CA View®

Release Notes

Release 11.7

CA Technologies Product References

This document references the following CA products:

- CA ACF2
- CA Deliver™
- CA Mainframe Software Manager (CA MSM)
- CA Output Management Web Viewer
- CA Top Secret®

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This document provides information about the new features and functions in CA View Version 11.7.

Important! Be aware that version 11.7 is built on CA View r11.6, and includes changes or updates that are directly connected to encryption, use of ESD PAX or MSM installation, Health Checks and information about the higher user threshold, REGDAYS, the enhanced MAXLINES parameter and the improved STATUS command.

The encryption feature *does not* support Centera storage. This will be added in an APAR or future release.

This section contains the following topics:

New Features

CA View r11.7 is a feature-specific release built on CA View r11.6. It provides the following:

- Higher user threshold for XMS and DRAS
- Support for retaining reports based on regulatory requirements
- Improvements in the MAXLINES parameter
- Backward compatibility with CA View r11.6, r11.5, and r11

Note: With the exception of the information contained in this document, all pre-existing product documentation is accurate and timely.

Higher User Threshold Under XMS and DRAS

The maximum number of users that can access a Cross Memory region (XMS) or Distributed Repository Access System region (DRAS) in previous releases was limited due to high usage of below-the-line storage which varied based on the number of extents (data sets) defined to the CA View and CA Deliver databases.

Upwards of 60K of private below-the-line storage was allocated per user. This amount, coupled with MVS system below-the-line requirements for allocation and open, could exhaust available below-the-line storage at 60 to 100 users.

In Version r11.7, the below-the-line storage requirements are dramatically reduced. Certain data areas were moved to above-the-line storage and now share database related control areas. The per user private and system below-the-line storage usage has been reduced to approximately 5 KB (kilobytes). Also private and system below-the-line storage related to allocation, open, and access of each database extent is approximately 2.5 KB. Therefore, if the region size (REGION on the EXEC JCL statement or system default region size) is large enough, these reductions allow the maximum number of users to exceed 500.

At a minimum allow 20 MB (megabytes) of REGION storage for the XMS and DRAS region plus 1 MB for every two users. For example, to support 200 users, specify a minimum region size of REGION=120M (20 MB + (200 users / 2) MB).

Due to address space limits the maximum amount of XMS users should not exceed 1000 users.

REGDAYS - Retaining Reports Based on Regulatory Requirements

REGDAYS is a new ERO parameter that places reports in non-deletable status. It works this way:

- When REGDAYS is used in the ERO table, matching reports are flagged as non-deletable until a calculated REGDAYS date has been reached. Valid values are 0 to 32767.
- The REGDAYS date is calculated by adding REGDAYS to the report ARCHIVE date.
- Once a REGDAYS date is assigned to a report, it can only be extended and never shortened via changes in the ERO table.

Note: If you try to use the SARBCH /CHANGE ARCHDATE function, it will fail with a message if the target report is under REGDAYS control.

Example 1

If a report is archived on 10/01/2011 with REGDAYS=20, it cannot be deleted before 10/21/2011. If on 10/05/2011 the ERO table entry is changed to REGDAYS=5, new reports for that day (10/05) cannot be deleted until 10/10 but the 10/01 copy remains non-deletable until 10/21/2011.

Example 2

If on 10/05/2011 the ERO table entry is changed to REGDAYS=25, new reports for that day cannot be deleted until 10/30/2011.

In addition the 10/01 copy will be non-deletable until 10/26 because the new REGDAYS value (25) was greater than its old REGDAYS value (5).

Important! Even if a user is authorized to delete the report, the delete will fail if the date is prior to the REGDAYS date.

Centera and the REGDAYS Parameters

Any time a report under REGDAYS control is migrated to Centera storage, the Centera retention period is set to the CA View REGDAYS date.

Centera retention is specified in seconds from the Centera creation date which is based on GMT time. CA View applies a local time zone adjustment to the number of seconds so the report is retained until midnight local time ensuring that a Centera Compliance Plus device also enforces the REGDAYS date.

Notes:

- Centera applications outside of CA View cannot delete the report. Therefore, a restriction is placed on indexing a REGDAYS controlled report that is stored on Centera. Because the old index cannot be removed, the report cannot be re-indexed. CA View fails the Index operation and displays an appropriate fail message.
- Any time a REGDAYS date is extended, the change is sent to Centera during the next backup cycle.

Enhanced MAXLINES Parameter

MAXLINES allows large SYSOUT groups to be truncated in CA View. Once the MAXLINES value has been reached, the remainder of the Sysout group is truncated. Now you can specify BYPASSDS to only truncate the current dataset. Subsequent datasets in the sysout group will still be archived.

Improved STATUS Command

Because of a change in the database structure, the online STATUS command now provides a quick and accurate allocation percentage for the database. To take advantage of the feature, version the database to release level 11.6 or 11.7.

In Release 11.0, the response time for this command was slow, but it provided accurate allocation percentages. In Release 11.5 the response time for this command was quick, but it only produced an approximate allocation percentage for the index.

Environment

This section discusses the current operating systems supported, scalability, compatibility, and the security interfaces.

Supported Operating Systems

The minimum operating system required to run this version of the product and meet the performance requirements is IBM z/OS 1.9 and higher.

Scalability, Availability, and Prior Versions

CA View Release 11.7 has the same scalability as previous releases. Improvements to the XMS and DRAS regions now support a larger number of users per task.

Availability is almost 24x7 except for periodic maintenance which can vary in frequency according to the needs of your site.

Note the following:

- CA Deliver allows concurrent archiving to CA View r11.0, r11.5, r11.6, and Release 11.7.
- The release 11.7 XMS and DRAS tasks allow concurrent viewing of CA View r11, r11.5, r11.6, and Release 11.7 databases.

Compatibility

This section discusses compatibility with prior releases and backward compatibility and encryption.

Backward Compatibility and Encryption

CA View r11.7 is able to access r11.6, r11.5, and r11 release databases and read all prior versions of report data found on tape.

If you revert to a prior release of CA View, compatibility PTFs must be applied as follows:

Release 11.6

Apply PTF RO28310 to be sure that release 11.6 can read Release 11.7 tapes.

Release 11.5

Apply PTF RO17278 and PTF RO31552 to be sure that release 11.5 can read release 11.6 and Release 11.7 tapes.

Release 11.0

Apply PTF RO17241 and PTF RO31777 to be sure that release 11 can read release 11.6 and Release 11.7 tapes.

Starting in release 11.6 of CA View, report data on disk and tape can be encrypted if you enabled encryption using the ENCRYPT initialization parameter.

Note: Because compatibility PTFs for pre-11.6 releases are not provided, special procedures must be performed to allow access to this data. These procedures are outlined in the "Reverting to a Prior Installation" chapter in the Reference Guide.

Compatibility with Prior Releases

If prior releases of CA Deliver are running on your systems, release 11.7 compatibility PTFs must be applied as follows:

- If you are running CA Deliver r11.0/EBC r11.0, apply PTF RO19371, RO12652, and RO29509
- If you are running CA Deliver r11.5/EBC r11.5, apply PTF RO19402, RO13763, and RO31766
- If you are running CA Deliver r11.6/EBC r11.6, apply PTF RO26210

Security and Privileges

Once reports are encrypted, they are secure. We are using AES encryption with 256 or 128 bit keys.

External security interface is provided to CA Top Secret, CA ACF2, and IBM RACF.

Chapter 2: Installation and Upgrade

CA View is installed using the MSM or ESD PAX process.

For the CA View installation steps see your Release 11.7 CA View Installation Guide and the following sections:

- CA View Installation Guide - Chapter 3.
- Upgrade Considerations in this guide.

This section contains the following topics:

The ESD PAX Installation Process

You can obtain CA View in a compressed format (pax.Z file) that enables you to install directly from DASD. This is known as the ESD PAX process.

To install CA View using the ESD PAX process, see the *CA View Installation Guide*.

Changes to Data Set Names

The names of the data sets/libraries have changed. We recommend that you review the following table to determine the impact this may have to your installation:

Original Name	New Name	Description
AHACLS0	ABRMCLS0	CLIST library
AHALOAD	ABRMMOD	Load library
AHAJCL	ABRMJCL	JCL library
AHAMAC	ABRMMAC	Macro library
AHAMBP	ABRMDATA	Banner pages
AHAOPTN	ABRMOPTN	Options library
AHAOLIBD	ABRMPDAN	Danish panel library
AHAOLIBE	ABRMPENU	English panel library

Original Name	New Name	Description
AHAOLIBF	ABRMPFRC	French-Canadian panel library
ABRMOLIBG	ABRMPDEU	German panel library
AHAPNL0	ABRMPNL0	ISPF Panel library
AHAPROC	ABRMPROC	Procedure library
AHASRC	ABRMSRC	Source library
AHATBL0	ABRMTBL0	ISPF tables
AHAXML	AHAXML	CA MSM Deployment and Configuration Services
AHCMAC	ABROMAC	Macro library
AHCLOAD	ABROMOD	Load library
AHCOPTN	ABROOPTN	Optionsl library
AHCPNL0	AHCPNL0	ISPF Panel library
AHCPROC	ABROPROC	Procedure library
AHCSRC	ABROSRC	Source library
AHFLOAD	CBY3LOAD	CA DRAS load library
AHFPROC	CBY3PROC	CA DRAS procedure library
AHFOPTN	CBY3OPTN	CA DRAS options library
AHFSASC	ASARLOAD	SAS/C library
CAICLS0	CVDECLS0	CLIST library
CAIVBP	CVDED133	Banner pages
CAIJCL	CVDEJCL	JCL library
CAILIB	CVDELOAD	Load library
CAIMAC	CVDEMAC	Macro library
CAIOPTN	CVDEOPTN	Options library
CAIOLIBD	CVDEPDAN	Danish panel library
CAIOLIBE	CVDEPENU	English panel library
CAIOLIBF	CVDEPFRC	French-Canadian panel library
CAIOLIBG	CVDEDEU	German panel library
CAIPNL0	CVDEPNL0	ISPF Panel library
CAIPROC	CVDEPROC	Procedure library

Original Name	New Name	Description
CAISRC	CVDESRC	Source library
CAITBL0	CVDETBL0	Banner pages
CAIXML	CVDEXML	CA MSM Deployment and Configuration Services

Global Changes for Release 11.7

Be aware of the following changes that appear throughout this documentation set:

- HAB6 is changed to HAB7
- EB6 is changed to EB7
- XMB6 is changed to XMB7
- SAMPJCL contains the following non-MSM install JCL members:

  BRMAREAD, BRMEDALL, BRMSEDIT, BRM1ALL, BRM2CSI, BRM3RECD, BRM3RECT, BRM4APP, BRM5ACC, BRM6RECP, BRM7APYP, BRM8ACCP

Upgrade Considerations

Be aware of the following:

- CA View Release 11.7 is available to all CA View customers with active maintenance contracts.

  There is no specific license required to upgrade to Release 11.7.
- CA View Release 11.7 is backward compatible with CA View r11, r11.5, and r11.6.

  XMS and CA Deliver direct archival can concurrently browse or archive to CA View Release 11.7, r11.6, r11.5, and r11 databases.
- For upgrades from CA View r11.6 to Release 11.7, be sure that PTF RO30477 is applied to your CA View r11.6 system before you upgrade. This PTF is required to ensure the integrity of the Release 11.7 SMP/E environment during the upgrade process.

See Backward Compatibility for information about encryption compatibilities.

Index