



Securing your Oracle Fusion Middleware Environment, On-Prem and in the Cloud

MAY 16 & 17, 2018

**CLEVELAND PUBLIC AUDITORIUM,
CLEVELAND, OHIO**


WWW.NEOOUG.ORG/GLOC

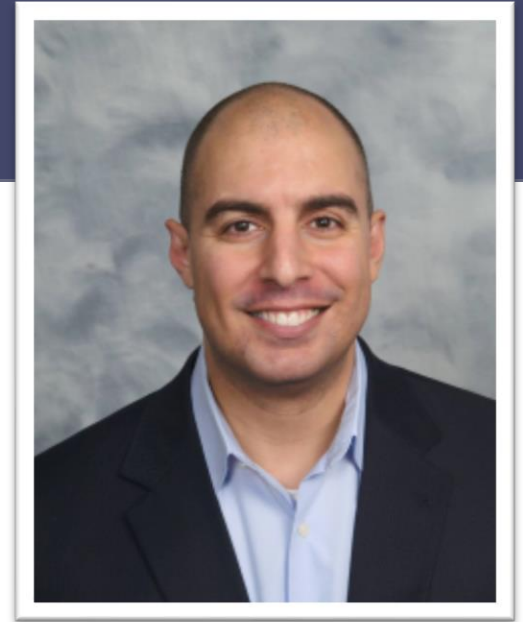
Agenda

1. About
2. Securing your Oracle Fusion Middleware Environment
3. Recap

About

About Me

- Senior Manager at Attain
- 20+ years Oracle experience
- Master's degree in Computer Science from George Mason University
- Past employment with Booz Allen Hamilton, IBM, CSC, and Oracle
- Recent emphasis on DevOps, cloud, and security in current projects
- Oracle ACE, OCE, OCA
- Author, Blogger, Presenter
- [@Ahmed_Aboulnaga](#) 



About Attain

- Headquartered in McLean VA
- Management, technology, and strategy consulting firm
- Supporting customers in government, healthcare, education, and nonprofit markets
- Industries:
 - Defense, Civilian, National Security, Federal Health, State and Local Government, and more
- Technology Partners:
 - Oracle, Red Hat, AWS, Salesforce, Microsoft, SAP, MicroStrategy, and more
- CMMI Level 5

Our Vision and Mission

- ◀ Built-to-last ▶
- ◀ Next-generation ▶
- ◀ Values-driven consultancy ▶

This vision is the foundation of Attain's culture. At the core of who we are and how we operate is a sense of purpose: to be and attain the best for those we serve.

Attain's mission is to change the world by disrupting the status quo and improving the lives we touch.



attain.com



facebook.com/AttainLLC



twitter.com/AttainLLC

Tips and Tricks for hardening Oracle Fusion Middleware

a presentation by
Jacco Landlust & Simon Haslam

TDBA

Veriton
IT INFRASTRUCTURE CONSULTING

zaterdag 8 december 12

Biggest Risks

➤ Cloud security risks

- Shared access
- Authentication, authorization, and access control
- Availability

<https://www.csoonline.com/article/2614369/security/the-5-cloud-risks-you-have-to-stop-ignoring.html>

➤ Insider threats

- See sidebar

<https://www.isdecisions.com/insider-threat/statistics.htm>



52 % OF EMPLOYEES SEE NO
SECURITY RISK TO THEIR
EMPLOYER IN SHARING
WORK LOGINS

A statistic presented in a light beige box. The number '52' is in a large orange font, followed by the text '% OF EMPLOYEES SEE NO SECURITY RISK TO THEIR EMPLOYER IN SHARING WORK LOGINS' in a smaller, grey, all-caps font.

➤ Up-to-date patching

- Article: "Equifax Officially Has No Excuse"

<https://www.wired.com/story/equifax-breach-no-excuse/>

Out of Scope

- Oracle Database
- Security testing/scanning efforts

Oracle WebLogic Server

WebLogic: Set User Lockout

➤ Configure User Lockout

➤ *Set User Lockout Attributes*

https://docs.oracle.com/cd/E57014_01/wls/WLACH/taskhelp/security/SetLockoutAttributes.html

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Mi

General RDBMS Security Store **User Lockout** Performance

Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

Save

Password guessing is a common type of security attack. In this type of attack, a hacker attempts to guess attributes to protect user accounts from intruders. This page allows us to define how user lockouts

☒ Lockout Enabled

Lockout Threshold: 5

Lockout Duration: 30

Lockout Reset Duration: 5

Lockout Cache Size: 5

Lockout GC Threshold: 400

WebLogic: Do Not Reuse WebLogic Account

➤ Create separate accounts for:

- boot.properties ← requires only 'Operator' group
- OEM Agent ← requires only 'Operator' group
- Foreign JNDI providers
- Other service accounts

➤ Example boot.properties:

```
username=weblogic_boot  
password=welcome2
```

➤ Example changing the OEM Agent password:

```
./emcli modify_target name="/soa_domain/" -type="weblogic_domain" -  
credentials="Username:oemagent;password=welcome3;" -on_agent
```

WebLogic: Do Not Share WebLogic Password

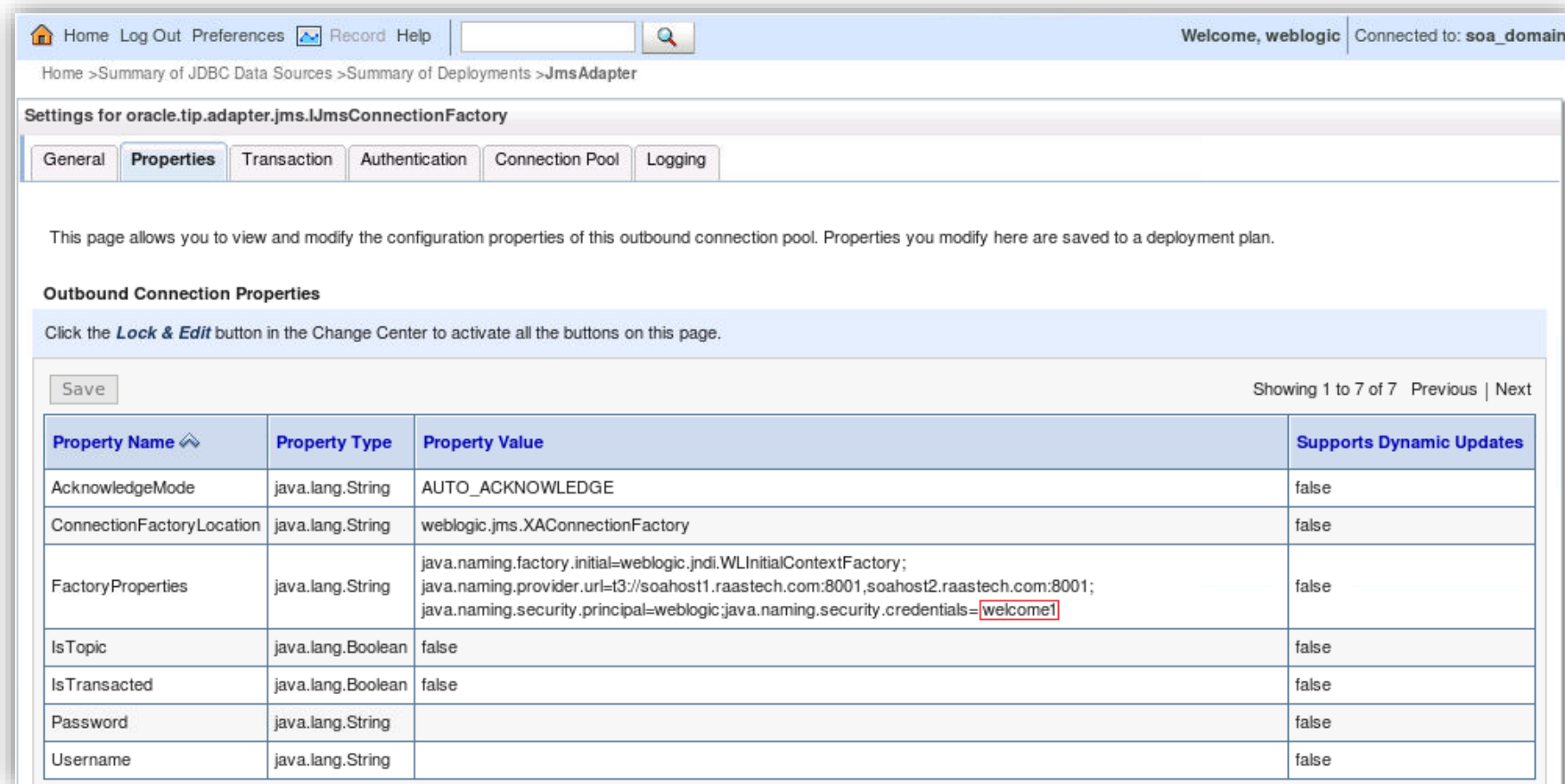
- Do not share or use the 'weblogic' password... ever
- Create local administrative accounts tied to individuals.
For example:
 - ahmed.aboulnaga
 - michael.jordan
- Administrators should use their individual admin accounts

```
wls_osb1.log:####<Mar 15, 2018, 8:08:21,277 AM EDT> <Notice> <WebLogicServer> <soahost1>  
<wls_osb1> <[ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-  
tuning)'> <ahmed> <> <bc97894a-f821-4413-bc8f-18a393ed24ac-000000ad> <1521115701277>  
<[severity-value: 32] [rid: 0] [partition-id: 0] [partition-name: DOMAIN] > <BEA-000396>  
<Server shutdown has been requested by ahmed.>
```

- Even with external LDAP authentication, need to still have local administrator accounts

WebLogic: Secure Cleartext FactoryProperties Credentials (1 of 3)

➤ Credentials in FactoryProperties are in cleartext



Home > Summary of JDBC Data Sources > Summary of Deployments > JmsAdapter

Settings for oracle.tip.adapter.jms.IJmsConnectionFactory

General **Properties** Transaction Authentication Connection Pool Logging

This page allows you to view and modify the configuration properties of this outbound connection pool. Properties you modify here are saved to a deployment plan.

Outbound Connection Properties

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Showing 1 to 7 of 7 Previous | Next

Property Name	Property Type	Property Value	Supports Dynamic Updates
AcknowledgeMode	java.lang.String	AUTO_ACKNOWLEDGE	false
ConnectionFactoryLocation	java.lang.String	weblogic.jms.XAConnectionFactory	false
FactoryProperties	java.lang.String	java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory; java.naming.provider.url=t3://soahost1.raastech.com:8001,soahost2.raastech.com:8001; java.naming.security.principal=weblogic:java.naming.security.credentials= welcome1	false
IsTopic	java.lang.Boolean	false	false
IsTransacted	java.lang.Boolean	false	false
Password	java.lang.String		false
Username	java.lang.String		false

WebLogic: Secure Cleartext FactoryProperties Credentials (2 of 3)

- 1. Create a wallet.

```
java -jar $ORACLE_HOME/wlserver/server/lib/wljmsra.rar create $JAVA_HOME/jre/lib/security
```

- 2. This creates an Oracle Wallet with the file name cwallet.sso under the \$JAVA_HOME/jre/lib/security directory.

- 3. Create an alias for your property. This is a name-value pair property and will have a name of "weblogicPwdAlias" and a value of "welcome1".

```
java -jar $ORACLE_HOME/wlserver/server/lib/wljmsra.rar add weblogicPwdAlias welcome1
```

- 4. List the aliases in the Oracle Wallet to confirm all is good.

```
java -jar $ORACLE_HOME/wlserver/server/lib/wljmsra.rar dump $JAVA_HOME/jre/lib/security
```

- 5. On the WebLogic Server Administration Console, click on *Deployments*.
- 6. Navigate to *Deployments > JmsAdapter > Configuration > Outbound Connection Pools*.
- 7. Expand oracle.tip.adapter.jms.IJmsConnectionFactory.
- 8. Click on eis/wls/Queue.

WebLogic: Secure Cleartext FactoryProperties Credentials (3 of 3)

- 9. Add the following *FactoryProperties* property. Make note of *java.naming.security.credentials* (which is now the alias) and *weblogic.jms.walletDir* (which is the path to *cwallet.sso*).

```
java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory;java.naming.provider.url=t3://soahost1:8001,soahost2:8001;java.naming.security.principal=weblogic;java.naming.security.credentials=->weblogicPwdAlias;weblogic.jms.walletDir=/u01/app/oracle/middleware/products/jdk1.8.0_102/jre/lib/security
```

- 10. Click on *Save*.
- 11. On the Save Deployment Plan page, enter the Path
(e.g., /u01/app/oracle/middleware/products/fmw1221/user_projects/applications/soa_domain/dp/JmsAdapterPlan.xml).
- 12. Click on *OK*.
- 13. Click on *Save*.
- 14. Activate Changes.

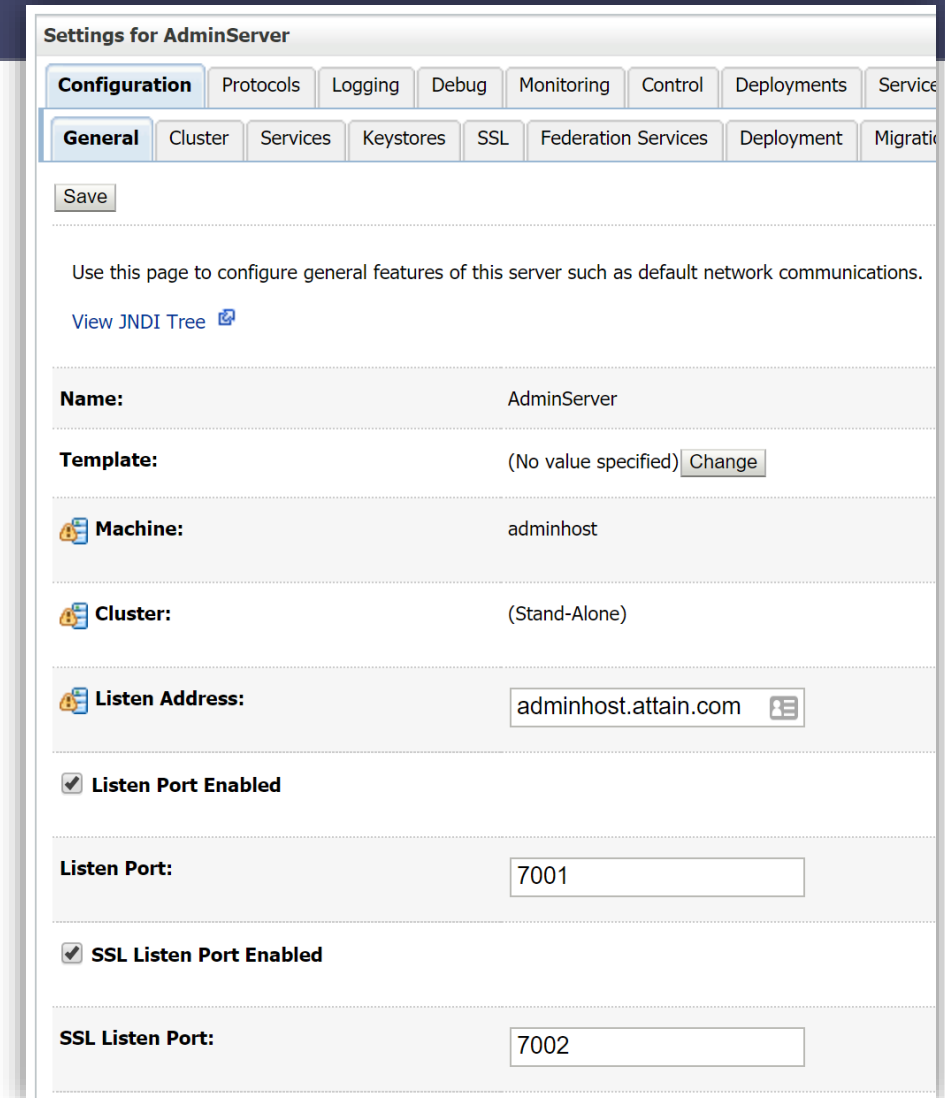
WebLogic: Enable SSL on Managed Servers

➤ “Using SSL is computationally intensive and adds overhead to a connection.” ~Oracle Documentation

➤ Still it should be considered

➤ SANS: *Clear Text Password Risk Assessment Documentation*

<https://www.sans.org/reading-room/whitepapers/authentication/clear-text-password-risk-assessment-documentation-113>



The screenshot displays the 'Settings for AdminServer' page in the WebLogic Admin Console. The 'General' tab is selected, showing configuration options for the AdminServer. The 'Name' is 'AdminServer', the 'Template' is '(No value specified)', the 'Machine' is 'adminhost', and the 'Cluster' is '(Stand-Alone)'. The 'Listen Address' is 'adminhost.attain.com'. The 'Listen Port' is '7001' and the 'SSL Listen Port' is '7002'. Both 'Listen Port Enabled' and 'SSL Listen Port Enabled' are checked. A 'Save' button is at the top left of the configuration area.

Settings for AdminServer	
Configuration Protocols Logging Debug Monitoring Control Deployments Services	
General Cluster Services Keystores SSL Federation Services Deployment Migration	
<input type="button" value="Save"/>	
Use this page to configure general features of this server such as default network communications. View JNDI Tree	
Name:	AdminServer
Template:	(No value specified) <input type="button" value="Change"/>
Machine:	adminhost
Cluster:	(Stand-Alone)
Listen Address:	adminhost.attain.com
<input checked="" type="checkbox"/> Listen Port Enabled	
Listen Port:	7001
<input checked="" type="checkbox"/> SSL Listen Port Enabled	
SSL Listen Port:	7002

WebLogic: Configure Network Connection Filters

➤ Connection filters let you deny access at the network level.

0.0.0.0/0	*	7001	allow	# AdminConsole
0.0.0.0/0	*	8011	allow	# OSB
127.0.0.1/0	*	8001	allow	# SOA
192.168.1.10/0	*	8001	allow	# SOA
0.0.0.0/0	*	8001	deny	# SOA

➤ *Using Network Connection Filters*

https://docs.oracle.com/middleware/11119/wls/SCPRG/con_filtr.htm

WebLogic: Auditing Provider

- Operating requests and outcome of those requests are collected (i.e., an electronic trail of computer activity)
- *Configuring the WebLogic Auditing Provider*

<https://docs.oracle.com/middleware/1213/wls/SECMG/audit.htm#SECMG137>

WebLogic: Password Validation Provider

- Manages and enforces a set of configurable password composition rules
- Used to determine whether the password meets the criteria established by the composition rules
- *Configuring the Password Validation Provider*

https://docs.oracle.com/middleware/1221/wls/SECMG/password_atn.htm#SECMG206

WebLogic: Cross-Domain Security

➤ To enable trust between multiple WebLogic domains

➤ *Configuring Cross-Domain Security*

<https://docs.oracle.com/middleware/1221/wls/SECMG/domain.htm#SECMG402>

WebLogic: Securing Node Manager

- Set up SSL communication between Node Manager and the Administration Server
 - Generate self-signed certificates
 - Create trust and identity keystores
 - Configure Node Manager and managed servers to use the custom keystores
 - Change the host name verification setting for each managed server

- *Enabling Host Name Verification Certificates for Node Manager*

https://docs.oracle.com/cd/E23943_01/doc.1111/e15483/node_manager.htm#CMEDG641

Oracle Fusion Middleware

Oracle Fusion Middleware: Enable TLS & Disable Weak Ciphers

➤ Oracle WebLogic Server (config.xml):

```
<arguments>-  
weblogic.security.SSL.protocolVersion=TLSv1.2</arguments>
```

➤ Oracle HTTP Server (ssl.conf):

```
SSLProtocol -All +TLSv1.2  
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!RC4:!MEDIUM:+HIGH
```

➤ OPMN-based products (opmn.xml):

```
<ssl enabled="true" wallet-file="/u01/wallet" ssl-  
versions="TLSv1.2" ssl-ciphers="SSL_RSA_WITH_AES_256_GCM_SHA384"/>
```

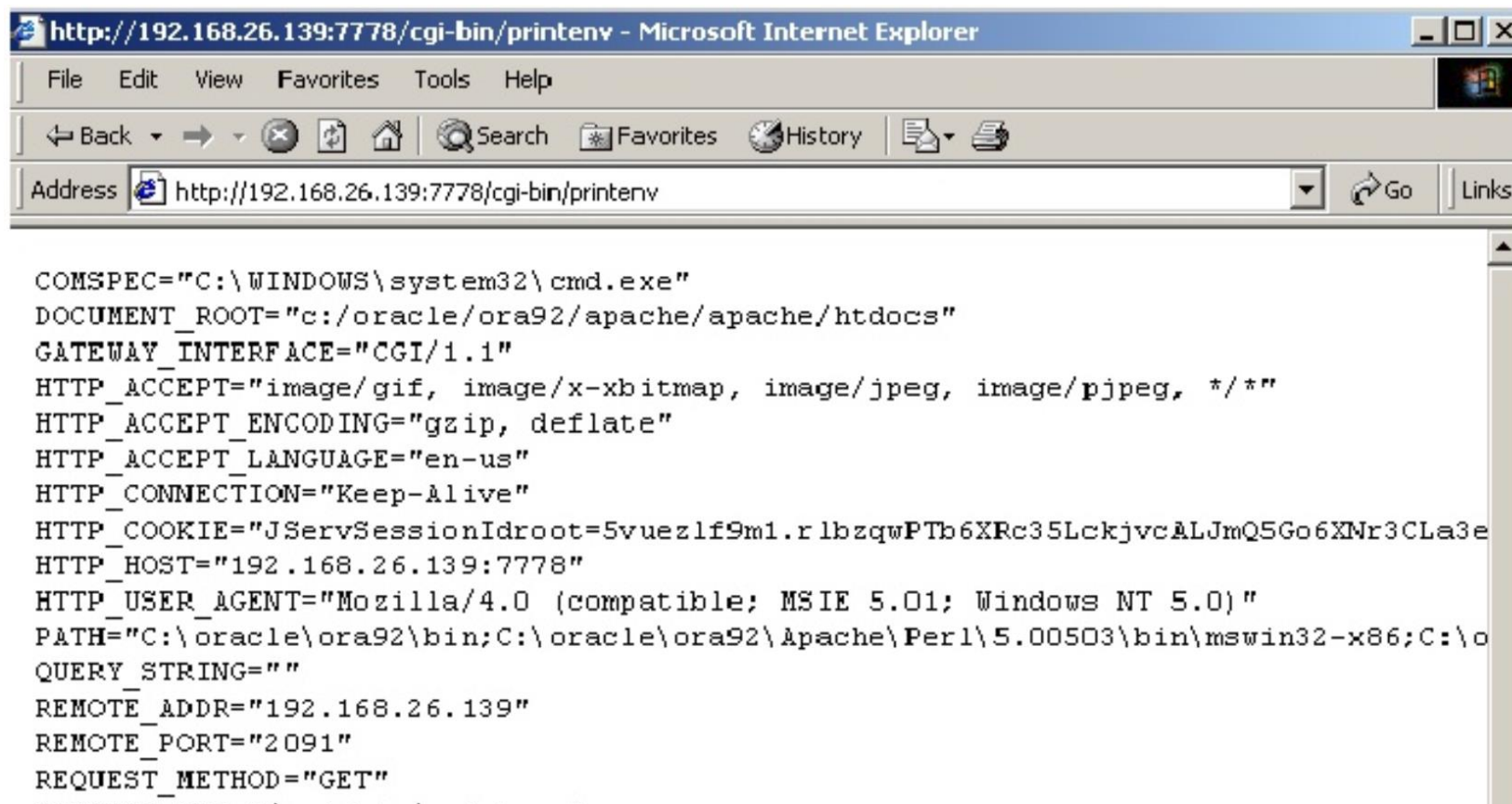
Oracle HTTP Server: Basic Web Server Hardening

➤ Oracle HTTP Server (ssl.conf):

```
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
Header set X-XSS-Protection "1; mode=block"
Header set X-Content-Type-Options nosniff
Header always append X-Frame-Options SAMEORIGIN
Header set Cache-Control: "no-cache, no-store, must-revalidate"
Header set Pragma no-cache
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains"
Header unset X-Powered-By
```

Oracle HTTP Server: Remove printenv

➤ Remove the default `printenv` from `/cgi-bin`

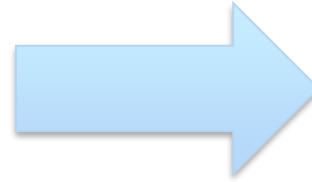


The screenshot shows a Microsoft Internet Explorer window with the title bar "http://192.168.26.139:7778/cgi-bin/printenv - Microsoft Internet Explorer". The address bar contains "http://192.168.26.139:7778/cgi-bin/printenv". The main content area displays the output of the `printenv` command, which lists various environment variables and their values. The variables include `COMSPEC`, `DOCUMENT_ROOT`, `GATEWAY_INTERFACE`, `HTTP_ACCEPT`, `HTTP_ACCEPT_ENCODING`, `HTTP_ACCEPT_LANGUAGE`, `HTTP_CONNECTION`, `HTTP_COOKIE`, `HTTP_HOST`, `HTTP_USER_AGENT`, `PATH`, `QUERY_STRING`, `REMOTE_ADDR`, `REMOTE_PORT`, and `REQUEST_METHOD`.

```
COMSPEC="C:\WINDOWS\system32\cmd.exe"
DOCUMENT_ROOT="c:/oracle/ora92/apache/apache/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*"
HTTP_ACCEPT_ENCODING="gzip, deflate"
HTTP_ACCEPT_LANGUAGE="en-us"
HTTP_CONNECTION="Keep-Alive"
HTTP_COOKIE="JServSessionIdroot=5vuezlf9m1.r1bzqWPt6XRc35LckjvcALJmQ5Go6XNr3CLa3e"
HTTP_HOST="192.168.26.139:7778"
HTTP_USER_AGENT="Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
PATH="C:\oracle\ora92\bin;C:\oracle\ora92\Apache\Perl\5.00503\bin\mswin32-x86;C:\o"
QUERY_STRING=""
REMOTE_ADDR="192.168.26.139"
REMOTE_PORT="2091"
REQUEST_METHOD="GET"
```

Oracle Access Manager: Enable Audit Events (1 of 2)

➤ Available audit events for Oracle Access Manager



- User sessions
- Authorization
- Account Management
- OAM Server
 - Authentication Attempt
 - Server Startup/Shutdown
 - Login
 - Authorization
 - User Account Locked/Unlocked
 - User Account Password Change Failed/Success
 - Server Upgrade Start
 - Server Upgrade
- OAM Admin Console
 - Resource Creation/Deletion
 - Agent Creation/Modification/Deletion
 - Server Domain Creation/Modification/Deletion
 - Host Identifier Creation/Modification/Deletion
 - Generic Admin Operation

Oracle Access Manager: Enable Audit Events (2 of 2)

- OAM Administrative Tasks:
 - "Common Settings > Choose Filter Level > All" and apply
- OAM Server Components:
 - "Security > Audit Policy > Audit Component Name: Oracle Access Manager"
 - Select category *User Sessions / Authorization / Account Management / OAM Server / OAM Admin Console*
- Perform rolling restart of managed servers
- Check \$MSERVER_HOME/oam_server1/logs/auditlogs/OAM/audit.log

Oracle Identity Manager: Enable Audit Events (1 of 2)

- Enable User Profile Audit:
 - "System Management > System Configuration"
 - Modify "User profile audit data collection level"
- Enable Role Profile Audit:
 - "System Management > System Configuration"
 - Modify "Level of Role Auditing"
 - Provide value for "Role Hierarchy"
- Enable Issue Audit Messages Task:
 - "System Management > System Configuration > Schedule"
 - Enable "Issue Audit Messages Task"

Oracle Identity Manager: Enable Audit Events (2 of 2)

➤ Generate initial snapshot by running GenerateSnapshot.sh:

```
cd $OIM_HOME/server/bin  
./GenerateSnapshot.sh -username xelsysadm -numOfThreads 8 -  
serverUrl t3://oimhost:14100/identity -ctxFactory  
weblogic.jndi.WLInitialContextFactory
```

➤ Perform rolling restart of managed servers

```
2018-02-14 23:27:36.621 "ahmed" "Authentication" false "" "anonymous"  
"inband_OHS_7777" "inband_OHS_7777" "oam_server(11.1.2.0.0)" "FORM"  
"Protected Resource Policy" "005PJHopXvYFc5RayXMAMG000AZC00001^"  
"UserSession" "-" "PROXY_IP_ADDRESS = unknown" "oam_domain" "0:4"  
"192.168.1.1" "-1494975013135090797" "HTTP:ohshost_7777::/app/**::"  
"ohshost_7777" "89"
```



Linux

Linux: Set Appropriate Umask

➤ Set "umask 0077"

➤ Include it in these files:

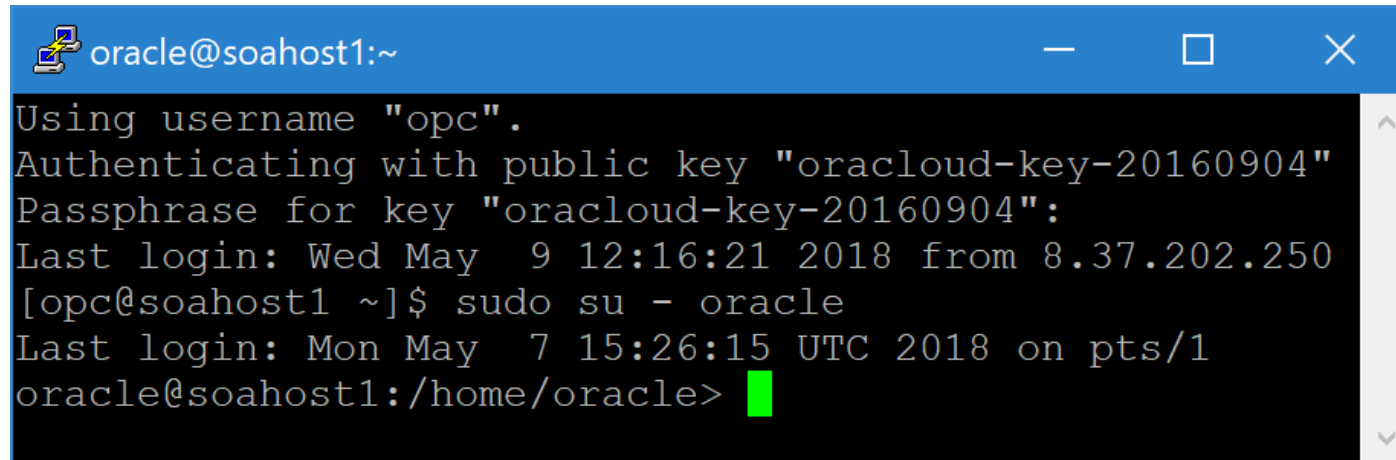
- /etc/bashrc
- /etc/csh.cshrc
- /etc/profile

➤ Defaults the file permissions to 600

```
-rw----- 1 oracle oinstall    18 May 10 22:58 file.txt
```

Linux: Disable Direct Login to 'oracle' Unix Account

- Enable "sudo su" to Oracle product accounts
- Do not share the "oracle" Linux password



```
oracle@soahost1:~  
Using username "opc".  
Authenticating with public key "oracloud-key-20160904"  
Passphrase for key "oracloud-key-20160904":  
Last login: Wed May  9 12:16:21 2018 from 8.37.202.250  
[opc@soahost1 ~]$ sudo su - oracle  
Last login: Mon May  7 15:26:15 UTC 2018 on pts/1  
oracle@soahost1:/home/oracle>
```

- Also implement logging (/etc/sudoers):
%admins ALL=(ALL) NOPASSWD: LOG_INPUT: LOG_OUTPUT: ALL
Defaults iolog_dir=/var/log/sudo-io/{user}

Linux: SSH Hardening Considerations

➤ Basic SSH hardening considerations (/etc/ssh/sshd_config):

```
X11Forwarding no           # If GUI access not required
PermitRootLogin no         # Disallow direct root login
PasswordAuthentication no  # Use public key auth instead
MaxAuthTries 3             # For lockout
Protocol 2                 # SSH protocol, version 2
ClientAliveInterval 300    # Disconnect idle sessions
ClientAliveCountMax 2      # Disconnect idle sessions
AllowUsers ahmed           # Whitelist users
```

➤ Ideally use public key authentication and disable password logins

Linux: Enable Local Firewall

➤ May cause challenges with Oracle Coherence, Oracle SOA Suite, or other applications reliant on UDP ports when trying to figure out what needs to remain open between clustered nodes

➤ Sample commands:

```
systemctl status firewalld
```

```
systemctl start firewalld
```

```
systemctl stop firewalld start
```

```
firewall-cmd --state
```

```
firewall-cmd --zone=public --add-port=80/tcp --permanent
```

Linux: Check for Suspicious Files

- Manual visual checks for suspicious files are necessary
- Especially for publicly exposed servers

```
root@mobile:/u01/hack/scripts
root@mobile:/u01/hack/scripts> ll
total 175924
-rw----- 1 root root      772 Nov 15  2016 Administrator.sh
drw----- 8 root root     4096 Nov 10  2016 btc
-rw-r--r-- 1 root root    28741 Nov  9  2016 index.html
drwx----- 2 root root     4096 Nov 17  2016 nmap0
drw----- 2 root root     4096 Nov 14  2016 nmap1
drw----- 2 root root     4096 Nov 14  2016 nmap10
drw----- 2 root root     4096 Nov 14  2016 nmap11
drw----- 2 root root    113360 Nov 14  2016 nmap12
drw----- 2 root root     4096 Nov 17  2016 nmap13
drw----- 2 root root     4096 Nov 17  2016 nmap14
drw----- 2 root root     20480 Nov 17  2016 nmap15
drw----- 2 root root     57344 Nov 17  2016 nmap16
drw----- 2 root root    139264 Nov 17  2016 nmap17
drw----- 2 root root     73728 Nov 17  2016 nmap18
drw----- 2 root root     36864 Nov 17  2016 nmap19
drw----- 2 root root     4096 Nov 11  2016 nmap2
drw----- 2 root root     12288 Nov 17  2016 nmap20
drw----- 2 root root     4096 Nov 17  2016 nmap21
drw----- 2 root root     4096 Nov 11  2016 nmap3
drw----- 2 root root     4096 Nov 11  2016 nmap4
drw----- 2 root root     4096 Nov 14  2016 nmap5
drw----- 2 root root     4096 Nov 14  2016 nmap6
drw----- 2 root root     4096 Nov 14  2016 nmap7
drw----- 2 root root     4096 Nov 14  2016 nmap8
drw----- 2 root root     4096 Nov 14  2016 nmap9
-rw----- 1 root root 21858982 Nov 17  2016 nmap.sh
-rw----- 1 root root 59169576 Nov 17  2016 nohup.out
-rwxr-xr-x 1 root root     2201 Jun 17  2016 ping.jar
-rw----- 1 root root 98488320 Nov 17  2016 SantaClara.tar
drwxr-xr-x 18 root root     4096 Nov 17  2016 scripts
-rw----- 1 root root     151 Nov  9  2016 status
root@mobile:/u01/hack/scripts>
```

```
/u01/app/oracle/middleware/products/fmw1221/user_projects/domains/soa_domain
oracle oinstall 4096 Oct 16  2016 security
oracle oinstall 4096 Oct 16  2016 servers
oracle oinstall 246 May  7 15:26 shutdown-AdminServer.py
oracle oinstall 240 Aug 24  2017 shutdown-wls_mft1.py
oracle oinstall 240 Aug 24  2017 shutdown-wls_osbl.py
oracle oinstall 240 Jan  1 23:21 shutdown-wls_soal.py
oracle oinstall 240 Aug 24  2017 shutdown-wls_wsm1.py
oracle oinstall 1166 Oct 16  2016 startManagerWebLogic_readme.txt
oracle oinstall 292 Oct 16  2016 startWebLogic.sh
oracle oinstall 4096 Oct 16  2016 sysman
oracle oinstall 20480 Mar 17 22:23 tmp
oracle oinstall 2384177 Oct 31  2017 zhangmini
:/u01/app/oracle/middleware/products/fmw1221/user_projects/domains/soa_domain>
```

Real World Example #1

Wednesday, February 10, 2016

Red Hat Enterprise Linux Server release 5.5 - Hacked and fixed

One of our public, rarely used, sandbox servers was hacked last January. Even Amazon Web Services got hit with one of the three we've gotten rid of.

Several of the OS binaries would have been overwritten by a 1135000 byte binary file, so you will have to re-copy them from a different server.

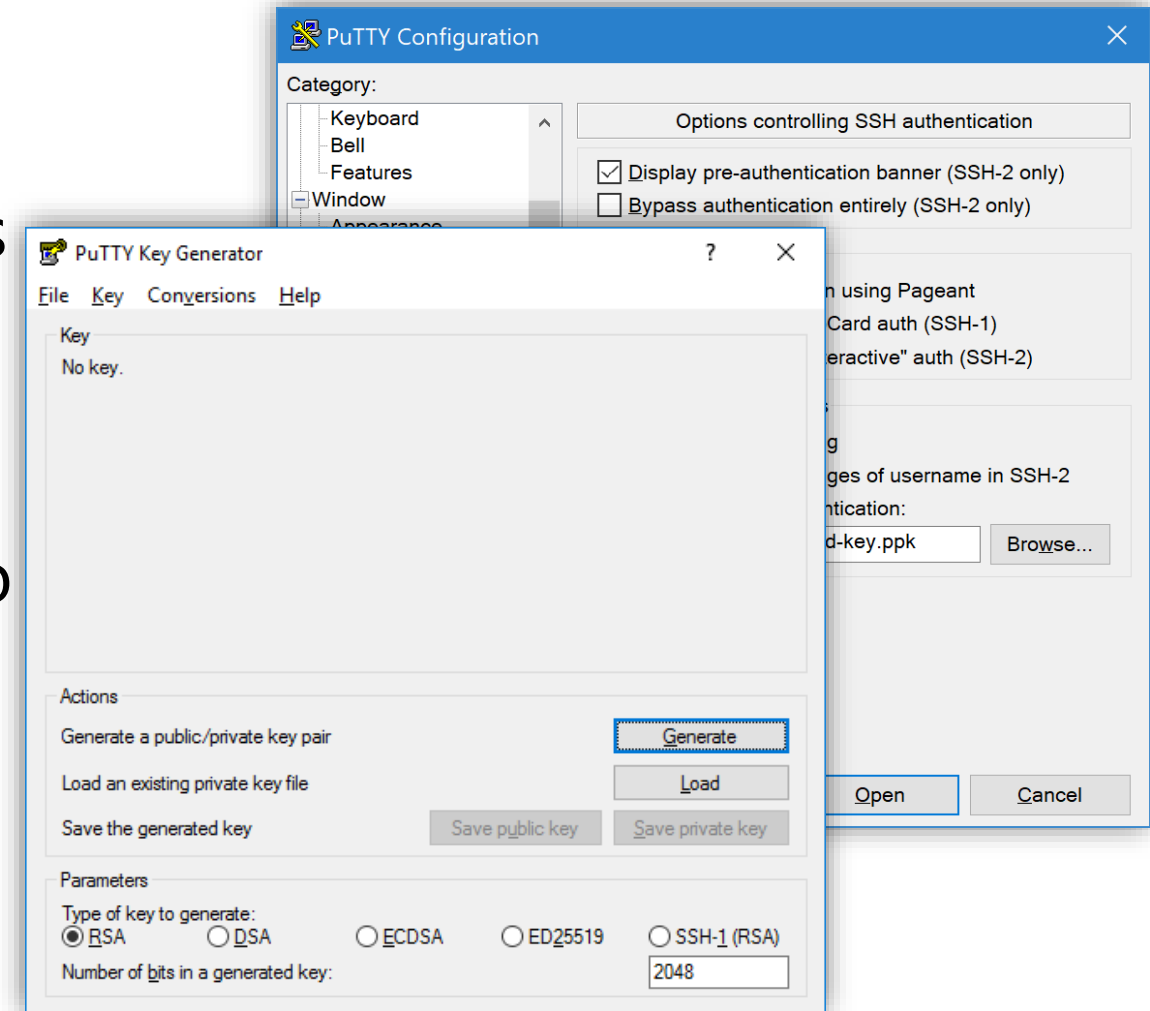
Run these commands to get rid of the offending trojans/viruses:

```
chattr -i /usr/bin/.sshd
chattr -i /usr/bin/kernel
chattr -i /usr/bin/acpid
chattr -i /etc/bash
rm -rf /usr/bin/dpkgd
rm -rf /usr/bin/bsd-port
rm -f /l26.tmp
rm -f /usr/bin/.sshd
rm -f /usr/bin/kernel
rm -f /usr/bin/acpid
rm -f /etc/bash
rm -f /etc/Centos-ssh
rm -f /etc/Centos-sshd
rm -f /etc/fake.cfg
rm -f /etc/http.sh*
rm -f /etc/https.sh*
```

Cloud

Cloud: Set Password on Private SSH Keys

- Use puttygen.exe
- Set passwords on private keys
- Otherwise anybody who has the file can log into everything you have access to
- If you leave the passphrase blank, the key is not encrypted



Cloud: Separate SSH Keys Per Administrator

➤ Self-explanatory

Add SSH Public Key

Enter an SSH key name to reference this key for launching virtual machine instances. Copy your SSH public key value and paste it here. Paste the key value exactly as it was generated. Don't append or insert any spaces, characters, or line breaks. [Learn more.](#)

?

*

Name

myPublicKey

?

*

Value

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACxys3iwQioSt57h3QGixhbE
NnxsXOF6fJiyQPaCfcREH+aFrTem
eVIU6VVcBqdq43Zhxc4yIGPnhzmr
91FM3fMztl3h4gCZtL/FTX4jj0Q9k8l
cODFtqsWHDGMzbnz6Hu41dqYgc
GKa06K6VmsinZrPMWiohjd69Hj
/oxsbQesvRgxqKog7XvVw+Xeog4E

Select File

Enabled

☒

Add

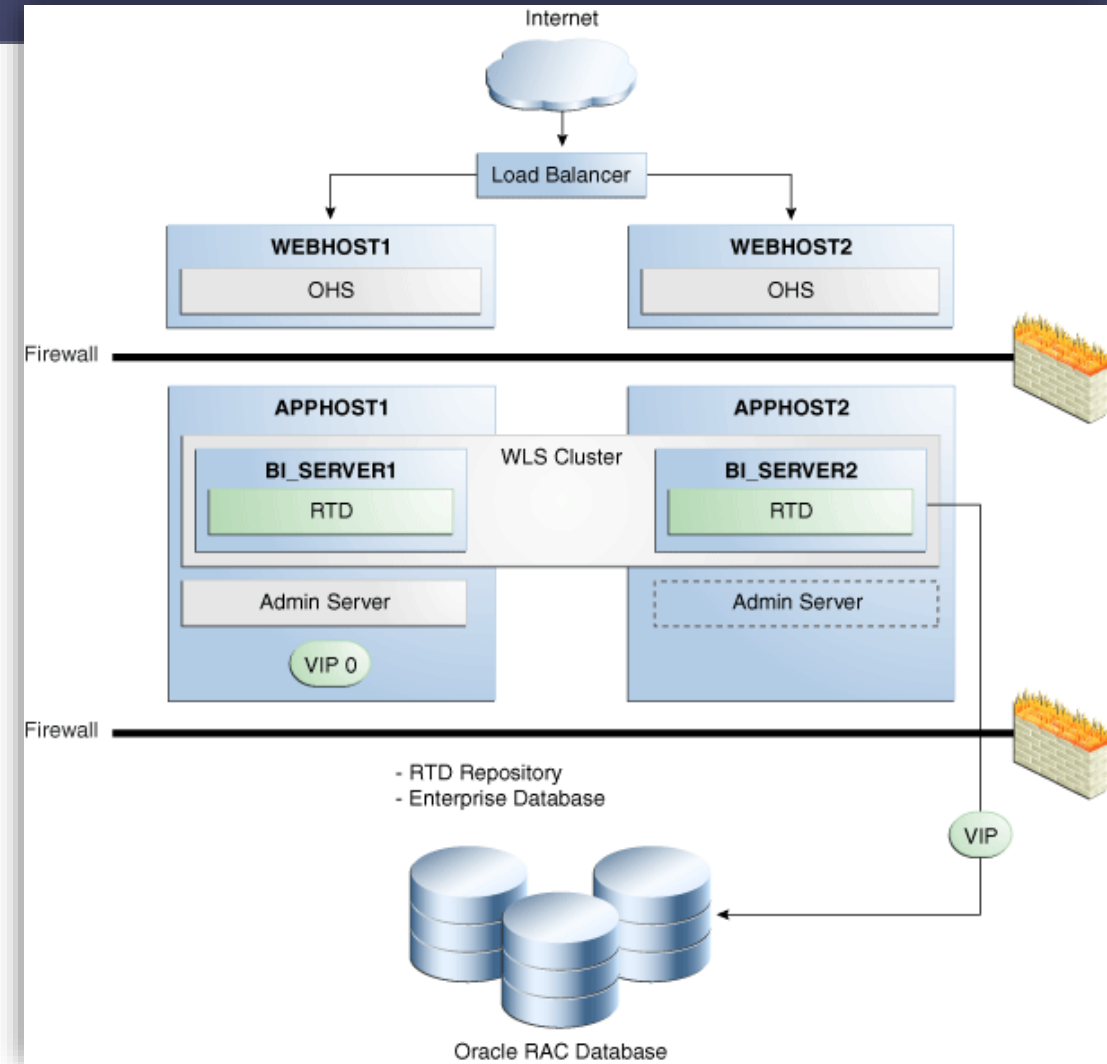
Cancel



Architecture

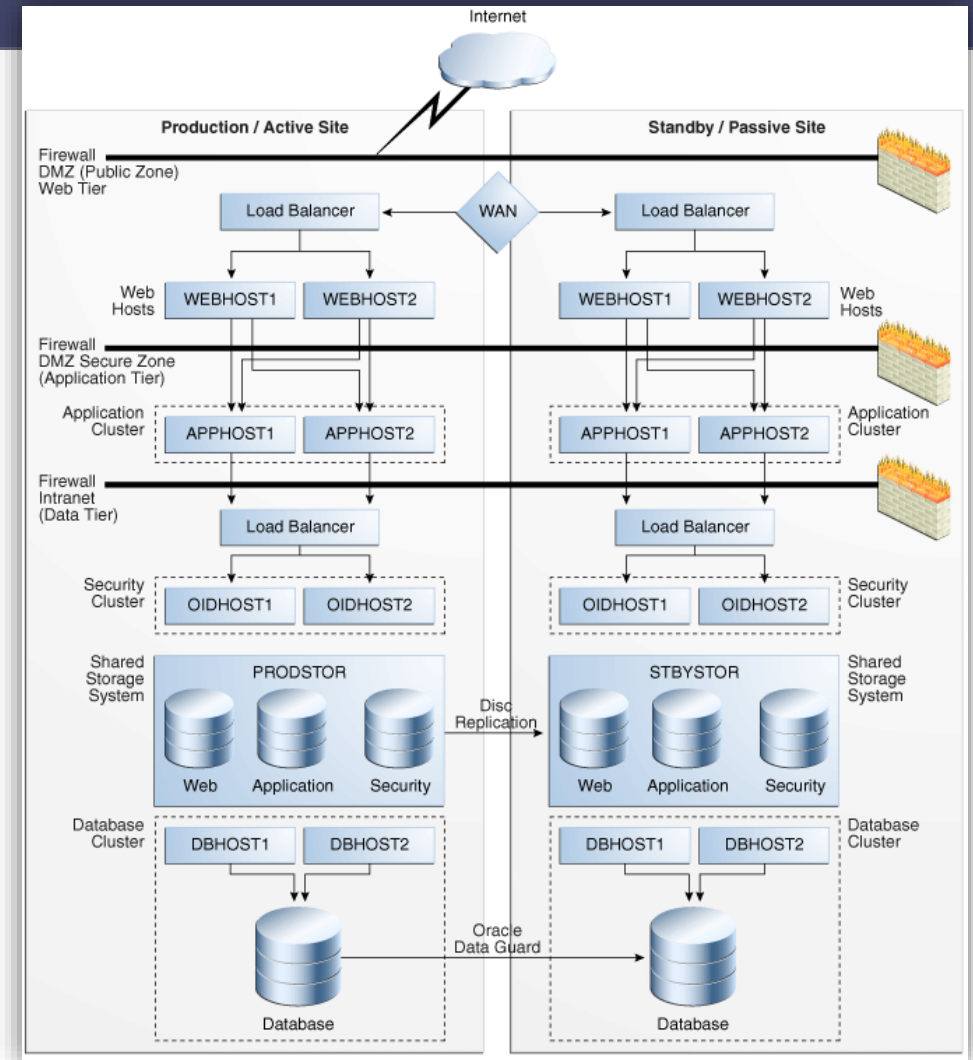
Architecture: Implement High Availability

- To ensure continued operation in the event of hardware failure
- Mostly for business continuity



Architecture: Implement Disaster Recovery



- To ensure continued operation in the event of catastrophic data center failover
- Mostly for business continuity



Documentation

Documentation: Baseline Configuration

- Too large of a scope to collect baseline configurations across various Oracle Fusion Middleware products
- Understand the reasoning behind this
- How about WebLogic configuration at least as a start?

Configuration Audit Type:	<input type="text" value="Change Audit"/>	Returns the criteria used for auditing configuration events (configuration changes and other operations): More Info...
<input checked="" type="checkbox"/>  Configuration Archive Enabled		If true, then backups of the configuration will be made during server boot. More Info...
 Archive Configuration Count:	<input type="text" value="10"/>	The number of archival versions of config.xml saved by the Administration Server each time the domain configuration is modified. More Info...

Documentation: Verify Ports Lists

➤ All ports need to be accounted for and documented

```
oracle@soahost1:~  
oracle@soahost1:/home/oracle> netstat -anp | grep LISTEN | grep -v LISTENING  
(Not all processes could be identified, non-owned process info  
will not be shown, you would have to be root to see it all.)  
tcp        0      0 127.0.0.1:45678      0.0.0.0:*            LISTEN  
tcp        0      0 0.0.0.0:22           0.0.0.0:*            LISTEN  
tcp6       0      0 fe80::c4b0:2bff:f:35850 :::*                LISTEN  
tcp6       0      0 127.0.0.1:35850      :::*                LISTEN  
tcp6       0      0 10.106.99.194:35850  :::*                LISTEN  
tcp6       0      0 :::1:35850           :::*                LISTEN  
tcp6       0      0 :::1521              :::*                LISTEN  
tcp6       0      0 10.106.99.194:5556   :::*                LISTEN  
tcp6       0      0 :::22               :::*                LISTEN  
tcp6       0      0 127.0.0.1:1527       :::*                LISTEN  
tcp6       0      0 :::44439             :::*                LISTEN  
tcp6       0      0 10.106.99.194:7001   :::*                LISTEN  
tcp6       0      0 :::5500              :::*                LISTEN  
tcp6       0      0 10.106.99.194:8001   :::*                LISTEN  
tcp6       0      0 10.106.99.194:8002   :::*                LISTEN  
tcp6       0      0 fe80::c4b0:2bff:fe:9991 :::*                LISTEN  
tcp6       0      0 127.0.0.1:9991       :::*                LISTEN  
tcp6       0      0 10.106.99.194:9991   :::*                LISTEN  
tcp6       0      0 :::1:9991            :::*                LISTEN  
oracle@soahost1:/home/oracle>
```

Documentation: Quarterly CPU Patching

- Develop and document a formal *Quarterly CPU Patching* process
- How to handle critical patches?
- Article: *10/10 would patch again: Big Red plasters 'easily exploitable' backdoor in Oracle Identity Manager*
https://www.theregister.co.uk/2017/10/30/oracle_releases_patch_for_remotely_exploitable_backdoor_in_identity_management_system/
- The OIM bug has a CVSS score of 10.0 –or critical– and could allow a remote, unauthorized hacker access to systems

Documentation: Standard Operating Procedure (SOP)

- Develop and document a formal *Standard Operating Procedure* (SOP)

Process

Process: Restrict Administrative Accounts

- Don't share the *weblogic*, *oamadmin*, *oimadmin*, *cn=orcladmin*, etc., to all administrators
- Preferably grant permissions to individual administration accounts and restrict access to default admin accounts

Process: Create Service Accounts

- Restrict the use of administration accounts
- For example: *weblogic*, *cn=orcladmin*, etc.
- Create as many service accounts as necessary

Process: Separation of Duties

- Do not grant *Administrator* group to all administrators “just because”
- Do not grant *Administrator* group to service accounts if it is not needed (recall OEM Agent, boot.properties)

Process: No Password Sharing

- No password sharing

Process: Avoid Emails

- Don't send usernames/passwords in email
 - At least put them in separate emails
 - Avoid altogether if possible
- Don't send architecture diagrams or network details via email unless in a password protected document
 - Avoid accidental exposure, help minimize content indexing online
- Avoid emails
 - Link to access-controlled content management system (e.g., SharePoint)



Other

Other: SSL Certificates to Match Hostnames

- SSL certificate common name (cn) should match hostname

Other: Implement Log Aggregation

- Audit logs use to:
 - Detect suspicious activity
 - Investigate incidents after an attack/hack
- Can administrators manipulate audit logs?
- Integrate logs in near realtime with log aggregation tools (e.g., Splunk) which should be controlled by another team



ORACLE®
LOG ANALYTICS
CLOUD SERVICE

Oracle Log Analytics can monitor, aggregate, index, and analyze log data from a wide variety of Oracle and non-Oracle log sources.

Rapidly enable log data monitoring from ANY log file (including Syslog sources) and securely transport this data to the Oracle Log Analytics service.

Significantly compress the log data (10:1) and transport the compressed data over HTTPS.

Other: Password Management

- Use a password management tool
- Administrators maintain tens to hundreds of system passwords
- Passwords on Microsoft Excel spreadsheets can easily be cracked and removed

Application

Application: Timeout Settings

- Set application and single sign-on (SSO) timeout settings whenever/where applicable

Application: Web Service Security

➤ Enable WS-Security for web service security (tomorrow!)

GETTING STARTED WITH SECURITY FOR YOUR ORACLE SOA SUITE INTEGRATIONS

LL06 May 17, 2018 Presentation

Other 04:00 PM - 05:00 PM

Like 0 Share Tweet Share Add to Calendar



Many companies are leveraging the boom in cloud services, and integration between them is becoming more and more important. It is not unusual for an organization to have a combination of on-premise and cloud applications, all talking to each other. For SOA-based integrations, security becomes more critical than ever. This presentation is a technical deep dive on how to secure your integrations via WS-Security and Oracle Web Services Manager (OWSM), for the SOAP and RESTful services. We will discuss authentication, message encryption, two-way SSL verification, certificates, and more.

SPEAKERS



MICHAEL MIKHAILIDI

Attain

Application: Development

- Run web application vulnerability scanning tools against your applications

Network

Network: Restrict Administrative Console Access via Firewall

➤ Restrict administrative console access via firewall

➤ Isn't it a bit overkill?

- Firewall
- Local Linux firewall
- WebLogic network filtering

To Continue the Discussion



**Want to learn more about how
Attain is different?**

**Please contact us.
We're eager to work with you.**

Ahmed Aboulnaga
ahmed.aboulnaga@attain.com

info@attain.com
www.attain.com



