CA View®

Best Practices Guide

Release 12.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- CA Chorus™
- CA 1® Tape Management (CA 1)
- CA ACF2™ for z/OS (CA ACF2)
- CA Deliver™ (CA Deliver)
- CA LPD Report Convergence (CA LPD)
- CA Output Management Web Viewer (CA OM Web Viewer)
- CA Output Management Document Viewer (CA OM Document Viewer)
- CA Spool™ (CA Spool)
- CA Tape Encryption
- CA TLMS® Tape Management (CA TLMS)
- CA Top Secret® Security for z/OS (CA Top Secret)
- CA View® (CA View)
- CA Vtape™ Virtual Tape System (CA Vtape)

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.

Best Practices Guide Process

These best practices represent years of product experience, much of which is based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are truly a collaborative effort stemming from customer feedback.

To continue and build on this process, we encourage users to share common themes of product use that might benefit other users. Please consider sharing your best practices with us.

To share your best *practices, c*ontact us at techpubs@ca.com and preface your email subject line with "Best Practices for product name" so that we can easily identify and categorize them.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Introduction—Streamlined and improved.
- CA View Installation and Configuration Best Practices > Implement a proactive Preventive Maintenance Strategy (see page 11)—Added to the guide.

Contents

Chapter 1: Introduction

The guide provides a brief introduction to the CA Technologies mainframe management strategy and features, and describes the best practices for installing and configuring your product.

The intended audience of this guide is systems programmers and administrators, who install, maintain, deploy, and configure CA View.

Chapter 2: Your Product Installation and Configuration Best Practices

This section contains the following topics:

Implement a Proactive Preventive Maintenance Strategy

CA Technologies formerly delivered product maintenance using Service Packs. We have replaced this model with CA Recommended Service (CA RS) for z/OS, which provides more flexibility and granular application intervals. CA RS is patterned after the IBM preventive maintenance model, Recommended Service Upgrade (RSU). With CA RS, you can install preventive maintenance for most CA Technologies z/OS-based products in a consistent way on a schedule that you select (for example, monthly, quarterly, annually).

We recommend that you develop and implement a proactive preventive maintenance strategy whereby you regularly apply maintenance. You could follow the same schedule that you use to apply IBM maintenance, or you could implement a schedule for CA Technologies products only.

Business Value:

Keeping your products current with maintenance helps your team remain productive and minimize errors while safely protecting your systems. If you do not install preventive maintenance regularly, you risk encountering known problems for which we have published and tested fixes.

Our mainframe maintenance philosophy is predicated upon granting you the flexibility to maintain your sites and systems consistent with industry best practices and site-specific requirements. Our philosophy focuses on two maintenance types. Understanding each type can help you maintain your systems in the most efficient manner.

Note: This philosophy applies to the CA Next-Generation Mainframe Management stack products. For legacy products, contact CA Support for maintenance details.

Corrective Maintenance

Helps you address a specific and immediate issue. This type of maintenance is necessary after you encounter a problem. We may provide a test APAR when a new problem is uncovered, or a confirmed PTF when the problem has been resolved. Your primary goal is to return your system to the same functional state that it was before you experienced the issue. This type of maintenance is applied on an as-needed basis.

Preventive Maintenance

Lets you apply PTFs that we have created and made public. You may have experienced the issues that each PTF addresses. CA RS provides a way to identify all published maintenance that has been successfully integration-tested. This maintenance has been tested with other CA Technologies products, current z/OS releases, and IBM subsystems, such as CICS and DB2. Major CA RS service levels are published quarterly, with updates for HIPER and PE-resolving PTFs that are published monthly. After you test the CA RS level, we recommend that you accept that level before you apply a new CA RS level.

You can initiate a maintenance installation activity at any time. You can then install the current CA RS level of maintenance (recommended) or an earlier level. Additionally, you can install maintenance to support a new hardware device, software upgrade, or function using our FIXCAT method.

For all maintenance, *before* you initiate any maintenance action, obtain the current SMP/E HOLDDATA.

Important! CA Chorus™ Software Manager (CA CSM) - formerly known as CA Mainframe Software Manager™ (CA MSM) - is an intuitive web-based tool that can automate and simplify many CA Technologies product installation and maintenance activities. We strongly recommend that you use CA CSM to maintain your CA Technologies z/OS-based products.

More Information:

To apply preventive maintenance using CA CSM or from CA Support Online on http://ca.com/support, see the *Installation Guide* for your product and the CA CSM online help.

Installation

Use CA CSM to acquire, install, and maintain your product.

Business Value:

CA CSM provides a common way to manage mainframe products. CA CSM provides a web interface, which works with Electronic Software Delivery (ESD) and standardized installation and management of mainframe products. You can use it to download and install CA View.

CA CSM lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. After you use CA CSM to download your product or maintenance, you use the same interface to install the downloaded software packages using SMP/E.

Additional Information:

After you install the product, use the *CA View Installation Guide* to set it up. CA CSM can continue to help you maintain your product.

More Information:

For more information about CA CSM, see the *CA Chorus™ Software Manager* documentation. For more information about product setup, see the *Installation Guide*.

Keep Current on CA Common Services

Be sure that the most current release of CA Common Services is installed.

Business Value:

The latest release of CA Common Services contains the most current infrastructure updates. These updates allow you to use newer features of CA View, including licensing changes, service desk integration, and product health checks. Staying on the current release and service pack of CA Common Services helps you avoid problems encountered by others, getting you up to speed sooner.

More Information:

For more information about CA Common Services, see the *CA View Installation Guide*.

Installation in a Test Environment

Perform your installation and initial evaluations of the product and its components on a test system.

Business Value:

New releases of CA View can be installed in different SMP/E zones or data sets to allow a new release to run on a test system while the old release continues to run on production systems. Evaluating the product in a test environment lets you detect any possible problems before you roll out the product to a production system, which will help ensure a seamless transition to the new release.

Additional Considerations:

After you install the product, use the *CA View Installation Guide* to set it up. CA CSM can continue to help you maintain your product.

More Information:

Always be sure to review any upgrade considerations in the *Installation Guide* prior to upgrading CA View.

Use a Common CA High-Level Qualifier Symbolic

When you are installing more than one CA Mainframe Enterprise Report Management (ERM) Release 12.1 product, we recommend that you use one common high-level qualifier for the '**CAI**' symbolic that is shared by all of the products.

Business Value:

By installing and maintaining a single version of a CA common high-level qualifier, you do the following:

- Reduce your maintenance effort
- Save disk space
- Eliminate the possibility of executing symbolic utilities that might not be up-to-date with the latest maintenance.

Additional Considerations:

Be sure to install CA View Release 12.1 and CA Deliver Release 12.1 into the same SMP/E CSI data set and SMP/E zones.

CA View and CA Deliver both require the EBC Common Component. Placing both products in the same SMP/E environment is the best way to enforce cross-product dependencies and to be sure that both products are at current maintenance levels.

Note:

- While it is a best practice for CA View Release 12.1 and CA Deliver Release 12.1 to share a common SMP/E CSI, CA View Release 12.1 cannot be installed into an SMP/E target and distribution zone that contains a different version or release of CA Deliver and the EBC Common Component.
- If CA View Release 12.1 and CA Deliver Release 12.1 are in the same SMP/E CSI and SMP/E zones, each CSM configuration of CA View and CA Deliver contains the complete set of libraries of the combined products.

If you want to upgrade to CA View Release 12.1 in a shared SMP/CSI that contains a different version or release of CA View and CA Deliver, you can do one of the following:

- RECEIVE CA View Release 12.1 and CA Deliver Release 12.1, then APPLY and ACCEPT CA View Release 12.1 and CA Deliver Release 12.1 simultaneously.
- Install CA View Release 12.1 and CA Deliver Release 12.1 into new SMP/E target and distribution zones.

  Note: You have to allocate new target data sets.

Downward Compatible Libraries and Databases

If there are several CA View databases in your operating environments, use the CA View Release 12.1 target libraries for online access to r11, r11.5, r11.6, r11.7, and Version 12.0 databases until you are ready to version the databases up to the Release 12.1 level. You can also archive and reprint reports and bundles from CA Deliver r11, r11.5, r11.6, r11.7, and Version 12.0.

Note: To use the new features, upgrade your database to Release 12.1.

Business Value:

Downward compatibility with earlier release databases eliminates the need to invest excessive time and resources to immediately upgrade all of the databases simultaneously.

Additional Considerations:

- For CA View databases residing on multiple logical partitions (LPARs), upgrade CA View target libraries to Release 12.1 before upgrading databases to Release 12.1. Databases can be updated independently of each other.
- Use CA View Release 12.1 Interactive System Productivity Facility (ISPF) and Time Sharing Option (TSO) CLIST programming language to access previous release databases.
- The CA DRAS Release 12.1 task can access CA View r11, r11.5, r11.6, r11.7, Version 12.0, and Release 12.1 databases.
- The CA View Release 12.1 cross-memory task can access r11, r11.5, r11.6, r11.7, Version 12.0, and Release 12.1 databases.
- You can perform direct archival to CA View Release 12.1 using CA Deliver r11, r11.5, r11.6, r11.7, Version 12.0, and Release 12.1.

More Information:

See the *CA View Installation Guide* and *CA Deliver Installation Guide*.

Database File Size Considerations

Be conservative when deciding how much space to allocate for the CA View database. It is much easier to increase the size of a database by allocating more extents than it is to reduce the size of a database. The CA View database can be expanded when the product is running to avoid downtime.

Business Value:

Using a minimal amount of disk space for initial CA View database files will contribute to optimal system performance and cost-effective DASD utilization, without impacting active processing operations.

More Information:

Detailed information and formulas for database file size estimation is located in the chapter "Database Utilities", in the SARDBASE ADDDS section of the *CA View Reference Guide*.

Library Authorization

APF-authorize the target library by adding an entry for CAI.CVDELOAD to member PROGxx of SYS1.PARMLIB.

Business Value:

Running an APF-authorized library ensures that CA View executes with the appropriate permissions and approvals.

Data Encryption

Use the CA View ENCRYPTION feature to secure and protect your data.

Business Value:

Protecting your data is of utmost importance. Customers that store credit card data must abide by PCI compliance. One of the most important factors in this compliance is to provide optimum security–data at rest must be encrypted using strong encryption. Reports are encrypted on both disk and tape.

More Information:

For more information about Encryption, see the *Release Notes* and the chapter *Data Encryption* in the *Reference Guide*.

Special Character Support

The report and distribution identifiers are 1-to 32-character fields with a limited set of acceptable characters. Release 12.1 provides additional character support for these fields.

Business Value:

If you use these new special characters and later decide to revert to a previous release, you cannot access these definitions in batch. If you have started using any of these new characters, avoid reverting to a previous release.

More Information:

For more information about special characters, see the *Release Notes*.

Configuration

Expanded Retention Option (ERO)

Use the Expanded Retention Option (ERO) to provide additional retention capabilities for specific reports or groups of reports. Implementing ERO involves the configuration of the ERO initialization parameters and the creation of an ERO table.

Business Value:

Provides the flexibility to specify report retention options at the individual report level. This lets you match report retention to your business needs and Records Management policies.

Additional Considerations:

The base CA View product allows retention based on database generations. A report may be retained in the database for a specified number of generations and on a backup tape for specified number of generations. The Expanded Retention Option allows for more flexibility in assigning retentions to individual reports.

More Information:

See “Initialization Parameters” and “Expanded Retention Option” chapters in the *CA View Reference Guide*.

Expanded Retention Option (ERO) Table Validation

Use the ERO table validation utility every time the table is updated to verify the following ERO table specifications:

- Correct syntax
- Correct report retention settings
- Reports are deleted as expected

Business Value:

Problems in the ERO table can cause reports to be unexpectedly deleted, or retained too long, in breach of your desired target Records Management policy. Use this utility to validate ERO table content so it can easily be debugged and corrected to assist in quick implementation. The validation utility helps secure your valuable archived data and greatly reduces the risk of retention errors.

More Information:

See the chapter “Expanded Retention Option” in the *CA View Reference Guide*.

Use a Catch-all Entry to Determine Where Report Retention is Controlled

Use a catch-all entry as the last entry in the ERO table to make it easier to determine where report retention is controlled. This will enable all reports in the CA View database to be under ERO retention, and you will only have to look in one place to determine report retention specifications.

Business Value:

The catch-all entry is a simple technique to define safe retention criteria to all reports in the database as a safety net, and it significantly reduces the risk of data loss due to human error.

Additional Considerations:

The following SARINIT parameters and ERO table entries can be used as an example for describing the benefits of a catchall entry:

```
NGENT=60
NGEND=3
EROOPT=YES
EROPRO=NEW
PRETAIN=TABLE
```

Include the following entry at the end of the ERO table:

```
/*      ALL GENS=60 DGENS=3
```

Note: GENS=NGENT and DGENS=NGEND.

Since the ERO table is searched in entry sequence, this catchall table entry will match reports that have not been defined by any previous entry. Therefore, every report in the whole database will be under ERO retention and you will only have to look in one place to determine report retention.

Use EROPRO=YES when reports are under ERO retention

The EROPRO parameter should be set to EROPRO=YES unless a large percentage of the database is not under ERO retention. This will efficiently handle new report entries in the ERO table by allowing existing copies of a report to be re-evaluated based on new entries in the ERO table.

Business Value:

The re-evaluation of existing report copies based on the new entries in the ERO table will prevent data loss when report retention is being increased from the standard NGEND/NGENT values.

Additional Considerations:

The default value for the EROPRO parameter is EROPRO=NEW because ERO retention is not activated in CA View by default and it is the most efficient option when reports in the database are under standard retention. However, if you plan to use ERO retention and define a catch-all entry in the ERO table, all reports will be put under ERO retention control and EROPRO=YES becomes the preferred setting.

Use PRETAIN=TABLE When Reports are Under ERO Retention

We recommend setting PRETAIN=TABLE with a catch-all entry in the ERO table. This makes the ERO table statements the single point of control for the retention of the ERO reports.

Business Value:

Using PRETAIN=TABLE provides more efficient utilization of DASD and TAPE resources.

Additional Considerations:

The PRETAIN parameter has two settings - INIT and TABLE. This controls when an expired report is physically removed from DASD storage and logically removed from TAPE storage. When this parameter is set to TABLE, reports are removed when the ERO retention criteria is met. The INIT setting causes reports to remain on DISK and TAPE until both the ERO retention and the NGENT/NGEND settings have met.

Temporary Changes to the ERO Table

Sometimes it is necessary to make temporary changes to the ERO table for a situation such as the need to apply a legal hold to a group of reports. It is important to have a procedure for this situation that will not compromise the retention schedule of the reports.

Business Value:

This technique allows reports to be kept until an external event allows them to be deleted. During a legal action, reports need to be retained until the action is settled. If they are allowed to expire using their normal retention, legal evidence could be destroyed and fines could be imposed.

Additional Considerations:

Assume that a report called STATEMENT is normally kept for 10 years, using the following ERO entry:

```
/STATEMENT ALL RETPD=3650 DRETPD=5
```

It is extremely important not to delete the entry from the ERO table. Unless you have a catchall entry, this will cause all STATEMENT reports to expire from ERO and the PRETAIN=TABLE entry will cause them to be deleted during the next backup cycle. You could change the RETPD parameter to RETPD=9999, but when the legal hold is removed, you would have to change them back to their previous values - RETPD=3650 DRETPD=5

Using comments in the ERO table is a good way to handle this situation. As shown below, an asterisk in column 1 indicates a comment line.

```
************************************************************************
* LEGAL HOLD FOR STATEMENTS REQUESTED
* DATE: YYYY/MM/DD
* CHECK WITH LEGAL BEFORE REMOVING THIS HOLD
************************************************************************
*  STATEMENT-ALL    ALL RETPD=3650 DRETPD=5
/STATEMENT-ALL    ALL RETPD=9999 DRETPD=5
**************************  END LEGAL HOLD  **************************
```

Expanded Access Server (EAS)

Use the Expanded Access Server (EAS) for tape and robotics to enable reports on tape to be browsed, without having to manually load the report back to disk. Activation of EAS is accomplished by specifying the corresponding CA View initialization parameters and customizing the SAREAS task JCL.

Business Value:

EAS provides all CA View users with faster and more efficient process speed for report browsing. Using EAS, viewing from tape is transparent and your users will not have to issue report recalls from tape. In turn you will not waste DASD with reports that have been recalled and then remain on disk, unused.

Additional Considerations:

EAS has the following benefits:

- No need to wait for a LOAD batch job or a tape mount.
- No need for extra Direct Access Storage Device (DASD) space in the disk database to accommodate reports temporarily loaded from tape
- No need to dedicate tape drives to the tape server. The server is allowed to access as many drives as specified. Drives are automatically freed after a specified idle time

More Information:

See the chapter “Configuring”, section entitled ‘Expanded Access Server for Tape and Robotics’ in the *CA View Reference Guide*.

EMC Centera Option

Use the CA View EMC Centera Option to enable the migration and retrieval of reports from a Centera disk cluster. These reports can also be migrated to the CA View database for viewing or printing.

Business Value:

The EMC Centera Option reduces Direct Access Storage Device (DASD) load operations and minimizes performance impact by viewing or printing directly from a Centera cluster. Customers can migrate reports held on tape to Centera, which will save money.

More Information:

See the "EMC Centera Disk Option" Chapter in the *CA View Reference Guide*.

Backup/Cleanup Task

Configure your CA View initialization parameters for automatic scheduling of the CA View Backup/Cleanup task. This task can be configured for scheduling by: day of the week, time of day, and interval (frequency).

Business Value:

The Backup/Cleanup Task helps to ensure accurate and timely scheduled backup and cleanup of data. This greatly reduces the amount of manual time and effort required to maintain database, and keeps associated DASD costs at a minimum.

Additional Considerations:

Backup

The backup task creates copies of your CA View data that can be used for restore in case of database problems. The following initialization parameters control when the backup task is run: TBACKUP, TIME, DAYS, and INTERVAL.

Backup tape types

You can configure your CA View initialization parameters to create up to three different types of backup tapes: Primary, Duplex, and DR (Disaster Recovery) tapes.

- Primary – main backup tape
- Duplex tapes - mirror images of the Primary tapes
- DR (Disaster Recovery) - can be taken offsite for disaster recovery purposes

More Information:

See the “Backing Up and Recovering the Database” chapter in the *CA View Reference Guide*.

Prevent Inadvertent Scratching of Backup Tapes

Consider excluding CA View archive tapes from your tape management abend retention policy to prevent premature scratching of backup tapes.

Business Value:

Help insure the security and integrity of archived data.

More Information:

See the Exclude Archive Tapes from Tape Management Abend Retention section in the “Installation” chapter in the *CA View Installation Guide*.

Forward Recovery Feature

If it becomes necessary to restore the CA View database, use the Forward Recovery feature to recover the SYSOUT data that was archived after the last successful backup was taken.

Business Value:

Prevent loss of reports that had been archived in the CA View database after the last full backup was taken.

Additional Considerations:

With the CA View initialization parameters configured to activate forward recovery, all SYSOUT data archived by the CA View started task is also stored in forward recovery data sets.

Note that Forward Recovery does not include SYSOUT written to the database by CA Deliver direct-to-CA View archival, SARXTD, or by any of the CA View FSS Collectors.

More Information:

For more information, about Forward Recovery, see the “Backing Up and Recovering the Database” chapter in the *CA View Reference Guide*.

External Security Debug Issues

Activate the Security RACROUTE WTO to help with analysis of problems with external security configuration.

Business Value:

The RACROUTE WTO is an effective troubleshooting tool that can be used to help ensure that sensitive report data is secured.

Additional Considerations:

This feature provides informational messages you can use to help diagnose the security problem and can be enabled by adding feature ‘1’ to the FEATURE initialization parameter and running SARINIT.

To disable the WTO, remove the feature number ’1’, run SARINIT to change the feature value in the database, and recycle interactive tasks as needed.

Note: This feature can cause excessive WTO traffic and should only be used for debugging external security issues.

More Information:

Refer to the FEATURE parameter in the ”Initialization Parameters” chapter in the *CA View Reference Guide*.

Requirements for UPDATE Authority to CA View Database

Grant UPDATE authority to all started tasks or users that will be directly accessing the CA View database, including users who will not modify anything in the database. CA View requires UPDATE authority to access the database so that it can save user profile information such as last access date, current access mode, and to retain access information like the last time a report was browsed.

Business Value:

This technique will allow all users to have their required level of access to CA View database without compromising the security of the data.

Additional Considerations:

Cross-Memory (XMS) users do not need UPDATE access. In this case the ACID associated with the Cross-Memory task will need UPDATE authority. After the users gain access, their authority to perform online functions is controlled by the security rules that have been built.

Native PDF Indexing

We recommend using the PDF FSS collector to collect, archive, and index PDF reports. Once collected, the PDF report can be viewed from the CA OM Web Viewer. If the PDF report is indexed, individual sections of the report can be viewed by selecting indexes through cross-report selection.

Business Value:

An increasing number of applications are producing PDF as an output format. Use the power of the mainframe and CA View to index and store PDF documents. If a PDF file is a concatenation of many customer statements, indexing will save time and enable the user to quickly retrieve an individual customer statement.

Additional Considerations:

After establishing your PDF FSS Collector JES printer and proc, (see the *CA View Reference Guide,* chapter entitled 'PDF Indexing in CA View' for details), set up the PDF Indexing member for your PDF report. It is in this member that you instruct the PDF Collector how to index the report. Initially you will specify XYDUMP=YES to produce a PDF Report that displays which fields within the PDF document can be indexed and their associated X and Y coordinates. After reviewing the PDF Report, you will modify this PDF Indexing member specifying and index name and the coordinates of the data to be indexed.

The report is processed again using the modified Indexing member and a list of these index values can be seen in CA Output Management Web Viewer. The individual indexed report page can now be selected for viewing.

More Information:

For more information about the CA View PDF FSS collector, see the chapter "PDF Indexing in CA View" in the *CA View Reference Guide*.

Enhanced Flexibility for AFP Printing

If you archive AFP reports to CA View, use the 'INCLUDE AFP RESOURCE' field to determine whether AFP reports collected by the ACIF FSS collector should be reprinted with or without the archived ACIF resources. This field allows the user to override the system default value for the ACIFRES initialization parameter.

Business Value:

End users can now enjoy greater flexibility when printing their AFP reports. This can enhance their productivity because a user saves time when deciding how their AFP report should be printed.

Additional Considerations:

A field, 'INCLUDE AFP RESOURCES', has been added to the online and batch reprint panels to allow override of the ACIFRES initialization parameter setting. When archived resources are excluded, PSF will use current resources found in either the USERLIB or printer data sets.

More Information:

For more information about the ACIFRES initialization parameter, see the chapter "Initialization Parameters" in the *CA View Reference Guid*e. For more information about the 'INCLUDE AFP RESOURCES' field on the reprint panels, see the chapter 'Printing Output' in the *CA View User Guide*.

Interfaces and Integration Points

This section discusses the interfaces and integration between CA View and CA Deliver, CA Output Management Web Viewer, CA Spool, CA LPD, CA security products, and CA tape management products.

Integrate CA Deliver with CA View

Use CA Deliver in conjunction with CA View as a complete Output Management solution for managing reports. CA Deliver reports can be archived directly to the CA View databases, viewed online, and backed up on storage media. All CA Deliver report attributes and distribution data are retained in the CA View database.

Business Value:

Creating a complete solution optimizes report management. By implementing an automated archival and retrieval system you can automate day-to-day report management and minimize time-consuming manual tasks and lower document delivery costs. Viewing reports online and printing fewer reports saves cost and reduces time spent reformatting, tracking, handling and rerunning reports.

Interface with CA Output Management Web Viewer

Use CA Output Management (OM) Web Viewer as a single Web-based point of access to all enterprise documents stored in CA View. In addition to being able to view reports originating from the mainframe, CA OM Web Viewer enables online web viewing of all report types that cannot be viewed from the 3270 panels, such as AFP and PDF reports.

Business Value:

CA OM Web Viewer provides immediate, secure, web-based access to enterprise documents, protects your organizations current investment in internet or intranet-accessible hardware and software, and can significantly reduce printing costs.

Additional Considerations:

CA OM Viewer is the solution used to view all of the documents that are archived to the CA View database, including reports distributed by CA Deliver for the CA Deliver Email Notification feature.

Information on configuring CA OM Web Viewer with CA View can be found in the *CA Output Management Web Viewer Administration Guide* and the *CA DRAS Operations Guide*.

Use CA Spool Integration for More Effective Document Management

Integrate CA Spool with CA View to archive reports directly from CA Spool into the CA View database. CA Spool has the ability to write all types of print files, including PDF/HTML/RTF wrapped text files, directly to a CA View database for archiving and viewing.

Business Value:

CA Spool integration reduces JES resource and JES spool dataset utilization, and enables centralized control of the CA View FSS Collectors to simplify management of these resources. CA Spool can also transform reports into PDF format, which can be used to take advantage of the CA View PDF Indexing feature, allowing quick and easy report navigation.

Additional Considerations:

CA Spool can be integrated with CA View in the following ways:

- CA Spool printer node definitions can be configured to directly archive reports into the CA View database.
- CA View FSS Collectors can be defined and controlled directly from CA Spool.
- CA Spool output can be transformed to PDF format and directed to the CA View PDF Indexing Collector FSS to be archived and indexed into the CA View database.
- CA Spool printer nodes can be defined within CA View using the DEF DEV command for initiating reprints from CA View back to the printer nodes.

More Information:

Refer to the following for information:

- *CA View Installation Guide* section entitled ‘Install the Interface with Print Management’
- *CA View User Guide* chapter ‘System Administration, Defining Online Specifications’, ‘Defining and Adding Output Devices’ and ‘ Defining Attributes for Print Management’.
- *CA Spool Customization Guide* sections entitled ‘SAR Print Driver’ and ‘CA View Print Requests’
- *CA Spool System Guide*, sections entitled ‘SAR Print Driver’ and ‘CA View Interface’

Use the CA Spool LPD Interface for Distributed File Archival and Viewing

The CA Spool LPD Interface is a component of CA Spool that supports the TCP/IP LPR/LPD remote print protocol and makes it possible for mainframe report management products and spooling systems to receive reports and print files from all other platforms within the enterprise.

CA View provides a repository option for the storage and viewing of distributed file types. A distributed file type is any associated or native file type that is not created in a z/OS environment. The files can originate from any platform, including Windows, UNIX, or Linux, and are transferred to the z/OS platform using the native LPR command. These distributed file types can be viewed directly from this repository using the CA OM Web Viewer.

Business Value:

The CA Spool LPD Interface empowers end users with the ability to view and print distributed reports from one central repository, the CA View database.

The CA Spool LPD Interface enables you to use the CA View database as the one central repository for all of your enterprise documents, and empowers end users to view and manage multiple file types. This can result in a more unified and integrated output management environment.

More Information:

For complete information see the following:

- 'TCP/IP LPD Interface' and 'CA View Print Requests' in the *CA Spool Customization Guide*
- 'LPD Interface' in the *CA Spool System Guide*

Use CA ACF2 or CA Top Secret with the CA View external Security Interface

Protect and secure your business reports and data stored in the CA View database and tapes with CA ACF2 and CA Top Secret security systems. The security features in CA View provide extensive and complete security functions for every type of end-user database access.

CA View can be configured to activate security calls to CA ACF2 and CA Top Secret. CA View performs external security authorization based on a resource type and name. The resource type represents a predefined name, and the resource name identifies the data being accessed within the CA View database. The resource type and name correspond to the class and entity parameters of the RACROUTE macro. If a user is not authorized to access specific data within the CA View database, a violation is recorded and access is denied.

Business Value:

Prevent unauthorized access to your mission critical reports and data. Track and audit any violations found.

More Information:

For complete information about configuring CA View for CA Top Secret and CA ACF2, see the *External Security* chapter in the *Reference Guide*.

CA 1, CA TLMS, CA Vtape, CA Tape Encryption

Utilize CA 1, CA TLMS, and CA Tape Encryption to manage and protect your CA View reports stored on CA View archive tapes.

CA View backup tapes can be written to tapes owned by CA 1, CA TLMS, CA Vtape, or other third party tape management systems.

In addition, CA Tape Encryption can be used as a convenient and secure method for automating the encryption and decryption of confidential data on CA View tape volumes in the z/OS operating environment.

Business Value

CA Tape management products help provide complete and automated management of your CA View tape datasets. CA Tape Encryption provides an additional layer or protection for your critical business data and reports.

Index

C

I