

OS/390 Considerations

This section describes OS/390 considerations.

It covers the following topics:

- OS/390 Access Method Modules
 - OS/390 Accounting
 - OS/390 Common JES Interface
 - OS/390 Security Considerations
 - Setting Up RACF Security for Operator Commands on OS/390
 - REVIEW Considerations
-

OS/390 Access Method Modules

There are two access method modules available under OS/390:

- OS/390 Access Method Module for CA-LIBRARIAN
- OS/390 Access Method Module for PANVALET

OS/390 Access Method Module for CA-LIBRARIAN

If CA-LIBRARIAN is available at your site, you can install the CA-LIBRARIAN access method module as follows:

1. Set &LIBRMOD in source NATPAML to the name of the CA-LIBRARIAN batch module and set &LIBROPT to the default parameters of the batch module. These options can be modified dynamically in the Natural programs using the OPTION field in the views LIB-UPDATE and WRITE-FILE.

Set &SECALOC in source NATPAML to the number of blocks for secondary allocation. The default of 10 blocks is normally sufficient, but this can be increased if you receive a NAT5995 error while writing LIBRARIAN members.

2. Assemble the module NATPAML and link-edit it using the CA-LIBRARIAN load library. The link attributes NON-REUSABLE and NON-REentrant must be set. The module name must be NATPAML, no alias is necessary. The CA-LIBRARIAN MACLIB must precede the Entire System Server source library so that the correct FAIR m CA-LIBRARIAN macro is used.
3. Add startup parameter PRODUCT=L to the Entire System Server startup parameters.

When accessing CA-LIBRARIAN using Entire System Server views, users must specify the product code L in the PRODUCT field.

OS/390 Access Method Module for PANVALET

Set &SECALOC in source NATPAMP to the number of blocks for secondary allocation. The default of 10 blocks is normally sufficient, but this can be increased if you receive a NAT5995 error while writing PANVALET members.

OS/390 Accounting

The Entire System Server can optionally collect accounting information. This information is available through the view NATPROC-USERS (see also the LOOP startup parameter in the section Startup Parameters).

For OS/390 only:

The layout of this user SMF record is as follows:

Location		Length	Format	Contents	
Dec	Hex				
0	0	2	Binary	Length or record.	
2	2	2	-	Reserved.	
4	4	1	Binary	System indicator:	1 - VS1
					2 - OS/390
					6 - XA
5	5	1	Binary	Record type; value is stated in SMFRECORD parameter.	
6	6	4	Binary	Time in 100th of a seconds, record was moved to SMF buffer.	
10	A	4	Packed	Date record was moved to SMF buffer (00YYDDDF).	
14	E	4	Character	SYSID.	
18	12	8	Character	User ID.	
26	1A	4	Binary	CPU used in units of 26ths of a second.	
30	1E	4	Binary	Number of I/Os.	

An SMF record is written:

- if a user logs off him/herself;
- if a user is logged off due to inactivity;
- if SMFTIME parameter was set and this time window popped;
- if Entire System Server terminates.

In all cases, the SMF parameter must be set.

OS/390 Common JES Interface

The former JES2 and JES3 interfaces have been rewritten and integrated into a Common JES Interface, exploiting the OS/390 MVS subsystem interface functions 79 (SYSOUT API) and 80 (Extended Status). However, for JES3 some restrictions apply (see Restrictions for OS/390 JES3 below), that will be lifted with a future release.

The Common JES Interface needs not be assembled during installation and therefore is distributed only as load module. It currently supports all JES2 and JES3 releases from OS/390 V2R6 to V2R10. Support for new releases of JES2 and JES3 will be added via problem solutions.

All required security checks are done within the Common JES Interface and the SYSOUT API implementations using the SAF router interface. Therefore the former security exit JESVRACF is no longer required. However, for compatibility reasons, a dummy exit is provided that may be used to perform additional authorization functions.

For JES3 only, earlier releases of Entire System Server required that the Dynamic Support Program (DSP) IATUQJ3 was installed as a USERMOD in JES3 and the DSPDATA file was allocated to both JES3 and Entire System Server. As this type of communication is not used by the Common JES Interface, you may RESTORE the USERMOD and delete the DSPDATA file when you no longer use an earlier release of Entire System Server.

Restrictions for OS/390 JES3

- Input JCL (JESJCLIN) and SYSIN Datasets are not selectable. (READ-SPOOL, SPOOL-FILES)
- Active SYSOUT Datasets (not yet closed and freed) are not selectable. (READ-SPOOL, SPOOL-FILES). This includes the active SYSLOG (CONSOLE-LOG).
- UPDATE authority is required to access spool datasets. (READ-SPOOL, SPOOL-FILES)
- No parallel access to spool datasets from different tasks. (READ-SPOOL, SPOOL-FILES)
- Entire Output Management (NOM) does not work due to the restrictions described above.

If you are running OS/390 JES3 and your applications require these missing functions or you are using Entire Output Management (NOM), you will have to continue to use Entire System Server Version 2.2.2, until the missing functions are implemented in the next maintenance level or release of Entire System Server.

OS/390 Security Considerations

Security Logon

The Entire System Server region accesses datasets and other resources as requested by the Natural user. Therefore, if a security system is installed (identified by the SECURITY startup parameter), the Natural user must identify himself or herself to Entire System Server before any view can be accessed. A logon operation must be performed, specifying the user's system user ID and password. SECURITY will be called to validate these parameters. If validation is successful, SECURITY will build a control block for the user. This control block will be used for future validations.

If the user attempts to access a view before logging on, Response Code 510 (LOGON REQUIRED) will be returned. However, if the startup parameter AUTOLOG is set to YES, an implicit logon is performed as part of the first user request. A password is only required if the Natural user ID does not match the user ID defined in the SECURITY system.

When a view requests access to resources such as datasets, batch jobs, etc., SECURITY will be called to check whether access is allowed (see the following section). If access is not allowed, the user will receive an appropriate error message.

The Entire System Server online tutorial contains a sample logon program that uses the view NATPROC-LOGON.

The logon operation is not needed if Entire System Server is used in single-user mode.

If no security system interface is requested (SECURITY=NONE), no security check is performed: all logon attempts will be successful. In this case, each attempt to access an object which is protected by security is treated in the same way as defined for the Entire System Server started task.

If ACF2 is installed at your site, you must define Entire System Server as the multi-user address space (using the parameter MUSASS in ACF2).

If TOP-SECRET is installed, the following parameters must be set:

```
FAC (USERS=NAME=PROCESS)
FAC (PROCESS=ACTIVE,NOASUBM)
FAC (PROCESS=NOABEND,AUTHINIT)
FAC (PROCESS=MULTIUSER,WARNPW)
FAC (PROCESS=MODE(FAIL),PGM=NAT)
FAC (PROCESS=UIDACID=8, ID=P)
```

Setting Up RACF Security for Operator Commands on OS/390

Assemble the distributed source for the OPRVRACF and VTMVRACF exits with conditional assembly variable &RACF set to **0**, in order to generate the RACROUTE code for validating the OPERCMDS resource class. Set the &JESC to your JES command character. The default is the dollar sign (\$).

If &RACF is set to 1, the OPERATIONS flag in the ACEE control block will be examined instead of the RACROUTE approach.

REVIEW Considerations

If Review 4.1 and Entire System Server 3.1 (OS/390 only) are installed, each of the following steps has to be performed.

For OUTGOING Calls:

Outgoing calls for Entire System Server are Adabas calls from the Entire System Server's address space to any Adabas database or any other Entire System Server.

An Entire Operations Monitor, for instance, is running as a Natural subtask in Entire System Server's address space and should be monitored via REVIEW:

1. Edit ADALNA5 from the Adabas source lib and change the value of LRVINFO from 0 to 256 (workarea size for REVIEW).
2. Apply the zap RD41327 if REVIEW 41 is used.
3. Assemble and link with REVIEW:

```
INCLUDE SYSLMOD(ADALNA5)
INCLUDE REVLIB(RDBLXMVS)
NAME ADALNA5(R)
```

This load module must be REUS but not RENT.

4. Link the Natural subtask with ADANPR from Entire System Server.
5. Edit Entire System Server's startup parameter module and add the string ADAPRM=ON to the Natural startup parameter, i.e.:

```
STRNTNP1=AUTO=OFF,ADAPRM=ON,STACK=(LOGON SYSSAT NCLMON NCLMON)
```

6. Edit Entire System Server's startup parameter module and set the following:

```
UEX4=RAOSEXIT
```

For INCOMING Calls:

Incoming calls are Adabas calls from any Natural or non-Natural system to one Entire System Server:

1. Edit Entire System Server's startup parameter module:
Set all LOGGING parameters to YES (LOGGING; LOGCB; LOGFB; LOGRB; LOGVB; LOGSB).
2. Include a CLOG dataset in the JCL. Attributes for this file are the same as for an Adabas command log file (see your Adabas documentation).
3. Edit Entire System Server's startup parameter module. Set the following:

UEX4=RAOEXIT