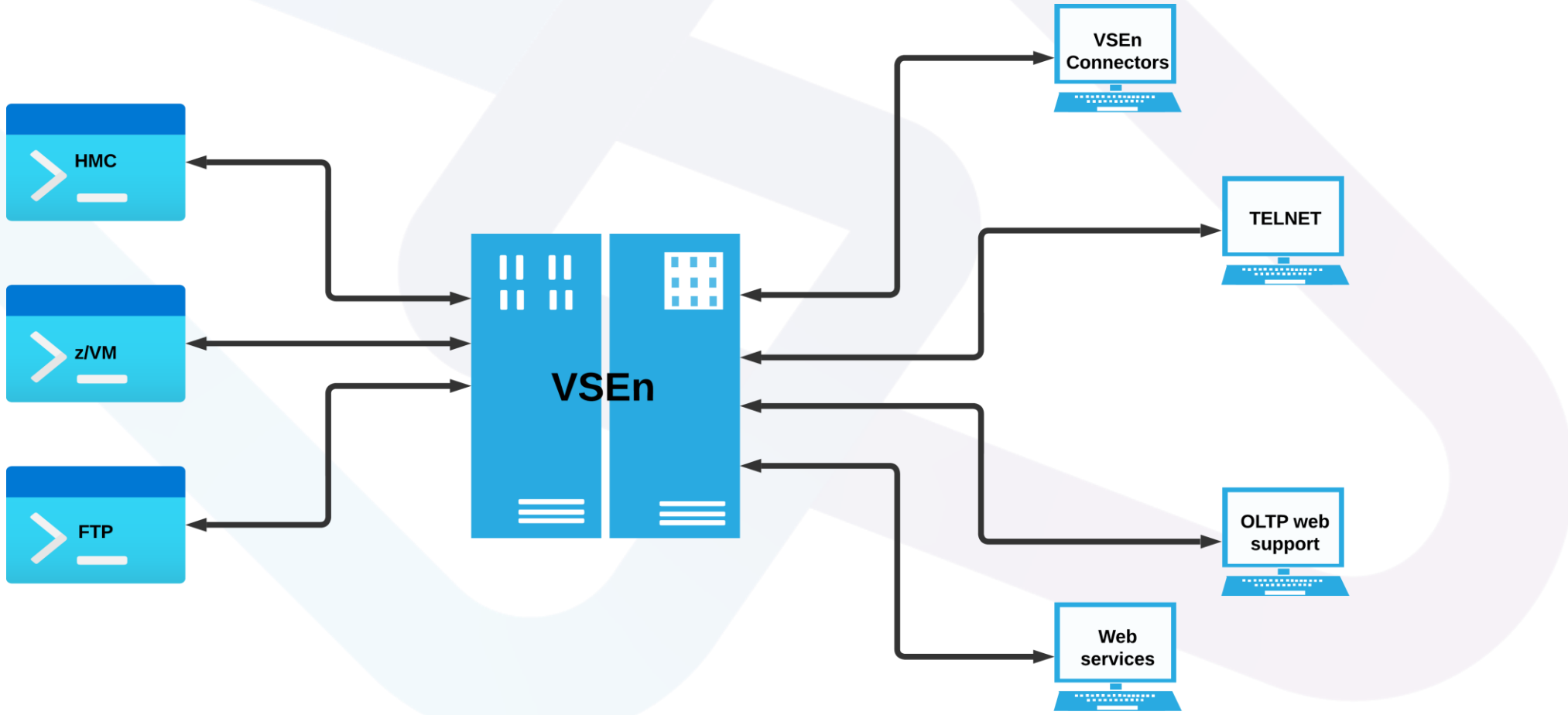
Securing 21CS VSE^{n}

Shahin R Krishna
VSE^{n} Software Engineer

Why & What?

- Safeguarding Data & Access
  - Ensure that secret data remains confidential.
  - Prevent unauthorized modifications
- System Protection
  - Guard against accidental damage
  - Control unauthorized job submissions
- Securing Remote Access
  - Control nodes within the network from connecting to VSE^n machine

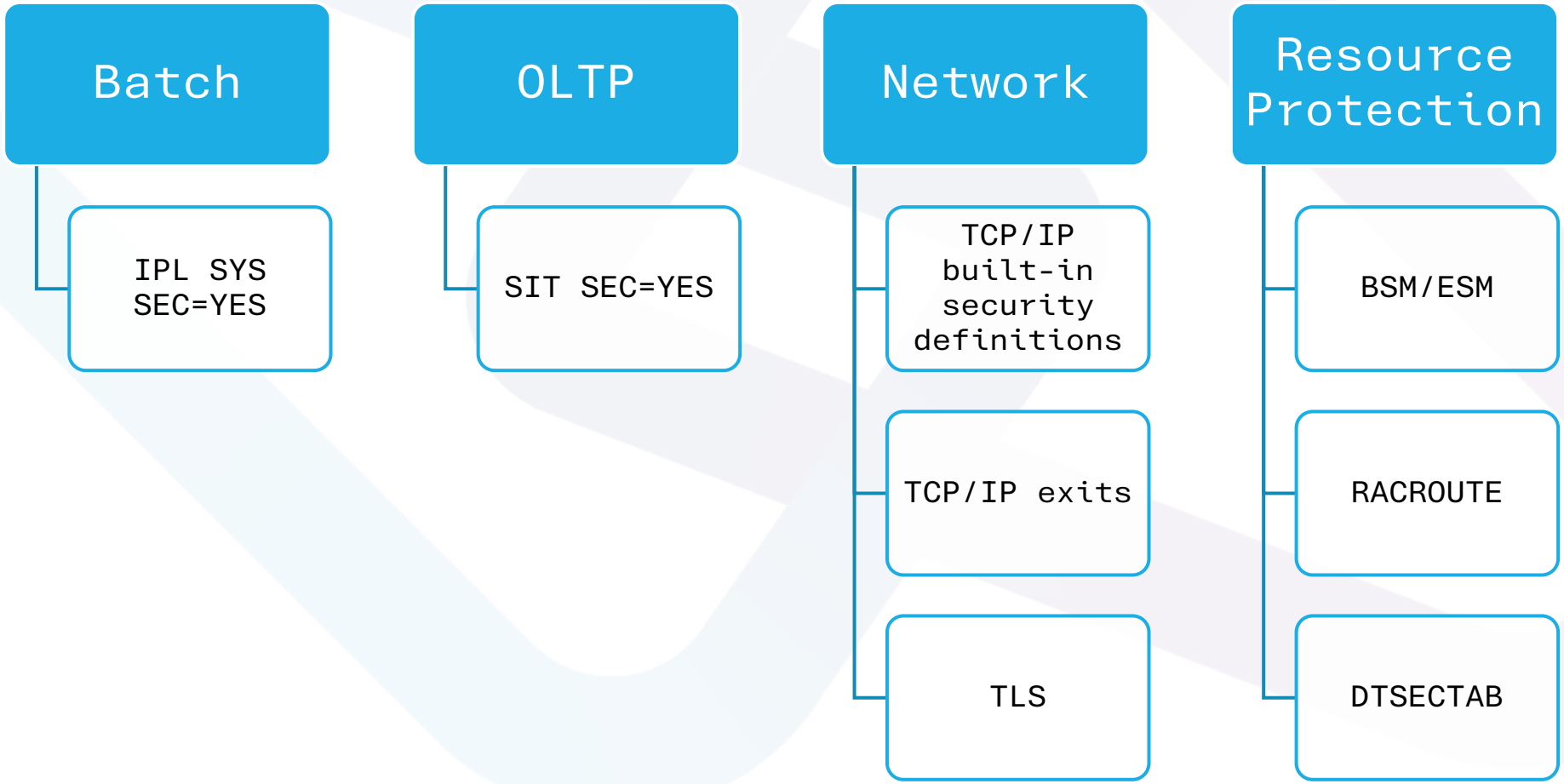
Access Paths to VSE^{n}



VSE^{n} Security Components

- **Basic Security Manager (BSM)**
- System Authorization Facility (SAF)
- RACROUTE (interface to SAF)
- DTSECTAB
- DTSFILE (ICCF)
- LDAP utilities

How to Secure?

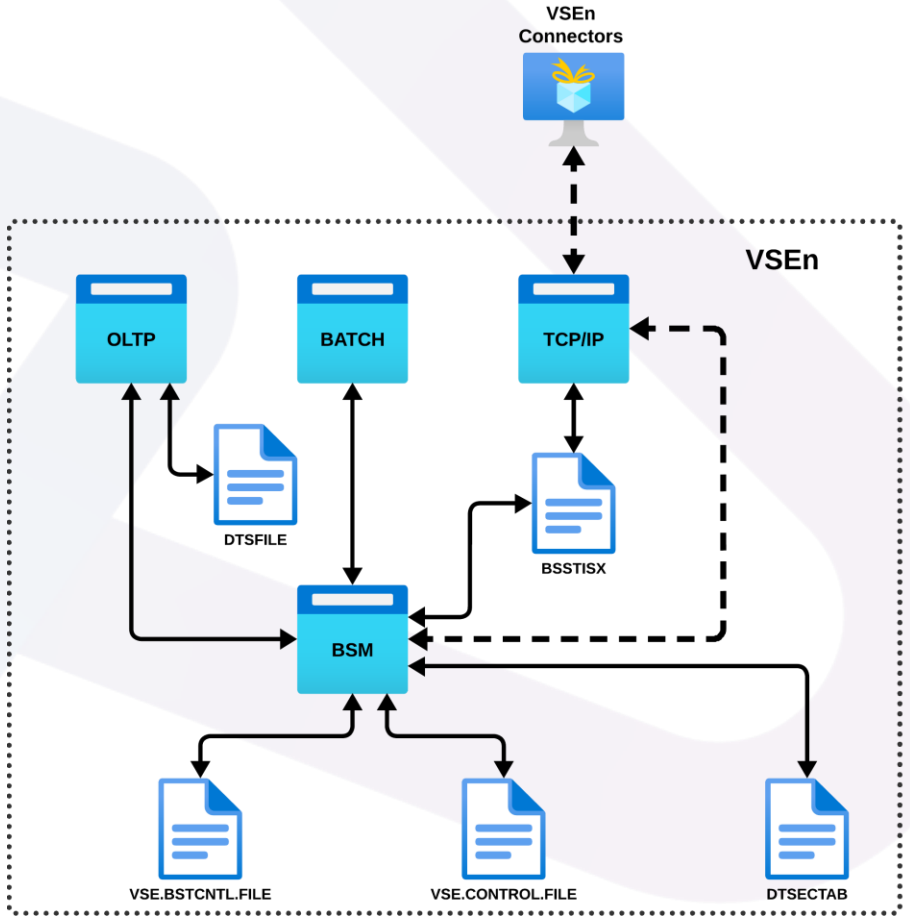


Basic Security Manager (BSM)

- Default Security Manager in VSE^n
- Built to provide basic security functions
- Receives & processes RACROUTE requests from SAF
- Always activated during start, independent of SYS SEC=YES|NO

Basic Security Manager (BSM)

- Online/Sign-on Security
- Batch Security
- OLTP Transactions & Resources Security
- MQ for VSEⁿ Resources
- Logging & reporting – DTSECTAB Resources
- JCL statements
- Reports



BSM Startup

Securing Manager (BSSINIT) must initialize before other partition or POWER are active.

BSSINIT will fail, if there are other partitions active.

Static partition is required for Security Server.

Use SYS ESM=phase for External Security Manager.

If no ESM is started, BSM is activated.

For SYS SEC=YES with ESM, DTSECTAB protection is active until ESM is initialized.

BSM Repositories

VSE Control File (IESCNTL)

- VSAM KSDS
- User Profiles

DTSECTAB

- Link-edited as PHASE
- Resources – Libraries, Sub libraries & members
- 3 User IDs – FORSEC, DUMMY & VCSRV

BSM Control File (BSTCNTL)

- Resource Profiles
- Password Rules
- User Groups

RACROUTE Interface

- External Interface to SAF
- Used by Resource Managers & Subsystems
  - OLTP
  - VSE^n Connector Server
  - SMDMU for VSE^n
  - TCP/IP Security Exits
  - Interactive Interface Sign on

Batch Security

IPL: SYS SEC=YES

- * $$ JOB JNM=MYJOB,….,SEC=(user,password)
- // ID USER=user,PWD=password
  - User ID & Passwords are verified against
    - DTSECTAB
    - RACROUTE (Security Manager)
- Subsystems like VSAM,LIBR, etc., will use DTSECTAB to verify the access rights
- When submitted from ICCF
  - No need to specify userid or password explicitly (unless required to access a restricted resource)
  - Inherits the userid &* password of the ICCF user

Batch Security with JCL statement check

```
IPL: SYS SEC=YES,JCL
```

- FACILITY class profiles used for JCL statement control
  - IBMVSE.JCL.ASSGN.PERM
  - IBMVSE.JCL.LIBDEF.PERM
  - IBMVSE.JCL.LIBDROP.PERM
  - IBMVSE.JCL.OPTION.PARSTD
  - IBMVSE.JCL.OPTION.STDLABEL
- Minimum access right required : READ

BSM Resource Profiles – Class: FACILITY

JCL

- ❑ IBMVSE.JCL.ASSGN.PERM
- ❑ IBMVSE.JCL.LIBDEF.PERM
- ❑ IBMVSE.JCL.LIBDROP.PERM
- ❑ IBMVSE.JCL.OPTION.PARSTD
- ❑ IBMVSE.JCL.OPTION.STDLABEL

VSAM (IDCAMS)

- ❑ IDCAMS.GENERAL

SMDMU

- ❑ DITTO.DISK.INPUT
- ❑ DITTO.DISK.UPDATE
- ❑ DITTO.FUNCTION.*fn*
- ❑ DITTO.OAM.OUTPUT
- ❑ DITTO.OAM.UPDATE
- ❑ DITTO.OTHER.ALL
- ❑ DITTO.SPOOL.CONTROL
- ❑ DITTO.SPOOL.DISPLAY
- ❑ DITTO.TAPE.DUPLICATE
- ❑ DITTO.TAPE.INPUT
- ❑ DITTO.TAPE.OUTPUT
- ❑ DITTO.TAPE.UPDATE
- ❑ DITTO.VSAM.UPDATE

VSEⁿ MQ

- ❑ MQADMIN
- ❑ MQCMDS
- ❑ MQCONN
- ❑ MQNLIST
- ❑ MQQUEUE
- ❑ MXTOPIC

OLTP

- ❑ TCICSTRN
- ❑ MCICSPPT
- ❑ FCICSFCT
- ❑ JCICSJCT
- ❑ SCICSTST
- ❑ DCICSDCT
- ❑ ACICSPCT
- ❑ SURROGAT

BSTADMIN

- Batch interface to BSM
  - From system console
  - A batch job
- BSM commands:-

Resource Class Management	Group Management	Information Display	Generic Commands
ADD | AD	ADDGROUP | AG	LIST | LI	USERID | ID
CHANGE | CH	CHNGROUP | CG	LISTG | LG	PERFORM | PF
DELETE | DE	DELGROUP | DG	LISTU | LU	
PERMIT | PE	CONNECT | CO	STATUS | ST	
	REMOVE | RE		

Ref: VSEn 6.3 Administration - Chapter 30

BSTSAVER Utility

- Builds BSTADMIN commands representing current BSM status

```
// EXEC BSTSAVER,PARM='library.sublibrary.member.type'
```

  - To create backup of BSM control file
  - Migrate content of BSM control file to current VSE^{n} release

- To restore: provide the backup file as input to BSTADMIN

```
// EXEC BSTADMIN
* $$ SLI MEM=member.type,S=library.sublibrary
/*
```

Ref: VSEn 6.3 Administration – Chapter 30

BSTXREF Utility

- BSM Cross Reference report generation
  - User IDs `PARM='USERID=[user|*][,L]'`
  - Groups `PARM='GROUP=[group_name|*]'`
  - Access Control classes `PARM='ACC=[1…32|*]'`
  - Resources controlled by UACC definitions `PARM='UACC'`
  - Undefined user IDs found in groups and access list of resource profiles. `PARM='INCONS[,L]'`
- Can invoke from
  - System Console
  - Batch job

BSTXREF Sample

```
// EXEC BSTXREF,PARM='ACC=*'
```

IUI FASTPATH - 285

```
IESADMBSXT              BSM CROSS REFERENCE REPORT


OPTIONS:  1 = REPORT   2 = DETAILED REPORT

   OPT    REPORT NAME

    _     Information about user-ID *________
    _     Information about group *________
    _     Information about access control class *_ (1..32)
    _     Information about all user-ID inconsistencies
    _     Information about UACC that allow resource access


   * = ALL




PF1=HELP                          3=END
```

Ref: VSEn 6.3 Administration - Chapter 26

Audit-Logging & Reporting

- Access attempts to protected resources can be logged
- Failed logon attempts
- Who accessed what and when
- Summary of logs
- Detailed report of all access attempts
- Logging of BSTADMIN commands
- Logging of DTSECTAB resources

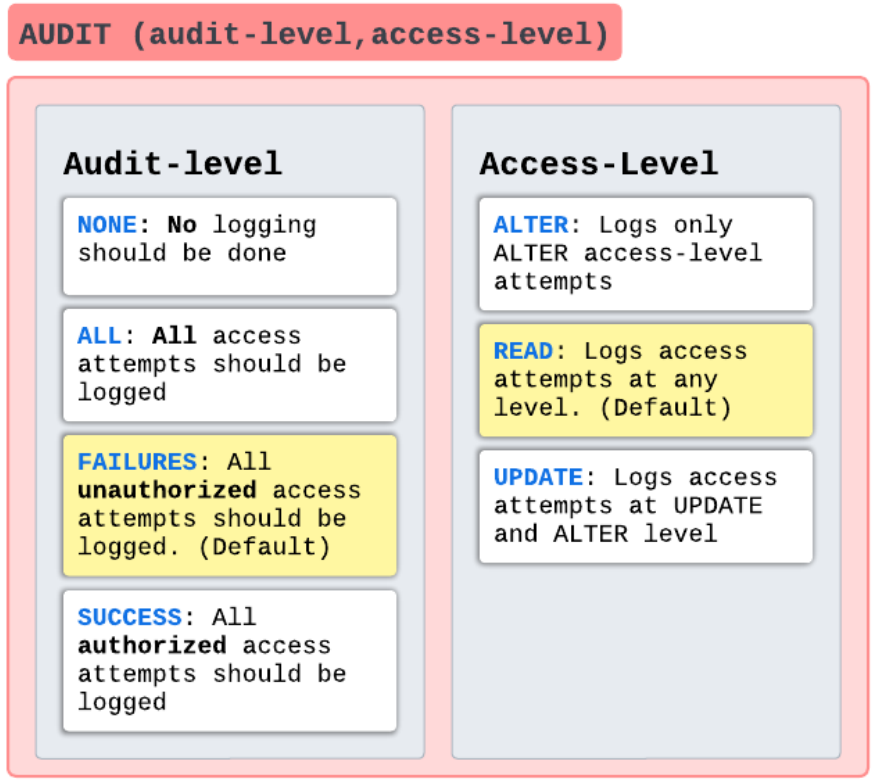
Ref: VSEn 6.3 Administration – Chapter 40

Audit-Logging & Reporting

- The OLTP issues a RACROUTE request each time a user wishes to access a resource.
- The BSM processes these RACROUTE requests and creates SMF80 records.
- The DMF, supplied with the OLTP for VSE^n, collects and stores these SMF80 records.
- Use utility DFHDFOU to dump audit records to an intermediate file (SMF80)
- Use utility BSM Report Writer (BSTPRWTR) to create report
  - A detailed listing of the processed records.
  - A summary of the user entries.
  - A summary of the resource entries.
  - A summary of security commands.
  - A general summary.

Audit-Logging & Reporting

- The BSM resource profile should be defined with AUDIT option.



AUDT for VSE^{n} (IBM ACLR)

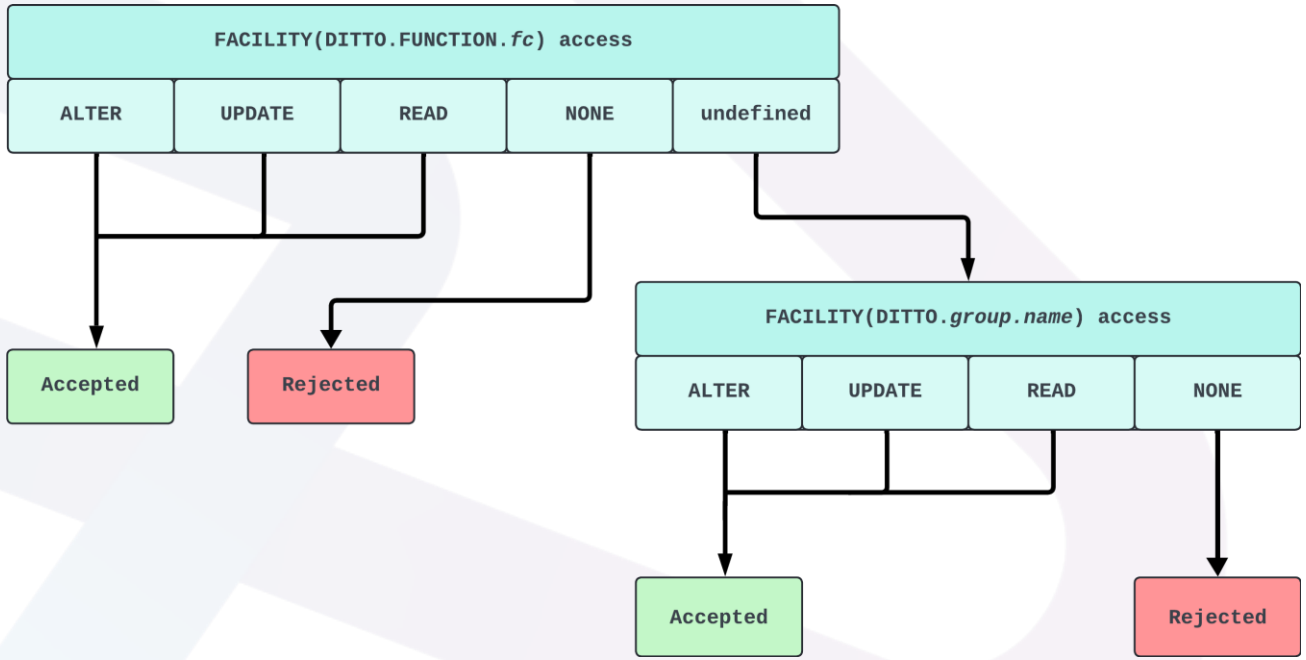
- Logging of Access Control events
  - Access to disk/tape files
  - Access to library/sub-library
  - Access to library member
- Enables auditing of system resource accesses
- Formatted report
  - Identify access violations and the user responsible for them.
  - Find security weak points.
  - Adapt access control measures to changing conditions.
  - Recognize a need for corrective action by management.
  - Use the system more efficiently.

SMDMU Security using DITSECUR

- SMDMU uses FACILITY profiles to protect resources
  - Ensure that batch security is active.

    IPL SEC=YES
  - Ensure that FACILITY profiles are defined

SAF controls access to SMDMU functions



Connector Security

- VSE^n Connector Server acts as a Resource Manager
  - Issues RACROUTE calls for
    - User verification
    - Resource security
  - Connector user ids are same as for OLTP & Batch
  - No additional user profile setup is required
  - Multiple logons with same userid is possible
  - VCS runs under a special userid - VCSRV
    - Defined in DTSECTAB

Connector Security

- Additional restrictions can be enforced on
  - User IDs
  - IP address

```
IP   = *,                LOGON = ALLOWED
* IP = 9.164.123.456,    LOGON = DENIED
* IP = 9.165.*      ,    LOGON = DENIED
* IP = 10.0.0.*     ,    LOGON = ALLOWED
* IP = 2001:0DB8:85A3:0000:0000:8A2E:0370:7334 , LOGON = DENIED
* IP = 2001:0DB8:85A3:0000:0000:8A2E:0370:*    , LOGON = ALLOWED
* ============================================================
* THESE USERS ARE ALLOWED OR DENIED TO LOGON
* UNCOMMENT THE SAMPLES AND MODIFY THEM
* ============================================================
USER = *,                LOGON = ALLOWED
* USER = BOBY,           LOGON = ALLOWED
* USER = SYS*,           LOGON = DENIED
```

TCP/IP Security

TCP/IP for VSEⁿ

Own Definitions

```
DEFINE USER,ID=user,PASSWORD=pwd
```

VSEn BSM Security Exit

```
SECURITY ON,PHASE=BSSTISX,EXIT=ON
```

IPV6 for VSEⁿ

Own Definitions in BSTTSCTY.T

```
FTP-USER userid password
FTP-ACCESS ....
FTP LUSER ....
```

VSEn BSM Security Exit

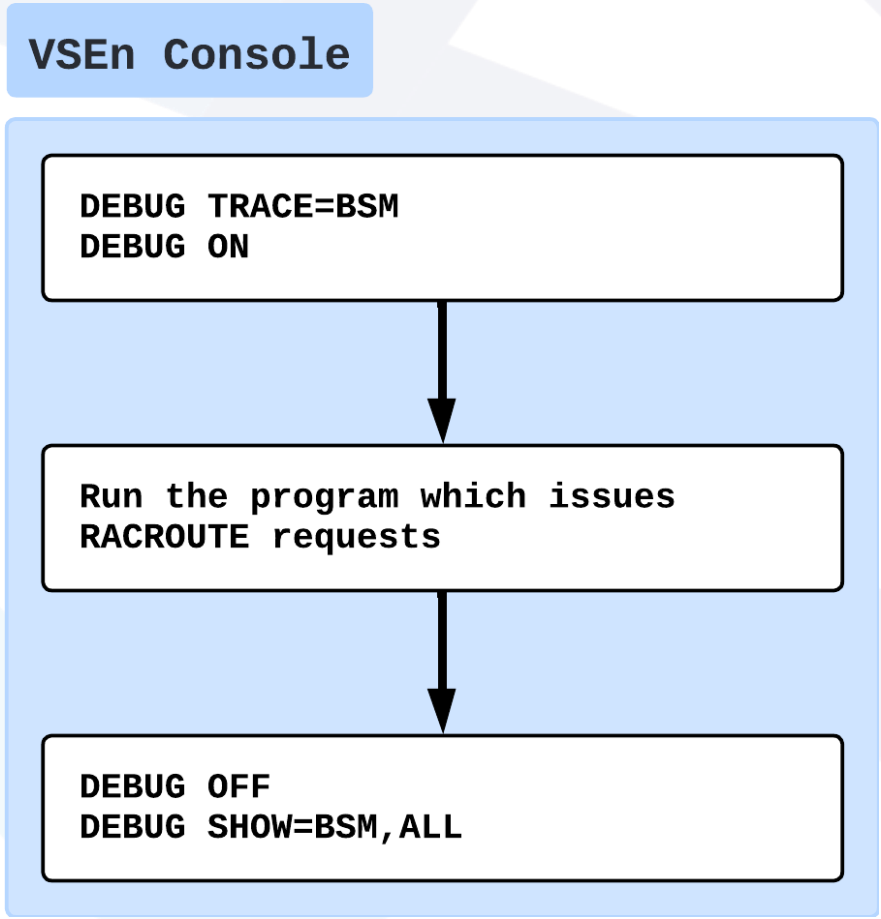
```
Copy BSTTFTS1.PHASE to a lib.slib as
BSTTFTSX.PHASE

Add BSSTISX command to BSTTFTPS startup commands
```

BSM Startup Recovery

If an active Security Manager doesn't allow to recover from a problem

- Performing these steps will prevent BSSINIT from starting a security manager
- Re-IPL is required to start the Security Manager again

Tracing RACROUTE Requests



Thank You