VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Securing JES Resource Classes

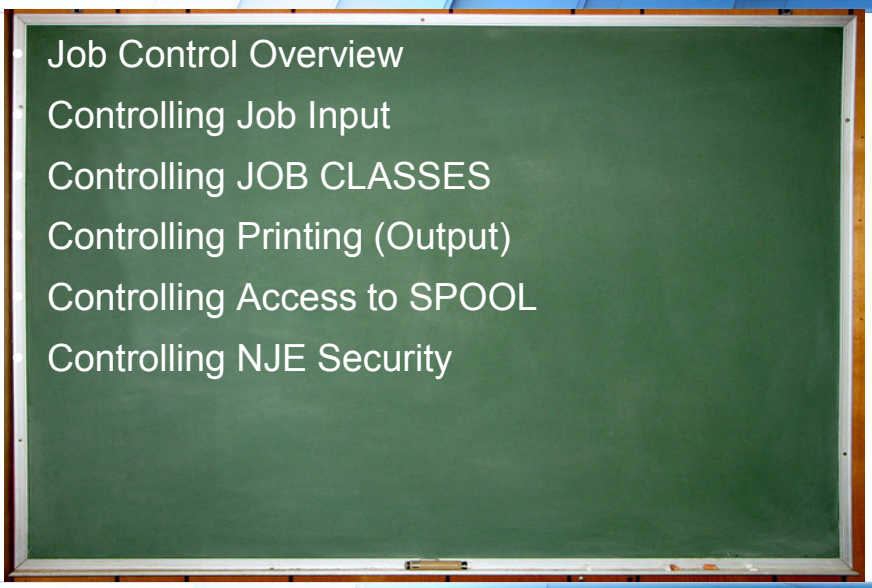
Jim McNeill

NYRUG November 25, 2014

IBM Server Proven · Business Partner IBM

Session Topics

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

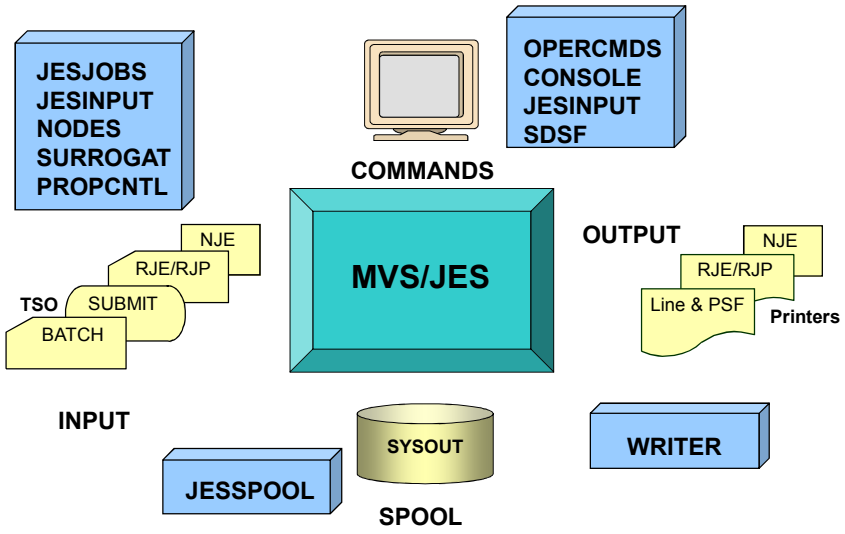


IBM Server Proven

Business Partner IBM

RACF Related Classes

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



Input and Output Controls

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- Input Controls
  - Allow control of job names (JESJOBS)
  - Allow control of who can use which job classes
  - Allow control of who can enter jobs from where (JESINPUT/NODES)
  - Allow control of Surrogate submission (SURROGAT)
- Output Controls
  - Allow control of who can send JOBS & SYSOUT where (WRITER)
  - Allow control of who can access SYSOUT on the spool (JESSPOOL)

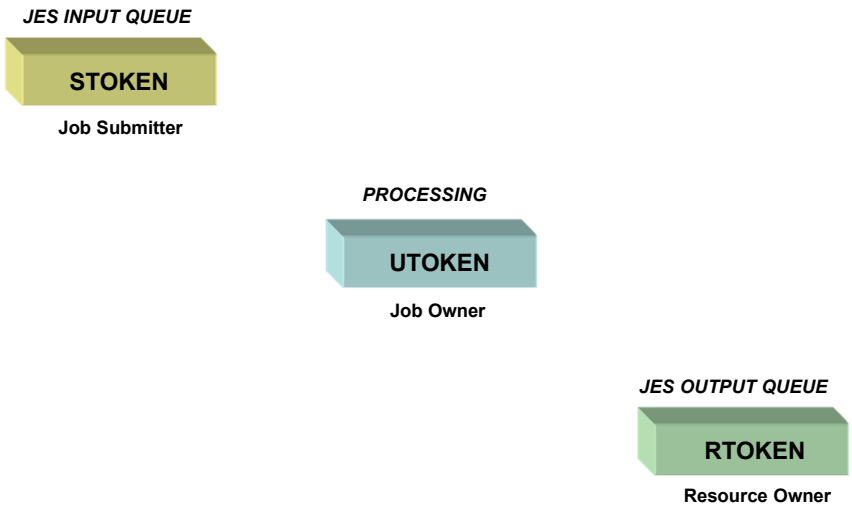
Security Tokens

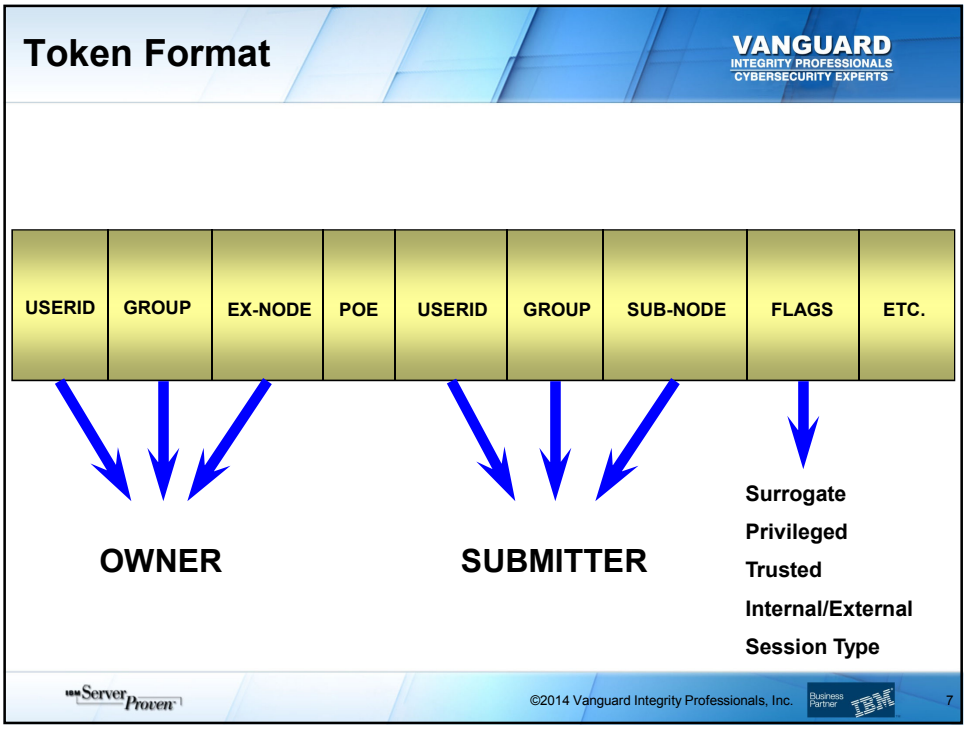
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

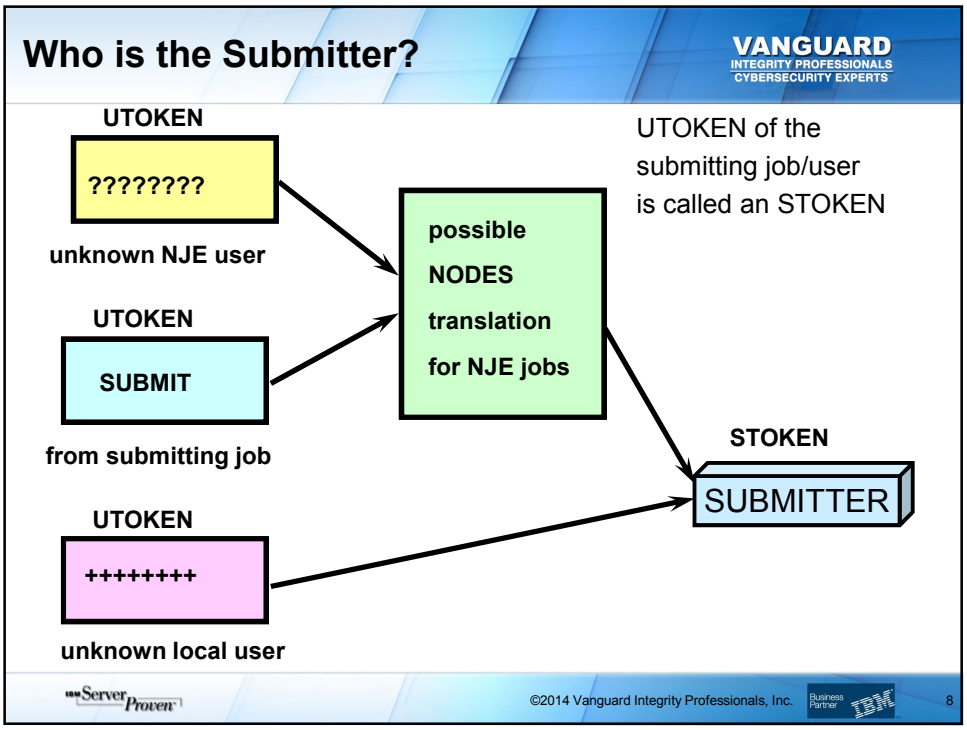
- Associated with JOB during input services
  - Identifies Submitter of JOB
  - Identifies Owner of JOB
  - Identifies Owner of all resources associated with the JOB
    - SYSIN
    - SYSOUT
- Transportable - not associated with a particular address space

Security Tokens

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

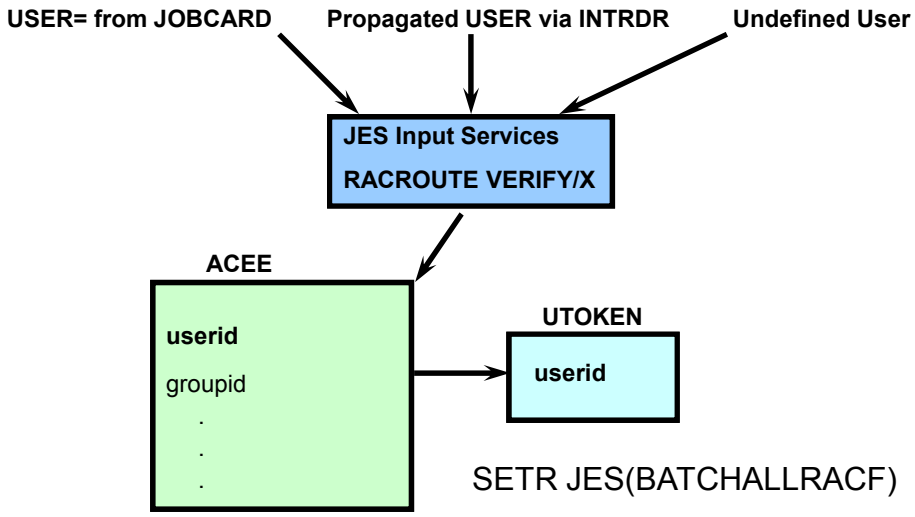



Token Format
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS
USERID
GROUP
EX-NODE
POE
USERID
GROUP
SUB-NODE
FLAGS
ETC.
OWNER
SUBMITTER
Surrogate
Privileged
Trusted
Internal/External
Session Type
Server Proven
©2014 Vanguard Integrity Professionals, Inc.
Business Partner
IBM
7


Who is the Submitter?
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS
UTOKEN
????????
unknown NJE user
UTOKEN
SUBMIT
from submitting job
UTOKEN
++++++++
unknown local user
possible
NODES
translation
for NJE jobs
UTOKEN of the
submitting job/user
is called an STOKEN
STOKEN
SUBMITTER
Server Proven
©2014 Vanguard Integrity Professionals, Inc.
Business Partner
IBM
8

Who is the Job Owner?

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



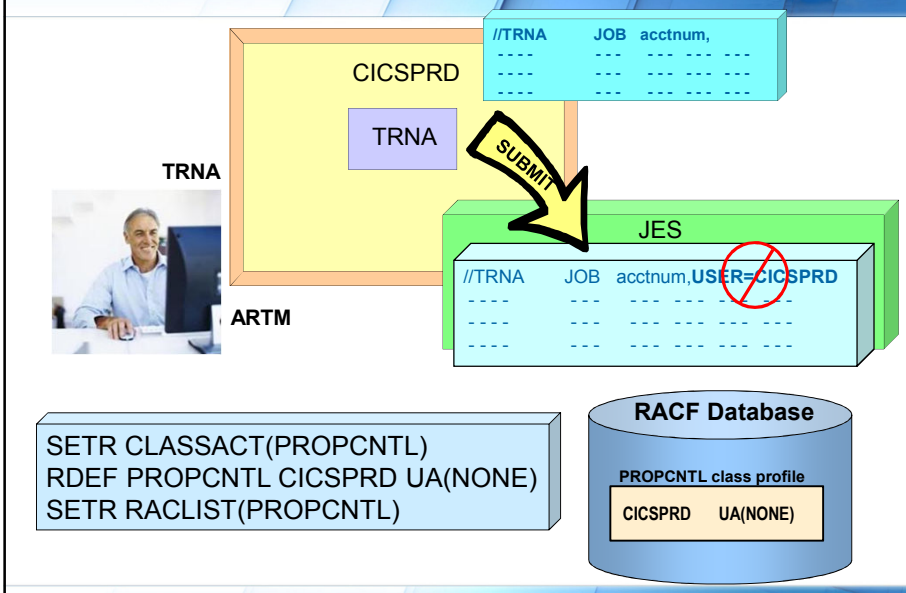
Determining the Job's Owner

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

	Internal Reader	Local & RJE/RJP Devices	NJE Nodes
USER / PASSWORD coded on Job Statement or user translated (NJE)	Coded Value	Coded Value	Coded Value
USER / PASSWORD not coded on Job Statement or user not translated (NJE)	Submitting User ID is propagated	++++++++	????????

Preventing JES Propagation

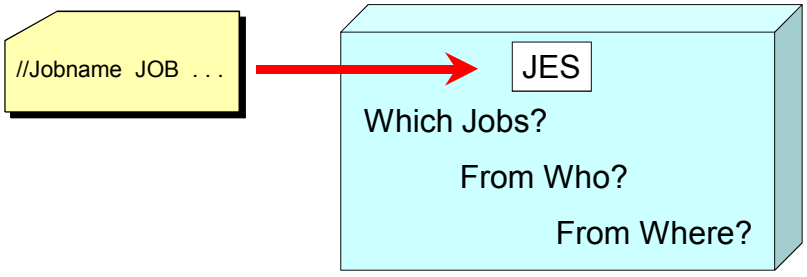
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS




```
SETR CLASSACT(PROPCNTL)
RDEF PROPCNTL CICSPRD UA(NONE)
SETR RACLIST(PROPCNTL)
```


Control of Job Submission

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



Steps to Protect Job Input

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Decide Job Name Standards

Decide What Jobs are to be Restricted

Decide Who is Allowed to Submit Each Job & From Where

Define Profiles:

JESJOBS

JESINPUT

SURROGAT

Activate Classes & Test

Controlling Job Names – JESJOBS

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

'Nasty Class' RC=8

//VANPAY1 JOB . . .

JES

Job name control based on "who" and "from where"

RACF Database

JESJOBS Profiles

SUBMIT.node.job.user	UACC	Access List
CANCEL.node.user.job	UACC	Access List
SUBMIT.**	READ	
CANCEL.**	NONE	

Defining JESJOBS Class Profiles

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

- To allow only the PAYROLL group to submit the VANPAY job from node LVPROD:

```
RDEF JESJOBS SUBMIT.LVPROD.VANPAY*.* UACC(NONE)
PERMIT SUBMIT.LVPROD.VANPAY*.* CL(JESJOBS)
          ID(PAYROLL) AC(READ)
```

- To allow only KAREN to cancel the VANPAY job from LVPROD:

```
RDEF JESJOBS CANCEL.LVPROD.*.VANPAY* UACC(NONE)
PERMIT CANCEL.LVPROD.*.VANPAY* CL(JESJOBS)
          ID(KAREN) AC(ALTER)
```

- To allow anyone to submit all other jobs:

```
RDEF JESJOBS SUBMIT.** UACC(READ)
```


Controlling Job Classes – JESJOBS

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

'Nasty Class' RC=8

//VANPAY1 JOB . . .CLASS=B → JES

Facility profiles determine who is checked – Submitter, Owner or NO check made.

NEW in z/OS 2.1

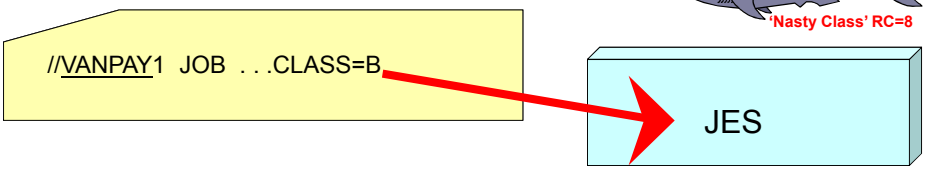
RACF Database

FACILITY Profiles	UACC	Access List
JES.JOBCLASS.OWNER	n/a	n/a
JES.JOBCLASS.SUBMITTER	n/a	n/a

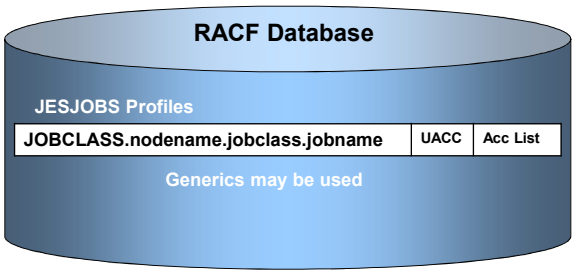
Profile(s) must be Discrete – used as switches only

Controlling Job Classes – JESJOBS

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



JESJOBS profiles determine who can use a certain JOB Class.



Defining JESJOBS Class Profiles

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

User JIMM submits a CLASS=B job named JIMMX with USER=BOB in the JOBCARD. The local node is VANLV. Of course SURROGAT profile check.

If there is a JES.JOBCLASS.OWNER profile in the FACILITY class, a check is made if user BOB has READ access to JESJOBS profile:

```
RDEF JESJOBS JOBCLASS.VANLV.B.JIMMX OWNER(SECADMN) UACC(NONE)
PE JOBCLASS.VANLV.B.JIMMX CLASS(JESJOBS) ID(BOB)  ACC(R)
```

If there is a JES.JOBCLASS.SUBMITTER profile in the FACILITY class, a check is made if user JIMM has READ access to JESJOBS profile:

```
RDEF JESJOBS JOBCLASS.VANLV.B.JIMMX OWNER(SECADMN) UACC(NONE)
PE JOBCLASS.VANLV.B.JIMMX CLASS(JESJOBS) ID(JIMM)  ACC(R)
```

If both FACILITY class profiles exist, then JIMM and BOB must have READ access to the JESJOBS class profile

Hints for defining JESJOBS Class Profiles

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

You probably want to define a backstop profile to allow all users access to all job classes.

```
RDEF JESJOBS JOBCLASS.** OWNER(SECADMN) UACC(READ)
```

Then define profiles to limit certain classes.

```
RDEF JESJOBS JOBCLASS.*.P.* OWNER(SECADMN) UACC(NONE)
PE JOBCLASS.*.P.* CLASS(JESJOBS) ID(PRODJOBS)  ACC(R)
```

If JESJOBS was not previously active, be sure to define SUBMIT.** and/or CANCEL.** before activating the class. Remember JESJOBS is a “nasty” class.

Create the Facility class profiles after the JESJOBS profiles.

Port-of-Entry Control – JESINPUT Class

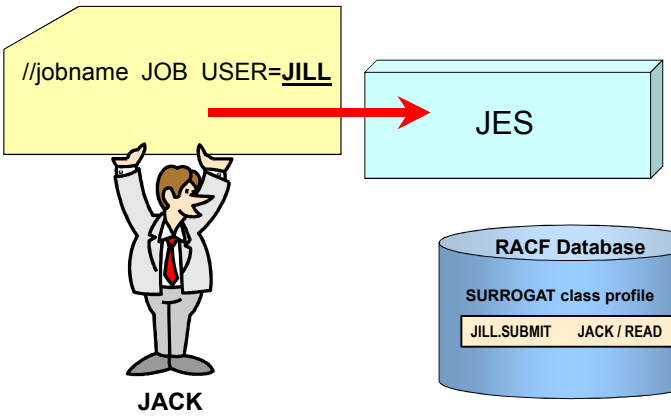
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

DEVICE	JES2 POE NAME	JES3 POE NAME
JES reader	RDRnn	Jname of reader
Disk reader	n/a	DR member name
RJE/RJP reader	Rnnnn.RDn	Workstation name
NJE reader	Adjacent Nodename	NJERDR
Dump Job	n/a	DUMPJOB
Spool Offload	OFFn.JR	n/a
Internal Reader	INTRDR	INTRDR
TSO SUBMIT	INTRDR	INTRDR
Started tasks	STCINRDR	STCINRDR
TSO logons	TSUINRDR	TSO terminal name

```
RDEF JESINPUT R124.RD1 UACC(NONE)
PE  R124.RD1 CL(JESINPUT) ID(PAYROLL) AC(READ)
RDEF JESINPUT ** UA(READ)
```

Surrogate Job Submission

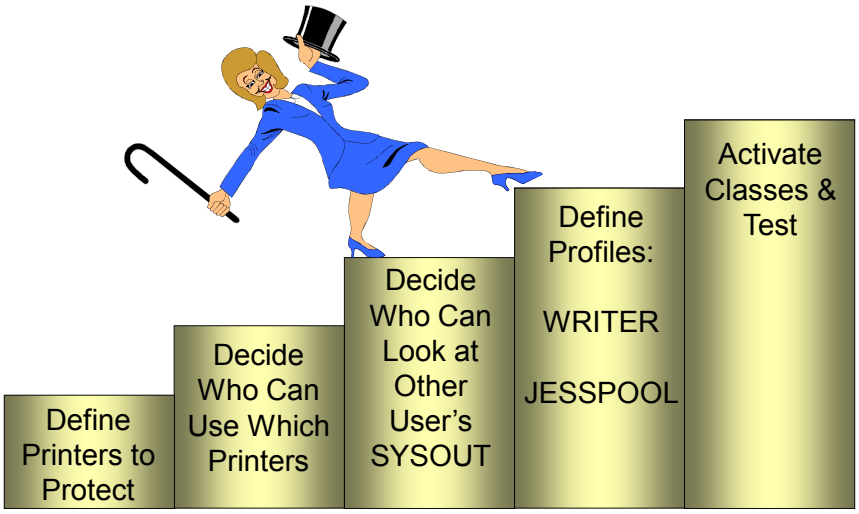
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



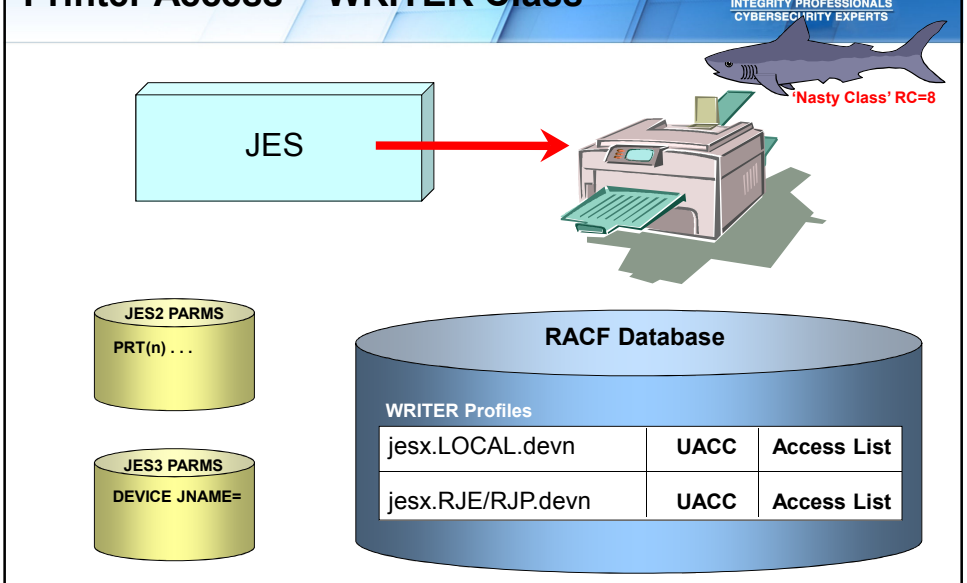

```
RDEF SURROGAT JILL.SUBMIT OWNER(SECADMN) UACC(NONE)
PE JILL.SUBMIT CLASS(SURROGAT) ID(JACK) AC(READ)
```


Steps to Protect Job Output

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



Printer Access – WRITER Class



Defining WRITER Class Profiles

- To allow only the PAYROLL group to use local printer PRT45:

```
RDEF  WRITER  JES%.LOCAL.PRT45  UACC(NONE)
PE JES%.LOCAL.PRT45 CL(WRITER) ID(PAYROLL) AC(READ)
```

- To allow only the PAYROLL group to use the remote printer R5:

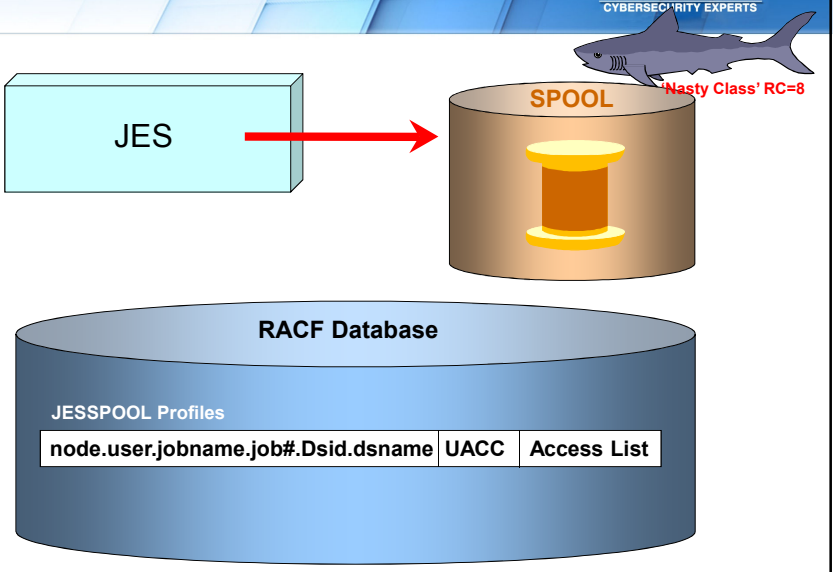
```
RDEF  WRITER  JES%.RJE.R5  UACC(NONE)
PE JES%.RJE.R5 CL(WRITER) ID(PAYROLL) AC(READ)
```

- To allow all users to use all other printers:

```
RDEF  WRITER  JES%.*.**  UACC(READ)
```

Access Control to SYSOUT – JESSPOOL

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



Access to SYSOUT

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Requirement	Auth.	JESSPOOL Profile Name
Allow viewing of CAROL's data for the ACCOUNT job on LVPROD	READ	LVPROD.CAROL.ACCOUNT.**
Allow deletion of BETH's data for the BACKUP job on LVPROD	ALTER	LVPROD.BETH.BACKUP.**
Allow receipt of data sent to FRANK for the BLKMAIL job, MAILDATA data set on LVPROD	ALTER	LVPROD.FRANK.BLKMAIL.*.*.MAILDATA

Steps to Protect NJE

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Control JOBS / SYSOUT?

Control Inbound / Outbound Work?

Control Whose Work is Sent and Received?

Define Profiles:

WRITER

NODES

Activate Classes, RACLIST & Test

NJE – WRITER and NODES Class

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

	To Control Sending: WRITER Class	To Control Receipt: NODES Class
JOBS	JES%.NJE.node	node.USERJ.userid node.GROUPJ.groupid
SYSOUT	JES%.NJE.node	node.USERS.userid node.GROUPS.groupid

Target node

Sending node

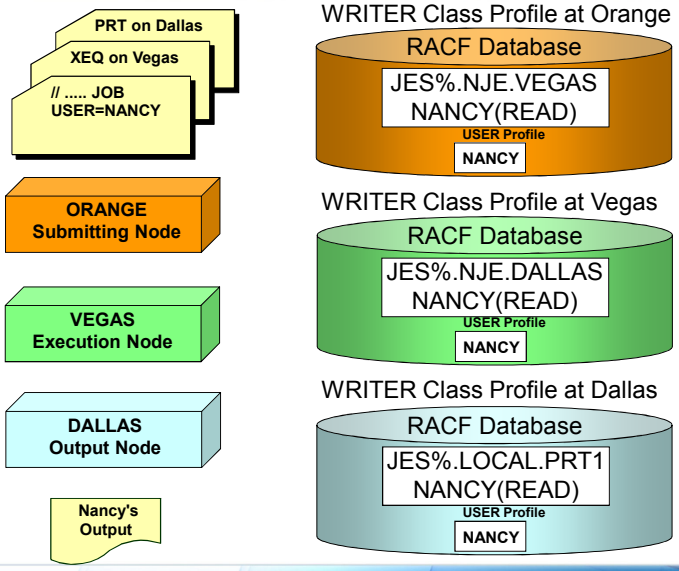
NODES Class Profile – UACC

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Requirement	Regard for Sending Node/User ID	Needed UACC
No Need to Re-verify Password on Incoming Jobs (No Password Needed)	TRUSTED	CONTROL / UPDATE
Re-verify User ID and Password on Incoming Jobs (Password Needed)	SEMI-TRUSTED	READ
No Jobs Accepted from Node/User/Group	UNTRUSTED	NONE

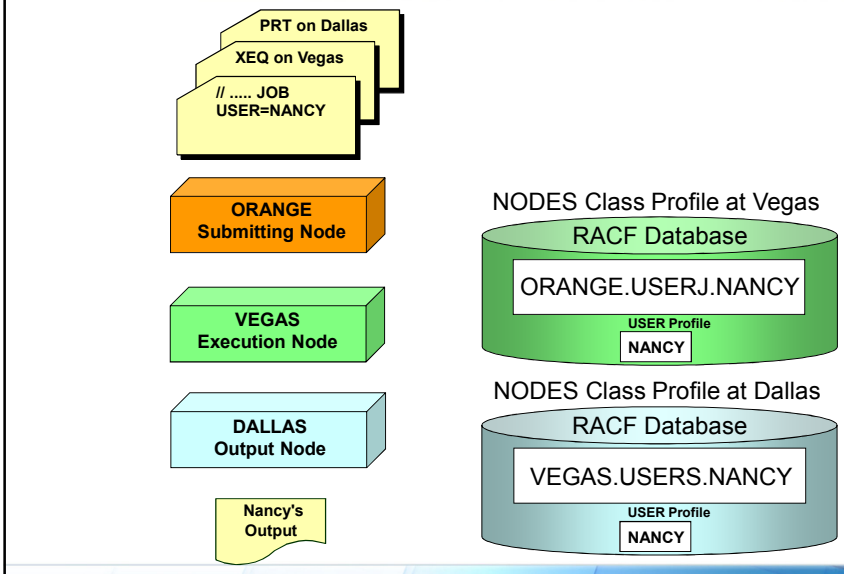
Controlling Outgoing Jobs and SYSOUT

VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS



IBM Server Proven
©2014 Vanguard Integrity Professionals, Inc.

Controlling Entry of Jobs – NODES Class



USERID Translation