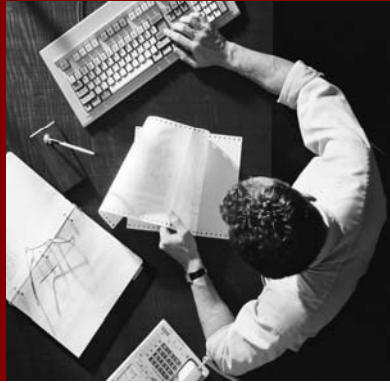


SAP NetWeaver™ 2004s



Operational Guide - SAP Content Server

Document Version 1.00 – April 2006



SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

© Copyright 2004 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.






Documentation on SAP Service Marketplace

You can find this documentation at
service.sap.com/instguidesNW04

Typographic Conventions

Type Style	Represents
<i>Example Text</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.
Example text	Cross-references to other documentation. Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example text	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Contents

1	OPERATING MANUAL FOR SAP CONTENT SERVER	1
	Introduction	1
1.1	CONTENT SERVER	1
	Purpose	1
	Implementation Considerations	2
	Constraints	2
1.1.1	Architecture of the Content Server	2
1.1.2	Preparing the Administration Host	3
1.1.3	Database Manager GUI (DBMGUI)	3
1.1.4	Log Mode	3
1.1.5	Description of the Content Server Configuration File	4
	File Structure and Parameter	4
	Storage Location	4
	Structure	5
	General Information on Parameters	5
	Parameter Description for File ContentServer.INI (Windows)	6
1.1.6	Parameter Description for File cs.conf (Unix)	9
	Parameters for the [ContentServer] Section	9
	Parameters for the [contRep-<RepositoryName>] Section	10
1.1.7	Starting and Stopping the Content Server Correctly	12
	Windows	12
	Unix	13
1.1.8	Points to Note when Manually Upgrading Content Server	13
	Upgrade Procedure	13
1.1.9	Monitoring the Database Fill Level and Content Server Operation	13
	Monitoring the Fill Level of Database Instances	13
	Procedure	14
	Monitoring the File System Fill Level	14
	Automatic Repository Fill Level Indicator in the Content Server	14
1.1.10	Monitoring the Operation of the Content Server: CCMS	14
	Purpose	14
	Features	14
1.1.11	Content Server and Firewalls	15
	Secure Operation of the Content Server	15
1.1.12	Secure URLs	15
	Relationship between Certificate, Certificate List, and PSE	16
	Switching On and Off Signature Checking	17
1.1.13	Protecting the DataStream	17
1.1.14	Protecting Against Data Loss	17
1.1.15	Content Server Access: Creating the Public Key and Private Key	18
	Use	18
	System PSE Versus Own PSE	18
	Procedure	18
	Access Protection	19
1.1.16	Backing Up a Database	20
	Backup Types	20
	Security Concepts	20
	Related Notes	20
1.1.17	Repairing a Log Volume	21
	Procedure	21
1.1.18	Point-in-Time Recovery	21
	Consistency Check	21
	Prerequisites	21
	Procedure in the Database Manager	22
1.1.19	Content Server Administration	22
	Features	22
	Choosing a Server	23

1.1.20	<i>Functions</i>	24
	Overview Information.....	24
	Details.....	26
	Settings.....	27
	Statistics.....	28
	Creating New Content Repositories.....	28
1.1.21	<i>Content Server Monitoring</i>	29
1.2	CACHE SERVERS.....	34
	Caching.....	34
	Purpose.....	34
	Implementation Considerations.....	35
1.2.1	<i>Architecture of the Cache Server</i>	35
1.2.2	<i>Cache Server Administration</i>	36
	Features.....	37
1.2.3	<i>Functions</i>	37
	Overview Information.....	37
	Settings.....	37
	Access Statistics.....	38
	Changing the Password for Database Access.....	39
1.2.4	<i>Monitoring for Cache Server</i>	39
1.2.5	<i>Secure Operation of the Cache Server</i>	41
	Backup Strategy for the Cache Server.....	41
1.2.6	<i>Cache Preload</i>	41
1.2.7	<i>Multi-Layer Caching and Content Server Aliases</i>	42
	Using Content Server Aliases.....	42
	Using Multi-Layer Caching.....	43
	Incorporating a Content Server Alias.....	44
	Determining the Alias.....	45
	Constraints.....	45
	Related Notes.....	46
1.2.8	<i>Using the Cache Server with Third-Party Content Servers</i>	46
	Related Notes.....	47
1.3	SPECIAL PROCEDURES.....	47
1.3.1	<i>Relocating the SAP Content Server</i>	47
	Procedure.....	47
	Relocating a Repository.....	48
	Relocating Using the Database.....	48
	Relocating Using Export and Import.....	49
1.3.2	<i>Incorporating a Patch</i>	49
	Use.....	49
	Navigation.....	49
1.3.3	<i>Setting Up Client-Specific Repositories</i>	51
	Purpose.....	51
	Features.....	51
	Using Several Database Instances.....	53
	Changing the Password for Database Access.....	54
1.3.4	<i>Troubleshooting</i>	55
	Problem: Multiple Entries for Object SCMS in Application Log Manifestation.....	55
	Problem: Errors in Document Access.....	55
	Problem: Content Server is Rejecting Large Files.....	56
	Problem: SAP Content Server Comes to a Standstill.....	57
	Notes Relating to SAP Content Server (Selection).....	58

1 Operating Manual for SAP Content Server

Introduction

This operating manual for SAP Content Server is mainly aimed at system administrators who have already installed SAP Content Server. Other documentation covers preparatory aspects such as content server planning and sizing, and the installation process itself.

The structure of this manual reflects the administrative procedure itself. The following topics are dealt with, in this order:

[Content Server Architecture](#) ,
[Preparing the Administration Host](#),
[Starting and Stopping the Content Server](#),
[Monitoring Fill Level and Operation](#),
[Secure Operation of SAP Content Server](#).

Procedures that do not come under the basic functions, and once-off adjustments, such as setting up client-specific repositories and content server aliases, are dealt with in the section

[Special Procedures](#)

The section [Troubleshooting](#) and a selection of SAP Notes provide assistance on dealing with unforeseen occurrences and problems on the content server.

1.1 Content Server Overview

Purpose

The SAP Content Server is based on the database system MaxDB and as of Release 4.6 is available on Windows 2003 Server for SUN Solaris, Hewlett Packard HP-UX, HP-IA, IBM AIX, SUSE Linux, and RedHat Linux (Linux Intel, Linux PPC, Linux x86_64, Linux PPC). The precise release names are defined in the Platform Availability

Matrix (PAM).

Therefore, besides the SAP DB, an independent content server is always available in every SAP system installation. Thus, the SAP system provides the necessary technical infrastructure for all document-centric applications and business scenarios that do not require a long-term archiving solution. Since the SAP Content Server is also integrated via the HTTP interface (see SAP HTTP Content Server 4.5 Interface), the actual storage medium used remains completely transparent to SAP applications.



Documentation on the database system and database tools can be found in the SAP Library.

Applications that use the technical infrastructure of the SAP Content Server include the SAP Business Workplace, SAP ArchiveLink, the Document Management System (DMS), and the Knowledge Warehouse.

Implementation Considerations

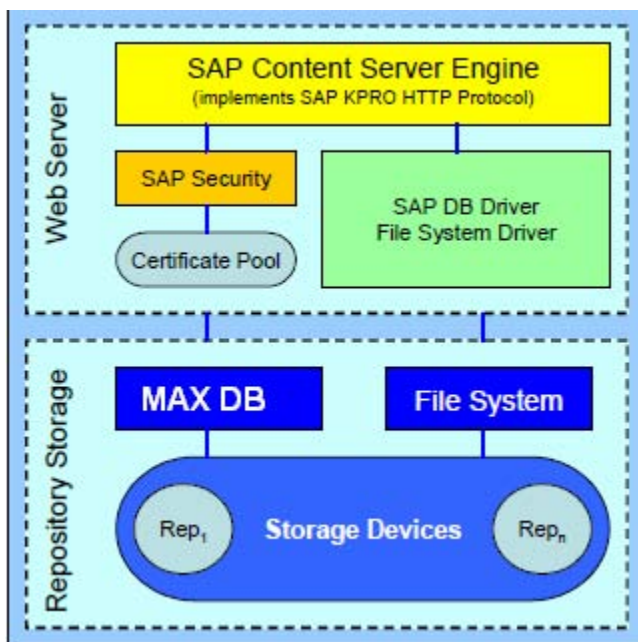
To find out how to install SAP Content Server see the *Installation Guide for SAP Content Server*, which you can find on the Service Marketplace under the quick link /instguides → *Installation and Upgrade Guides* → *SAP Components* → *SAP Content Server*.

Constraints

The SAP Content Server is **not** intended to replace optical storage systems and other storage media for long-term document archiving.

1.1.1 Architecture of the Content Server

The SAP Content Server consists of the following components:



The basis of the SAP Content Server is the *content server engine*. The engine is either implemented as an ISAPI extension on the Microsoft Internet Information Server or as a server module for the Apache Web Server.

The engine receives all URLs, checks their validity, and triggers the processing of requests. The SAP Content Server saves data either in the Database Instance or in the file system. However, the content server engine does not communicate directly with the storage medium. It uses special adapters known as storage drivers. Storage drivers hide the specific access mechanisms of the storage medium behind a consistent, byte stream-oriented interface. This makes it possible to support several storage mediums using only one server engine.

1.1.2 Preparing the Administration Host

You need a SAPGUI on your administration host. Once you have this, you can use the Computing Center Management System (CCMS) to monitor, control, and configure your SAP system. Specifically, you need the SAPGUI to perform administration and Customizing tasks for the SAP Content Server. All versions of the SAPGUI (SAPGUI for Windows, SAPGUI for JAVA, and SAPGUI for HTML) can be used.

1.1.3 Database Manager GUI (DBMGUI)

With one Database Manager GUI any number of content server databases can be managed on several database servers, as the database manager GUI communicates via the network connection to the database servers. Unlike content server administration where HTTP issued, a proprietary, TCP/IP-based protocol is used for communication between the database manager GUI and the database instance.

Calling the Database Manager GUI

1.1.4 Log Mode

By setting the Log Mode you can decide how the log entries are backed up:

- Simply (in older versions SINGLE)
- Mirrored (in older versions DUAL)

For security reasons, we recommend that you always mirror the Log Area .This is either done with a hardware-based mirroring or using database software.

If your system provides hardware-based mirroring (RAID-1 systems), we recommend that you use this.

Mirrored Log Areas

The advantage of this configuration is that the system can continue operating even if one log area is temporarily out of action, and this log area can be reincorporated into the system while the system is running.

Simple Log Area

If you are using hardware-based RAID-5 or RAID-1 systems, you can use a simple log area, as these systems provide adequate operating backups for productive operation. Accesses to the log volume greatly influence the performance of the system as a whole. Therefore, watch out for a high data throughput when choosing a RAID system.

Only one log area is configured in this case. The log area should be backed up regularly.



If a disk error occurs, the content of the Log volume is lost and the data volume is therefore no longer consistent with the transaction.

The database can be more or less fully restored by means of a complete Data Backup and, possibly, other Log Backups. Exceptions to this are any log entries that has not yet been backed up, and any open transactions.

See also:

Concepts, Logging

1.1.5 Description of the Content Server Configuration File File Structure and Parameter

As well as parameters that affect the general behavior of the server, the configuration file contains all the communication parameters necessary for each repository. Usually, the content server keeps the file up to date automatically; in other words, manual editing is not required. The transaction CSADMIN is used for maintaining and administrating the content server.

The ContentServer.INI file is vital for the smooth operation of the whole SAP Content Server. In particular, you must ensure that besides the regular [Data Backups](#) the latest version of this file (as appropriate for the repository backup) is also always backed up (in line with the [Database Backup](#)). This is because without an up-to-date record of the repository, the content server cannot access a restored database.

Depending on the operating system the configuration file is called ContentServer.INI (Windows operating systems) or cs.conf (Unix). Depending on the server variant different parameters or different parameter values are used. For this reason the parameters for the two files are described separately.

Storage Location

The ContentServer.INI file must be stored in the content server installation directory. The storage location of file cs.conf is specified in the Web server configuration table

CSConfigPath in the Web server configuration profile. When the content server is installed this value is set to <ServerRoot>/conf/cs.conf.

Structure

The ContentServer.INI file is subdivided into a number of sections. Each of these sections contains parameter-value pairs that are valid within that section. The first section is an exception, however. All entries in this section represent default values for subsequent sections. You can change these defaults in each individual section.

The sections are as follows:

```
[ContentServer]
```

The [ContentServer] section contains all generally valid parameters that influence the runtime of the server.

```
[contRep-<RepositoryName>]
```

The section defines a content repository. This means that it contains all the parameters that describe access to the database repository. If the corresponding section does not exist, any repository defined in the database will be inaccessible. A [contRep-<RepositoryName>] section must be created for every repository that you want to be accessible from the SAP system.

All repository parameters can also be defined as global default settings in section

[ContentServer]. They are then valid the same for all repositories, they can however be redefined for each repository if required.

General Information on Parameters

- One parameter-value pair is allowed per line.
- Every parameter-value pair must contain the assignment sign '='.
- Parameter-value pairs are case-sensitive.



If you want a particular parameter to be ignored, insert a semicolon ';' at the beginning of the line.

- Parameters are only valid within their own sections.
- If a number of parameters with the same name but different values exist, the last one is used.

Parameter Description for File ContentServer.INI (Windows)

Parameters for the [ContentServer] Section

Name: `LogRequests`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: log of all client requests in file `cs_trace.txt`.

Name: `ResponseTrace`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: log of all client responses in file `cs_trace.txt`.

Name: `Log404Response`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: log of all NOT FOUND requests in file `cs_trace.txt`.

Name: `FullTrace`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: log of all request/response pairs in their full length in file `cs_trace.txt`.

This switch should only be used for diagnostic purposes and only in connection with controlled server requests. Do not activate this switch in the productive system.

Name: `KeepConnection`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: `KeepConnection=0` ends the client connection after the response has been transferred. `KeepConnection=1` keeps the connection open, thus allowing the client to send more requests on this connection. This second option enhances performance, as it saves on the resources required to establish a new connection.

Name: `MaxTransferBlockSize`

Type: Integer

Default setting: 65535

Values: 1..4294967296

Mandatory: no

Description: **MaxTransferBlockSize** determines the block length of the IIS responses.

Zero-byte responses can occur in very busy systems. This is because no send buffer can be allocated on the server. In such cases, we recommend that you reduce the block size (for example, to a minimum of 4096 bytes). The size is specified in bytes.

`maxTransferBlockSize` is effective from Server Build 161)

See also:

Note 328209

Parameters for the `[contRep-<RepositoryName>]` Section

Name: `Storage`

Type: Character

Default setting: `ContentStorage.DLL`

Values: `ContentStorage.DLL`

Mandatory: yes

Description: the **Storage** parameter contains the name of the storage layer required for accessing a repository.

Name: `ContentStorageHost`

Type: Character

Default setting: `localhost`

Values: qualified host name, IP address, local host

Mandatory: yes, if "Storage" is set to `ContentStorage.DLL`.

Description: the **ContentStorageHost** determines the host on which the database containing the repository is located.



The database cannot be run on any machine other than the content server machine.

Name: `ContentStorageName`

Type: Character

Default setting: `SDB`

Values: `SDB`



You need to change the default value `SDB` if a different name was used for the Database Instance when the content server was installed.

Mandatory: yes, if "Storage" is set to `ContentStorage.DLL`.

Description: the parameter **ContentStorageName** contains the name of the database instance.

Name: ContRepRoot

Type: Text

Values: each valid system path

Mandatory: yes, if "storage" is set to FileSystemStorage.dll.

Description: **ContRepRoot** specifies the root directory for this repository. A full, absolute path name to a directory that exists (or is mounted) must be specified. This directory must have sufficient authorizations to create subdirectories for the user ID, who started the content server.

Name: ContRepDescription

Type: Character

Default setting: ""

Values: free text


Mandatory: yes

Description: **ContRepDescription** contains a free text line that explains what the repository is used for.

Name: Security

Type: Boolean

Default setting: 0

 Signature checking should always be switched on in a productive system. This is because signature checking is the only method of preventing unauthorized access to documents.

However, it may be necessary to temporarily switch off signature checking if you are analyzing problems or carrying out an installation.

Values: 0, 1

Mandatory: yes

Description: switches signature checking on and off.

If there are inconsistencies between the content server and the SAP system, documents cannot be accessed. In this case, you should remove all certificates from the content server and in R/3 Customizing. The transactions involved are **CSADMIN** and **OAC0**.

Name: DefaultDocProt

Type: Character

Default setting: ""

Values: {r c u d} r - Read, c - Create, u - Update, d - Delete

Mandatory: no

Description: **DefaultDocProt** determines document access protection for this repository. The default value for the security level can be overwritten when this document is stored. As the default value is usually used, however, this parameter is relatively unimportant. This parameter mainly influences whether or not a signature is required for creating a document.

Name: `sqltrace`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: if **sqltrace==true**, an SQL trace is written to the directory `c:\winntsystem32`. This trace should be activated for diagnostic purposes only, and is switched off in a productive system.

Name: `driver`

Type: Character

Default setting: LiveCache

Values: ODBC driver name

Mandatory: no

Description: **driver** contains the ODBC driver names required for DB access. The suitable ODBC driver has to be registered under the driver name in the ODBC service layer. Only the ODBC drivers of the database instance are available for productive operation.

1.1.6 Parameter Description for File `cs.conf` (Unix)

Parameters for the `[ContentServer]` Section

Name: `AdminSecurity`

Type: Boolean

Default setting: 0

Values: 0, 1

Mandatory: no

Description: switches administrative authentication on and off. If `AdminSecurity` is activated, the server for security-relevant administration URLs sends return code "401 (authorization required)" back to the client. Only when a valid user and password for an administration request is sent by the client, does the content server process this command.

Name: `AdminSecurityGroup`

Type: Text

Default setting: none

Mandatory: yes, if "AdminSecurity" is set to 1.

Description: The content server checks whether the operating system user specified in the request is a member of the user group specified in **AdminSecurityGroup**. When the content server is installed this group is interrogated and assigned the default value "sapsys".

Name: `AuthService`

Type: Text

Default setting: local

Values: NIS, Local

Mandatory: no

Description: **AuthService** specifies the password or group file against which the transferred user is to be checked. If **AuthService** is not specified the check is always made against `/etc/passwd`. If `AuthService=NIS` is set, the check is made against the "Network Information System (NIS)". The check against `/etc/passwd` can also be set explicitly by using `AuthService=Local`.

Name: `TraceLevel`

Type: Text

Default setting: error

Values: emergency, alert, critical, error, warning, notice, info, debug

Mandatory: no

Description: **TraceLevel** specifies, how detailed the actions in content server are to be recorded. The lower the trace level, the quicker the server log file grows. Trace level debug is only relevant for maintenance and diagnosis. Generally the content server cannot issue messages that exceed the trace level set for the Web server. So, if the trace level of the Web server is set to Warning and the trace level of the content server to debug, no messages of type notice, info or debug will be issued. If you change the trace level of the Web server, you must restart it.

Name: `TraceOverride`

Type: Boolean

Values: 0

Mandatory: no

Description: You can use this parameter to override the trace level of the Web server for diagnostic purposes. All content server actions are logged with at least the trace level of the Web server. This parameter is intended for diagnostic and support purposes, as it enables the debug trace to be activated without having to restart the server.

Parameters for the [contRep-<RepositoryName>] Section

Name: `StorageDriver`

Type: Text

Values: SAPDBStorage, FSStorage

Mandatory: yes

Description: **StorageDriver** specifies the storage medium the repository is created on.

Name: `Storage`

Type: Text

Values: ContentStorage.dll, FileSystemStorage.dll

Mandatory: yes, but deprecated

Description: Parameter **Storage** is included for compatibility reasons and at present it has the same meaning as the parameter **StorageDriver**.

Name: `ContRepRoot`

Type: Text

Values: each valid system path

Mandatory: yes, if "StorageDriver" is set to FSStorage.

Description: **ContRepRoot** specifies the root directory for this repository. A full, absolute path name to a directory that exists (rsp. is mounted) must be specified. This directory must have sufficient authorizations to create subdirectories for the user ID, who started the content server.

Name: ContentStorageName

Type: Text

Values: each valid SAPDB instance name

Mandatory: yes, if "StorageDriver" is set to SAPDBStorage.

Description: **ContentStorageName** is the name of the SAPDB instance, in which the current repository is stored.

Name: ContentStorageHost

Type: Text

Values: each valid host name, IP address

Mandatory: yes, if "StorageDriver" is set to SAPDBStorage.

Description: **ContentStorageHost** is the name of the host, on which the SAPDB instance is running.

Name: SQLTrace

Type: Boolean

Mandatory: no

Description: If **SQLTrace** is activated, all database operations are recorded. The resulting log is used by SAP for support and diagnosis purposes. In normal operation this trace should always be deactivated, since the resulting traces become very large and affect the performance of the server.

Name: ContRepDescription

Type: Text

Mandatory: no

Description: Free text description of the repository logged in transaction CSADMIN.

Name: UncompressedMimes

Type: Text

Values: all

Mandatory: no

Description: This parameter deactivates the compression for all new objects you want to create.

Name: *Security*

Type: Boolean

Default setting: 0

Mandatory: no

Description: **Security** activates and deactivates the signature check for URLs directed to this repository. To check signatures an appropriate certificate must have already been sent to the content server and activated

Name: *DefaultDocProt*

Type: Text

Values: c, r, u, d

Mandatory: no

Description: Specifies the security level for checking signatures of documents.

1.1.7 Starting and Stopping the Content Server Correctly

Windows

If you want or have to stop the content server, you should do this in the correct way, to ensure that all content server transactions are terminated correctly. You can reboot the operating system.

You can also use the following commands to stop and re-start the content server (all commands are entered in a DOS window):

- **net stop w3svc**: ends the Web service This command stops all websites that are set up on your server.
- **net start w3svc**: re-activates all websites on your system.



Note that the Microsoft Internet Information Server (IIS) is a multi-function server. This means that it provides multiple Internet services in one process (http, mail, ftp, telnet).

Stopping the w3svc service does not stop the other services.

The Microsoft IIS appears as the process *inetinfo* in the task manager process list. This process cannot be terminated using the task manager.



Stopping the Web server does not terminate the database process.

Unix

The Apache Web server is started and stopped using shell script **apachectl**. The respective calls are **apachectl stop** and **apachectl start**.

If the content server cannot be stopped with this call, you have to terminate all httpd processes manually using the operating system command **kill**. First try using **kill** without any further signals, so that the content server can send logged- on shared memory segments and semaphores back to the operating system. Only if this does not work, should you use **kill -9** to terminate the processes. Afterwards you have to release the shared memory segments and semaphores using the commands **ipcs** and **ipcrm**.

1.1.8 Points to Note when Manually Upgrading Content Server

The content server is an ISAPI extension and is implemented as a dynamic link library (DLL). When the content server is accessed for the first time, the Microsoft IIS loads the content server DLL into main memory and locks write access to the DLL on the hard disk. This lock is removed only once the DLL is removed from main memory. The **net stop w3svc** command does not terminate the *inetinfo* process. Therefore, this command alone does not update the content server programs. You can use the command **kill.exe** to terminate process *inetinfo*.

You have to use the Microsoft Resource Kit to install the command **kill**.

Upgrade Procedure

1. Stop the content server using the command **net stop w3svc**.
2. Enter the command **kill inetinfo**.
3. Complete the upgrade.
4. To restart the content server, enter **net start w3svc**.

The Database Manager can start and stop the Database Instance.

1.1.9 Monitoring the Database Fill Level and Content Server Operation

Monitoring the Fill Level of Database Instances

You need to monitor the Data Area and the Log Area in order to prevent a possible database crash.

Once the data or the log area is 100% full, the Database Instance can no longer accept any more Transactions. Although this is a valid operating status, the content server cannot process any more requests and it therefore appears "frozen".

Therefore, to enable the database instance to continue to accept transactions, either the data area has to be increased, or the log area has to be backed up.

In particular, regularly backing up the log area is an absolute requirement for smooth database operation. Therefore we recommend you activate the Automatic Log Backup.

Procedure

Use the following functions in the database manager GUI:

- Display Data Area Information
- Display Log Area Information
- Activating and Deactivating Automatic Log Backup
- Creating Volumes

Monitoring the File System Fill Level

The fill level of the file system where the repositories are has to be monitored from the operating system.

Automatic Repository Fill Level Indicator in the Content Server

If the fill level of the storage medium (database or file system) reaches 70%, the fill level percentage is displayed instead of the operation status running in transaction CSADMIN.

1.1.10 Monitoring the Operation of the Content Server: CCMS

Purpose

You can use the Computing Center Management System (CCMS) to monitor, control, and configure your SAP system. The CCMS tools allow you to analyze and distribute the load on the clients in your system, and can display the resource usage of the system components. The transactions in question are SCMSMO and CSMONITOR (both open the same view).

Features

The CCMS provides a range of monitors and administration functions for the following:

- Starting and Stopping SAP Systems and Instances
- Non-supervised system administration using Instances and Operating Types
- System Monitoring and automatic notification of alerts
- Dynamic user distribution
- SAP system configuration: profiles
- Processing and Managing Background Jobs, Scheduling Database Backups

See also:

[Content Server Monitoring](#)

1.1.11 Content Server and Firewalls

If you want to access a content server via a firewall, you can install an IP filter on the firewall. The IP filter forwards the requests unchanged to the content server. From the point of view of the SAP system, the filter functions as a content server alias. It therefore needs to be made known to the Customizing of the SAP system.

See also:

[Multi-Layer Caching and Content Server Aliases](#)

Secure Operation of the Content Server

Inevitably, using a content server poses a certain element of risk for stored document content and the availability of functions. Besides data loss due to hardware failure, these risks are:

- URLs may be forged, thus allowing the forger unauthorized access to data.
- The data stream may be “tapped” or forged.
- Unauthorized persons may perform administrative tasks with malicious intent.

The following security mechanisms counteract these risks:

- Secure URLs
- Encoding Data Transfer
- Security Mechanisms Against Data Loss
- Access Protection for Administration

1.1.12 Secure URLs

To prevent unauthorized access to stored content on the SAP Content Server, the SAP system carries out an authorization check. However, access to the SAP Content Server is gained via the open SAP Content Server interface. Therefore, URLs must be secure so that they allow only authorized access to stored content and, correspondingly, so that forged requests are rejected.

To make a URL secure, it is given a characteristic (like a watermark on a banknote) which allows the receiver to detect whether or not the URL has been tampered with (like if the watermark is missing from a banknote).

In the case of a Content Server URL, the characteristic in question is the signature. The signature is an encoded copy of the URL itself and is transferred to the content server as part of the URL.

Most notably, the signed URL contains the additional parameters *expiration time* and *digital signature*. A signed URL is only valid if the expiration time has not been exceeded and if it contains a valid signature.

The content server decodes the signature and compares it with the URL it received. The content server only executes the request if the URL and the signature match. If an intruder changes the plaintext in the URL, the signature will not match the URL. The content server will accordingly reject the request.

The signature is based on the RSA procedure and MD5 hashing.

The RSA procedure is also known as the public key procedure. This procedure is based on a private key and a public key. You need the private key to create the signature, while you need the public key to check the validity of the signature. For a description of the technical details of this procedure, see the documentation *Secure Store & Forward / Digital Signatures* (BC-SEC-SSF).

As the main partner in the three-way relationship of client → SAP system → content server, the SAP system is the only partner that may send request URLs to the client. Because of this, the SAP system has to create the URL signature using a private key.

The public key (Certificate) of the SAP system must be stored on the content server, and the relevant repository must have access to it (see also Content Repositories).

Transactions **OAHT**, **OACO** (from release 4.6C) and **CSADMIN** (from release 4.6C for SAP Content Server, see also Content Server and Cache Server Administration) are used to transfer the certificate. The certificate has to be activated on the content server for the repository in question. This is done using transaction **CSADMIN** (for SAP Content Server).

Relationship between Certificate, Certificate List, and PSE

Certificate

A certificate is an ASCII-encoded exchange format for public keys, in accordance with ISO standard X.509.

Besides the public key, a certificate also contains other information such as the issuer and the validity period.



The terms “certificate” and “private key” are often used synonymously in everyday use. In particular, the term “certificate generation” is used incorrectly in the SAP system, because in reality a pair, consisting of a private key and a public key, is generated.

Certificate List

A Content Server and the repositories it contains can be used by multiple SAP systems.

Therefore, the Content Server has to be able to store certificates of varying origins for every repository. To facilitate this, the Content Server creates a certificate list for every repository.

Public Key Security Environment (PSE)

A PSE is a binary representation of a certificate list. Before a public key can be used by the Content Server security module, it has to be converted from the ASCII format of the certificate to a binary format. This conversion is known as “certificate activation” (see also transaction CSADMIN). The signatures of activated certificates only are checked.

If a public key belonging to the same issuer was available before the certificate was activated, the old public key is overwritten.

When the certificate is deactivated, the public key is deleted from the PSE, but the certificate is not deleted from the certificate list.

Switching On and Off Signature Checking

Signature checking has to be switched on and off for every repository. To do this, use the parameter “Security” in the [ContentServer.ini](#) or [cs.conf](#) file.

Once signature checking has been switched on, active certificates have to be available for every SAP System that sends URLs!



The Customizing transaction OAC0 is used to activate URL signatures. If signature checking is not switched on the Content Server, any signatures sent with the URL may be ignored.



Every SAP system must have its own unique certificate, so that the SAP system’s digital signature can be used properly.

In particular, when copying an SAP system, you have to make sure that the copy also has its own certificate.



Signed URLs can slow down performance, as it takes increased processing power to create the signature.

See the section [Creating a System-Specific Certificate for Content Server Access](#).

1.1.13 Protecting the DataStream

Data transfer itself must be encoded, so that a potential intruder cannot access the data while it is in transit between client and server. Standard procedures exist for this, such as secure HTTP (HTTPS). This type of encoding is usually implemented between the client and the HTTP server and is not part of the SAP HTTP Content Server interface.



Signed URLs can slow down performance, as it takes increased processing power to create the signature.

1.1.14 Protecting Against Data Loss

The SAP Content Server is based on the SAP DB. To avoid data loss, take the usual measures against data loss in databases. These measures could include the following:

- Redundant hardware

Mirror disks, RAID systems, and so on

- Regular standard security measures

Log area, data area



Note that when you make backups, to ensure a full backup, the file **ContentServer.ini**, and the directory **Security** must also be backed up, in addition to the Data Backup and the Log Backup.

See also note 319332 (Content Server Backup Strategies).

1.1.15 Content Server Access: Creating the Public Key and Private Key

Use

To ensure that every SAP system has its own certificate, a Personal Security Environment (PSE) (see also Personal Security Environment) must be created on every SAP system directly after the system is installed. This only needs to be done once for every system. The PSE is set up in the Trust Manager (transaction **STRUST**; see also the SAP Library under *mySAP Technology Components* → *SAP Web Application Server* → *Security* → Trust Manager).

System PSE Versus Own PSE

By default, this system PSE is used to sign URLs. From SAP Web Application Server release 6.10, you can also generate your own PSE to sign and verify KPro URLs.

You *must* create your own PSE, if you are using a security product other than SAPSECULIB.

You *should* create your own PSE, if you let your Web AS function as a content server for other SAP systems. Your own PSE prevents certificates belonging to the other SAP systems from being stored in the system PSE. They should not be stored there, since there they cannot be deleted in transaction **CSADMIN**.

You *could* create your own PSE if for example you want to use the system PSE for administration purposes, and not for signing and verifying KPro URLs.



Carry out the procedure for creating a PSE, described below, before you create repositories.

If you have already distributed certificates, you have to send any new certificates to all the repositories in question, and activate the certificates, after you have generated your own PSE.


If you do this after you create repositories, you will have to re-send the certificates to all HTTP repositories and reactivate all the certificates. This is because the certificate changes when you create a new PSE.



Note that PSEs are valid as soon as they are created. That is, signatures are created with the new private key immediately. The content server rejects these URLs until the certificate are updated.

Procedure

Take the following steps to create your own PSE:

1. In client 000 call transaction **SSFA**.
2. Choose *New Entries*.
3. Use F4 Help to select *HTTP Content Server* and confirm this by choosing *Enter*.
4. Additional fields for application-specific Secure Store & Forward (SSF) parameters and standard values for empty fields are grayed out.
5. Make the following entries:
 - a. In the field *Security/Product*, enter **SAPSECULIB**.
 - b. In the field *SSF Format*, choose **International standard PKCS#7**.
 - c. In the field *Priv. add. book*, enter **SAPHTTPCS.pse**.
 - d. In the field *SSF profile*, also enter **SAPHTTPCS.pse**.
 - e. Check *Distribute PSE (Only SAPSECULIB)*.
6. Save your entries.
7. Call transaction **STRUST**.
8. In the PSE status frame (Window on screen left) select the entry *HTTP Content Server*.
9. (The red font means that there is no PSE in the database.)
10. Choose *Create* from the context menu.
11. In the next dialog box, *Create PSE*, correct or complete the entry and confirm with .

Access Protection

Administration for the SAP Content Server is carried out partly inside the SAP system (see Content Server and Cache Server Administration), and partly outside (see reference Manual: SAPDB 7.2 and 7.3). Note the following security considerations in relation to administration on the content server:

- Make sure that only authorized persons have (administrative) access to the computer on which the SAP Content Server is running.
- Make sure that (administrative) access to the database is appropriately restricted. To ensure that only authorized persons have administrative access to the SAP Content Server from the SAP system, you need to set the parameter **AdminSecurity** on the SAP Content Server to **1: AdminSecurity=1**. For more information, see the section [Content Server Administration](#) and the installation documentation *SAP Content Server Installation Guide*.

1.1.16 Backing Up a Database



For general information about the database system see Database System Concepts

Backup Types

There are two types of backup – Data Backups and Log Backups.

Security Concepts

- Backup strategy for the content server database with SAP content only:



Because in this case the content is not changed, we recommend that you make a full data backup of the content server database (save date) after installation.

- Backup strategy for a content server database with customer content: The backup strategy depends on the size of the content server database and on the volume of changes per day and week.



We recommend that you make a full data backup of the content server database once a week. If a large volume of content is changed or added in the course of a full data backup, rebuilding the log entries may take longer in any recoveries carried out later. Therefore, it may be sensible to make incremental data backups on some days or even daily.

The Log Area should be backed up using the automatic log backup in Version Files.

Backup generations (data and log backups) should remain available for at least four weeks. The fifth full backup is then sufficient to overwrite the first full backup. This means you can recover a data backup that is four weeks old.

- Backup Strategy for the Cache Server

The cache server gets its data from the connected content servers. The cache server runs in the Overwrite Mode for the Log Area (in older versions the log mode DEMO), that is, the log area is not saved. In overwrite mode the restart function following a database failure and intact Volumes are kept.

After installing the Cache Server, but before using it in a productive system, make a full data backup, and a copy of the file **cacheserver.ini**. In the case of a recovery, you can then use this full backup to restore the initial status of the Cache Server.

If there is a **volume failure**, you have to first make sure that an error-free disk periphery is available. Then proceed as described in Restoring Data.

Related Notes

350067 Administration Content Server/SAP DB

351647 Cache Server Administrations

354819 Composite note SAPSECULIB

361123 SAP Content Server and Security

1.1.17 Repairing a Log Volume

The content server database with customer-defined data runs with a mirrored Log Area, either by mirroring the hard disks (e.g. RAID1), or by using the Log Mode. If you choose to use the log mode, a defective log volume can be repaired as follows:

Procedure

Recovering a Mirrored Log Volume

If you restore a log volume, the log volume is only re-initialized. The data is not copied from the old volume to the new. Data is then written sequentially to both log volumes.

Only once the volume originally marked as BAD is full are the contents of both volumes again identical and both volumes can be read.

The defective volume remains marked as BAD during this whole reintegration phase.

1.1.18 Point-in-Time Recovery

The content server database supports point-in-time recovery. The time up to which log entries are to be processed is already determined in the Database Manager at the start of the Recovery. When setting up a point-in-time recovery for the database instance and the content server database, you should choose a point in time for the content server that is shortly after the point in time for the database.

After the recovery, there may be some documents in the content server that cannot be accessed from the SAP system, if documents were deleted after the point in time selected for the recovery.

However, all documents known to the SAP system are available in the content server database.

Therefore, the content server is consistent from the point of view of the SAP system.

Consistency Check

The content server database has a function for checking the consistency of the data. Check the consistency of the data before backup generations are overwritten. We recommend that you do this every four weeks.

Prerequisites

The database instance has the Operating Status ONLINE or ADMIN.

Procedure in the Database Manager

1. Database Manager GUI: Checking Database Structures Database Manager CLI: Use command:

```
dbmcli -u <dbm_user>,<password> -d <database_name> -uUTL
<dbm_user>,<password> util_execute verify
```

2. The information returned by the database kernel is written to the file Database Errors. Check the database files, for example, whether they can be read in the database manager GUI Reading Database Files.

1.1.19 Content Server Administration

This SAP Content Server can be administrated directly from the SAP system. There are special tools available for monitoring and administrating the underlying database system (for example, Database Manager GUI, Database Manager CLI).



Use transaction **CSADMIN** to go to the Content Server and Cache Server Administration screen.

Access restrictions or permissions for the *ini* file of the Content Server can be set during the installation routine (see installation instructions in *SAP Content Server Installation Guide* on the *SAP Server Components2* CD).

To activate access restriction, the variable **AdminSecurity=1** has to be set in the INI file. In this case, a password is requested when the user branches to the Content Server Administration screen, as well as in individual areas of the *CSADMIN* transaction.

You do not have to repeat the password until you launch Content Server Administration again.

Features

You can display the following information in the Administration screen:

- General information on the Content Server and Cache Server
- Detailed information on the individual content repositories and cache servers
- Certificates of the individual content repositories
- Settings of the individual content repositories
- Content server and cache server statistics
- Create individual content repositories

The *Create* tab is only visible if you are in change mode.

As of Release 4.6C, you can also go to the Customizing from every screen concerned with a particular content repository. If you do this from change mode, the current values (HTTP server, port number, HTTP script, version number, and description) are copied automatically.

To display this information and use these functions, you must first select a content server.

Choosing a Server

Use

In the Content Server Administration screens, you select a content server in order to obtain information on this content server or the associated content repositories, and to use the Content Server Administration functions. You can also call up information on a cache server.



You can go to the screen for administrating a different server in Content Server Administration by choosing the icon.

Prerequisites

- Content Server Administration is open.
- or:
- Go to Content Server Administration using transaction **CSADMIN**.

Procedure

1. Choose a content server or a cache server.
 - The first time you call up Content Server Administration, the content server selection screen is displayed automatically.
 - If you are already in Content Server Administration, you can choose a server by choosing .
2. The following options are available for calling up the administration functions for a content server:
 - On the *Repository* tab, enter the name of the content repository that you defined in the Maintain Content Repositories screen.
Choose F4 to display a list of options.
 - Alternatively, make the appropriate entries in the *HTTP Server*, *Port number*, *HTTP script*, and *Versions no.* fields on the *Server* tab.
Choose F4 to display a list of options.

If you do not make an entry in the field *HTTP script*, the default setting **ContentServer/ContentServer.dll** is used.
3. Choose *Enter* to confirm your entries.

Result

The details of the HTTP server, port number, HTTP script, and version appear in the header of the Content Server Administration screen.

1.1.20 Functions

The Content Server administration screen contains the following tab pages with the various functions:

[Overview](#)

[Details](#)

[Settings](#)

[Statistics](#)

[Create](#)

Overview Information

Use

The *Overview* tab contains general information on your content server or cache server.

Prerequisites

The Content Server Administration screen is open.

Features

- The *Overview* tab page contains the following information:
- Information on the content server or cache server itself
 - Status
Possible statuses: *running, defined, stopped, error*
 - Status description
Explanation of the status
 - Manufacturer
Manufacturer of the content server or cache server
 - Version
Version of content server or cache server
 - Build
Build of storage system
 - pVersion
Version of the SAP HTTP Content Server interface
 - Server date
Current date
 - Server time
Current time on content server or cache server
 - Start date
Date on which the content server or cache server was started
 - Start time
Time at which the content server or cache server was started







All times are specified in UTC.

- Information on the content repositories of the content server
 - Repository name
 - Customizing

Information on whether the repository is known to the SAP system in the Customizing and whether the Customizing is consistent. Here, the system checks whether the HTTP server, port number, HTTP script, and version number match and whether the data entered manually or using F4 Help matches the Customizing data.

The following options are available:

Icon	Description	Explanation
	Customizing ok	Customizing is consistent
	Customizing partially ok	There are minor differences between the data in the Administration screen and Customizing, such as upper-case and lower-case letters.
	Customizing missing	No Customizing settings have been maintained for the repository
	Customizing differences	The data in the Administration screen differs from the Customizing data.

The Customizing information is shown on all the screens that refer to repositories.

- Description
Description of the content repository
- Status
Possible statuses: *running, defined, stopped, error*
- Status description
- pVersion
Version of the SAP HTTP Content Server interface
- Further content server-specific settings

In addition to the information described here, other content server-specific values can be output. Double-click on a Content Repository to see detailed information.

Activities

You can update the information on the respective server by clicking the *Refresh* icon.

Details

Use


The *Details* tab contains detailed information on the content repositories of the content server.

Prerequisites

The Content Server Administration screen is open.

Features

The following functions are available:

- You can switch to the detailed information screen of a different content repository.
- You can go to the Customizing (transaction OAC0) of every repository simply by choosing .

If you are currently in change mode, the change mode of **OAC0** opens. Similarly, if you are currently in display mode, the display mode of OAC0 opens.

- You can refresh the detailed information screen.
- In change mode, you can do the following:
 - ✓ Change the description of the content repository.
 - ✓ Go directly to the maintenance screen for the Customizing settings for a repository.

The current values for HTTP server - port number, HTTP script, version number, and Description (if any) - are copied over automatically.

- ✓ Activate/deactivate the digital signature check.
- ✓ Start the content repository, that is, change its status from defined to running.
- ✓ Stop the content repository, that is, change its status from running to defined.
- ✓ Delete the content repository.

Activities

You can execute the above functions by choosing the relevant icons.

Settings

Use


The *Settings* tab contains information on the settings for your content repositories.

Prerequisite

The Content Server Administration screen is open.

Features

The following functions are available:

- You can display information on the settings of a different content repository
- To go to the Customizing, choose  .
- You can refresh the settings information
- You can display and edit the settings that apply to **all** content repositories.

To do so, choose the *All repositories* entry in the F4 Help for the *Content Rep.* field.



This function is available as of SAP system release 4.6D.

- In change mode, you can do the following:
 - Change and save the settings for the content repository, or delete individual settings



These entries are content server-specific.

- Changes to the settings might not take effect until you restart the content repository.
- Go directly to the maintenance screen for the Customizing settings for a repository.

The current values for HTTP server - port number, HTTP script, version number, and description (if any) - are copied over automatically.

Activities



Generally, you should not make any changes here. The options provided in the *Details* tab are sufficient for any changes that are required in standard operation.

You can execute the above functions by choosing the relevant icons.

Statistics

Use

The *Statistics* tab provides statistical information from the content server on the individual HTTP commands.

Prerequisite

The Content Server Administration screen is open.

Features

The following functions are available:

- You can update the information read from the content server by choosing *Refresh*.
- You can delete the information in change mode.

In this case, a request to reset the statistics is sent to the content server.

Activities

You can execute the above functions by choosing the relevant icons.

Creating New Content Repositories

Use

On the tab page *Create*, you can create new content repositories.

Prerequisites

You are in change mode in Content Server Administration.

Features


When creating a new content repository, you can use an existing one as a model.

When carrying out a standard installation of SAP Content Server, you can transfer the values from the Table control.

Activities

1. Enter a name for the new content repository.
2. If you are using an existing repository as a model, choose and the system automatically fills in the subsequent fields.
2. Enter a short description.
3. Set whether or not digital signatures should be checked.
4. The communication parameters that need to be entered in the dialog table vary depending on the operating system and on your decision to create the repository in the file system or in an SAPDB instance. For more information about these parameters see [Description of the Content Server Configuration file](#).

	Microsoft Windows	Unix Operating System
Repository to be created in an SAPDB instance	Storage=ContentStorage.dll ContentStorageName=<DBID> ContentStorageHost=<host name>	StorageDriver=SAPDBStorage (Storage=ContentStorage.dll) ContentStorageName=<DBID> ContentStorageHost=<host name>
Repository to be created in the file system	Storage=FileSystemStorage.dll ContRepRoot=<absolute path>	StorageDriver=FSStorageStorage=FileSystemStorage.dll ContRepRoot=<absolute path>

5. Save your entries.
6. You now have two options:
 - i. If the creation process is successful, the detailed view (tab page *Detail*) opens automatically. The content repository should have the status *Running*.
 - ii. If the creation process is unsuccessful, check the settings and correct them if required (tab page *Settings*). Then try to create the repository again.
7. Make your content repository known to the SAP system. To do this, go to the Customizing by choosing  .

For further information on Customizing, see Content Repositories.

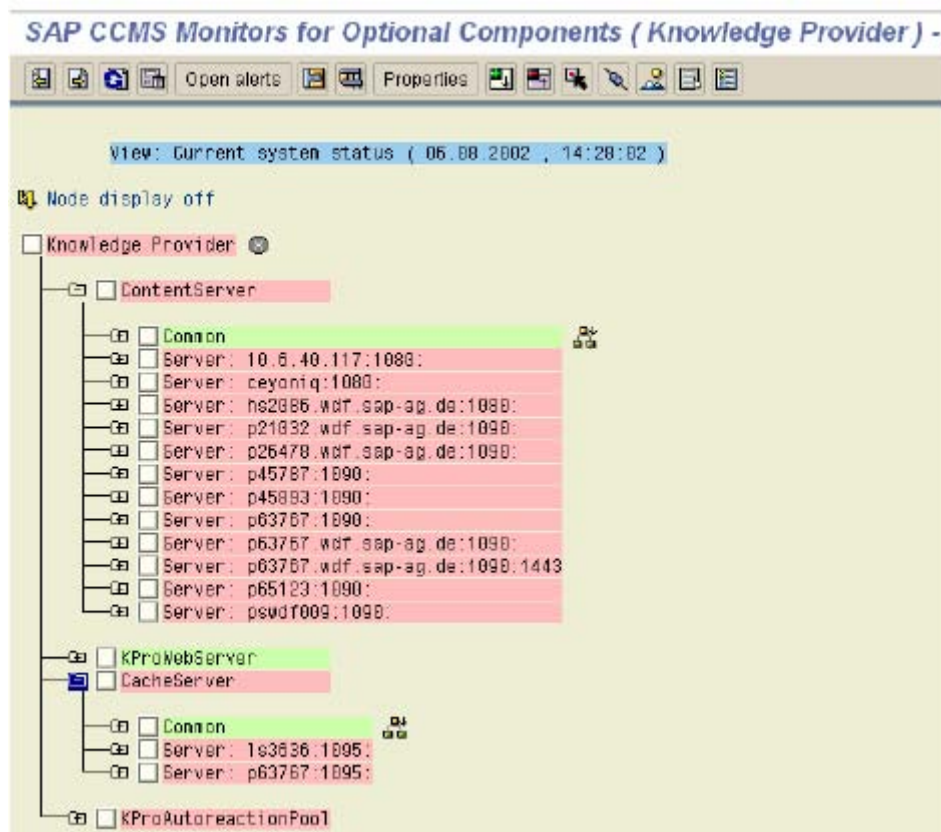
1.1.21 Content Server Monitoring

Use

The HTTP Content Server is monitored automatically as part of the Computer Center Management System (CCMS). All repositories defined in Customizing are monitored, along with their associated content servers. A monitoring function for Web servers and cache servers known to the Customizing is also provided.

For further information on the CCMS, see Monitoring in the CCMS and Alert Monitor.

Call up the monitoring function by entering transaction **SCMSMO**, as shown below.



Alternatively, you can go from the CCMS (transaction RZ20) to the monitoring function for the Content Server and Cache Server.

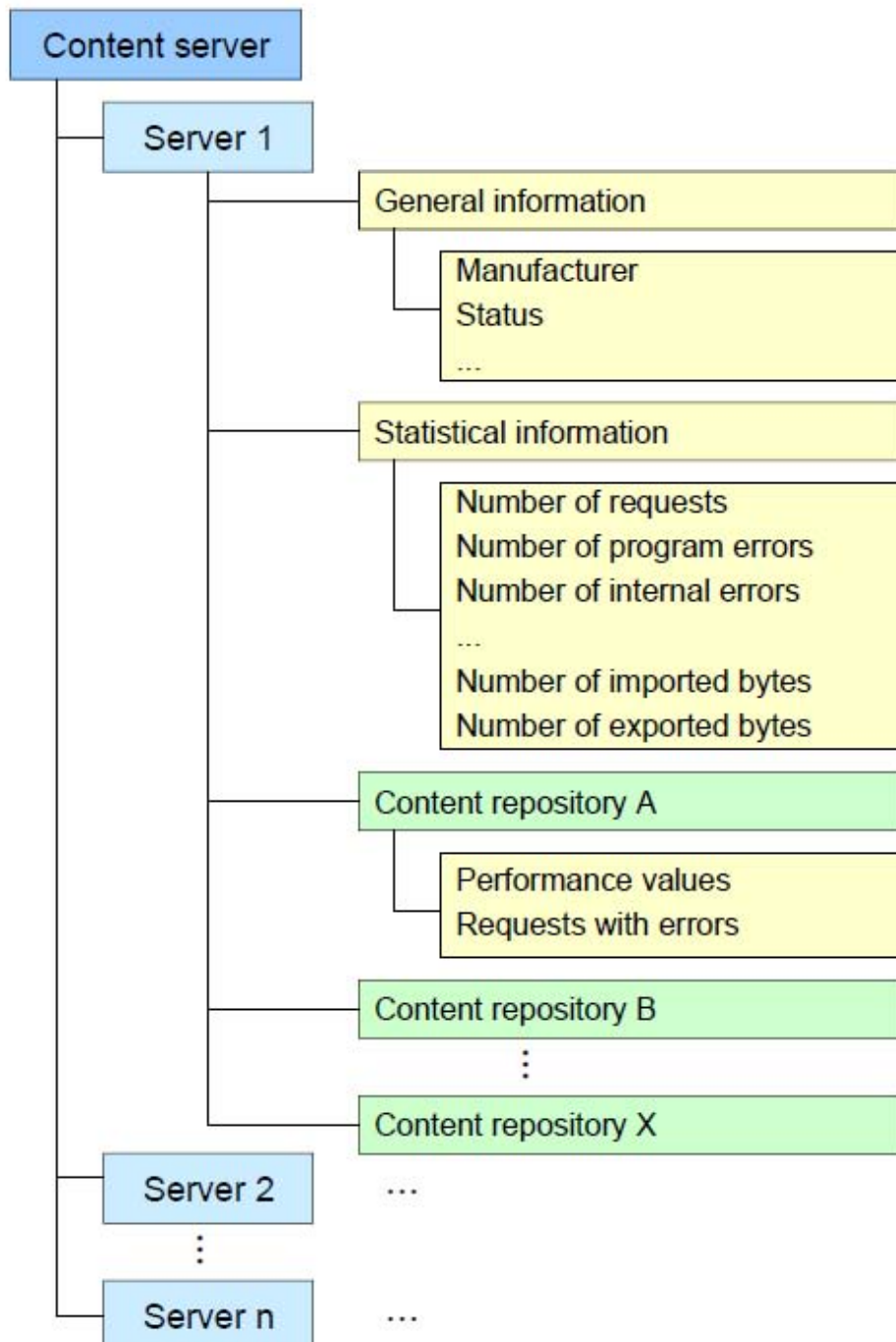
To do this, choose *SAP CCMS Monitors for Optional Components* → *Knowledge Provider*.


Prerequisites

- The Knowledge Provider monitoring function is currently open on your computer.
- The Customizing recognizes the content server repositories (see also OAC0).

Features

The following graphic shows an overview of the information provided by the monitoring function:



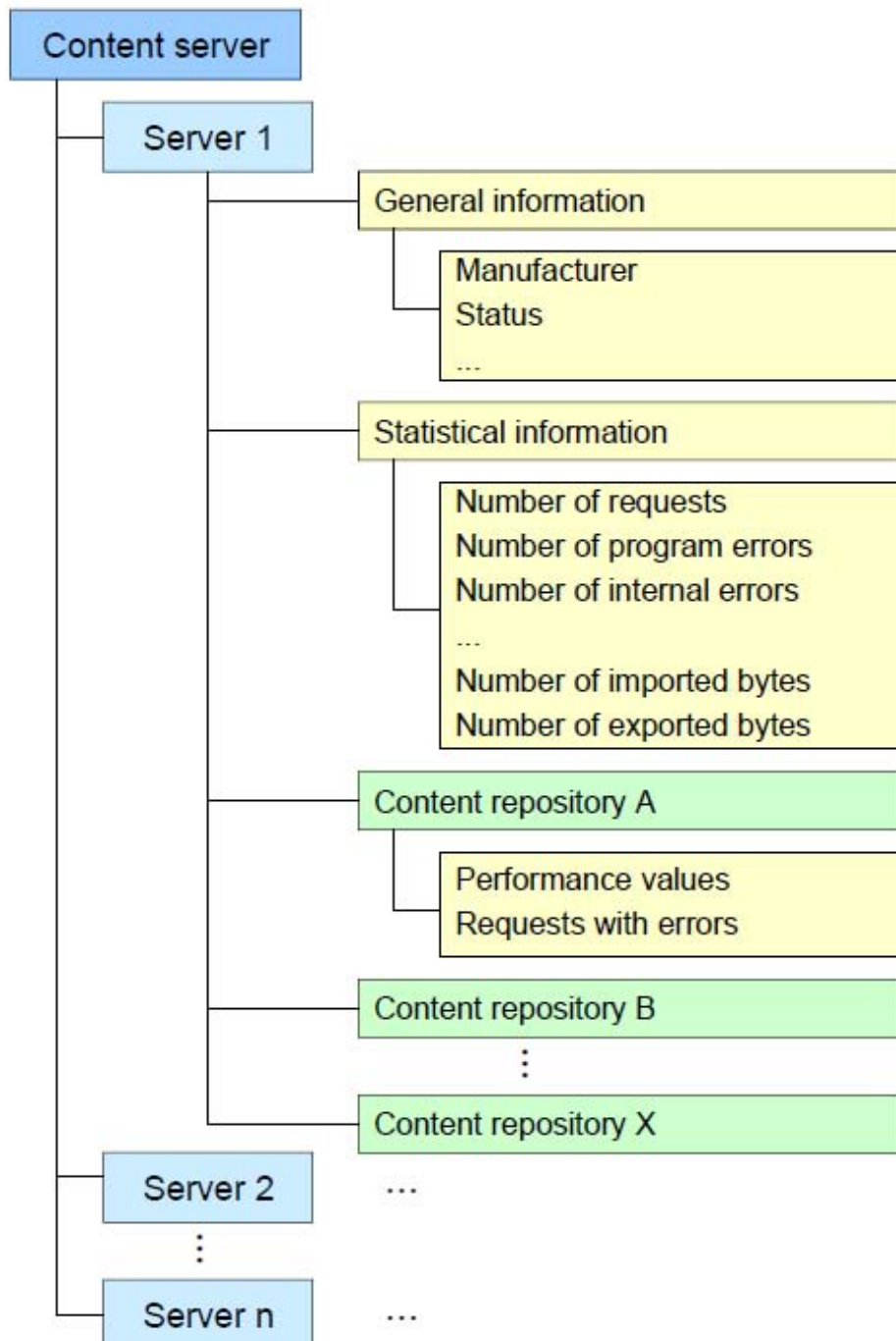
 The monitor also outputs data for content servers of SAP partners. The information on these content servers may not always be as complete as the information on the SAP Content Server. This is because more information is available for the SAP Content Server than for external content servers.

Prerequisites

- The Knowledge Provider monitoring function is currently open on your computer.
- The Customizing recognizes the content server repositories (see also OAC0).

Features

The following graphic shows an overview of the information provided by the monitoring function:



The monitor also outputs data for content servers of SAP partners. The information on these content servers may not always be as complete as the information on the SAP Content Server. This is because more information is available for the SAP Content Server than for external content servers.

Activities

For information on the activities of the CCMS monitor, see Alert Monitor.

You can get detailed information on a particular repository, or an overview of the content server.

To do this, double-click on the name of the content server or the repository in *Current Status* mode. This takes you to the administration screen (see also Content and Cache Server Administration), which displays the required information.



Note that this only works for the SAP Content Server and its content repositories.

1.2 Cache Servers

Caching

A cache is used to store copies of documents when they are accessed for the first time. As a result, the documents can be accessed again more quickly, since the contents are taken directly from the cache. Caching, however, must not be confused with replication (see below). With caching, the original documents are stored in one location, namely on the content server. The copies in the cache can be replaced with newer content at any time.



Documents are checked in Walldorf. An employee in South Africa wants to access and display these documents. The transmission time, however, is extremely long and the intercontinental network connections would be overloaded. By using cache servers, the documents are only copied over the connection once.



Caching is not the same as replication.

These are the main characteristics of caching:

- The original document is still located on the content server.
- The content server can retrieve the cache content at any time.
- Only documents that are actually requested (and therefore genuinely needed) are copied and delivered.

The cache server is used to cache special content server requests. Remote accesses are cached and executed locally. This type of caching is ideal for scenarios in which many different users have joint access to the cache, as the documents only have to be sent once across the wide area network.

Any number of content servers can be installed in different locations. The contents are transferred directly between the client and content server. If the content servers are accessed from different locations that are linked only via a wide area network (WAN), cache servers should be used.

Network traffic across the WAN can be reduced to a minimum and performance enhanced by installing at least one cache server at each location.

A client cache is also available on the user's front-end computer.

Purpose

The purpose of the Cache Server is to provide the following benefits:

- Seamless, transparent integration into existing content server landscapes
- Significant reduction in client response times
- As little administration work as possible

Cache servers are used to speed up access to document content. This is particularly useful if the content is required for display in a Web browser, for example. Cache servers can also reduce the network load and thereby enhance performance. It is therefore also a task of the cache to provide the client with documents from a physically close location, even if the content server is located on a different continent.

Cache servers are similar to content servers, but require less administration with the same level of access protection.



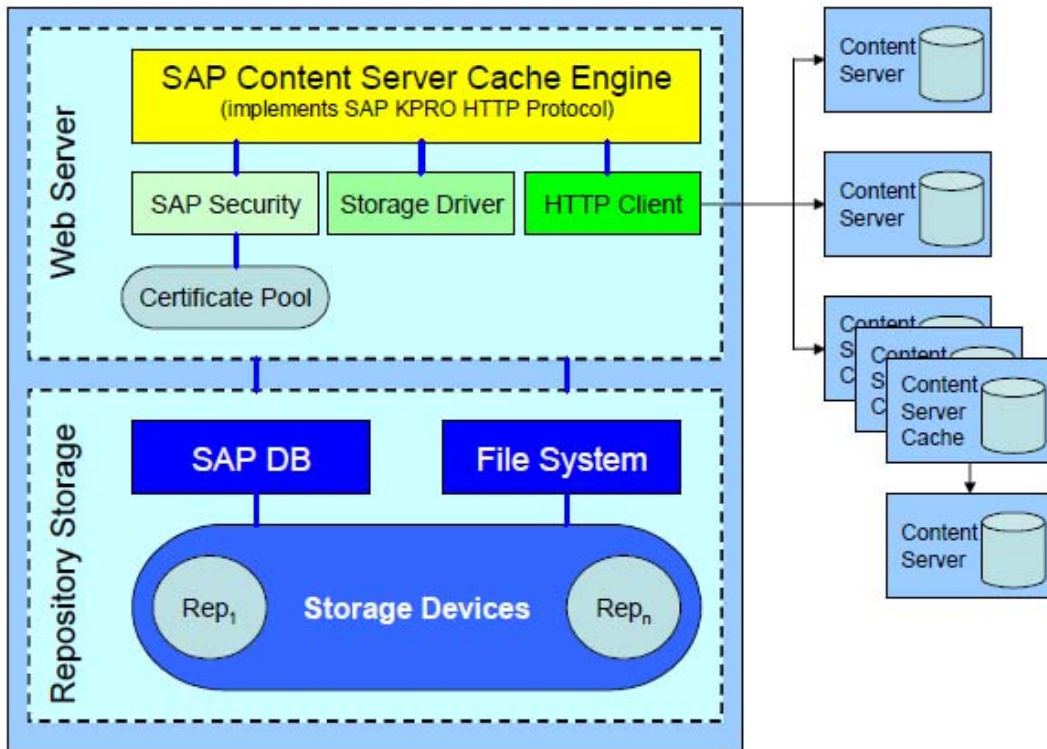
The Cache Server only uses HTTP. To make this possible, the SAP Content Server HTTP Interface has been extended (see SAP Content Server HTTP 4.5 Interface). By using cache servers, you are simply extending your existing infrastructure in a transparent way. There is no need to re-structure the existing content server landscape.

Implementation Considerations

The Cache Server is installed as part of the SAP Content Server installation procedure, using the *SAP Web Application Server Components CD 2*. The installation guide is contained on this CDROM in PDF format in the folder \CONTSERV\DOCU. The guide is available in both English and German.

1.2.1 Architecture of the Cache Server

Despite their similar architecture, the Cache Server and the Content Server have some basic differences. The cache server can set up its own HTTP connections to other servers and can forward incoming client requests. The “other servers” can be content servers or other cache servers. If the server in question is another cache server, this architecture is known as cascaded or multi-layer caching (see also Cascaded Caches).



A notable feature of the cache is its almost complete freedom in terms of administration. As soon as the cache is integrated into the server topology, it can start performing its services without the need for log monitoring or backups.

Caches are always used for **read access** to documents. “Lazy write” is not supported. In other words, a client that wants to store documents must always be directly connected to the corresponding cache server.

Cache URLs can be signed, in the same way that the SAP Content Server interface supports signed URLs. However, it would be very inconvenient if the cache had to rely on the Content Server to carry out signature checks every time. It therefore makes sense for the cache to check the signatures itself. To this end, the cache contains all the necessary certificates, or else it gets them from the appropriate content server. For more information on this topic, see [Secure Operation of the Cache Server](#).



The Cache Server has the same security mechanisms as the Content Server.

1.2.2 Cache Server Administration

Once you have installed the Cache Server, it is virtually maintenance-free. All you have to do to put it into operation is the make the required Customizing settings in the SAP system (for more information also see note 0216419).

This SAP Content Server cache can be administrated directly from the SAP system.

Go to the administration of the cache server using transaction **CSADMIN**. At the start of the transaction enter the host name of the cache server, its port number and path

/Cache/CSProxyCache.dll or /sapcsc (only Unix).

Section [Content Server Administration](#) explains how to use transaction CSADMIN; so here only its functions are described.

You can call up the report RSCMSLOC to get an overview of the locations and servers.

See note 216419: *Multilevel Caching and Content Server Proxies*.

Features

You can display the following information and execute the following actions on the *Administration* screen:

- Overview information of the cache server
- Settings
- Resetting the Cache
- Access Statistics

1.2.3 Functions

The tab pages in the content server administration are also used for selecting cache server functions:

- Overview
- Settings
- Detail
- Statistics

Overview Information

On the *Overview* tab page the same server details as with the content server are displayed. The current cache repositories are also displayed in the Unix version of the cache server.

Settings

The tab page *Settings* shows which global parameters are set for the cache server. In principle, all content server parameters (for the respective operating system) that specify the behavior of the server (tracing, administration security, etc.) and repository definitions can also be used for the cache server. In addition, there are other parameters for the Unix cache server, which you can set to affect the behavior of the reorganization runs.

Name: **CacheThreshold**

Type: numerical

Values: 0-100

Default setting: 70

Mandatory: no

Description: **CacheThreshold** specifies the level to which the storage medium can be filled before it is memory is reorganized. You should never set the threshold to 100 percent, since this could result in continual displacement, and the cache server would not be able to process any more requests.

Name: **MaxReorgProcs**

Type: numerical

Values: 1-20

Default setting: 5

Mandatory: no

Description: **MaxReorgProcs** specifies the maximum number of parallel reorganization processes for file system caches. For database reorganizations this value is 1 and cannot be changed.

Resetting the Cache

On the *Detail* tab page you can completely remove the present contents of the cache by choosing *Delete*. Depending on the size of the cache and user storage resetting may take some time.

Access Statistics

Access Statistics Windows

The ratio cacheHits:cacheMiss indicates how well the cache server can respond to document accesses. If the counter cacheMiss is higher than cacheHits, performance must be poor.

This may be caused by:

- Cache is too small, and/or
- Stored documents are not requested again often enough.

With counters cacheDelete (number of displaced documents) and cacheDeletedBytes you can establish if the size of the cache is too small. The total size of the cache is specified in the counter cacheMaxSize in bytes. Counter cacheCurrentSize indicates the current size of the cache.

Access Statistics Unix

Cache Requests: cacheRequests

Cache hits: cacheHits

Counter contentServerRequests is the difference between the values of cacheRequests and cacheHits. In addition, unsuccessful content server requests are logged in a separate counter. (contentServerBadRequests).

reorgPasses counts how often the cache has to be reorganized (documents displaced).

reorgFreeK specifies how many kilobytes are displaced during the reorganization.

Counter reorgProcsFS specifies how many processes are currently occupied with the reorganization of the file system.

reorgPidDB is not a counter. It specifies the process ID of the process that is currently reorganizing the database.

Relevant SAP Notes:

310218 Delete SAPDB Installations

319332 Content Server Backup Strategies

Changing the Password for Database Access

To change the password for database user "SAPR3", follow the instructions for the content server.

Report RSCMSPWS though requires a fully configured repository to select the respective content server. As there are no repositories in the cache server, you have to manually copy a SAPDB user / SAPDB password from an existing content server configuration file (cs.conf) to the cache server configuration file (csc.conf).

1.2.4 Monitoring for Cache Server**Use**

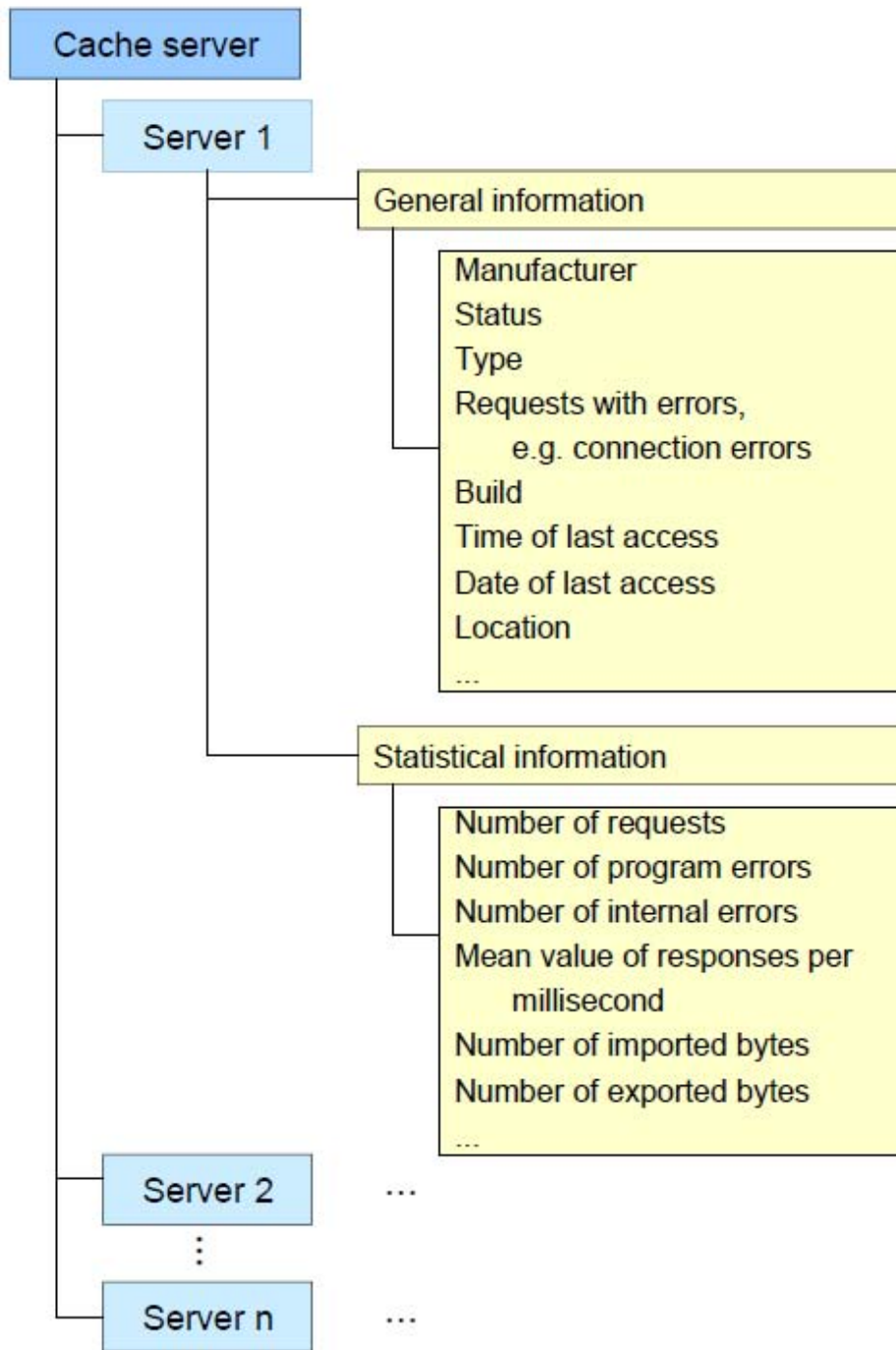
The cache server has an automatic monitoring function.

Prerequisites

- The Knowledge Provider monitoring function is currently open on your computer.
- The Customizing recognizes the cache server (see also SCMSCA).

Features

The following graphic shows an overview of the information provided by the monitoring function:



Activities

For information on the activities of the CCMS monitor, see Alert Monitor.

To go directly to the Administration screen, double-click on the server name (see also Content and Cache Server Administration).

1.2.5 Secure Operation of the Cache Server

The same points apply to the secure operating of the cache server as apply to the content server. Also note the following points:

Signed URLs

- Unlike in the case of the Content Server, you cannot define whether signatures are checked for individual repositories on the cache server. Signature checking must be set globally on the cache server.
- To do this, open the CSProxyCache.INI file. In the section [CSProxyCache], set the entry Security=1.

Backup Strategy for the Cache Server

The cache server gets its data from the connected content servers. The cache server runs in the Overwrite Mode (in older versions the log mode DEMO), that is, the log area is not saved. In overwrite mode the restart function following a database failure and intact Volumes are kept.



After installation, before you connect the cache server to the content server, make a full Data Backup.

Related Notes

361123 SAP Content Servers and Security

409104 SAP Content Server Installations 6.10

1.2.6 Cache Preload

Use

The transaction that controls the cache preload function is **RSCMSPLD**.

Content supplied by SAP should be imported both into an SAP Content Server and a cache server.

Your cache server must support preload. This is automatically the case from build 162. You can find out which build you have using transaction **CSADMIN** (tab page *Details*).

Before you carry out the preload, ensure the following:

- Your cache supports preload.
- SAP Gateway and SAPKPROTP are available on the cache server.
- Your SAP system also contains an RFC destination that links to program SAPKPROTP via the SAP Gateway. To set this up, go to transaction **SM59** and save the RFC destination SAPKPROTP there under a name of your choice. Then make the corresponding changes in the Gateway options.
 - After doing this, ensure that the I-file to be imported is available on the cache server.
 - Now start the report RSCMSTPLD.

- Enter the name of the I-file. Because this file is read by SAPKPROTP, the file name has to have a format that the cache server can understand.
- Enter the RFC destination. The F4 Help provides a list of all destinations where SAPKPROTP is stored as a program.

1.2.7 Multi-Layer Caching and Content Server Aliases

The SAP system knows the locations of the connected content servers, cache servers, and client.

The concepts of multi-layer caching and content server aliases work together to determine the optimal access path for client requests.

- **Multi-layer caching** means that **multiple caches** between the client and the server are accessed when a read access attempt is made on the content server.
- In complex environments, especially those with firewalls, multiple servers may be involved in the handling of a request, regardless of the locations of the servers. Each of these servers plays a role in retrieving the requested content, or, as the case may be, in forwarding the request (similarly to cascaded caches).

These servers are known as **content server aliases** (in the sense that they “represent” the content server).



A content server alias can be, for example, an **IP filter** on a firewall that forwards the requests unchanged to the content server. An alias can also be an instance of a distributed content server, provided that the content server in question supports this. This option is particularly intended for content server providers who can themselves organize distributed storage or content caching, or both.

The concepts of multi-layer caching and content server aliases mutually support each other. The main aim of multi-layer caching is to minimize access times. Also, URLs received via a content server alias can be handled in such a way that controlled content server accesses from the extranet can be allowed via a firewall.

Using Content Server Aliases

- **Firewalls:** regardless of the location of the client, the client may on occasion directly access the content server using the actual host name (intranet) or via a firewall using an abstract domain name (extranet).
- **Distributed servers that all access the same physical database:** there are some third party providers that use what are known as “satellite servers” instead of caching. Satellite servers make it possible to access a repository via multiple content servers. Using the alias concept, you can designate one of these satellites as the actual content server, and the others as its aliases.

Using Multi-Layer Caching

To use multi-layer caching, the locations of the client, content server, and caches have to be known, just like with single-layer caching. You must also decide which path will be used to access the content server from a specific location. You have to maintain the following tables:

- **SDOKLOC** - locations (transaction **OALO**)
The table SDOKLOC defines the possible locations. Enter all the locations here.

- **SCMSIPNET** – location for sub-nets (TA SCMSIP from release 4.6C)
The table SCMSIPNET allows you to define the location using the IP address. The sub-net is defined using the format XXX.XXX.XXX.XXX/YY. XXX.XXX.XXX.XXX is the usual format for IP addresses. /YY (/00 .. /32) defines how many bits, beginning from the left, are valid. If multiple sub-nets are assigned to one IP address, the smallest sub-net is the one that applies (that is, the one for which the most bits are defined). The location determined for the user in this way can be overwritten by the user parameter LCA.

- **SCMSHOST** – properties of hosts (transaction **SCMSHO** from release 4.6C).
The table SCMSHOST defines the location of hosts. Enter all hosts here that are used as content servers or cache servers. Make sure that you enter the host names correctly, including upper case and lower case letters.

- **SCMSCACHE** – definition of caches (transaction **SCMSCA** from release 4.6C) The table SCMSCACHE defines the cache server. Enter all cache servers here. If a particular cache server is inactive, you can mark it accordingly.

- **SCMSLOPA** – location path for multi-layer caching To enable multi-layer caching, enter the path on which the cache server should be used. Do this for two locations at a time. The fields LOC_CLNT and LOC_DEST define the location of the client and the content server. The field LOC_INDX is numbered from 1 to N. The locations between the client and the server are entered in the field LOC_NODE. Do not enter the locations of the client and the server themselves. The location LOC_NODE = 1 is the closest to the client, while the location LOC_NODE = N is closest to the server. If signed URLs are being used, the content server and the cache server have to closely interoperate. Therefore, caching can only work if the content server has the version number 0046, or if no signature is used for access.

Procedure for Read Access

1. The system determines the location of the client (LCA parameter, SCMSIPNET).
2. The system determines the location of the content server (SCMSHOST, SCMSIPNET).
3. The system determines the path between the client location and the server location (SCMSLOPA). If the client and the server are at different locations, the client location is inserted at the beginning of the path.
4. The available cache servers are determined for every location on the path. If multiple caches are available at one location, one is selected. Load distribution is automatically used at this location.
5. A URL is then constructed that ensures that the content servers and cache servers along the path are searched for the content in question. The retrieved content is then stored in all cache servers between the client and the content server or the cache where the content was found.

Incorporating a Content Server Alias

You have to make the following Customizing settings:

- **SCMSCSPX** – content server aliases (the CSPX here comes from content server proxies, an alternative term for aliases).

The technical data of the alias is stored in this table. By specifying the technical data of the content server, you define which content server is represented. Ensure that you enter all the technical details correctly, including upper-case and lower-case characters. The individual fields have the following meanings:

PX_SERV Host name of the alias server
 PX_PORT Port of the alias server
 PX_SPORT SSL port of the alias server
 PX_SCRPT HTTP script of the alias server
 CS_SERV Host name of the content server
 CS_PORT Port of the content server
 CS_SPORT SSL port of the content server
 CS_SCRPT HTTP script of the content server
 NO_GET Alias is not used for 'cacheable' get requests
 INACTIVE Entry inactive

- **SCMSCSPL** – other locations of content server aliases (the CSPL here comes from content server proxy locations).

This table contains other locations, besides those entered in table SCMSHOST, that can also be used for the alias server.

The data for the content server must be exactly the same as that in the Customizing for the repository (transaction OAC0).

- Only from release 4.6D can you explicitly specify the port. Up to release 4.6C, the port is added at the end of the content server name in the form :<port>.
- You have to explicitly define the HTTP port when defining the alias server. In releases before 4.6D, leave the SSL port at its initial value.
- The field NO_GET can be used to specify that a content server alias is not to be used for 'cacheable' get requests.



This is useful if the caches can support the cacheable get requests better than the alias.

The field INACTIVE can be used to stop the alias in question being used.

Determining the Alias

- The system checks whether there is an alias for the content server in question at the client's location.
- If there is no alias at that location, the system looks for another alias that can be used.
- If an alias is found, the technical data of that alias is used instead of those of the content server.
- If more than one alias is found, load distribution is used automatically.
- Multi-layer caching and aliases can also be used in combination. The system always looks for an alias first. If it finds one, the technical data of the alias is used instead of the data of the content server. This means that the location of the server may change. This information is then taken into account when the cache server is being located.

Constraints

Caching and content server aliases are only used if the client location is known when the URL is being constructed. Usually, the client location is known if the Knowledge Provider processes the URL. If, on the other hand, the URL was requested by another application, and the Knowledge Provider does not know where the URL is going to be used, the system cannot find out the location of the client. In this case, the URL that points directly to the content server is always returned. The caches and the alias server do not, therefore, play any role.

This can often be the case with ArchiveLink.

Related Notes

0181696, Caching

0209478, SAP KPro Server Infrastructure Components 4.6C

0303278, SAP KPro Server Infrastructure Components 4.6D

0352518, Using the SAP Content Server Cache

0376033, Cache Server Knowledge Warehouse 5.1

0407520, Information on the Cache Server

1.2.8 Using the Cache Server with Third-Party Content Servers

From Basis release 4.6B, the cache server can be used in conjunction with the SAP Content Server (see note 216419).

If you want to use signed URLs, the interaction between the Content Server and the cache server requires some adjustments to the Content Server interface.

These and other adjustments have been made in the SAP Content Server. To facilitate this, the interface version 0046 has been developed for the SAP Content Server.

To ensure that the cache server can be used without any restrictions, including with third-party content servers, the cache server has to be able to use all the commands that are defined for the interface version 0045 even if version 0046 is being used. The content server, for its part, has to be able to implement the getCert command.

The effect of this is that the list of certificates that are active for a specified repository is returned.

The client sends an HTTP GET request with the following parameters:

Parameter	Optional / mandatory	Meaning
ContRep	Mandatory	Content repository
PVersion	Mandatory	Interface version

Example:

<http://pwdf0033.wdf.sapag.de:1090/ContentServer/ContentServer.dll?getCert&contRep=R1>

The body of the response contains information on whether the signature is active (1) or inactive (2). It also may return the list of active certificates.

In addition to the (optional) description of the certificates, the data that is transferred to the content server in the body with the corresponding putCert command is returned in hexadecimal form. The list has the following format:

```
security="<value>";CRLF<key1>="<value11>";<key2>="<value12>";...<keyN>="<value1N>";
CRLF
<key1>="<value21>";<key2>="<value22>";...<keyN>="<value2N>";CRLF
```

... <key1>=<valueM1>;<key2>=<valueM2>;...<keyN>=<valueMN>;"CRLF

The following keys are used for the descriptions of the certificates:

Key	Optional / Mandatory	Meaning
Subject	Optional	Description
issuer	Optional	Issuer of the certificate
serialNumber	Optional	Serial number
notBefore	Optional	Valid from
notAfter	Optional	Valid until
keyInfo	Optional	Info
certificate (hex-encoded)	Mandatory	Certificate from putCert

The SAP Content Server returns all the parameters described here. It is sufficient for interoperability with the cache that a value is assigned to the parameter certificate.

Also, in the header of the response to a get command, the content server must return the security level that was set when the document was created.

Key	Optional / Mandatory	Meaning
X-docProt	Mandatory	Security level

Adjustments are necessary only if the following apply:

- You are using a third-party content server
- You want to use the SAP Cache Server
- You want to implement read access with signed URLs

Related Notes

216419 Multi-Layer Caching and Content Server Aliases

433723 Cache Server for Third-Party Suppliers – Build 164

1.3 Special Procedures


1.3.1 Relocating the SAP Content Server

Procedure

If you want to move your SAP Content Server **and all the repositories it contains** to a different server, you have to copy the ContentServer.INI file and the security directory to the new server. To do this, use the backup/restore functions of the SAP DB to copy the content of the database.




If the host name or the HTTP port of the content server change due to the move, you have to change the repository definitions in the SAP systems accordingly.

 We advise you against making a physical copy of the old content server and simply putting it onto a server with a different IP address. This procedure has been known to cause problems with the IIS, and the problems could only be solved by reinstalling the operating system.

If this situation does occur, it is not sufficient to simply reinstall the content server.

Relocating a Repository

This section deals with the scenario where you want to move a repository from one SAP Content Server to another SAP Content Server.

 The following instructions presume that both the source repository and the target repository are located on an SAP Content Server, and not on a third-party content server. Otherwise, you can relocate individual documents (see also note 389366).

Relocating Using the Database

If the target content server is being newly set up, proceed as follows:

1. Create a copy of the complete content server. You can use the database to do this. For more information on this procedure, see note 350067.
2. Change the Customizing of the relocated repositories so that they point to the new content server.



You are thus preventing documents from being stored on the affected repositories during the relocation procedure. Therefore, you must carry out this step before deleting the repositories.

3. On the source content server, delete all the repositories that you want to relocate, and delete all others from the target content server. You can use transaction **CSADMIN** to delete the repositories.

Relocating Using Export and Import

1. Ensure that no new data is saved to the affected repositories during the relocation procedure.
2. Use report RSCMSEX to export the repository.
3. Create a repository of the same name on the target content server and change the Customizing of the repository so that it points to the target content server.
4. Import the data into the target repository using report RSCMSIM.
5. Delete the relocated repositories from the source content server.

The program **sapkprotp** controls the export and import. **sapkprotp** is started on the application server by default. If required, you can start **sapkprotp** on the content server or on another server. To set this up, enter an RFC destination when starting the report. Set the path of the transport file relative to **sapkprotp**.

You should use this option if **sapkprotp** is not available on the application server (so far, **sapkprotp** is not available for AS/400). You should also use it if the content server is at a remote location, to avoid the data being transferred twice over the WAN.

See also:

Note 371220

1.3.2 Incorporating a Patch

Use

You can download patches for SAP components from the SAP Service Marketplace Software Distribution Center: <http://service.sap.com/swcenter>.

You can also use the link <http://service.sap.com/swcenter-main> to go directly to the „SAP Maintenance“ area of the Software Center (*Support* → *SAP Software Distribution Center* → *SAP Maintenance*). This page contains Support Packages and Binary Patches.

Navigation

You select the patch you require from the product hierarchy in the right-hand navigation bar. Choose *SAP WEB AS*, followed by the release in question.

Procedure

Solution

The Support Packages for the SAP Content Server are available as self-extracting ZIP files.

The files are located in the SAP Service Marketplace Software Center:

<http://service.sap.com/patches>

You will find the SAP Content Server under:

SAP Software Distribution Center ->

 SAP Support Packages and Patches ->

 Entry by Application Group ->

 SAP NetWeaver Components ->

 SAP NetWeaver 04 ->

 SAP Content Server ->

 SAP Content Server 6.40 -> <PLATFORM>

The ZIP archive for Windows contains the relevant current versions of the files:

- ContentServer.dll
- ContentStorage.dll
- FileSystemStorage.dll
- CSProxyCache.dll
- CSUtil.dll
- sapsecu.dll

The ZIP archive for Unix contains the relevant current versions of the files (the file extensions can vary depending on the Unix variant):

1. mod_sapcs.so
 2. mod_sapcsc.so
 3. libsapsecu.so...
- mod_sapcs2.so
 - mod_sapcsc2.so

Install the patch under Windows:

- Unpack the files to a temporary directory.
- Stop the IIS via 'net stop w3svc'.
- Replace the DLLs in the following directories with the relevant files in the ZIP file. If you have installed into a different directory, you must adjust the relevant paths.
 - C:\Program Files\SAP\Content Server
 - C:\Program Files\SAP\Cache Server
- Restart the IIS via 'net start w3svc'.

Install the patch under Unix:

- Log on to the Unix system as the Content Server Administrator.
- Unpack the files to a temporary directory.
- Stop the Apache Web Server with the command "apachectl stop". You will find this command in the directory "bin" of the server installation.
- Replace the Shared Libraries in the directory "libexec" (for apache 1.3) or modules (for apache 2.0) of your Content Server/Cache Server installation against the files from the ZIP archive.
- Check the execution rights of the program files. Some UNIX variants require execution rights to be set for Shared libraries The relevant command is "chmod755 <file name>".
- Start the Apache Web Server with the command "apachectl start".

See Also :

Refer the note 514500

1.3.3 Setting Up Client-Specific Repositories

Purpose

In the Knowledge Provider, different repositories can be used to store document content, depending on the client in question. This type of repository is known as a client-specific repository. Client-specific repositories allow content to be separated according to client, including when external content servers are used.

The benefits of client-specific repositories are as follows:

- Client-specific repositories allow content to be separated according to client, including in cases where external content servers are used. This is particularly useful for application service provider enterprises, and in cases where live and test clients and running in parallel.
- Client-specific repositories also greatly simplify the administration of your system landscape.

Features

Previously, client-specific content storage was only possible in the Online Transaction Processing (OLTP) database. The functionality has been introduced to Knowledge Provider in response to customer demand, especially from application service providers.

The concept of the **logical repository** is central to implementing client-specific repositories. It is the logical repository that makes it possible to access different physical repositories by means of the client and the system ID.



Logical repositories are maintained in transaction OAC0.

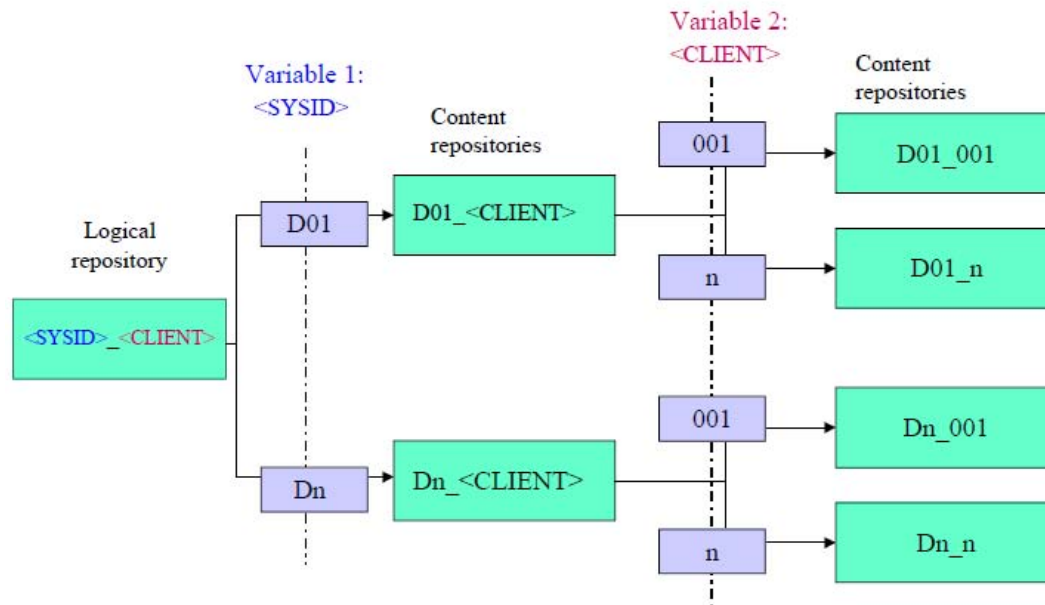
You define the logical repository along with the content repository in the SAP system. A definition template is used to map the logical repository to a physical repository.

The definition template can contain the following values:

<CLIENT> Client

<SYSID> System ID

Definition template: <SYSID>_<CLIENT>



These variables are replaced by concrete values during the actual mapping process.

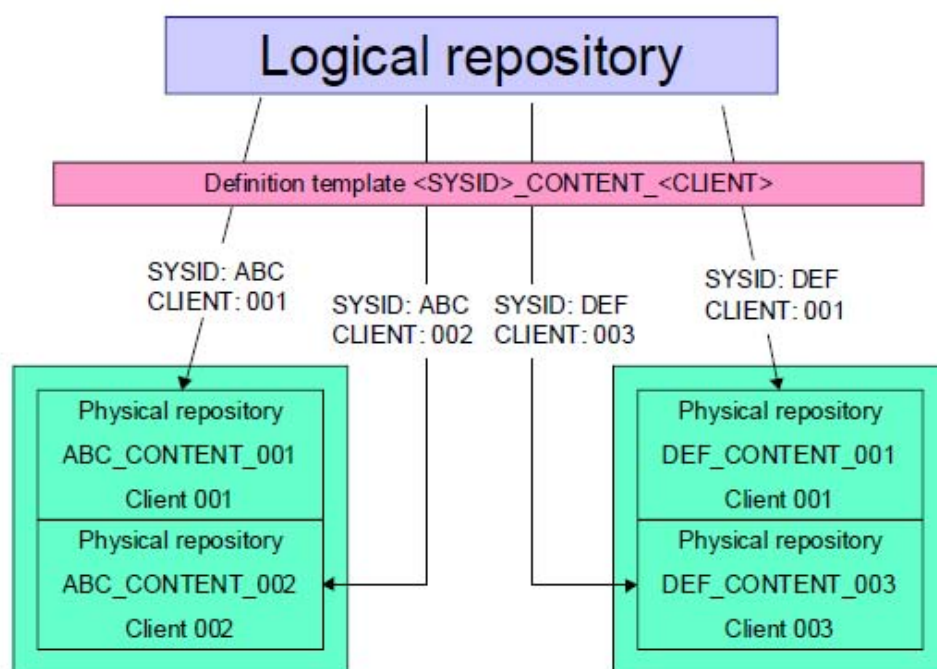
Example

In client 001 of the SAP system ABC, the definition template <SYSID>_CONTENT_<CLIENT> is mapped to the physical repository ABC_CONTENT_001.

In client 002 of the same system (ABC), the definition template is mapped to the physical repository ABC_CONTENT_002.

In client 001 of the SAP system DEF, the same definition template is mapped to DEF_CONTENT_001.

In client 003 of system DEF, the same definition template is mapped to DEF_CONTENT_003.



You can now use the SYSID to centrally administrate the assignment of repositories in several SAP systems and to distribute the assignments to other systems. The various systems can then use different repositories.

Using Several Database Instances

By default, all repositories on a content server use just one Database Instance. You can however distribute the repositories across several database instances, for example, if you want to handle the repositories differently when making backups.

You install the required SAP DB instances when installing the Content Server or using the Database Manager GUI.



The repository names have to be unique on the Content Server in question.

If required, you can manually create multiple websites, so that you can run multiple Content Servers on one machine. Use the Microsoft Management Console to do this. In the IIS, open the context menu for the node "SAP Content Server", and choose *New* → *Website* to open the Website Creation Wizard.

In the Wizard, you are asked for the IP address, port settings, the path on which the website home directory should be created, and the access authorizations for the home directory.

Once you have created the new website, it appears in the tree structure.

Changing the Password for Database Access

Use

The SAP Content Server uses the Database User **SAPR3** for accessing its Database Instance. You can change the standard password for this user, in order to prevent the database instance from unauthorized use.

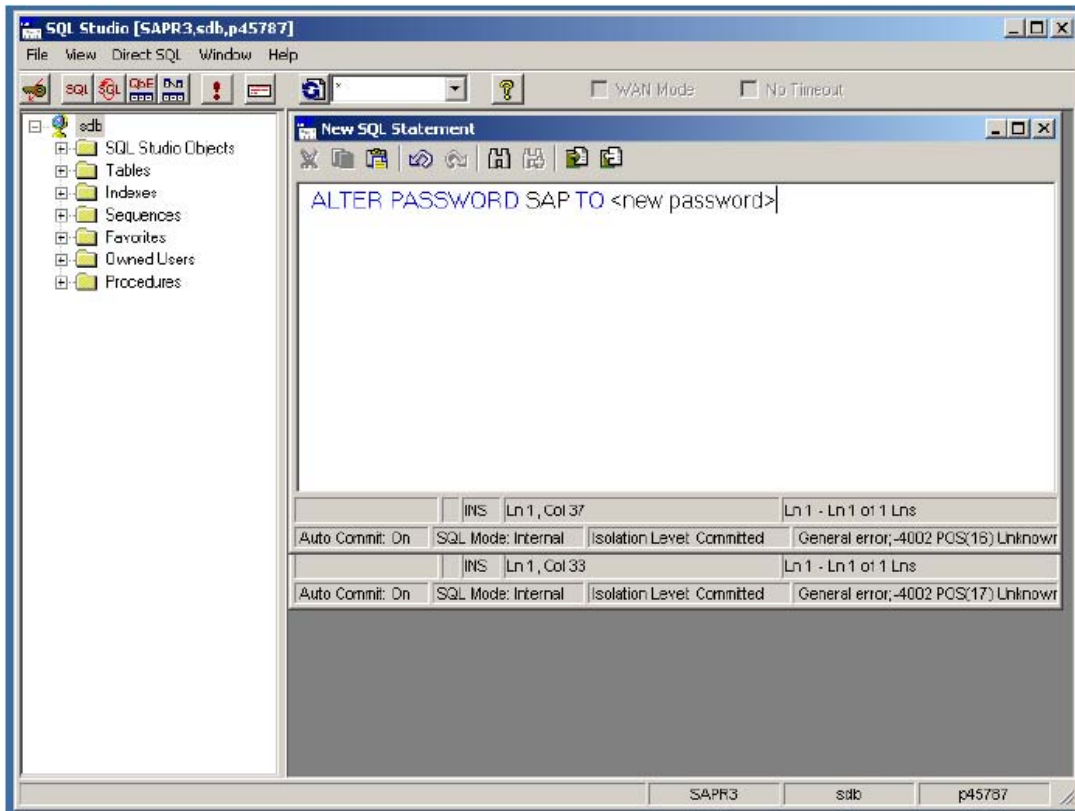
To change the password, follow the procedure described below.

Procedure

Change the password in the database instance using the tool SQL Studio.

Log on to the relevant database instance as user **SAPR3** (default password: SAP).

Under *View* → *Direct SQL*, enter as a *New SQL Statement* the command **OLD PASSWORD** <old password> **TO** <new password>.



To execute the command, enter **CTRL+F5** or choose the exclamation mark icon. If you do not receive any error messages, the new password has been successfully set up in the database.

The database user and the new password now just have to be encrypted and stored in file ContentServer.ini/cs.conf abgelegt werden. To encrypt and set the user name and password use report RSCMSPWS in the SAP system. Then you can reset the user and the password either for a repository or for the whole content server.

See also

Note 661852.

1.3.4 Troubleshooting

Problem: Multiple Entries for Object SCMS in Application Log Manifestation

Multiple entries are listed for the object SCMS in the application log (transaction SLG1).

Explanation and Solution

Content servers are automatically monitored from release 4.6C. If problems occur with the monitoring process, entries may be written to the application log. This may cause an excessive load on the application log, especially if the Customizing for the content repositories has not been set up correctly.

Check the Customizing for the content repositories (transaction **OAC0**).

Correct any incorrect Customizing.

Also see notes 308977 and 315604. Note 392242 describes a procedure which ensures that error messages in relation to monitoring are no longer logged in the application log.

Problem: Errors in Document Access

Manifestation

The following problems indicate a document access error:

Problems when accessing documents or report RSIRCCON

Database error with <INSERT INTO KPRO>, error message number SO 013

Database error with <GET DATA FROM KPRO>, error message number SO013

Error with data transfer, error message number 42 638

Knowledge Provider transfer error, error message number SBDS 205

Explanation and Solution

The Knowledge Provider (KPro) has functions for storing and reading documents on external storage systems (content servers). The programs **saphttp**, **sapftp** and **sapkprotp** are used for this. These programs are accessed via RFC. The program **sapkprotp** is usually only used on the application server or other selected servers, while **sapftp** and **saphttp** are also used on the front end. An RFC destination has to exist before programs can be used.

The corresponding RFC destinations are as follows:

SAPHTTP: starts **saphttp** on the front-end workstation

SAPFTP: starts **sapftp** on the front-end workstation

SAPHTTPA: starts **saphttp** on the application server

SAPFTP A: starts **sapftp** on the application server

SAPKPROTP: starts **sapkprotp** on the application server

KPro automatically creates these RFC destinations when it is first used.

Manually Changing RFC Destinations

For testing and debugging purposes, you can change the destinations using transaction **SM59**. You can also change the flag for 'trace'. This activates a special trace for the program in question, in addition to the RFC trace. Programs **RSHTTP40** and **RSFTP001** are used to display and delete the traces for **saphttp** and **sapftp**.

If the RFC destinations contain incorrect values (such as the wrong program, or the program is being started on the wrong machine), this can cause errors that are difficult to resolve.

If problems occur in connection with HTTP access to the Content Server, or with transferring documents to and from the front end, you should check the destinations listed here.



If you are not sure that the destinations are in their original state, you can delete them. As explained earlier, this resets them to their initial state.

Related Notes

093042, Problems with SAPFTP

164203, Problems with SAPHTTP

Problem: Content Server is Rejecting Large Files

Manifestation

Error code 10055

Explanation and Solution

The Content Server rejects checkin requests for documents greater than 50 MB. So far, this error has been observed on Windows 2000 only, but may also occur on NT4 in the case of sufficiently large documents.

It has been our observation that requests are rejected because the kernel buffer space requirement in the IIS is too high.

To solve the problem, first ensure that you have Content Server build 163 or higher. If your Content Server has an older build, install build 163 in accordance with the instructions in note 410779.

If the problem occurs with build 161 or higher, change the parameter MaxTransferBlockSize in the INI file in accordance with your system's requirements. This parameter has the default value 64 KB.

Problem: SAP Content Server Comes to a Standstill

If an SAP Content Server in productive use comes to a sudden standstill, it is more important to try to solve the problem quickly than to establish the exact cause. This section describes a possible procedure for resolving a Content Server standstill.

Procedure

Check in the Database Manager GUI, whether the Log Area or the Data Area is full.

For information on Content Server standstills and the fill level of the database instance, see [Monitoring the Fill Level of the Database Instances](#).

- If the log area is full or almost full (>95 %), make a Log Backup.

Once some of the log entries have been backed up, you can continue working with the content server.

To ensure that the log area does not become full again, you should activate the Automatic Log Backup.

- If the data area is exhausted:

It must be increased in size (Create Volumes).

Check the capacity of the database instance again.

Restart the Web service, as described in [Starting and Stopping the Content Server Correctly](#).

Restart the server host.



You should also make a note of the incident, including the date and time, the server name, and how you solved the problem, so that you can trace the cause if errors become more frequent.

Other Possible Causes of the Problem

Check the following in the ISS Management Console:

Do the port numbers on the SAP system and the Content Server match?

Are the website settings correct?

Does the virtual directory "ContentServer" still have execution authorization?

Is the site active?

Have you checked that the security settings are correct?

Notes Relating to SAP Content Server (Selection)

0093042 Problems with SAPFTP

0119863 SAP DB: Backup Tools

0164203 Problems with SAPHTTP

0181696 Caching

0209478 SAP KPro Server Infrastructure Components 4.6C

0212394 Initial Password for DBM, DBA, and Domain User

0216419 Multi-Layer Caching and Content Server Aliases

0303278 SAP KPro Server Infrastructure Components 4.6D

0310218 Delete SAPDB Installation

0315604 Customizing the Content Repositories

0319332 Content Server Backup Strategies

0203721 Content Server: Backup Tools

0328209 Content Server: Large Objects – Build 161

0350067 Administration Content Server/SAP DB

0351647 Cache Server Administration

0352518 Using the SAP Content Server Cache

0354819 Composite note SAPSECULIB

0361123 SAP Content Server and Security

0371220 Content/Cache Server on Windows 2000 Platforms

0376033 Cache Server Knowledge Warehouse 5.1

0389366 Relocating Documents

0308977 Repositories BIE_QMM, BIE_NET and HME_CONTENT

0392242 Multiple Entries in Application Log

0407520 Information on the Cache Server

0409104 SAP Content Server Installation 6.10

0410779 Content Server: Large Files and Win 2000 - Build

0433723 Cache Server for Third-Party Suppliers – Build 164