf			
Total	18				

Create new "Custom properties" via "New". The necessary properties:

Property	Value
birt.root.dir	\${ECM_SM_CONSOLE_WAR}
birt.resource.html	\${ECM_SM_CONSOLE_WAR}/reports/html
birt.resource.pdf	\${ECM_SM_CONSOLE_WAR}/reports/pdf
eclipse.consoleLog	true
eclipse.log.level	ALL
finca.functional.usermgmt.icons	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/icons
java.security.auth.login.config	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/auth/ login.conf
de.cenit.eb.sm.finca.functional.services_xml.config. filename	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/cfg/ finca-cfg.xml
de.cenit.eb.sm.finca.functional.services_xml.config. filename.rap	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/cfg/ finca-cfg.xml
de.cenit.eb.sm.finca.functional.services_xml.config. filename.server	\${ECM_SM_SERVER_WAR}/WEB-INF/res/cfg/fin- ca-cfg.xml
de.cenit.eb.sm.finca.functional.services_xml.config. main.path	cfg/
de.cenit.eb.sm.finca.functional.services_xml.config. main.pattern	finca-cfg.xml
felix.fileinstall.dir	\${ECM_SM_SERVER_WAR}/WEB-INF/res/cfg/

© Copyright Cenit AG 2000, 2016, © Copyright IBM Corp. 2005, 2016

Property	Value
de.cenit.eb.sm.finca.functional.services_xml.config. main.root	\${ECM_SM_CONSOLE_WAR}/WEB-INF/res/
de.cenit.em.sm.pwdcrypt.agentid	You can define the agent ld by your- self, in lower case. Use the format <serverhostname>_primary.</serverhostname>
	E.g. mywasserver_primary
de.cenit.em.sm.pwdcrypt.keyfilecontent	Add the content of your keyfile in here. See the description (1) below this table for details.

(1) The following description shows how to create the keyfile.

- Open the cmd / bash and change directory to \$CENIT_ROOT
- set CENIT_ROOT=.
- jre\bin\java.exe -cp gui/jars/de.cenit/finca.functional.utils.jar de.cenit.eb.sm.finca.functional.utils.pwdcrypt.PwdCrypt -l <agetnld> In the example above, agent Id is "mywasserver_primary"
- The key will be printed out to the command line. Copy the complete key into the properties field of your WebSphere Adminsitrative Console.

C:\ECMSM52>java -cp gui/jars/de.cenit/finca.functional.utils.jar de.cenit.eb.sm.finca.functiona l.utils.pwdcrypt.PwdCrypt -l w2k8r264was855_primary agent52 :AES12B:BASE64:k15UU5n+vGu9mkNwaHhKsM359Tc83x9dFhtgY4ujB5gIuXasQDB4n7R1MbumHA/PRXEjACzOslnPk1vGi +C7TpYPpiFazM5bYLMnUC6t0Ww=

Creation of a datasource on IBM WebSphere

The creation of a datasource for the WebSphere based installation (e.g. Microsoft SQL Server):

View: All tasks
 Welcome
Guided Activities Guided Activi
E Servers Servers
Services
E Resources
 Schedulers Object pool managers JMS
 JDBC JDBC providers Data sources Data sources (WebSphere Application Server V4)

Security
Environment
Users and Groups
Monitoring and Tuning
Troubleshooting
Ervice integration
■ UDDI

Click on "Resources" > "JDBC Providers".

Cell=was7	/suseNode01Cell, Profile=AppSrv01				
JDBC prov	viders		?		
JDBC p	providers				
Use the enviror	is page to edit properties of a JDBC provider. The JDBC provid ment. Learn more about this task in a quided activity. A quid	ler object encapsulates the specific JDBC driver implementation ed activity provides a list of task steps and more general inform	class for access to the specific vendor database of your ation about the topic.		
E Sco	pe: Cell=was7suseNode01Cell, Node=was7suseNode01, Serv	er=server1			
	Scope specifies the level at which the resource definition is it works, <u>see the scope settings help.</u> Node=was7suseNode01, Server=server1	visible. For detailed information on what scope is and how			
🕀 Pret	erences				
New	New Delete				
Select	Name 🗘	Scope 🗘	Description 🗘		
You c	an administer the following resources:				
	DB2 Universal JDBC Driver Provider	Node=was7suseNode01,Server=server1	One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS and supports 2-phase commit processing.		
	Derby JDBC Provider	Node=was7suseNode01,Server=server1	Derby embedded non-XA JDBC Provider		
Total	2				

Select your scope in the dropdown box. Click "New" to create a new JDBC Provider.

→ Step 1: Create new	
Step 2: Enter database class path information Step 3: Summary	Create new JDBC provider Set the basic configuration values of a JDBC provider, which encapsulates the specific vendor JDBC driver implementation classes that are required to access the database. The wizard fills in the name and the description fields, but you can type different values. Soge Cells:wes7suseNode01Cell:nodes:wes7suseNode01:servers:server1 * Database type SQL Server SQL Server Connection pool data source Connection pool data sour

Step 1: Select the type of the provider. The necessary settings are shown in the screenshot above.

Step 1: Create new	Enter database class path information		
Step 2: Enter database class path information	Set the environment variables that represent the JDBC driver class files, which WebSphere(R) Application Server uses to define your JDBC provider. This wizard page displays the file names; you supply only the directory locations of the files. Use complete directory paths when you type the JDBC driver file locations. For example: C:\SQLLIB\yava on Windows(R) or /home/db2inst1/sqllib/java on Linux(TM).		
	If a value is specified for you, you may click Next to accept the value.		
	Class path:		
	\${MICROSOFT_JDBC_DRIVER_PATH}/sqljdbc.jar .::		
	Directory location for "sqljdbc.jar" which is saved as WebSphere variable \${MICROSOFT_DBC_DRIVER_PATH}		
	Native library path		
	Directory location which is saved as WebSphere variable \${MICROSOFT_JDBC_DRIVER_NATIVEPATH}		

Step 2: Nothing to do here.

ate a new JDBC Provider				
Create a new JDBC Provider				
Step 1: Create new	Summary			
Step 2: Enter	Summary of actions:	Summary of actions:		
database class path	Options	Values		
	Scope	cells:was7suseNode01Cell:nodes:was7suseNode01:servers:server1		
	JDBC provider name	Microsoft SQL Server JDBC Driver		
	Description	Microsoft SQL Server JDBC Driver. This provider is configurable in version 6.1.0.15 and later nodes.		
	Class path	\${MICROSOFT_JDBC_DRIVER_PATH}/sqljdbc.jar		
	\${MICROSOFT_JDBC_DRIVER_PATH}			
	Native path	\${MICROSOFT_JDBC_DRIVER_NATIVEPATH}		
	\${MICROSOFT_JDBC_DRIVER_NATIVEPATH}			
	Implementation class name	com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource		

Step 3: Shows the summary, click "Finish".

				Welcome wasadmir		
View: All tasks	Cell=W2K8	R264WAS855Node01Cell, Profile=AppSrv01				
	WebSpher	re Variables				
Welcome	WebS	WebSphere Variables				
Guided Activities	Use th	Use this page to define substitution variables. Variables specify a level of indirection for some system-defined values, such as file system root				
E Servers	directo	directories. Variables have a scope level, which is either server, node, cluster, or cell. Values at one scope level can differ from values at other levels. When a variable has conflicting scope values, the more granular scope value overrides values at grater scope levels. Therefore, server variables				
Applications	overrid	when's venicular has community scope values, me more granitian scope values vanitues as greater scope revers. Therefore, server variables override call variables, which override call variables, which override cell variables.				
E Services	E Sco	Scope: Cell=W2K8R264WAS855Node01Cell, Node=W2K8R264WAS855Node01, Server=server1				
Resources		Score exertises the level at which the resource definition is visible. For detailed information on what score				
Security		Scope specifies the revents which the feasibility demonstration is visible. For detailed internation on what scope is and how it works, see the scope settings help.				
Environment		Node=W2K8B264WAS855Node01, Server=	server1			
Virtual bosts						
We date glabel Web samer plug-in configuration	+ Pre	ferences				
WebSphere variables	Nev	v Delete				
SIP application routers		B # 12				
Replication domains				1		
Naming	Select	Name 🛟	Value 🗘	Scope 🗘		
■ OSGi bundle repositories	You c	an administer the following resources:				
System administration		DB2UNIVERSAL JDBC DRIVER NATIVEPATH	C:\WAS85_jdbc_drivers\DB2	Node=W2K8R264WAS855Node01,Server=server		
Users and Groups		DB2UNIVERSAL JDBC DRIVER PATH	C:\WAS85_jdbc_drivers\DB2	Node=W2K8R264WAS855Node01,Server=serve		
Monitoring and Tuning						
Troubleshooting		ECM SM CONSOLE WAR	C:\Programme\IBM\WebSphere \AppServer\profiles\AppSrv01 \installedApps \W2K8R264WAS855Node01Cell \ECM_SM_SERVER.ear	Node=W2K8R264WAS855Node01,Server=serve		
Service integration						
UDDI						
			\war\ECM_SM_SERVER_gui_app.war			
		ECM SM SERVER WAR	C:\Programme\IBM\WebSphere \AppServer\profiles\AppSrv01 \installedApps \W2K8R264WAS85SNode01Cell \ECM_SM_SERVERSERVER.ear \war\ECM_SM_SERVER_server_app.war	Node=W2K8R264WAS855Node01,Server=server		
		JAVA HOME	\${JAVA_LOCATION_1.7_64}	Node=W2K8R264WAS855Node01,Server=server		
		ORACLE JDBC DRIVER PATH	C:\WAS85_jdbc_drivers\ORACLE\java6	Node=W2K8R264WAS855Node01,Server=server		
		SERVER LOG ROOT	\${LOG_ROOT}/server1	Node=W2K8R264WAS855Node01,Server=serve		
		WAS SERVER NAME	server1	Node=W2K8R264WAS855Node01,Server=serve		
	Total	8				

Create Microsoft JDBC driver path. Click Environment > WebSphere variables > New...

WebSphere. software		Welcome wasadmin
	Cell=W2K8R264WAS855Node01Cell, Profile=AppSrv01	
View: All tasks	WebSphere Variables	
Welcome	WebSobere Variables > New	
+ Guided Activities	Use this page to define substitution variables. Variables specify a level of indirection for some system	stem-defined values, such as file system root
± Servers	directories. Variables have a scope level, which is either server, node, cluster, or cell. Values at	one scope level can differ from values at other levels
+ Applications	override node variables, which override cluster variables, which override cell variables.	greater scope levels. meretore, server variables
± Services	Configuration	
+ Resources		
+ Security		
∃ Environment	General Properties	
Virtual hosts Update global Web server plug-in configuration WebSphere variables Shared libraries StP application routers Replication domains @ Naming OSGi bundle repositories	* Name MICROSOFT_JDBC_DRIVER_PATH Value WAS85_jdbc_drivers\MSSQL\java6 Description MS SQL server driver path	
• System administration		
Users and Groups		
Monitoring and Tuning	Arabi OK Brand Carrel	
Troubleshooting	Apply OK Reset Galicer	
E Service integration		
+ UDDI		

Enter the name MICROSOFT_JDBC_DRIVER_PATH and set value to the path to your JDBC driver directory, containing the sqljdbc4.jar file. Click OK.

WebSphere. software				Weld	come wasadmi
lew: All tasks Welcome Guided Activities Servers		Changes have been made t Save d rectly to the master Review changes before sav A The server may need to be	o your local configuration. You can: configuration. ing or discarding. restarted for these changes to take effect.		
Applications	Webs	ophere Variables			
Services	Use th	is page to define substitution variables. Variable	as specify a level of indirection for some sy	stem-defined values, such as file system	em root
Resources	direct	ories. Variables have a scope level, which is eith	er server, node, cluster, or cell. Values at	one scope level can differ from values	at other level
Security	overri	ide node variables, which override cluster variab	e grandial scope value overhaus values at	greater scope levels. mererore, serv	er vanabies
Environment	E So	ope: Cell=W2K8R264WAS855Node01Cell, No	de=W2K8R264WAS855Node01, Server=	server1	
Vitual hosts Udata global Web server plug-in configuration WebSphere variables Shared libraries SIP application routers Replication domains * Naming OSGi bundle repositories	+ Pre	Scope specifies the level at which the resou scope is and how it works, <u>see the scope se</u> Node=WZK8R264WAS855Node01, Server sferences w Delete	rce definition is visible. For detailed informa tim <u>e help.</u> =server1 💌	tion on what	
System administration		n # \$			
Users and Groups	Select	Name 🗅	Value 🗅	Scope ①	
Monitoring and Tuning	You	can administer the following resources:	•		
Troubleshooting		DB2UNIVERSAL JDBC DRIVER NATIVEPATH	C:\WAS85_jdbc_drivers\DB2	Node=W2K8R264WAS855Node01,S	erver=server1
Service integration					
UDDI		DB2UNIVERSAL JDBC DRIVER PATH	C:\WAS85_jdbc_drivers\DB2	Node=W2K8R264WAS855Node01,S	erver=server1
		ECM SM CONSOLE WAR	C:\Programme\IBM\WebSphere \AppServer\profiles\AppSrv01 \installedApps \W2K8R264WASBSSNode01Cell \ECM_SM_SERVER.ear \war\ECM_SM_SERVER.gui_app.war	Node=W2K8R264WAS855Node01,S	erver=server1
		ECM SM SERVER WAR	C:\Programme\IBM\WebSphere \AppServer\profiles\AppSrv01 \installedApps \W2K8R264WAS95SNode1Cell \ECM_SM_SERVERSERVER.ear \war\ECM_SM_SERVER_server_app.war	Node=W2K8R264WAS855Node01,S	erver=server1
		JAVA HOME	\${JAVA_LOCATION_1.7_64}	Node=W2K8R264WAS855Node01,S	erver=server1
		MICROSOFT JDBC DRIVER PATH	C:\WAS85_jdbc_drivers\MSSQL\java6	Node=W2K8R264WAS855Node01,Se	erver=server1
		ORACLE JDBC DRIVER PATH	C:\WAS85_jdbc_drivers\ORACLE\java6	Node=W2K8R264WAS855Node01,Se	erver=server1
		SERVER LOG ROOT	\${LOG_ROOT}/server1	Node=W2K8R264WAS855Node01,S	erver=server1
		WAS SERVER NAME	server1	Node=W2K8R264WAS855Node01,S	erver=server1

Accept the changes by clicking Save.

All Analys	Cell=was7suseNode01Cell, Profile=AppSrv01
View: All tasks	Cohol zacuity 2
Welcome	uoou accarcy
Guided Activities	Global security
E Servers Servers	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
■ Applications	security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.
■ Services	
E Resources	Security Configuration Wizard Security Configuration Report
Bickedviers Object powders Dobie powders Object powders Object powders Object sources Object sources Object sources Object sources Object sources Object sources Object Object	Administrative security <u>Administrative security</u> <u>Bradie application security <u>Bradie application security</u> <u>Bradie Application Security</u></u>
B Resource Environment Security Global security Security domains	Besticita scess to resource authentication data Artification format Section access to resource authentication data Section format Section format
Administrative Authorization Groups SSL cartificate and key management Security volting Bus security	Curret realm definition Federated repositories Federated repositorie
Environment	Custom properties
System administration	
Users and Groups	Apply Reset
Monitoring and Tuning	
Troubleshooting	
Service integration	
E UDDI	
	1

Navigate to "Security" > "Global Security" and click on the "J2C authentication data" link.

Cell=was7suseNode01Cell, Profile=AppSrv01
Global security
B Messages
A-Changes have been made to your local configuration. You can:
 <u>Save</u> directly to the master configuration.
 <u>Review</u> changes before saving or discarding.
Δ The server may need to be restarted for these changes to take effect.
Global security > JAA5 - J2C authentication data > New
Specifies a list of user identities and passwords for Taxa(TM) 2 connector security to use
General Dronettes
weren i operado
Hilds MSSOL
testuser
▼ Pasw0rd
Description
Apply OK Reset Cancel

Enter the name of your database, the user and the password. Then press "OK".

)ata :	sources					
lse th earn	nis page to edit the settings of more about this task in a <u>quic</u>	a datasource that is associated with y led activity. A guided activity provides	your selected JDBC provider. The datasource object su a list of task steps and more general information abo	pplies your application with connections out the topic.	for accessing t	he databas
Sco	ope: Cell=was7suseNode01Cel	l, Node=was7suseNode01, Server=se	rver1			
Pre	Scope specifies the level a it works, <u>see the scope sel</u> Node=was7suseNode01 aferences w Delete Test connection	t which the resource definition is visibi times help. , Server=server1 v	le. For detailed information on what scope is and how			
C						
elect	Name 🗘	JNDI name 🗘	Scope 🗘	Provider 🗘	Description \diamondsuit	Category
fou (can administer the following re	sources:				
	<u>DB2</u>	DB2	Node=was7suseNode01,Server=server1	DB2 Universal JDBC Driver Provider	DB2 Universal Driver Datasource	
	A contraction of the Academic State Academic Academic State Contract of Academic State	DefaultDatasource	Node=was7suseNode01,Server=server1	Derby JDBC Provider	Datasource	

Navigate to "Resources" > "Data Sources". Select your scope. Click "New" to create a new datasource.

ate a data source	
Step 1: Enter basic	Enter basic data source information
data source information	Set the basic configuration values of a datasource for association with your JDBC provider. A datasource supplies the physical connections between the application server and the database.
provider	Requirement: Use the Datasources (WebSphere(R) Application Server V4) console pages if your applications are based on the Enterprise JavaBeans(TM) (EIB) 1.0 specification or the Java(TM) Servlet 2.2 specification.
Step 3: Enter database specific properties for the	Scope cells:was7suseNode01Cell:nodes:was7suseNode01:servers:server1
data source Step 4: Setup socurity aliasos	* Data source name MSSQL
Step 5: Summary	* JNDI name MSSOI

Step 1: Enter the name of the datasource and the JNDI name of the datasource. Both names should be the same. Remember the name for the installation. It is used to identify the database connection in our application.



Step 2: Select the JDBC provider we created before.

		·			
data source	Enter database specific propertie	es for the data source			
Step 2: Select JDBC provider	Set these database-specific properties through the datasource.	Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through the datasource.			
Step 3: Enter					
	Name	Value			
 Step 3: Enter database specific properties for the 	Name Database name	Value TESTDB			
 Step 3: Enter database specific properties for the data source 	Name Database name Port number	Value TESTDB 1433			

Step 3: Enter the database name, the port and the host name.

ell=was7suseNode01Cell, Profile=App Create a data source	Srv01
Create a data source Step 1: Enter basic data source information Step 2: Select JDBC provider Step 3: Enter database specific properties for the data source Step 4: Setup security aliases Step 5: Summary	Setup security aliases Select the authentication values for this resource. Component-managed authentication alias was7suseNode01/MSSQL w Mapping-configuration alias (none) w Container-managed authentication alias (none) w
Previous Next Cancel	Note: You can create a new J2C authentication alias by accessing one of the following links. Clicking on a link will cancel the wizard and your current wizard selections will be lost. <u>Global J2C authentication alias</u> <u>Security domains</u>

Step 4: Select the J2C authentication alias we created before.

te a data source				
Step 1: Enter basic	Summary			
lata source nformation	Summary of actions:	Summary of actions:		
	Options	Values		
	Scope	cells:was7suseNode01Cell:nodes:was7suseNode01:servers:server1		
Step 3: Enter	Data source name	MSSQL		
roperties for the	JNDI name	MSSQL		
	Select an existing JDBC provider	Microsoft SQL Server JDBC Driver		
	Implementation class name	com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource		
ecurity aliases	Database name	TESTDB		
	Port number	1433		
	Server name	localhost		
	Use this data source in container managed persistence (CMP)	true		
	Component-managed authentication alias	was7suseNode01/MSSQL		
	Mapping-configuration alias	(none)		
	Container-managed authentication alias	(none)		

Step 5: Shows the summary. Click "Finish".

	rces					
	 ☐ Messages ▲ Change: <u>Save</u> bin <u>Review</u> c ▲ The service 	s have been made to your local cor ectly to the master configuration. changes before saving or discarding ver may need to be restarted for th	nfiguration. You can: ee changes to take effect.			
ita s	sources					
e th arn i	is page to edit the settings of a o more about this task in a <u>quided</u>	datasource that is associated with y <u>activity</u> . A guided activity provides	our selected JDBC provider. The datasource object sup a list of task steps and more general information abo	oplies your application with connections ut the topic.	s for accessing th	he databas
Sco	pe: Cell= was7suseNode01Cell , N	lod e=was7suseNode01 , Server =ser	ver1			
	Scope specifies the level at w it works, see the scope setting	hich the resource definition is visible as help.	e. For detailed information on what scope is and how			
	Node=was7suseNode01, Se	erver=server1				
Drol	forences					
New	v Delete Test connection	Manage state				
ra (n 1997 -	in ange statem				
lect	Name 🗘	JNDI name 🗘	Scope 🗘	Provider 🗘	Description 🗘	Category
lect ou c	Name 🗘	JNDI name 🗘	Scope 🗘	Provider 🗘	Description 🗘	Category
lect ou c	Name an administer the following resou DB2	JNDI name 🗘	Scope 🗘	Provider 🗘	Description 🗘 DB2 Universal Driver Datasource	Category
lect ou c	Name an administer the following resou DB2 Default Datasource	JNDI name 🗘 urces: DB2 DefaultDatasource	Scope 🗘 Node=was7suseNode01,Server=server1 Node=was7suseNode01,Server=server1	Provider DB2 Universal JDBC Driver Provider Derby JDBC Provider	Description DB2 Universal Driver Datasource for the WebSphere Default Application	Category

Click "Save" to save it to the master configuration.
The deployment of the ECM_SM on IBM WebSphere

The deployment process for the WebSphere based installation:

View: All tasks	Cell=was7	7suseNode01Cell, Profile=AppSrv01				
Welcome	Enterprise	e Applications	2 -			
Guided Activities	Enterp	prise Applications				
E Servers	Use thi	is page to manage installed applications. A single application can b	be deployed onto multiple servers.			
Server Types WebSphere application servers	B Preferences					
WebSphere MQ servers Web servers	Star	rt Stop Install Uninstall Update Rollout Update Rer	lemove File Export DDL Export File			
Applications						
New Application	Select	Name 🗘	Application Status 👲			
Application Types	You can administer the following resources:					
WebSphere enterprise applications	23	DefaultApplication	•			
Assets		ivtApp	•			
Services		guery	•			
Resources	Total	3				
E Security						
Environment						
System administration						
Users and Groups						
Monitoring and Tuning						
Troubleshooting						
Service integration						
E UDDI						

Navigate to "Application" > "Application Types" > "WebSphere enterprise applications". Click "Install".

Enterprise Applications	
Preparing for the application installation Specify the EAR, WAR, JAR, or SAR module to upload and install.	2 -
Path to the new application Child Existem Full path Chiverkinsinstallation server Browse	
Remote file system Full path Browse	
Next	

Click on "Browse...", select the ear file on your disk and click "Next".

Enterprise Applications	Close page
Preparing for the application installation	2 🖾
New do yoe waat to install the application? Image: The second s	
Choose to generate default bindings and mappings	
Previous Cancel	

Click "Next".

Step 1: Select	Select installation options
installation options Step 2 Map modules	Specify the various options that are available to prepare and install your application.
to servers	Precompile JavaServer Pages files
<u>Step 3</u> Map virtual hosts for Web modules	Directory to install application
<u>Step 4</u> Summary	Distribute application
	Use Binary Configuration
	Deploy enterprise beans
	ECM_SM_SERVER
	Create MBeans for resources
	Override class reloading settings for Web and EJB modules
	Reload interval in seconds
	Deploy Web services
	Validate Input off/warn/fail warn w
	Process embedded configuration
	File Permission
	Allow all files to be read but not written to Allow executables to execute Allow HTML and image files to be read by everyone
	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755
	Application Build ID Unknown
	Allow dispatching includes to remote resources
	Allow servicing includes from remote resources
	Business level application name Create New BLA
	Asynchronous Request Dispatch Type Dispabled
	Allow FIB reference targets to resolve automatically

Click "Next".

Ce	ll=was7suseNode01Cell, P	Profile=AppSrv01					
In	stall New Application			2 -			
	Specify options for installi	ng enterprise applications and modules.					
	Step 1 Select	Map modules to servers					
	Step 2: Map modules to servers	Specify targets such as application servers or clusters of application servers where you want to install the modules that are contained in your application. Modules can be installed on the same application server or dispersed among serveral application servers. Also, specify the Web servers as targets that serve as routers for requests to this application. The plug-in configuration file (plugin-dgs.muf) for each Web server's as presented on the recorded through.					
	 <u>Step 3</u> Map virtual hosts for Web modules 	Clusters and servers: WebSphere:cell=was7suseNode01Cell,node=was7suseNode01,server=server1 //					
	Step 4 Summary	Summary · Apply					
		Select Module	URI	Server			
		ECM_SM_SERVER/war/ECM_SM_SERVER_gu	i_app.war ECM_SM_SERVER/war/ECM_SM_SERVER_gui_app.war,WEB- INF/web.xml	WebSphere:cell=was7suseNode01Cell,node=was7suseNode01,server=server1			
	Previous Next C	ancel					

Check the box under "Select". Click "Next".

cify options for installing enterp	prise applications and modules.	
Step 1 Select	Map virtual hosts for Web modules	
Step 2 Map modules to servers	Specify the virtual host where you want to install the Web modules that are contain the same virtual host or disperse them among several hosts.	ed in your application. You can install Web modules or
Step 3: Map virtual hosts for Web modules		
	Select Web module	Virtual host

Check the box under "Select". Click "Next".

y options for installing enterpris	se applications and modules.	
ep 1 Select	Summary	
	Summary of installation options	
<u>ep 2</u> Map modules servers	Options	Values
on 3 Man virtual	Precompile JavaServer Pages files	No
sts for Web	Directory to install application	
aules	Distribute application	Yes
p 4: Summary	Use Binary Configuration	No
	Deploy enterprise beans	No
	Application name	ECM_SM_SERVER
	Create MBeans for resources	Yes
	Override class reloading settings for Web and EJB modules	No
	Reload interval in seconds	영상 가 이 문화가 있는 것을 물러 물건을 가 하는 것을 했다.
	Deploy Web services	No
	Validate Input off/warn/fail	warn
	Process embedded configuration	No
	File Permission	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755
	Application Build ID	Unknown
	Allow dispatching includes to remote resources	No
	Allow servicing includes from remote resources	No
	Business level application name	요즘 것, 것은 것은 것을 하는 것을 가지 않는 것을 하는 것이야?
	Asynchronous Request Dispatch Type	Disabled
	Allow EJB reference targets to resolve automatically	No
	Cell/Node/Server	Click here

Click "Finish".

Cell=was7	suseNode01Cell, Profile=AppSrv01			
Enterprise	Applications	?		
Enterpr Use this	ise Applications , page to manage installed applications. A single application can be deployed onto multiple se	ervers.		
🕀 Prefe	erences			
Start	Start Stop Install Uninstall Update Remove File Export DDL Export DDL Export File			
Select	Name 🛟	Application Status 👲		
You ca	You can administer the following resources:			
	DefaultApplication	•		
	ECM SM SERVER	*		
	ivtApp	\$		
	guery	4		
Total 4				

Repeat the same for the server ear. And restart IBM WebSphere.

Appendix C. An example charset.alias file

An example /usr/lib/charset.alias file for Solaris 8

This file is needed by the ECM SM agent. # Filename: /usr/lib/charset.alias # 646 ASCII ISO8859-1 ISO-8859-1 ISO8859-2 ISO-8859-2 ISO8859-3 ISO-8859-3 ISO8859-4 ISO-8859-4 ISO8859-5 ISO-8859-5 ISO8859-6 ISO-8859-6 IS08859-7 ISO-8859-7 IS08859-8 IS0-8859-8 IS08859-9 IS0-8859-9 IS08859-15 ISO-8859-15 koi8-r KOI8-R ansi-1251 CP1251 BIG5 BIG5 Big5-HKSCS BIG5-HKSCS gb2312 GB2312 GBK GBK GB18030 GB18030 cns11643 EUC-TW 5601 EUC-KR ko_KR.johap92 JOHAB eucJP EUC-JP PCK SHIFT_JIS TIS620.2533 TIS-620 UTF-8 UTF-8

Appendix D. General Configuration of ECM SM Server

Introduction

This section describes how certain general properties of the *ECM SM Server* product can be configured in order to obtain a rather user-specific customization.

Flow Limiter

This section describes the configuration of the flow limiter.

Configuring the flow limiter in the configuration

In the file finca-cfg.xml the flow limiter can be configured. The flow limiter prevents the application from event storms.

Example for logging configuration

The following snippet from the finca-cfg.xml file shows an example flow limiter configuration.

```
<flowlimiter>
0002
        <!--
0003
         On an event storm, the events will be written into a log file. There are many \downarrow
     ways to configure this mechanism.
0004
          - name the name of the log file
0005
          - gzipped = true => the logfile is written gzipped
          - archive => no. of logfiles to archive (blocked_events.log.1.gz ... etc.)
0006
0007
          - size => maximum size which one log file shall have, before next is {\scriptscriptstyle \dashv}
   written. The unit is bytes. Write 'k' for kiloByte (e.g. 500k) 'M' for MegaByte (e.g. ↓
     12M) or G for GigaByte (e.g. 0.1G).
0008
          - location => the relative or absolute filepath of where the file shall be \downarrow
     stored.
0009
          -->
0010
        <logfile name="blocked_events.txt" gzipped="false"
     archive="3" size="4k" location="./test/"/>
0011
0012
         <!-- multiple timeframes are possible
0013
          - timeframe length = length of a timeframe in seconds
0014
          - remind = The time interval after a further blocked event is sent if the \dashv
   blocked condition still exists, to update the timestamp of the current blocked event \dashv
    in the event view.
0015
         - The elements of the timeframe tag are
0016
               -overall (all incoming events)
              -host (All events from a specific host)
0017
0018
              -datastream (all events from a specific host AND datastream)
0019
              -application (all events from a specific host AND application)
0020
             -application instance (all events from a specifiq host AND application AND \dashv
```

instance). 0021 The elements have the following attributes 0022 -block: Number of events per timeframe, which have to occur to block \dashv the events from this source. 0023 -unblock: The number of events must go under this value, that the \downarrow events are unblocked. 0024 --> 0025 <timeframe length="30" remind="60"> 0026 <overall block="500000" unblock="400000"/> 0027 block="10000" unblock="8000"/> <host 0028 block="5000" unblock="4000"/> <datastream 0029 <application block="3000" unblock="2000"/> 0030 <applicationinstance block="3000" unblock="2000"/> 0031 </timeframe> 0032 <!-- This gives the possibility to create a specific block event. The 'field' \dashv elements 0033 show the properties of a DataStream event. The $\{key\} \mid value \mid for example \{HOST\} \downarrow$ means that the block event will get the 0034 value from the original event. The timestamp will be overwritten in every case by \downarrow the program - with the current timestamp. 0035 It is also possible to insert individual text. For example in the MSG field. 0036 --> 0037 <blockevent> value="\${STREAM}"/> 0038 <field dest="STREAM" value="\${SEQNO}"/> 0039 <field dest="SEQNO" value="\${CLASS}}"/> 0040 <field dest="CLASS" value="\${TIMESTAMP}'"/> 0041 <field *dest="TIMESTAMP"* value="\${HOSTNAME}}"/> 0042 <field dest="HOSTNAME" value="\${IP_ADDRESS}"/> 0043 <field *dest="IP_ADDRESS"* dest="ADAPTER_HOSTNAME" value="\${ADAPTER_HOSTNAME}}"/> 0044 <field dest="ADAPTER_IP_ADDRESS" value="\${ADAPTER_IP_ADDRESS}"/>
dest="MSG" value="This event was blocked. \${MSG}"/> 0045 <field 0046 <field 0047 dest="SEVERITY" value="FATAL"/> <field 0048 <field dest="SOURCE" value="\${SOURCE}"/> value="\${SUB_SOURCE}"/> <field dest="SUB_SOURCE" 0049 value="\${SOURCE_NAME}"/> 0050 <field dest="SOURCE_NAME" value="\${SOURCE_TYPE}"/> 0051 <field dest="SOURCE_TYPE" value="\${APPLICATION}"/> dest="APPLICATION" 0052 <field value="\${MODULE}"/> 0053 <field *dest="MODULE"* value="\${INSTANCE}"/> 0054 <field dest="INSTANCE" value="\${ERROR_ID}"/> 0055 <field dest="ERROR ID" 0056 <field *dest="VALUE"* value="BLOCK"/> value="\${COUNT}"/> dest="COUNT" 0057 <field value="\${LOG}"/> 0058 <field dest="LOG" value="\${ANNOTATION}"/> dest="ANNOTATION" 0059 <field 0060 <field dest="ACKNOWLEDGE" value="\${ACKNOWLEDGE}"/> 0061 </blockevent> 0062 0063 0064 <!-- This gives the possibility to create a specific unblock event. The \dashv 'field' elements show the properties of a DataStream event. The $\{key\}$ 'value' for example $\{HOST\} \downarrow$ 0065 means that the unblock event will get the value from the original event. The timestamp will be overwritten in every case by \dashv 0066 the program - with the current timestamp. 0067 It is also possible to insert individual text. For example in the MSG field. 0068 --> 0069 <unblockevent> 0070 value="\${STREAM}"/> <field dest="STREAM" value="\${SEQNO}"/> 0071 <field dest="SEQNO" value="\${CLASS}'"/> dest="CLASS" 0072 <field dest="TIMESTAMP" value="\${TIMESTAMP}"/> 0073 <field

0074		<field< td=""><td>dest</td><td>="HOSTNAME"</td><td>value="\$</td><td>{HOSTNAME}"/></td></field<>	dest	="HOSTNAME"	value="\$	{HOSTNAME}"/>
0075		<field< td=""><td>dest="IP</td><td>ADDRESS"</td><td>value="\${I</td><td>P_ADDRESS }" /></td></field<>	dest="IP	ADDRESS"	value="\${I	P_ADDRESS }" />
0076	<field< td=""><td>dest="A</td><td>DAPTER_HOSTN</td><td>IAME" valu</td><td>e="\${ADAPTER</td><td>_HOSTNAME }" /></td></field<>	dest="A	DAPTER_HOSTN	IAME" valu	e="\${ADAPTER	_HOSTNAME }" />
0077	<field< td=""><td>dest="ADAP1</td><td>TER_IP_ADDRES</td><td>SS" value=</td><td>="\${ ADAPTER_I</td><td>P_ADDRESS[`]}"/></td></field<>	dest="ADAP1	TER_IP_ADDRES	SS" value=	="\${ ADAPTER_I	P_ADDRESS [`] }"/>
0078	<field< td=""><td>dest="MSG"</td><td>value="This</td><td>s event w</td><td>as unblocke</td><td>d. \${MSG`}"/></td></field<>	dest="MSG"	value="This	s event w	as unblocke	d. \${MSG`}"/>
0079		<fi< td=""><td>leld</td><td>dest="SEVE</td><td>ERITY" va</td><td>lue="FATAL"/></td></fi<>	leld	dest="SEVE	ERITY" va	lue="FATAL"/>
0080		<fie< td=""><td>ld ä</td><td>lest="SOURCH</td><td>E" value=</td><td>"\${SOURCE}"/></td></fie<>	ld ä	lest="SOURCH	E" value=	"\${SOURCE}"/>
0081		<field< td=""><td>dest="SU</td><td>B_SOURCE"</td><td>value="\${S</td><td>UB_SOURCE }" /></td></field<>	dest="SU	B_SOURCE"	value="\${S	UB_SOURCE }" />
0082		<field< td=""><td>dest="SOUR</td><td>CE NAME"</td><td>value="\${SO</td><td>URCE_NAME }"/></td></field<>	dest="SOUR	CE NAME"	value="\${SO	URCE_NAME }"/>
0083		<field< td=""><td>dest="SOUR</td><td>CE_TYPE"</td><td>value="\${SO</td><td>URCE_TYPE`}"/></td></field<>	dest="SOUR	CE_TYPE"	value="\${SO	URCE_TYPE`}"/>
0084		<field< td=""><td>dest="APPL</td><td>JICATION"</td><td>value="\${AP</td><td>PLICATION }"/></td></field<>	dest="APPL	JICATION"	value="\${AP	PLICATION }"/>
0085		<fie< td=""><td>ld ä</td><td>lest="MODULH</td><td>E" value=</td><td>"\${MODULE};"/></td></fie<>	ld ä	lest="MODULH	E" value=	"\${MODULE};"/>
0086		<field< td=""><td>dest</td><td>="INSTANCE"</td><td>value="\$</td><td>{INSTANCE} / /></td></field<>	dest	="INSTANCE"	value="\$	{INSTANCE} / />
0087		<field< td=""><td>dest</td><td>="ERROR_ID"</td><td>value="\$</td><td>{ ERROR_ID } " /></td></field<>	dest	="ERROR_ID"	value="\$	{ ERROR_ID } " />
0088		<	field	dest="V	'ALUE" va	lue="BLOCK"/>
0089		<fi< td=""><td>ield</td><td>dest="COUN</td><td>VT" value</td><td>="\${COUNT}"/></td></fi<>	ield	dest="COUN	VT" value	="\${COUNT}"/>
0090			<field< td=""><td>dest="</td><td>LOG" val</td><td>ue="\${LOG}"/></td></field<>	dest="	LOG" val	ue="\${LOG}"/>
0091		<field< td=""><td>dest="AN</td><td>NOTATION"</td><td>value="\${A</td><td>NNOTATION }"/></td></field<>	dest="AN	NOTATION"	value="\${A	NNOTATION }"/>
0092		<field< td=""><td>dest="ACKN</td><td><i>IOWLEDGE"</i></td><td>value="\${AC</td><td>KNOWLEDGE }"/></td></field<>	dest="ACKN	<i>IOWLEDGE"</i>	value="\${AC	KNOWLEDGE }"/>
0093						
0094						
0095						
0096					<	/flowlimiter>
0097						

External Users

The configuration settings for external users can be altered by the file **finca-cfg.xml**. The following snippet shows the default configuration.

0001 <external.users require_internal_user="true" carry_over_external_groups="true"/>

The attribute

- require_internal_user: If set to true, an internal user is required for external authentication. The user
 must be created manually in the User Management Console. If it is set to false, the user is created
 automatically during first log in of the user.
- *carry_over_external_groups:* If set to true, the group memberships for the user logging in are retrieved from the external LDAP system. If set to false, the group memberships are retrieved from the internal user management database.

Appendix E. FIR configuration

FIR configuration

FIR Receiver is the component that receives CALA FIR events from clients and transforms them to ECM SM 5.2.0 events that can be sent to the console. The FIR Receiver uses a field translation service to determine how the FIR fields must be handled.

If a FIR field is not listed in the *fir-translation* section of the configuration, a field with the same name and contents will be created in the new ECM SM 5.2.0 event. So only the following fields need to be listed in the translation config:

- fields that must be set to a constant value
- fields that must be renamed for new ECM SM 5.2.0 events (example: field containing datastream is called *\$SECTYPE* in FIR but must be called *STREAM* in ECM SM 5.2.0 event)
- fields that must be reformatted
- fields that must be set depending on another field

The FIR translation service is also used to import events from the older architecture to ECM SM 5.2.0.

A detailed list of fields mappings can be found below.

Current field mappings

Events from agents

These mappings are used when Events are received from an agent.

The configuration is located in <install_root>/eventserver/cfg/eventprocessing-cfg.xml in the XML tag <datastream name="fir">.

Field in ECM SM 5.2.0 event	Value
ORIGINAL_STREAM	fir
ORIGINAL_TIMESTAMP	FIR field <i>\$CTIME</i>
STREAM	depends on FIR field <i>\$SECTYPE</i> :
	• if <i>\$SECTYPE</i> starts with <i>calamon</i> , field is set to concatenation of FIR fields <i>\$area</i> and <i>\$info</i>
	• otherwise, field is set to FIR field \$SECTYPE
TIMESTAMP	depends on FIR field \$CTIME
	• if \$CTIME matches MMM dd hh:mm:ss yyyy, it will be converted to format yyyy-mm- dd hh:mm:dd

Field in ECM SM 5.2.0 event	Value
	otherwise field will be set directly to FIR field
	\$CTIME
CLASS	FIR field \$CLASS
MSG	FIR field msg
HOSTNAME	FIR field \$HOSTNAME
IP_ADDRESS	FIR field <i>\$ORIGIN</i>
ADAPTER_HOSTNAME	FIR field \$ADAPTER_HOSTNAME or \$HOSTNAME if \$ADAPTER_IP_ADDRESS is not set
ADAPTER_IP_ADDRESS	FIR field \$ADAPTER_IP_ADDRESS or \$ORIGIN if \$ADAPTER_IP_ADDRESS is not set
APPLICATION	depends on FIR field <i>\$SECTYPE</i> :
	• if <i>\$SECTYPE</i> starts with <i>calamon</i> , field is set to FIR field <i>\$CLASS</i>
	• otherwise, field is set to FIR field <i>\$area</i>
INSTANCE	FIR field \$info
INSTALL_PATH	<undef></undef>
SEQNO	-1
COUNT	0
SOURCE_NAME	FIR field \$LOGFILENAME
SOURCE	FIR field source
SUB_SOURCE	FIR field sub_source
MODULE	<undef></undef>
ERROR_ID	FIR field error_id
VALUE	depends on FIR field \$SECTYPE:
	• if <i>\$SECTYPE</i> starts with <i>calamon</i> , field is set to FIR field <i>value</i>
	• otherwise, field is set to <undef></undef>
SOURCE_TYPE	depends on FIR field \$SECTYPE:
	• if <i>\$SECTYPE</i> starts with <i>calamon</i> , field is set to <i>monitor</i>
	• otherwise, field is set to <i>logfile</i>
SEVERITY	depends on FIR field severity:
	numerical value is mapped to text:
	• 0 -> HARMLESS
	• 1 -> WARNING
	• 2 -> CRITICAL

Field in ECM SM 5.2.0 event	Value	
	• 3, 4, 5 -> FATAL	
	• text values HARMLESS, WARNING, CRITICAL, FATAL are copied	
	• for any other value of severity, field is be set to UNKNOWN	

Special fields in ECM SM 5.2.0 events

Most fields in the ECM SM 5.2.0 events are self-explanatory. The following table lists some fields with a special meaning:

Event field	Meaning	
ORIGINAL_STREAM	Used internally for rules processing. Set to <i>fir</i> for all events received from the FIRReceiver.	
ORIGINAL_TIMESTAMP	Contains the original event timestamp as received from the client. For events created by FIRReceiver, this is the contents of the field <i>\$CTIME</i> .	
INSTALL_PATH	Required to fill the field <i>INSTANCE</i> as only <i>INS</i> - <i>TANCE</i> and <i>INSTALL_PATH</i> together define the application instance where the event was created.	
SEQNO	Used internally. Set to -1 for all events received from the FIRReceiver.	
COUNT	Indicates the duplicate count of an event. Set to 0 in the FIRReceiver to make sure that the field is always visible in the events details view.	

Transfer CALA -> ECM SM 5.2.0 configuration

There are some basic differences between the CALA configuration and the configuration for ECM SM 5.2.0:

- some standard mappings required for all events are now done directly when receiving an FIR, e.g. setting the *SEVERITY* field to a valid value
- completers and remappers are no longer required; they were mainly used to fill event fields for the various emitters which is now done in the sink-specific configuration
- rules are now implemented as JavaScript, this is much more flexible than the old rules maps

Mappings

Transfer of old mappings

Mappings are configured in the Server Configuration console. See online help for this console for details.

CALA mappings	now located in configuration for		
*status.map	no longer required; the mapping is now done in the FIRReceiver configuration (cannot be changed in GUI)		
*smtp.map	smtpsink		
*snmp.map	snmpsink		
*dup.map	duplicatedetection		
apache_access_codes.map	no longer required; <i>\$httpcode</i> is visible in event details view		
<pre>fncap_trc_sev.map</pre>	• <i>MSG</i> and <i>ADDITIONAL_KEY</i> is set in script fncap_trc_script		
	SEVERITY is set in mapping		
fnds_auditlog_sev.map	• <i>MSG</i> and <i>ADDITIONAL_KEY</i> is set in script <i>fnds_auditlog_script</i>		
	SEVERITY is set in mapping		
fndw4log_evt.map	mapping		
fnislog_evt.map	mapping		
fnislog_except*.map	ADDITIONAL_KEY is in script fnislog_ script		
	• SEVERITY and MSG is set in mapping		
<pre>ibm_cm8_eventlog_sev.map</pre>	• MSG is set in script ibm_cm8_eventlog_↓ script		
	SEVERITY is set in mapping		

CALA mappings	now located in configuration for	
ibm_cm8_icmsrvlog_drop.map	mapping	
ibm_cmod_log_sev.map	• <i>MSG</i> is set in script <i>ibm_cmod_log_</i> , → <i>script</i>	
	SEVERITY is set in mapping	
oraalert_drop.map	mapping	
oralist_drop.map	mapping	
syslog_drop.map	mapping	

What is the ADDITIONAL_KEY field?

The mapping definition has a different approach than the old CALA map files. There is only one large table where mappings for all datatypes are defined. All fields that are affected by a mapping are shown as columns in the table.

There are some fields that are used as keys for mappings of different datatypes, e.g. ERROR_ID.

Other fields like EventType for datatype fncap_trc are used only by one datatype. Including all these "single-use fields" as key columns would increase the number of columns and make the configuration more confusing. To decrease the number of columns, the column ADDITIONAL_KEY is used instead. The value of the column is set in the datatype-related script as described in the table above.

Another usage for the ADDITIONAL_KEY column are the exception maps for the fnislog configuration. There are some exceptions from the "normal" event processing depending on a substring of the message text. This substring of the message is copied to the ADDITIONAL_KEY field as well as this cannot be handled in the mapping configuration table.

Rules

Transfer of old rules

Rules are implemented as JavaScript in the Rules and Scripts Administration. See online help for this console for details.

Some of the old rules have been implemented as configuration for the smtpsink.

CALA rule	now located in script	
bp8_mysql.rmp	bp8_script	
cala_check.rmp	cala_script,cala_timer_script	
fnds_auditlog_logon.rmp	fnds_auditlog_script	
fndslog_idxlog.rmp	fndslog_script	
fndslog_timer.rmp	fndslog_script,fndslog_timer_script	

CALA rule	now located in script	
ibm_cm8_icmsrvlog_mysql.rmp	ibm_cm8_icmsrvlog_script	
isce_mysql.rmp	isce_script	
p8srverror_mysql.rmp	p8srverror_script	
saperion*_smtp.rmp	config for smtpsink	

Code snippets for the CALA rules actions

You can implement the various CALA rules actions in the new configuration as well. The following code snippets must be added to the processEvent(evt) function of the corresponding <datastream>_script.

Actions that do not send events

CREATE_BASE - create an event on heap, do not send event

```
// get reference to heap var heap = rulesEngineCfgSrv.getHeap("scriptplugin",
    "event_timer"); // add event to heap var heapEntryId =
    rulesEngineCfgSrv.addHeapEntry(heap, evt); // return nothing return null;
    heap var heap = rulesEngineCfgSrv.getHeap("scriptplugin",
    "event_timer"); // add event to
    heap var heapEntryId = rulesEngineCfgSrv.addHeapEntry(heap,
    evt); // return
    nothing return
```

DISCARD_BASE - remove matching events from heap, do not send event

```
// get reference to heap
                                      var heap = rulesEngineCfgSrv.getHeap("scriptplugin",
  "event_timer"); // create key array to read events from heap
                                                                                                  var
keyArray = ["HOSTNAME", evt.get("HOSTNAME"), "STREAM", evt.get("STREAM")]; //
remove all events from heap that match the key array var eventidArray =
rulesEngineCfgSrv.getHeapEntries(heap, keyArray, null); if (eventidArray.length > 0)
           // process all events that were returned from heap for (var index=0;
 index < eventidArray.length; index++) { // remove entry</pre>
rulesEngineCfgSrv.deleteHeapEntry(heap, eventidArray[index]);
                                                                                         // return
                                                                           } }
nothing return null;
heap var heap = rulesEngineCfgSrv.getHeap("scriptplugin",
"event_timer"); // create key array to read events from
heap var keyArray = ["HOSTNAME", evt.get("HOSTNAME"), "STREAM",
evt.get("STREAM")]; // remove all events from heap that match the key
array var eventidArray = rulesEngineCfgSrv.getHeapEntries(heap, keyArray,
         if (eventidArray.length >
null);
0)
 {
         // process all events that were returned from
            for (var index=0; index < eventidArray.length; index</pre>
heap
++)
{
            // remove
entry
                rulesEngineCfgSrv.deleteHeapEntry(heap,
eventidArray[index]);
     // return
nothing return
```

DISCARD_CURRENT - do not change heap, do not send event

// return nothing return null;

ing return

Actions that send events

When using the SEND actions, either the current event or the base event can be sent. The following snippet shows how to get the base event:

```
var heap = rulesEngineCfgSrv.getHeap("scriptplugin",
    // get reference to heap
 "event_timer");
                    // create key array to read events from heap
                                                                             var keyArray =
["HOSTNAME", evt.get("HOSTNAME"), "STREAM", evt.get("STREAM")]; // get all events from
heap that match the key array var eventidArray = rulesEngineCfgSrv.getHeapEntries(heap,
keyArray, null); if (eventidArray.length > 0) { // simply return the first base
                                                          // simply return the first base
         return rulesEngineCfgSrv.getHeapEntryAsEvent(heap, eventidArray[0], true);
event
 else
       {
             // no base event found -> current event will be returned
                                                                             return evt;
       var heap = rulesEngineCfgSrv.getHeap("scriptplugin",
heap
"event_timer"); // create key array to read events from
heap
       var keyArray = ["HOSTNAME", evt.get("HOSTNAME"), "STREAM",
evt.get("STREAM")]; // get all events from heap that match the key
array var eventidArray = rulesEngineCfgSrv.getHeapEntries(heap, keyArray,
null);
         if (eventidArray.length >
0)
        // simply return the first base
{
            return rulesEngineCfgSrv.getHeapEntryAsEvent(heap, eventidArray[0],
event
true);
else
        // no base event found -> current event will be
returned
               return
evt;
```

You can combine this code with the snippets shown above to achieve the different SEND actions.

CALA supported sending a "new" event as well by specifying key=value pairs in the action. You can do this by setting the event fields to the required values

(evt.put("key", "value");

Architecture Model

The following chapter describes the functionality of the ECM SM Service and the GUI Service.

The Server Service



Figure: The Server Service

The following list describes the figure above:

JVM

The JVM (Version 5 or higher) is installed on the Physica Server machine. It runs all components of the Server Service. Also the OSGi Framework.

OSGi Framework

The OSGI framework handles the bundles. It starts, updates, stops, registers and installs bundles. At this point, the only thing to know about OSGi is, that it is an environment for the bundles to run in. The bundles are all plug-ins, which can be connected to each other but not run as an individual application. The OSGi framework has to plug these components together to a running application.

Server Service

The Server Service is the application, which runs inside the OSGi framework. This application is used to receive events, process and / or modify them and write them into the database.

FIR Receiver

The FIR Receiver is a component, which gets events from the old version and maps / transforms them into events of the new version, so that it fits into the database.

MCP

After events are transformed into the new format, they are sent to the MCP (Master Control Plugin). This is the head of the event processing. The event contains information for the MCP, so that it knows, what to do with the event.

• event processing bundles

These bundles are used to modify the events and send them back to the MCP in their modified format. Finally the event is written into the database by one of the event processing bundles.

- fumi bundles The FUMI bundles are bundles, which provide JMX, SCP and REST connection to our application. So it is possible to instrument the application from outside.
- functional bundles
 These bundles can best be explained as the "main backend components". They organize the trees, create reports, and are an abstract layer between database and other classes.
- functional.dblayer bundles
 These bundles have access to the database and are used to write items into the databases as well as deleting and updating them.
- base bundles
 These bundles define basic program structures like interfaces for the other (functional) bundles.
- helper bundles
 These bundles most likely contain mock (fake) implementations for tests.
- The Database Server The database server can be an separate machine or the same server as the Physical Server.

The RAP GUI Service



Figure: The RAP GUI Service

The following list describes the figure above:

JVM

The JVM (Version 5 or higher) is installed on the Physical Server machine. It runs all components of the RAP GUI Service. Also the OSGi Framework.

OSGi Framework

The OSGi Framework handles the bundles. It starts, updates, stops, registers and installs bundles. At this point, the only thing to know about OSGi is, that it is an environment for the bundles to run

in. The bundles are all plug-Ins, which can be connected to each other, but not run as an individual application. The OSGi Framework has to plug these components together to a running application.

- GUI Service The GUI Service is the application, which runs inside the OSGi Framework. This application is used to display the GUI to the user via RAP.
- functional bundles

These bin bundles can best be explained as the "main backend components". They organize the trees, create reports, and are an abstract layer between database and other classes.

- functional.dblayer bundles
 These bundles have access to the database and are used to write items into the databases as well as deleting and updating them.
- base bundles
 These bundles define basic program structures like interfaces for the other (functional) bundles.
- helper bundles These bundles most likely contain mock (fake) implementations for tests.
- gui bundles The gui bundles are the RAP application its perspectives, views and editors. So all the bundles, which provide views.
- The Database Server
 The database server can be an separate machine or the same server as the Physical Server.
- The Servlet Container / Application Server In this server there run several servlets which provide the RAP Framework, which makes it possible to show the GUI in RAP.
- Client

There is a web client (The web browser) for the RAP GUI consisting of the bundles needed to display the GUI.

Event Processing

The following chapter describes how incoming events are processed.

Event processing components

There are three kinds of event processing components. These are described in the list below.

- Source A component that creates events. (E.g the monitoring component on the client, but also the FIR receiver on the server - the FIR source). In the old architecture this was a reader.
- Processor

A component that modifies events (receives events, modifies them and sends them to the next component)

Sink

A component that receives events without sending them to another (internal) component. A sink consumes events from the view of ECM SM - meaning that if an event arrives in the sink, it leaves the ECM SM event processing system and goes into another system (e.g. database, smtp, snmp, etc.) In the old architecture it was an emitter.

Event Processing Overview



Figure: The Event Processing of ECM SM

The following list describes the figure above:

Event

The event is represented by the arrows in the graphic. This is a FIR event. At the moment no other events than FIR events are supported. The event is sent to several bundles which process the event and give the modified event to the next event processing instance.

• FIR Receiver (source)

The FIR Receiver transforms FIR events from the old architecture into events of the new architecture. In the installation directory there is a configuration file eventserver/cfg/eventprocessing-cfg.xml, in which a mapping for the FIR events is defined. This file is an entity for the eventserver/cfg/finca-cfg.xml file.

• Flowlimiter (processing)

The FlowLimiter receives the events and checks if there is an event storm (many events in short period of time). If there is an event storm, the events will not be forwarded, but be written out in a rolling log file system. A "block event" will be sent. When the event storm is over, an "unblock event " will be sent and after that the events are forwarded as usual.

- Eventjournal (processing) The EventJournaling writes the incoming events into a special database table.
- Incoming Database Table

This table stores unprocessed events. So it acts as a cache in case that the ECM SM server will crash. After the restart the events from the Incoming Events Table will be processed and after that the new events will be processed.

- RulesEngine Mechanism
 The RulesEngine Mechanism is the context in which the RulesEngine is running.
- RulesEngine (processing)
 The RulesEngine has several RulesEngine-Plug-ins. The RulesEngine is the main component to
 process events. There are RulesEngine Scripts, which process the event. There is one entrance
 script, which has several conditions. Those conditions lead the event to another script, etc. The
 scripts can send the event into the Plug-ins to modify it.
- Mapping Plug-in (RE-Plug-in) The mapping Plug-in is used to map fields of the evolution

The mapping Plug-in is used to map fields of the event, according to a mapping table and to conditions of the current event. After the event was processed, the modified event will be sent back to the RulesEngine.

- Duplicate Detection Plug-in (RE-Plug-in)
 This Plug-in detects duplicate events. The event severity might change depending on the rules,
 which are defined for the duplicate detection. If there are several events of the same type, the severi ty will increase to a higher level. The event is sent back to the RulesEngine.
- OVO Sink, SMTP Sink and File Sink RulesEngine Plug-ins These plug-ins can redirect the events to its destination. So for example another system like Open View for Operations (OVO sink), e-Mail (SMTP sink) or just a file (File sink).

• Database Sink The database sink writes the event into the Event Database. Every event is sent to this sink by the RulesEngine Plug-in.

Event Database

Contains all the events to be displayed. In the event database there is a table for current events and a history table.

User Management

The following chapter describes the relation between users, groups, roles, etc.

RBAC Basics

The user management and rights concept is based on the standard of RBAC (short for Role Based Access Control).

This means, that every user has one or several roles. The roles have none or several rights defined. So the user has all the rights, which are defined by the roles, to which the user belongs to. It is not part of the concept, that a user can have a right directly. So every user in our system gets a role, which is named just like the user.

The following chapter describes the different components of the roles rights management in detail.

RBAC Overview



Figure: The RBAC Concept

The following list describes the figure above:

User

The user is the instance, which represents a single real user, which works with the system, as well as technical users to administer the system. Users have a set of properties, which can be defined individually for every user. There is a _commonpropertiesuser_, which has defined all properties, that shall be available for all users per default. All users inherit the properties from this special technical user if they have not defined them by their own. Some properties like password, room, phone number are available for every user. Other properties like text decorators, icon decorators, severity colors are basically defined by the _commonpropertiesuser_ and can be adjusted individually for every single user afterwards.

Users are defined in the <code>UserEditor</code>. To edit the list of user properties, there is the special <code>UserPreferencesEditor</code>.

Users can belong to none or several groups and are a so called Orga Object. Orga Objects can be associated with roles. More about that relations can be found in description to Group, Role and Right.

• Group

It is possible to associate several users to one group as well as groups can also contain other groups. Groups can also be associated to roles. A user, which is inside a group is automatically associated with the roles which "belong" to the group. So it is possible to give a bunch of users the same rights.

Groups are Orga Objects and are defined in the GroupEditor.

Orga Object

An Orga Object is an abstract instance, which is whether a group or a user. It does not have any individual functionality. Combined with a role it is defined as a right.

There are no editors for Orga Objects, since users as well as groups are Orga objects by their self.

Right

The right is an association between Orga Objects (users and groups) and roles. Internal the permission handling uses these rights objects to resolve the relations between users and roles to verify whether a user has permission for an action or not.

Rights are not accessible by the user directly. Rights are defined by associating a group with a role in the GroupEditor and by associating a user with a role in the UserEditor.

Role

A role can have an arbitrary name. There exists a role for every user (with the same name of the user). When the user is renamed, also this special role is renamed. Roles are a central element in the RBAC.

Roles are edited in the RoleEditor, in which the association between roles, functions and access definitions are defined.

In the roles rights relation the role can be defined as "The instance WHICH is allowed to do something.

Function

Functions are used to define WHAT a role is allowed to do. So functions are named like <code>update</code>, <code>remove</code>, <code>create</code>.

A function can be enabled and disabled. If the function is disabled, the action which is represented by the function is not available any more. So if the function create is disabled, no more new items can be created.

Functions can be edited in the FunctionEditor.

AccessDefinition

An access definition represents every entity in the tree as a unique data type. So every host, every user, every datastream or every tree itself has an access definition, representing the object. So it is some kind of entity for all objects. It is used to define with WHAT something shall be done. An access definition can also have function arguments.

Access definitions are edited in the AccessDefinitionEditor. This editor is reached by opening the context menu in the TreeView and clicking "Edit Access Definition".

• Function Argument

A function argument can specify the access definition more detailed. It is like to define with WHAT something shall be done with WHICH limitations.

The function arguments are edited in the AccessDefinitionEditor and are globbing strings, like on bash. They are used to specify the access definition more detailed like an url or a path which specifies the access definition more detailed. Per default no access definition is needed. There are

also special function arguments like "*HOST", which for example makes it possible to enable the visibility for all hosts for a user.

Roles Rights

Roles Rights are the association between a role, a function and an access definition. It is the definition of WHO (the role) is allowed to do WHAT (the function) on WHICH (the access definition) entity.

Internally the roles rights definition is a table which stores the roles id, the function id and the access definition id in a row.

RBAC Explicit Example

The following section gives an explicit example about how RBAC works.



Figure: The RBAC Example

The figure above describes how the roles rights mechanism works. The list below describes the meaning of the tables.

Roles

The Roles table defines the roles in the system (manually created as well as automatically created). The administrator is supposed to have access to every item, the operator is supposed to have several access on several items and the guest role is supposed to have only read access on several items, for example.

Access Definitions

The Access Definitions table represents every visible and invisible tree item in the system. So it defines folders, users, hosts, datastreams, roles, groups, views and every other type of item which needs to have access control. In the example there are two hosts, a folder a view and two special access definitions. The access definition with the id "5" is the special "ALL" access definition. It has wildcard functionality and represents every access definition.

Another special access definition is the one with id "6". It is a "*user" access definition and represent "all users". It is also possible to define a *HOST or *FOLDER access definition, which represent "all hosts" respective "all folders".

The Name column defines the name of the access definition, the EntType represents the type of the entity which is represented by the access definition. EntId defines the id of the entity inside its own table and EntName is the name of the entity inside its table. It is also possible to create a second access definition for the same entity.

Functions

The functions table shows the basic functions of the system, such as create, delete and update. There is a special function "*" with the id "5". It has wildcard functionality and represents every function.

Roles Rights

The roles rights table brings all the other tables in relation to each other. Each row of the roles rights table will be treated manually.

- Row 1: Role Id "1" means that the administrator is allowed to perform function 5 (*) on access definition 5 (ALL). This means that the administrator is allowed to perform every function on every access definition. Total access.

- Row 2: Role Id "2" means that the <code>operator</code> is allowed to perform function 2 (delete) on the access definition 2 (Host1).

- Row 3: Role Id "2" means that the operator is allowed to perform function 3 (update) on the access definition 2 (Host1).

- Row 4: Role Id "2" means that the operator is allowed to perform function 4 (read) on the access definition 2 (Host1). So this role is allowed to delete, update (edit) and read (show in editor and in tree) the item Host1. It would also have been possible to use the function with the id 5 (*) to give the user all access to the item Host1.

- Row 5: Role Id "3" means that the guest is allowed to perform function 4 (show) on the access definition 2 (Host1). Guest is not allowed to perform any other functions on this item. So the role guest has read only access to this item.

- Row 6 and Row 7: Role Id "3" means that the guest is allowed to perform function 3 (update) and 4 (read) on the access definition 3 (Host2).

- *Row 8:* Role Id "2" means that the operator is allowed to perform function 5 (*) on access definition 6 (*user). This means that the operator role has full access (function *) on all users (access definition *user).

- Since there are no other rows in the roles rights table, no roles (except the administrator role, which has full access on every access definition) have any access to the access definition 1 and 4 (MyHosts folder and TreeView).

How to Reset the Admin Account?

If an administrator has changed the last account with administrator rights, it will not be possible to undo that action! So it can be necessary to re-enable the default administrator account, that was created while the IBM Enterprise Content Management System Monitor was installed. To allow the re-creation/re-enablement of that default admin account the following has to be done in that order:

- 1 Get the full host name of the ECM SM event server by calling the token generation script without any arguments, see below.
- 2 Open a call at the official ECM SM support asking to send you a token to reset the admin account, append the host name from step 1 to that call.
- 3 After the support has send you a token, call the reset admin script with the host name and the token as arguments, see below.

If nothing went wrong, it should be possible to login as "admin" with the default password "admin" again.

It is strongly recommended to change the default password right after the first successful re-login.

Getting the correct Host name

Preconditions

The following preconditions must be met to allow a successful execution of the script to resolve the correct host name of the ECM SM server:

- The DNS lookup for the host name of the event server host is functioning properly.
- A Java JRE with a version not lower than 7 is installed at the event server.
- The JAVA_HOME environment variable is set to point to the Java JRE's installation directory.
- The caller of the script is logged on at the event server.
- The caller of the script has access to the script's installation directory at the event server.
- The caller of the script has the permission to execute the script at its installation location.
- The caller of the script has changed the current directory of the command line interface to the directory the script is installed.

Getting the Host name

To get the host name to be used for the token generation and later on to reset the admin account, the resetter script has to be called without any arguments. Replace "<ext>" with "sh" for Unix(TM)/Linux(TM) and " cmd" for Microsoft Windows(TM) in the following.

ResetAdmin.<ext>

The result should look like the following:

Mention the host name shown in the first output line. That host name has to be send to the support with a request to get the token for that host (aka id).

Resetting the Admin Account

Preconditions

The following preconditions must be met to allow a successful execution of the admin account resetter script:

- The correct host name of the event server host is known, see above.
- The DNS lookup for the host name of the event server host is functioning properly.
- The official IBM Enterprise Content Management System Monitor support has provided the token for the correct host name of the ECM SM server. If not already done, the token must be requested. Beware: The token expires after 14 days after its creation. The expiration date it the part after the TX in the token.
- A Java JRE with a version not lower than 7 is installed at the event server.
- The JAVA_HOME environment variable is set to point to the Java JRE's installation directory.
- The event server database must be accessible through JDBC.
- The caller of the script is logged on at the event server.
- The caller of the script has access to the script's installation directory at the event server.
- The caller of the script has the permission to execute the script at its installation location.
- The caller of the script has changed the current directory of the command line interface to the directory the script is installed.

Calling the ResetAdmin Script

The admin account resetter script has to be called like shown below. Replace "<ext>" with "sh" for Unix(TM)/Linux(TM) and "cmd" for Microsoft Windows(TM) in the following.

ResetAdmin.<ext> <host name event server> <token>

On success, the result should look similar to this:

SUCCESS

Login as admin should now be possible again.

What to do Next?

Restart the GUI server.

Login as user "admin" with the default password "admin".

It is strongly recommended to change the default password right after the first successful re-login.

Error Codes and Messages

The so called error codes are the return codes of the script. They are not printed to stdout, but can be accessed by the platform specific environment variables. The return '0' (zero) signals success.

The following error codes and messages are possible.

Error code: 1

ERROR: Failed to load database settings from "dbcfg.properties".

Error code 2

ERROR: Database corruption too severe.

The database is too damaged to allow the automatic account restoration.

Details: The ANY entity does not exist.

Error code 3

Failed to persist the corrective actions.

Details: The database commit failed.

Error code 4 (case: Script called without any arguments)

The name of this host to be used is '<hostname>'.

Error code 4 (case: Script called with arguments)

ERROR: Wrong number of arguments!

Error code 5

Failed to retrieve host name.

Details: The host name of this host could not be resolved.

Error code 6

ERROR: Invalid id given.

Details: The host name given is not the full qualified domain name of this host.

Error code 7

ERROR: Invalid token given.

Details: The given token is not valid for the given id or invalid at all.

Error code 8

ERROR: Invalid token given.

Details: The given token is not valid for the given id or invalid at all.

Error code 9

ERROR: The name of this host could not be resolved.

Details: A working host name resolution via DNS is absolutely necessary for this program to function properly.

Error code 10

ERROR: The token has expired.

Details: The used token is too old. Every token has an expiration date. That date is shown as the last part of the token name after the letters TX. The expiration date has the format: YYYMMDDHHmmSS, where the hours are in the 24 hours format.

Note: Changing the expiration date by renaming the token file will invalidate the token. Renaming it back to its original name is possible and will enable the token again as long as the expiration date has not been passed.

Error code -1

ERROR: An unknown error occurred.

Details: Most likely this signals a Java RuntimeException.

Error code 99

Cannot find a valid Java installation.

A Java executable is essential for this tool.

Please install a Java JRE; at least version 7.

Set the JAVA_HOME environment variable appropriately.

Exiting.

Other error codes

ERROR: An unknown error occurred.

Details: The return code was <numeric error code>

Context-sensitive help

Windows

On a windows system only get focus of a view or something else and press F1 on the keyboard. Now will it open a new view with help for the given object.

UNIX/Linux

On a linux or unix system the context-sensitive help will working similar to windows, but some newer Linux systems like to press SHIFT+F1 on the keyboard to perform the desired action.

Appendix F. Logging Configuration Introduction

This section describes how diverse logging mechanisms of the *ECM SM Server* product can be adjusted in order to obtain a user-specific customization.

How to Configure Logging

The ECM SM Server software provides several ways to gather logging information.

Setting a Log Level

The log level can be defined in two ways:

- Globally for the whole application (default log level)
- Separately for each bundle, package or class.

NOTE The bundle log level overrides the global log level for this specific bundle.

The log level can be defined at two different locations:

- Via \$CENIT_ROOT/<componentName>/cfg/logging.conf (persistently)
- Via OSGi console (temporarily as long as the respective component is running)

You ought to distinguish between two fundamentally different log file types for the *GUI Server* and the *Event Server* component:

- Log files (e.g. gui.0.log or eventserver.0.log) These files log all messages of the INFO severity or worse.
- Trace files (e.g. gui.0.trace or eventserver.0.trace)
 Trace log files are deactivated per default. When activated during the installation process (see Enable ECM SM Event Server and GUI Debugging installer option in the Server Installation Process chapter), trace log files will contain all log messages of the FINE severity.
 The trace log settings can be changed in the \$CENIT_ROOT/<componentName>/cfg/logging.conf file at any time.
 This mechanism is used to be able to log the same processes at two different log levels. In this sense, the log file mechanism is used for a more product-internal view whereas the trace log file mechanism is used for a rather 3rd-party-bundle-oriented logging providing a high granularity of logged messages.

Change Logging on the OSGi Console

Log levels are alternatively set over the OSGi console. Log in to the OSGi console via Telnet or SSH.

Setting the log level via bundle name

0001 osgi> setloglevel <BundleName> <LogLevel>
0002 For example:
0003 osgi> setloglevel finca.functional.hashcode DEBUG

In the brief example above, the log level of the finca.functional.hashcode bundle is set to DEBUG for the current session - until the configuration is read in again.

Setting the log level via package name

The log level can specifically be set for a distinct package of a bundle.

0001 osgi> setloglevel <PackageName> <LogLevel> 0002 For example: 0003 osgi> setloglevel finca.functional.hashcode.internal DEBUG

In the brief example above, the log level of the finca.functional.hashcode.internal package is set to DEBUG for the current session - until the configuration is read in again.

Setting the log level via class name

It is possible to set the log level for a specific class inside a specific package of a bundle.

0001 osgi> setloglevel <ClassName> <LogLevel>
0002 For example:
0003 osgi> setloglevel finca.functional.hashcode.internal.OsgiHashCodeService DEBUG

In the brief example above, the log level of the finca.functional.hashcode.internal.OSGiHashCodeService package is set to DEBUG for the current session - until the configuration is read in again.

NOTE Class-specific log level configuration is only available for classes, logging was implemented for explicitly. This logging type should be used for debugging purposes only. Due to this reason the list of classes, that support this kind of logging, is not public.

Log Levels

There are several log level nuances on the OSGi console, to which the log level of a bundle can be set to:

- OFF Logging is turned off.
- SEVERE (Internal level ERROR) This log entry indicates the bundle or service may not be functional. It is used, when exceptions occur.
- WARNING (Internal level WARNING) This log entry indicates a bundle or service is still functioning but may experience problems in the future because of the warning condition.
- INFO (Internal level INFO) An informational message. This log entry may be the result of any change in the bundle or service and does not indicate a problem.
- CONFIG (*3rd party level ERROR and WARNING)
- FINE (Internal Level DEBUG) This is the most helpful log level for problem determination.
- FINER (*3rd party level INFO)

- FINEST (Internal Level TRACE)
- ALL (*3rd party level DEBUG)

This is the most granular log level, which can be defined. It is used for problem determination and may be irrelevant to anyone but the bundle developer. It contains detailed information about object values at runtime.

*3rd party levels are used by OSGi logging or SLF4J logging, which are used by several 3rd party components. Since they are not part of our product logging, they are logged with low priority.

Configure Logging and Tracing via logging.conf

The logging.conf can be found at \$CENIT_ROOT/<componentName>/cfg/logging.conf.

The logging.conf file is documented by detailed inline comments. This chapter only provides additional information about the log levels, which can be set for the logging mechanism.

• .level = SEVERE

This level sets the level for the 3rd party components of the product. It is recommended not to change it, unless a deep debugging / tracing should be performed.

- de.cenit.eb.sm.finca.level = FINE
 This is the default log level. Every component inherits at least from this log level, if it has no log level
 el defined for itself and its parent does not have any log levels. You can enter an arbitrary log level
 here. FINE is only used as example.
- java.util.logging.FileHandler.level = INFO This is the log level for the logging component. If there are any log entries, worse than the log level, which is defined here, they will not be written into the log file. You can enter an arbitrary log level here. INFO is only used as example.
- de.cenit.eb.sm.finca.helper.loghandler.TraceFileHandler.level = OFF
 This is the log level for the tracing component. If there are any log entries, worse than the log level, which is defined here, they will not be written into the trace file. You can enter an arbitrary log level here. OFF is only used as example. It is recommended, that it is a finer log level, than the level which is defined in java.util.logging.FileHandler.level.

Inheritance of log levels

There is a hierarchy between the log levels of the several bundles / packages. Since there is a package structure, the child inherits the log level of the parent, if no log level is set. The following example illustrates how the log levels are inherited.

0001	# Example for a log level configuration	
0002	finca.functional.dblayer.entitymanager.provider	<no level="" log="" set=""></no>
0003	- finca.functional.dblayer.entitymanager	<log debug="" level="" set=""></log>
0004	- finca.functional.dblayer	<log level="" set="" warning=""></log>
0005	- finca.functional	<default <math="" info="" level="" log="">_{\leftarrow}</default>
	set>	

Let's imagine, that there is an error assumed to be somewhere in the dblayer.entitymanager.
So it is possible to set the log level of the entitymanager to DEBUG, which allows a very detailed logging for this component.

Since dblayer is a very complex component, you might to reduce the output of non-entitymanager components of the dblayer and so set the level to WARNING.

The default log level (finca.functional) is set to INFO in logging.conf. As the finca.functional.dblayer log level is explicitly set to WARNING, the default log level is overwritten for this component.

The entitymanager.provider has no log level set. It inherits the log level of its parent. The parent of finca.functional.dblayer.entitymanager.provider is the bundle finca.functional.dblayer.entitymanager.

In case that fince.functional.dblayer.entitymanager had no level set, the parent's parent log level would be used, which means fince.functional.dblayer.Finally if fince.functional.dblayer was not set the next parent would be fince.functional (default log level).

Appendix G. InstallAnywhere Installer Variables

Documentation of the InstallAnywhere installer variables

The following table provides an overview of the public installer variables used by the *InstallAnywhere* software during the installation of *ECM SM Server*. In general, the value of a variable should not be altered. Please adapt it only in case, you know what you are doing, and exclusively use one of the specified allowable values listed below:

ECM SM server installer variable	Description
CENIT_ROOT	The CENIT tools base installation directory.
S_ADMIN_EMAIL	The e-mail address of the person or group respon- sible for administering this ECM SM (CALA remote execution) server and agent service.
S_APP_HOST	The WebSphere Server name (hostname).
S_APP_PORT	The WebSphere Server port.
S_APP_TYPE, S_APP_TYPE_LONG	Web Application Server type (in short and long ver- sion)
S_AUTH_LOGIN, S_AUTH_PLAIN, S_AUTH_DIGEST, S_AUTH_NTLM, S_AUTH_SASL	The supported SMTP authentication method (LOGIN, PLAIN, DIGEST-MD5, NTLM or SASL).
S_AUTH_LONG_METH	Authentication method written in long version. Al- lowable values: (Internal authentication, no LDAP)
S_AUTH_NONE	Disables the SMTP authentication.
S_AUTOMATIC_STARTUP, S_MANUAL_STARTUP	The startup behavior:
	Automatic Startup
	Manual Startup
S_CALA_REX_HOST	The full qualified IP name of the ECM SM server.
S_CALA_REX_HOST_DETECT	Full qualified system name for the CALA_REX.
S_CALA_REX_PASSWD_ORIG	The password of the Services/Agents User, only for MS SQL Windows Authentication.
S_CALA_REX_PORT	This parameter defines the server-side port of the agent that's responsible for client installation, task execution and other action taken on clients.
S_CALA_REX_USER_ORIG, S_CALA_REX_USER, S_CALA_REX_USER_SHORT	If this parameter is specified the services/agents will be installed with this user account. Otherwise the service/daemon will be started as Local System (Windows) or root (UNIX/Linux). The "_SHORT" version is the name without domain. The version "S_CALA_REX_USER" is the normalized version of the String.

ECM SM server installer variable	Description
S_CONFIGURE	The default Install type: Upgrade
S_CREATE_DB	Is set to 1, if the option to create the database and not to create DDL files was selected in the installer. In this case the installer will automatically create the database and no DDL files will be written out.
S_CREATE_DB_AND_DDL	Is set to 1, if the option to create the database by the installer and additionally write down the DDL files, else 0.
S_CREATE_DDL	Is set to 1, if DDL creation was selected in the in- staller, else 0. In this case the database is not creat- ed automatically, but must be created via script.
S_CUSTOM_FORMATFILE_ORIG	The custom event forwarding format file inclusive relative path to <install-dir>/eventserver.</install-dir>
S_DB_DB2, S_DB_MSSQL, S_DB_ORACLE,	The supported database access:
S_DB_POSTGSQL	• DB2
	MSSQL Server, only for Windows based ECM SM servers)
	Oracle
	 PostgreSQL, only supported for Demo and testing purposes
S_DB_HOST	The host name (IP address) of the host on which the database management system is running.
S_DB_INST_NAME	The instance name of the configured database.
S_DB_JNDI_NAME	The created WebSphere datasource name.
S_DB_NAME	Name of the database inside the database management system
S_DB_PASSWD_ORIG	The password to authenticate against the config- ured database.
S_DB_PORT	The port of the configured database.
S_DB_SCHEMA	The database schema of the configured database.
S_DB_SCHEMA_ORACLE_UC	The database schema of the configured database (special upper case handling for oracle databases).
S_DB_TYPE, S_DB_TYPE_LONG	Database type, like (DB2 or MSSQL) in short and long version
S_DB_TYPE_PREVIOUS	The database type of the FSM 4.0 installation whose events shall be imported.
S_DB_USER_ORIG	The user to authenticate against the DB management system.
S_DB2_COPY_LOC	The IBM DB2 driver file location.
S_DDL_FOLDER	The directory for create DDL's, when running in "create database automatically and additionally DDL files" mode.

ECM SM server installer variable	Description
S_DDL_FOLDER_ADDON	The directory for created DDL's, when running the AddOn installation.
S_DDL_FOLDER_ONLY	The directory for created DDL's, when running the installation in "create database manually via DDL files" mode.
S_DL_PORT	The ECM SM Download Server port. The default value of this port is 23990.
S_DONT_USE_SSL	Is set to 0 if the GUI was configured for HTTPS, else to 1.
S_EAR_CONTEXT_ROOT	The context root path of the ECM SM installation inside a WebSphere based installation for the GUI service. It is used insite the application.xml file, which is part of the ear file.
S_EAR_DISPLAY_NAME	This variable is used to specify the name of the ap- plication inside application.xml file, which is part of the ear file. This name will be visible in the We- bSphere Integrated Solutions console, after deploy- ment for the GUI service.
S_EAR_FILE	The name of the ear file, for the GUI service, which is created, when the application is installed in We- bSphere mode.
S_EAR_SERVER_CONTEXT_ROOT	The context root path of the ECM SM installation in- side a WebSphere based installation for the event server service. It is used inside the application.xml file, which is part of the ear file.
S_EAR_SERVER_DISPLAY_NAME	This variable is used to specify the name of the ap- plication inside application.xml file, which is part of the ear file. This name will be visible in the We- bSphere Integrated Solutions console, after deploy- ment for the event server service.
S_EAR_SERVER_FILE	The name of the ear file, for the event server ser- vice, which is created, when the application is in- stalled in WebSphere mode.
S_EEIF_ENABLE, S_EEIF_DISABLE	Enables/Disables the IBM EEIF Event forwarding.
S_EEIF_JARS	When configuring the EEIF sink, the path to the jar files, which must be copied from the server on which the Tivoli Enterprise Console is running, is stored in this variable.
S_EEIF_LIB_DIR	The IBM Tivoli EEIF Java library directory (location of evd.jar and log.jar).
S_EEIF_PORT	The IBM Tivoli EEIF port. The default value of this port is 5529.
S_EEIF_SERVER	The IBM Tivoli EEIF event server name or IP ad- dress.
S_ESX_COPY_LOC	The VMWare ESX driver file name (full name of file vim25.jar).

ECM SM server installer variable	Description
S_FIR_PORT	The event reception port. This is used to receive events from clients (managed systems). The default value of this ECM SM server monitoring port (CALA Port) is 23840.
S_IMPORT_DB	Is set to 1, when the option to import events from an old FSM 4.0 system was activated, else it is set to 0.
S_INSTALL_DEBUG	Enables the ECM SM server installer debugging.
S_JAVA_INSTALLER_DEBUG	The Java debug parameter '- Dde.cenit.eb.sm.installer.debug=true'.
S_JDBC_CLASS	The JDBC class, which is used for the InitDB process.
S_JDBC_CLASS_DBIMPORT	The JDBC class, which is used for the import db process, when importing for FSM 4.0 events was created.
S_JDBC_DBIMPORT_PASSWORD_ORIG	The password for the user to authenticate against the database management system, which is used to perform the import of old FSM 4.0 events.
S_JDBC_DBIMPORT_USER	The user to authenticate against the database man- agement system, which is used to perform the im- port of old FSM 4.0 events.
S_JDBC_DRIVER_PATH	The path to the JDBC driver path (jar file or directo- ry which contains the jar files), which is used for the database initialization.
S_JDBC_DRIVER_PATH_FW	The path to the JDBC driver path with forward slashes (jar file or directory which contains the jar files), which is used for the database initialization.
S_JDBC_FILE_PREVIOUS	The path to the JDBC driver path (jar file), which is used for the FSM 4.0 event import.
S_JDBC_MANIFEST_FILE	Gather JDBC driver file for Oracle, MSSQL or Post- greSQL.
S_JDBC_PROVIDER_DIR	The JDBC providers directory, that specifies the driver files that can be used to connect to a database.
S_JDBC_PROVIDER_DIR_PREVIOUS	The JDBC providers directory, that specifies the driver files that can be used to connect to a database, which is used for the FSM 4.0 event import.
S_JDBC_SETTINGS	The JDBC connection string, as example 'jdbc:postgresql: <database-name>' for the Post- greSQL.</database-name>
S_JETTY, S_WAS	The used type of the Web Application Server (Embedded Jetty Server or IBM WebSphere).
S_KEYSTORE_FILE_ORIG	The full qualified keystore file name including path.
S_KEYSTORE_KEY_PW_ORIG, S_KEYSTORE_PW_ORIG	The SSL key password. If unset the store password will be used.
S_KEYSTORE_PATH	The directory of the keystore.

ECM SM server installer variable	Description
S_LDAP	Allowable values: 0 or 1. (0): Internal authentication is used. (1): The used authentication type is LDAP. In this case, an external LDAP (Directory Service) system is required to authenticate users.
S_LDAP_CARRY_OVER_EXT_GRP	Allowable values: 0 or 1. (0): User groups will be assigned to the user from the internal RBAC data- base. (1): User groups will be carried over from an external system like an LDAP directory service.
S_LDAP_DEFAULT_PORT	The LDAP Server port (e.g. 389, 636 if SSL activated).
S_LDAP_DOMAIN_LC_ADS, S_LDAP_DOMAIN_LC_ADS2	The Domain name in lowercase letters, e.g. mydomain.com.
S_LDAP_GROUP_ATTRIBUTE_ADS, S_LDAP_GROUP_ATTRIBUTE_ADS2, S_LDAP_GROUP_ATTRIBUTE_ADAM, S_LDAP_GROUP_ATTRIBUTE_SUN, S_LDAP_GROUP_ATTRIBUTE_IBM, S_LDAP_GROUP_ATTRIBUTE_NOVELL	The LDAP Group attribute that contains group infor- mation.
S_LDAP_GROUP_NAME_INDEX_ADS, S_LDAP_GROUP_NAME_INDEX_ADS2, S_LDAP_GROUP_NAME_INDEX_ADAM, S_LDAP_GROUP_NAME_INDEX_SUN, S_LDAP_GROUP_NAME_INDEX_IBM, S_LDAP_GROUP_NAME_INDEX_NOVELL	The LDAP Group name index that contains group information. The default index is 1.
S_LDAP_GROUP_NAME_PATTERN_ADS, S_LDAP_GROUP_NAME_PATTERN_ADS2, S_LDAP_GROUP_NAME_PATTERN_ADAM, S_LDAP_GROUP_NAME_PATTERN_SUN, S_LDAP_GROUP_NAME_PATTERN_IBM, S_LDAP_GROUP_NAME_PATTERN_NOVELL	The LDAP Group name pattern.
S_LDAP_GROUP_QUERY_ADS, S_LDAP_GROUP_QUERY_ADS2, S_LDAP_GROUP_QUERY_ADAM, S_LDAP_GROUP_QUERY_SUN, S_LDAP_GROUP_QUERY_IBM, S_LDAP_GROUP_QUERY_NOVELL	The LDAP Group query.
S_LDAP_GROUP_URL_ADS, S_LDAP_GROUP_URL_ADS2, S_LDAP_GROUP_URL_ADAM, S_LDAP_GROUP_URL_SUN, S_LDAP_GROUP_URL_IBM, S_LDAP_GROUP_URL_NOVELL	The LDAP Group provider URL to search for groups.
S_LDAP_KIND	The prefix used in the specified LDAP URL. Allow- able values: Idap or Idaps. The URL format is Idap:// host:port/dn?attributes?scope?filter?extensions re- spectively Idaps://host:port/dn?attributes?scope?fil- ter?extensions
S_LDAP_OVER_SSL, S_LDAP, S_INTERNAL_AUTH	The used authentication type (LDAP over SSL, LDAP or ECM SM internal authentication).

ECM SM sorver installer variable	Description
	to the truststore file name and the password.
	• ECM SM internal authentication: In this case, no external LDAP (Directory Service) is required to authenticate users for ECM SM.
S_LDAP_PORT_ADAM, S_LDAP_PORT_ADS, S_LDAP_PORT_ADS2, S_LDAP_PORT_IBM, S_LDAP_PORT_NOVELL, S_LDAP_PORT_SUN	The LDAP Server port (e.g. 389, 636 if SSL activated).
S_LDAP_REQ_INT_USER	Requires internal ECM SM user.
S_LDAP_SERVER_ADS, S_LDAP_SERVER_ADS2	The ADS Server name (Domain Controller without DNS suffix, e.g. 'adsserv').
S_LDAP_SERVER_ADAM, S_LDAP_SERVER_SUN, S_LDAP_SERVER_IBM, S_LDAP_SERVER_NOVELL	The full qualified LDAP Server name.
S_LDAP_SSL_PASSWORD_ENC	Encrypts truststore password S_LDAP_SSL_PASSWORD to S_LDAP_SSL_PASSWORD_ENC
S_LDAP_SSL_PW	The LDAP password.
S_LDAP_SSL_SECURITY_PRINCIPAL_ADS2	The LDAP Security principal. The default value is '{0}' or '{0}@ <domain-name>'.</domain-name>
S_LDAP_SSL_SECURITY_PROTOCOL	Security protocol to use, eg: 'ssl'.
S_LDAP_TRUSTSTORE_FILE	The LDAP truststore file name.
S_LDAP_TRUSTSTORE_PATH	The keystore file including full path.
S_LDAP_TYPE, S_LDAP_LONG_TYPE	LDAP Type in short and long name, like "ADAM" for "Microsoft ADAM"
S_LDAP_USER	The valid LDAP user name of the specified directory server.
S_LDAP_USER_URL_ADAM, S_LDAP_USER_URL_SUN, S_LDAP_USER_URL_IBM, S_LDAP_USER_URL_NOVELL	The LDAP User URL.
S_LOCAL_HOST	Contains the full qualified host name of the local server.
S_LOGF_ENABLE, S_LOGF_DISABLE	Enables/Disables log file event forwarding.
S_LOGF_FILENAME_ORIG	The log file with path relative to <install-dir>/ eventserver or absolute path (directory must exist).</install-dir>
S_LOGF_MINLEVEL	Sets the log file logging level to the highest.
S_MSADS_AUTH, S_MSADS2_AUTH,	The (LDAP) authentication types:
S_MSADAM_AUTH, S_SUNJAVA_AUTH, S_IBMTIVOLI_AUTH, S_NOVELL_AUTH	• MS ADS (with SASL/GSSAPI authentication)
	• MS ADS (with simple authentication method)
	• MS ADAM
	SUN Java System Directory Server

ECM SM server installer variable	Description
	IBM Tivoli Directory Server
	Novell eDirectory
S_MSSQL_COPY_DLL_FILE	MSSQL Windows authentication DLL file sqljdbc_auth.dll inclusive full path.
S_MSSQL_COPY_LOC	The JDBC driver file name (full name of file sqljdbc4.jar).
S_MSSQL_DB_AUTH, S_MSSQL_WIN_AUTH	The MSSQL authentication method:
	• Database authentication, the technical user that connects to the database requires database authentication only.
	• Windows authentication (integrated authen- tication), this authentication method requires the access to an integrated authentication Windows DDL file.
S_MSSQL_DLL_FILE	The MSSQL Windows authentication file sqljdbc_auth.dll inclusive full path.
S_MULTILINE, S_SINGLELINE	The output format of the log file event forwarding.
	• The default multi line output format.
	• The default single line output format.
S_ALL_RE, S_NO_HARMLESS, S_NO_WARNING	The configuration of the report events.
	Report all events.
	Report all except HARMLESS events.
	Report all except HARMLESS and WARNING events.
S_ORACLE_COPY_LOC	The JDBC driver file name (full name of file ojdbc5.jar or ojdbc6.jar).
S_OVO_ENABLE, S_OVO_DISABLE	Enables/Disables the HP Operations forwarding (HP OVO Forwarding).
S_OVO_LIB_DIR	HO OVO Java library directory (location of jopcagtbase.jar and jopcagtmsg.jar).
S_OVO_PORT	HO OVO port. The default value of this port is 381.
S_OVO_SERVER	The HP OVO server name (full qualified DNS name).
S_PRG_OS_USER_ORIG, S_PRG_OS_USER	For Windows there is the possibility to define the user of the windows services. This user is also selected, when the MSSQL database installation setting is configured for Windows authentication instead of database authentication. This feature is only supported for MSSQL.
S_PROD_DEBUG	Enables ECM SM Server and GUI debugging.

ECM SM server installer variable	Description
S_PROD_DISP_NAME	The product display name (name, which is shown in the GUI).
S_PROD_NAME_LC	The internal product name. "_LC" stands for "lower case"
S_PROD_NAME_VENDOR	The internal product name, focused on the vendor of the product. It is used to build the name refer- ences of the downloadable content of the webstart directory.
S_PROD_SHORT_NAME	The internal product name in its short version.
S_PROD_TECH_NAME	The technical name is used to set the name of files and internal processes at the time of installation process.
S_PROD_TECH_NAME_SHORT	The technical name is used to set the name of files and internal processes at the time of installation process. This is the short version of this variable.
S_PROD_TECH_NAME_SHORT_LC	The technical name is used to set the name of files and internal processes at the time of installation process. This is the short version in lower case of this variable.
S_PROD_TECH_NAME_SHORT_UC	The technical name is used to set the name of files and internal processes at the time of installation process. This is the short version in upper case of this variable.
S_RAP_CONSOLE_ENABLED	Enables OSGi RAP (WEB GUI) console. (coded as alphanumeric value - can be true for enabled and false for disabled)
S_RAP_CONSOLE_NUM_ENABLED	Enables OSGi RAP (WEB GUI) console. (coded as number - can be 1 for enabled and 0 for disabled)
S_RAP_CONSOLE_PORT	The RAP console port (default: 23980) Default con- sole port of the Port of the OSGi console of the RAP (Rich Ajax Platform) Web server. Allows access to the OSGi console of the event server. Only used for maintenance.
S_RAP_HTTP_PORT	The port to access the RAP GUI via web browser. Default in Jetty based installations is 23990.
S_RAP_HTTP_SERVER	The RAP HTTP Server name. Full qualified IP name or address of the ECM SM RAP (Rich Ajax Plat- form) Web server.
S_RAP_REMOTE_DEBUG_PORT	The Server RAP Remote Debug port (Default: 8001).
S_SERVER_CONSOLE_ENABLED	Enables OSGi server console (coded as alphanu- meric value - can be true for enabled and false for disabled)
S_SERVER_CONSOLE_NUM_ENABLED	Enables OSGi server console (coded as number - can be 1 for enabled and 0 for disabled)
S_SERVER_CONSOLE_PORT	The Server console port (default: 23960). Port of the OSGi console of the event server. Allows access to

ECM SM server installer variable	Description
	the OSGi console of the event server. Only used for maintenance.
S_SERVER_INIT_REMOTE_DEBUG_PORT	Specifies the -Xdebug port for remote Java debug- ging for the InitDB component. Is empty, if the port was not set in the installer. It is only used in the Unix/Linux version of the initdb.sh script. The line for remote debugging is commented out and must be uncommented, if debugging shall be enabled. It is only used for manual execution of the InitDB process.
S_SERVER_INITDB_PORT	The Server InitDB console port (default: 23962). Port of the OSGi console of the database initializa- tion process. Allows access to the OSGi console of the database initialization process of the installer. Only used for maintenance.
S_SERVER_REMOTE_DEBUG_PORT	Specifies the -Xdebug port for remote Java debug- ging for the event server component. Is empty, if the port was not set in the installer.
S_SHELL_ARCHIVE	The name of the zip archive, which contains the Windows shell, when it was downloaded manually.
S_SHELL_PATH	The path to the zipped Windows shell, when it was downloaded manually and referenced in the installer.
S_SMTP_AUTH_PASSWD_ORIG	The password of authentication user.
S_SMTP_AUTH_USER	The user to authenticate against the SMTP server, when an authentication method was defined in the SMTP sink configuration panel.
S_SMTP_AUTH_USER_ORIG	The SMTP authentication user (if authentication is enabled).
S_SMTP_AUTHTYPE	Is not set, if SMTP authentication is not activated. Else it defines the authentication type with which the ECM SM SMTP components shall authenticate against the SMTP server.
S_SMTP_ENABLE, S_SMTP_DISABLE	Enables/Disables the email forwarding (SMTP).
S_SMTP_PORT	The SMTP Server port. The default value of this port is 25.
S_SMTP_SERVER	The SMTP Server name (full qualified DNS name).
S_SMTP_USER	The SMTP email account to forward events.
S_SNMP_ENABLE,S_SNMP_DISABLE	Enables/Disables the SNMP event forwarding.
S_SNMP_ENTERPRISE_OID	The SNMP Enterprise Object Identifier. The default identifier is 1.3.6.1.4.1.8235.
S_SNMP_PORT	The SNMP Server port. The default value of this port is 162.
S_SNMP_SERVER	The SNMP Server name or IP address.
S_SNMP_V1, S_SNMP_V2C, S_SNMP_V2C_INFORM	The used SNMP type (Version 1, Version 2C or Version 2C Inform).

ECM SM server installer variable	Description
S_START_NOW	Is set to 1, if the ECM SM services shall startup af- ter the installation finished. If it is set to 0, the ser- vices (GUI and Server) shall not be started.
S_STARTUP_TYPE	Is set to "auto", if the ECM SM services (GUI and Server) shall be started automatically after system startup. If "manual" is entered, the services won't start automatically at system startup, but have to be started manually.
S_NEWINSTALL, S_RECONFIGURE, S_UPGRADE	By detecting previous installations, it is possible to select the installation types:
	• New Install: The previous installation of the ECM SM server can no longer be used, because only one ECM SM server installation instance is supported on a server.
	• Reconfigure Only: The installer will not install components of ECM SM on the system into the existing installation directory. Use this for changing global configuration settings.
	• Upgrade: The installer will use the existing installation directory. All product components will be installed and configured again. Existing service/agent settings will be removed and installed again.
S_COMPLETEINSTALL, S_PRIMARY_INSTALL, S_COMPONENTINSTALL	By detecting previous installations, it is possible to select the Server types:
	 Complete Serevr Installation (S_COMPLETEINSTALL): All Server compo- nents of the ECM SM server will be installed. All components are: Database initialization, CALA_REX server, Event Server and GUI Server. A ECM SM CALA_REX Agent can optionally be installed on the server.
	 Primary Server installation (S_PRIMARY_INSTALL): The Primary Server er ECM SM installation contains the Database initialization, the CALA_REX Server, er, the Download Server or instead of the Downlaod Server the GUI Server component. Note: the Primary Server is a subset of the Complete installation, without an additional GUI Server and Event Server installation as Secindary Server installation the ECM SM System architecture is not complete. A ECM SM CALA_REX Agent can optionally be installed on the server.

ECM SM server installer variable	Description
	 Secondary Server installation (S_COMPONENTINSTALL): This server installation type is used to install the first or another GUI Server and / or Event Server comonent. A ECM SM CALA_REX Agent can optionally be installed on the server.
S_INSTALL_CALAREX, S_INSTALL_INITDB, S_INSTALL_GUI, S_INSTALL_EVENTSERVER, S_INSTALL_DOWNLOADSERVER, S_INSTALL_CALAREX_AGENT	Since this version of the product supports the instal- lation of specific components the following variables are set to 1, if the component is being installed or to 0 in the case the component wont be installed:
	• S_INSTALL_CALAREX: Defines the status of the CALA_REX Server installation.
	• S_INSTALL_INITDB: Defines the status of the Database initialization.
	 S_INSTALL_GUI: Defines the status of the GUI Server installation.
	 S_INSTALL_EVENTSERVER: Defines the status of the Event Server installation.
	• S_INSTALL_DOWNLOADSERVER: Defines the status of the Download Server installation.
	• S_INSTALL_CALAREX_AGENT: Defines the status of the CALA_REX Agent installation.
S_USE_DB2_FILES, S_DONT_USE_DB2_FILES	The IBM DB2 driver file location:
	The used of DB2 JDBC driver files for remote databases.
	• No used of DB2 JDBC driver files.
S_USE_ESX_FILES, S_DONT_USE_ESX_FILES	The VMWare ESX monitoring:
	• The used VMWare ESX driver file.
	• No used VMWare ESX driver file.
S_USE_KRB5	The Kerberos authentication in Active Directory, on- ly for MS ADS with GSSAPI.
S_USE_MSSQL_FILES,	The Microsoft SQL Server driver location:
3_DONT_03E_W33QL_FILES	The used MS SQL JDBC driver files for remote databases.
	• No used MS SQL JDBC driver files.
S_USE_ORACLE_FILES,	The Oracle Database driver location:
S_DUNI_USE_URAULE_FILES	• The used Oracle JDBC driver files for remote databases.
	No used Oracle JDBC driver files.

ECM SM server installer variable	Description
S_USE_SSL	Allowable values: 0 or 1. (0): Unsecured website access is used. (1): Secure website access is used.
_WAR_FILE	The GUI WAR file to deploy the WebSphere Appli- cation Server (\$S_PROD_TECH_NAME_SHORT \$_gui_app.war).
S_WAR_SERVER_FILE	The Server WAR file to deploy the WebSphere Application Server (\$S_PROD_TECH_NAME_SHORT \$_server_app.war).
S_WEB_PORT	ECM SM Web Server GUI and download port. The default value of this port is 23990 (any free port can be chosen).

Appendix H. Required database permissions

The following tables show the database permissions each monitor requires grouped by database. Additional tables show the permissions required by generic database monitors and configuration scripts that can access different database types.

All monitors and configuration scripts only require READ access to the listed tables.

DB2

These monitors are available for all products with a DB2 database component.

Monitor	Permissions	Note
DB2Status	SYSCAT.TABLESPACES	
DB2TablespaceStatus	Version 8 SYSCATV82. SNAPTBSPACEPART	
	Version 9 SYSIBMADM. SNAPTBSP_PART	
DB2TablespaceFree	Version 8 SYSCATV82. SNAPTBSPACEPART	
	Version 9 SYSIBMADM. SNAPTBSP_PART	
DB2TablespaceUsed	Version 8 SYSCATV82. SNAPTBSPACEPART	
	Version 9 SYSIBMADM. SNAPTBSP_PART	
DB2Statistic	UNIX OS execute permission for command line tool db2	cannot be used with UDC
	Windows OS execute permission for command line tool db2cmd	

Monitor	Permissions	Note
	In order to run the DB2Statistics command, the following roles are needed (for both operating sys- tems):	
	SYSADM	
	SYSCTRL	
	SYSMAINT	
	SYSMON	

MSSQL

These monitors are available for all products with an MSSQL database component.

Monitor	Permissions	Note
MSSQLDatabaseSize	mastersysdatabases	
	sysfiles	
	masterspt_values	
MSSQLDatabaseStatus	mastersysdatabases	
MSSQLDataspaceUsed	mastersysdatabases	
	exec for stored procedure sp_ spaceused	
MSSQLDataspaceUsedPct	mastersysdatabases	
	exec for stored procedure sp_ spaceused	
	exec for tool DBCC SQLPERF (LOGSPACE)	
	permission for VIEW SERVER STATE	
MSSQLLogspaceUsed	mastersysdatabases	
	exec for tool DBCC SQLPERF (LOGSPACE)	
	permission for VIEW SERVER STATE	
MSSQLLogspaceUsedPct	mastersysdatabases	
	exec for tool DBCC SQLPERF (LOGSPACE)	
	permission for VIEW SERVER STATE	
MSSQLNumberOfProcesses	mastersysdatabases	
	mastersysprocesses	

Oracle

These monitors are available for all products with an Oracle database component.

Monitor	Permissions	Note
OracleDatafileAvailable	sys.dba_data_files	
OracleFreeTablespace	sys.dba_free_space	
OracleNextExtend	sys.dba_tablespaces	
	sys.dba_tables	
	dba_free_space	
	sys.dba_indexes	
	sys.dba_clusters	
	sys.dba_rollback_segs	
	sys.dba_segments	
	v\$parameter	
OracleNonActiveRedologs	v\$log	
OracleRollbackSegmentOnline	sys.dba_rollback_segs	
OracleTablespaceAvailable	sys.dba_tablespaces	
OracleUserAccountStatus	dba_users	

Generic monitors

Generic monitors can monitor different database types.

Standard monitors

Monitor	Permissions	Note
ServiceLevel Monitor	DB2 <schema>.evt_mon_inst</schema>	
	<schema>.evt_new</schema>	
	<schema>.evt_hosts</schema>	
	MSSQL <schema>.evt_mon_inst</schema>	
	<schema>.evt_new</schema>	
	<schema>.evt_hosts</schema>	
	Oracle [<schema>.]evt_mon_ inst</schema>	
	[<schema>.]evt_hosts</schema>	
	PostGRESQL <schema>.evt_mon_inst</schema>	
	<schema>.evt_new</schema>	
	<schema>.evt_hosts</schema>	
SqlAlphaNumericMonitor		As the SELECT statement is a monitor argument, the required permissions depend on the giv- en SELECT statement. There are no default database permissions required by this monitor.
SqlNumericMonitor		As the SELECT statement is a monitor argument, the required permissions depend on the giv- en SELECT statement. There are no default database permissions required by this monitor.

Monitors for IBM FileNet Image Manager

Monitor	Permissions	Note
IndexDatabaseAvailability	DB2 SYSCAT. TABLESPACES	
	MSSQL mastersysdatabases	
	Oracle sys.dba_tablespaces	

Monitors for IBM FileNet P8 4.x/5.x

In addition to the below listed IBM FileNet P8 4.x/5.x monitors the IBM FileNet P8 4.x/5.x monitoring archive contains pre-configured IBM FileNet CE Objectstore monitors for the supported database types. These monitors (name prefix ObjectStore followed by the DB type) are equivalent to the basic DB-specific monitors listed in this chapter, but require only minimum parameters. All other Database specific parameters are configured using the task 'Configure Objectstore Database Settings'. These monitors require the same Database permissions described in the first section of this chapter.

Monitor	Permissions	Note
Content Search Services Index	DB2	DB2
Requests	<schema>. INDEXREQUESTS</schema>	<pre><schema> is the schema name either given as monitor argument or road from the file</schema></pre>
	MSSQL <dbname>. INDEXREQUESTS</dbname>	objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for
	Oracle [<schema>.]</schema>	details.
	INDEXREQUESTS	MSSQL
		<pre><dbname> is the data- base name name either given as moni- tor argument or read from the file objectstore_conf.prop, depending on monitor</dbname></pre>

Monitor	Permissions	Note
		configuration. See mon- itor documentation for details.
		Oracle <schema> is the schema name either given as monitor argument or read from the file <i>objectstore_conf.prop</i>, depending on monitor configuration. See mon- itor documentation for details.</schema>
		The schema name is optional.
Content Search Services Indexing	DB2	DB2
Errors	<schema>. INDEXREQUESTS</schema>	<schema> is the schema name either given as monitor argument or</schema>
	MSSQL <dbname>. INDEXREQUESTS</dbname>	depending on monitor configuration. See mon- itor documentation for
	Oracle	details.
	[<schema>.]</schema>	
	INDEXREQUESTS	MSSQL
		<pre><dbname> is the data- base name name either given as moni- tor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.</dbname></pre>
		Oracle
		<pre><schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor</schema></pre>

Monitor	Permissions	Note
		configuration. See mon- itor documentation for details. The schema name is optional
IccivianObjects	<pre> Schema>.DocVersion <schema>. ClassDefinition MSSQL <dbname>.DocVersion <dbname>. ClassDefinition </dbname></dbname></schema></pre>	<pre><schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.</schema></pre>
		MSSOL
	Oracle [<schema>.]DocVersion [<schema>.] ClassDefinition</schema></schema>	<pre><dbname> is the data- base name name either given as moni- tor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.</dbname></pre>
		Oraçla
		<pre><schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.</schema></pre>
		The schema name is optional.
IccMailInstances	DB2	DB2
	<schema>.Generic <schema>. ClassDefinition</schema></schema>	<pre><schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor</schema></pre>

Monitor	Permissions	Note
Mornitor	MSSQL <dbname>.Generic <dbname>. ClassDefinition Oracle [<schema>.]Generic [<schema>.] ClassDefinition</schema></schema></dbname></dbname>	configuration. See monitor documentation for details. MSSQL <dbname> is the database name name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See monitor documentation for details.</dbname>
		Oracle <schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details. The schema name is optional</schema>
IccObjectsNotStoredFinally	DB2 <schema>. CONTENTQUEUE MSSQL <dbname>. CONTENTQUEUE Oracle [<schema>.] CONTENTQUEUE</schema></dbname></schema>	DB2 <schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details. MSSQL <dbname> is the data- base name name either given as moni- tor argument or read from the file objectstore_conf.prop,</dbname></schema>

Monitor	Permissions	Note
		configuration. See mon- itor documentation for details.
		Oracle <schema> is the schema name either given as monitor argument or read from the file <i>objectstore_conf.prop</i>, depending on monitor configuration. See mon- itor documentation for details.</schema>
		The schema name is optional.
StorageAreaInformationSql	DB2 <schema>.StorageClass <schema>. ClassDefinition MSSQL</schema></schema>	DB2 <schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon-</schema>
	 <dbname>.</dbname> <dbname>.</dbname> ClassDefinition 	itor documentation for details.
	ClassDelinition	MSSQL
	Oracle [<schema>.] StorageClass [<schema>.] ClassDefinition</schema></schema>	<pre><dbname> is the data- base name name either given as moni- tor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.</dbname></pre>
		Oracle
		<pre><scriema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor</scriema></pre>

Monitor	Permissions	Note
		configuration. See mon- itor documentation for details.
		The schema name is optional.
StorageAreaStatusSql	DB2 <schema>.StorageClass <schema>. ClassDefinition MSSQL <dbname>.StorageClass <dbname>. ClassDefinition Oracle [<schema>.] StorageClass</schema></dbname></dbname></schema></schema>	DB2 <schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details. MSSQL <dbname> is the data- base name name either given as moni- tor argument or read</dbname></schema>
	[<schema>.] ClassDefinition</schema>	from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.
		Oracle <schema> is the schema name either given as monitor argument or read from the file objectstore_conf.prop, depending on monitor configuration. See mon- itor documentation for details.</schema>

Monitors for IBM Content Management (CM8, OnDemand, Common Store)

Monitor	Permissions	Note
NetSearchExtenderDiskSpace	DB2 DB2EXT. TTEXTINDEXES	MSSQL not supported for this monitor
	MSSQL n/a	Oracle not supported for this component
	Oracle n/a	
NetSearchExtenderError	DB2 DB2EXT. TTEXTINDEXES	MSSQL not supported for this monitor
	MSSQL n/a	Oracle not supported for this component
	Oracle n/a	
ResourceManagerHeartbeat	DB2 <schema>. ICMSTRESOURCEMGR</schema>	DB2 <schema> is the schema name given in the CM Ressource Manag- er configuration in the</schema>
	MSSQL n/a	field Database Schema Name
	Oracle ICMSTRESOURCEMGR	MSSQL not supported for this monitor
ResourceManagerServices	DB2 <schema>.RMVERSION <schema>. RMCONFIGURATION MSSQL n/a</schema></schema>	DB2 <schema> is the schema name given in the CM Ressource Manag- er configuration in the field Database Schema Name</schema>
		not supported for this monitor

Monitor	Permissions	Note
	Oracle RMVERSION	
	RMCONFIGURATION	
ResourceManagerVolumeSpace	DB2 <schema>. RMVOLUMES</schema>	DB2 <schema> is the schema name given in the CM Ressource Manag- er configuration in the</schema>
	n/a	Name
	Oracle RMVOLUMES	MSSQL not supported for this monitor
ResourceManagerWebStatus	DB2 <schema>. ICMSTRESOURCEMGR <schema>. ICMSTRMACCESS- TYPES</schema></schema>	DB2 <schema> is the schema name given in the CM Ressource Manag- er configuration in the field Database Schema Name</schema>
	MSSQL n/a	MSSQL not supported for this monitor
	Oracle ICMSTRESOURCEMGR	
	ICMSTRMACCESS- TYPES	
Monitoring for IBM Content Man- ager Version 8 Eventlog	DB2 <schema>. ICMSTSYSADMEVEN- TS <schema>. ICMSTITEMEVENTS</schema></schema>	DB2 <schema> is the schema name given in the CM Library Server configura- tion in the field Database Schema Name</schema>
	MSSQL n/a	MSSQL not supported for this type of monitoring
	Oracle ICMSTSYSADMEVEN- TS	

Monitor	Permissions	Note
ICMSTITEMEVENTS		

Monitors for AddOn components

Monitor	Permissions	Note
DatacapPagesProcessed	DB2 <schema>.queue</schema>	
	<schema>.tasks</schema>	
	<schema>.qstats</schema>	
	<schema>.taskstats</schema>	
	MSSQL <schema>.queue</schema>	
	<schema>.tasks</schema>	
	<schema>.qstats</schema>	
	<schema>.taskstats</schema>	
	Oracle [<schema>.]queue</schema>	
	[<schema>.]tasks</schema>	
	[<schema>.]qstats</schema>	
	[<schema>.]taskstats</schema>	
DatacapPagesQueued	DB2 <schema>.queue</schema>	
	<schema>.tasks</schema>	
	<schema>.qstats</schema>	
	<schema>.tmbatch</schema>	
	MSSQL <schema>.queue</schema>	
	<schema>.tasks</schema>	
	<schema>.qstats</schema>	

Monitor	Permissions	Note	
	<schema>.tmbatch</schema>		
	Oracle [<schema>.]queue</schema>		
	[<schema>.]tasks</schema>		
	[<schema>.]qstats</schema>		
	[<schema>.]tmbatch</schema>	I	

Configuration scripts

Configuration for IBM FileNet Image Manager

	Permissions	Note
Configure_IS_Server	DB2 no DB access required during configuration	
	MSSQL no DB access required during configuration	
	Oracle sys.nls_database_ parameters	

Configuration for IBM Content Collector, FileNet Email Manager and Records Crawler

	Permissions	Note
	F 611113310113	NUC
Configure ICC / Email Manager or Records Crawler	DB2 EM = 4.0 (ICC 2.1x, 2.2x	DB2 <schema> is the schema name given in the Email Manager configu-</schema>
	and 3.0) <schema>.schema_ version</schema>	ration in the field Data- base Schema
	EM < 4.0 <schema>.component_ config_option</schema>	MSSQL <dbname> is the data- base name given in the Email Manager configu- ration in the field Data- base Name</dbname>
	MSSQL	Subortanio
	EM = 4.0 (ICC 2.1x, 2.2x and 3.0) <dbname>.schema_ version</dbname>	

Per	missions	Note
	EM < 4.0 <dbname>.component_ config_option</dbname>	
Ora	cle	
	EM = 4.0 (ICC 2.1x, 2.2x and 3.0) schema_version	
	EM < 4.0 component_config_ option	

Appendix I. Upgrade Explanation IBM ECM SM Server Upgrade Path Explanation

The following graphic illustrates the upgrade path scenarios supported by IBM ECM SM Server 5.2.0.

Valid Upgrade Paths IBM ECM SM 5.2.0





Valid upgrade paths from IBM FSM 4.0.1 version to IBM ECM SM Server 5.2.0

- 1 Update FSM 4.0.1 with 4.0.1 Fix Pack 7, then either upgrade through FSM 4.5.0 GA or FSM 4.5.0 Refresh GA to ECM SM 5.1.0 GA and in a final step upgrade to *IBM ECM SM Server 5.2.0*
- 2 Update FSM 4.0.1 with 4.0.1 Fix Pack 7, then directly upgrade to ECM SM 5.1.0 GA and subsequently upgrade to *IBM ECM SM Server 5.2.0*
 - **NOTE** During each of these steps, it is strongly recommended to create a backup copy of the ECM SM Server environment and database. Please consider also the *Upgrade Notes* chapter in the *ECM SM Release Notes* of the IBM ECM SM Server version you want your system to be upgraded to.
 - **IMPORTANT** In case of uncertainty about how to properly upgrade your ECM SM Server system please contact the <u>IBM Support Portal</u>.

Appendix J. Copyright notice

IBM Enterprise Content Management System Monitor (December 2016)

© Copyright CENIT AG 2000, 2016, © Copyright IBM Corp. 2005, 2016 including this documentation and all software.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of the copyright owners. The copyright owners grants you limited permission to make hard copy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the original copyright notice. No other rights under copyright are granted without prior written permission of the copyright owners. The document is not intended for production and is furnished as is without warranty of any kind. *All warranties on this document are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose*.

NOTE US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Notices

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

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 grant 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi, Kanagawa 242-8502

Japan

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, MER-CHANTABILITY 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 illustrate 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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or [™]), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/ copytrade.shtml.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

Product Number: 5724-R91

Printed in USA

GC27-4907-04

