

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

Request Information				
Requestor	Rovie Salvatierra			
Implementing Team	System and Server Operations			
Ticket Number/s	201916513			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	June 22, 2019			
Proposed Change Start/End Time	16:00 – 18:00			
Proposed Change Verification Time	18:30			


Objective of the change
To create a new Linux File Share for JAKA site with the new Samba version 4.10.5 as recommended for PCI-DSS.

Technical/Operational Impact of the change		
Negative: There will be a 2-hour downtime to migrate files and swap IP Address.	Beneficial: The new shared drive will have the most recent version of Samba, complying with the PCI-DSS standard.	Neutral:

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
JAKA	JKA-VLIN-FNP02	172.17.0.124	Linux shared drive

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
System and Server Operations	Rovie Salvatierra	0917-627-4325
Finance	Ronel Ambrocio	rambrocio@openaccessbpo.com
Circles.Life	Bobby Jusayan	bjusayan@openaccessbpo.com
Postmates	Gary Canson	gcanson@openaccessbpo.com
HR	Emelda Perez	emelda@openaccessbpo.com
WFM	Jannie Lagran	jlagran@openaccessbpo.com
Performance Management	Roselle Mulles	rmulles@openaccessbpo.com
Nurse	Lorraine Lopez	llopez@openaccessbpo.com
Bird	Dulcisimo Torres	dtorres@openaccessbpo.com

Test Environment implementation and Verification Summary
<ol style="list-style-type: none"> Created a virtual instance of CentOS on VMware workstation installed. Downloaded the sources for samba-4.10.5.tar.gz at https://www.samba.org. Extract the package and configured the installation directories: <ul style="list-style-type: none"> > /sbin > /etc/samba > /usr/share/man

 OPEN ACCESS <small>THE OPEN ACCESS CORPORATION</small>	Proprietary and Confidential	Effectivity: April 1, 2019	Page 1
			Template Version : 02

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

4. Assigned the IP Address 192.168.220.131 and started the compilation.
 > **make**
 > **make -j 2**
5. After compiling, installed the compiled software by entering **make install**.
6. Next, configure smb.conf to add the test folder named IT.
7. Saved the settings.

Test Environment Results Summary

1. After installation, run the commands below to start the service:
 > **smbd -D**
 > **nmbd -D**

```
[root@jka-vlin-fnptest03 ~]# ps -ef | grep smbd
root      57307      1    0 18:41 ?        00:00:00 smbd -D
root      57309    57307    0 18:41 ?        00:00:00 smbd -D
root      57310    57307    0 18:41 ?        00:00:00 smbd -D
root      57311    57307    0 18:41 ?        00:00:00 smbd -D
root      57915    57307    0 19:43 ?        00:00:00 smbd -D
root      58305    58106    0 22:01 pts/0    00:00:00 grep --color=auto smbd
[root@jka-vlin-fnptest03 ~]# ps -ef | grep nmbd
root      57315      1    0 18:41 ?        00:00:00 nmbd -D
root      58307    58106    0 22:01 pts/0    00:00:00 grep --color=auto nmbd
```

Figure 1: SMB service showed that it's already running with no errors

2. Accessed the shared drive at 192.168.220.121 using the test credentials for user **jan**.

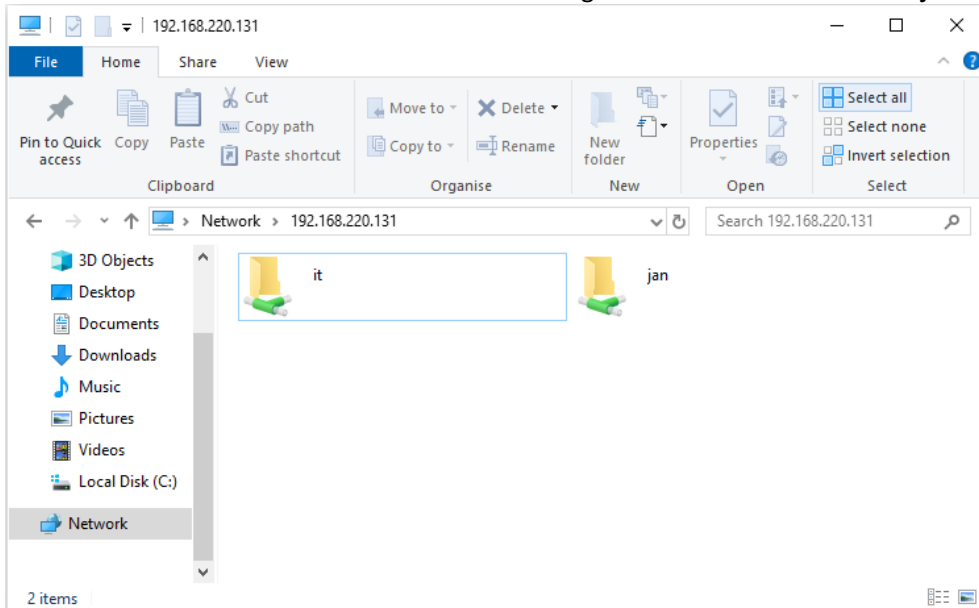


Figure 2: Access was successful

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Create New Linux Samba Share for JAKA Site</i>	

Configuration Change Template

Baseline File	3.1.146 JKA-VLIN-FNP02
Baseline Version	1

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing baseline configuration for the new server.	<ul style="list-style-type: none"> - Install the latest version of Samba, which is 4.10.5. - Migrate all Shared Drive users and files from JKA-VLIN-FNP01 to this new server. 	A new baseline configuration file will be created for this new server.	Server Information & Interface Configuration tab, File Share Users tab, Samba Config tab

Backup Procedures

No backup procedure as this is a completely new virtual instance on the ESXi machine.

Physical Implementation Procedures

No physical implementation will be done, as we'll be installing this server as a virtual machine on the JKA-PESX-HV01.

Technical Configuration Procedures

1. Log on to JKA-PESX-HV01 at <https://jka-pesx-hv01.openaccess.bpo/ui/#/login> using the root account.
2. Click on Virtual Machines > Create/Register VM > select Create new virtual machine.
3. Name the instance JKA-VLIN-FNP02. See details below:

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

Name
JKA-VLIN-FNP02

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility ESXi 6.7 virtual machine

Guest OS family Linux

Guest OS version CentOS 7 (64-bit)

Figure 1

4. Select the JKA-PESX-HV01.datastore2 for the storage.
5. Customize the Settings as indicated below:
 - > CPU – 2
 - > Cores per Socket – 1
 - > RAM – 4GB
 - > Hard Disk – 3TB
 - > Disk Provisioning – Thin Provisioned
 - > Network Adapter – VLAN 10
 - > CD/DVD Drive – Datastore ISO File, select CentOS-7
6. Click on Add Network Adapter for the management IP and select VM Network.
7. Start the virtual machine to install the OS by clicking on JKA-VLIN-FNP02 > Power On.
8. Follow the installation wizard.
 - > Choose Region and Language – English US
 - > Date and Time – Asia/Manila
 - > Keyboard – English US
 - > Software Selection – Minimal/Debugging Tool, Compatibility Libraries, Development Tools, Security Tools, System Administration Tools
 - > Security Policy – PCI-DSS v3 Control Baseline for RedHat Linux 7
9. Set the root password and begin the installation.

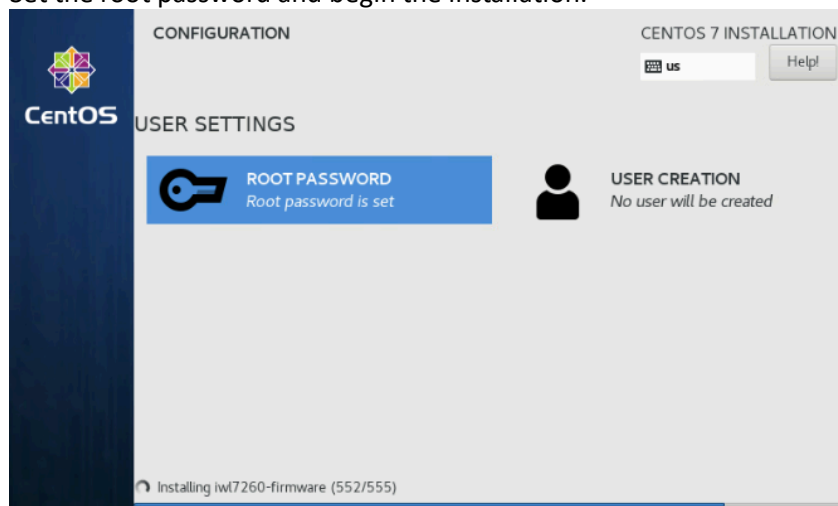
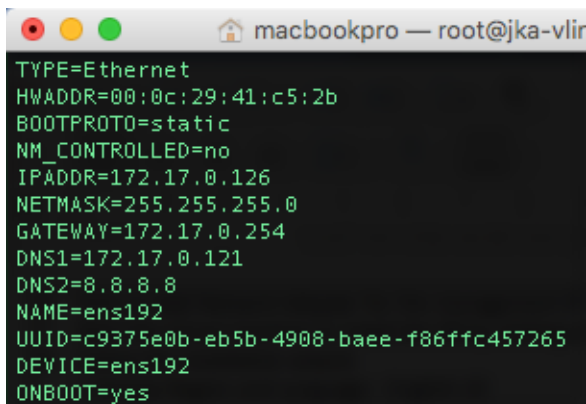


Figure 2

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

10. After the installation, reboot the server.
11. Next, set the IP Address to 172.17.0.126 temporarily by entering the command below:
 - > ifup /etc/sysconfig/network-scripts/ifcfg-ens192
 - > vi /etc/sysconfig/network-scripts/ifcfg-ens192



```

TYPE=Ethernet
HWADDR=00:0c:29:41:c5:2b
BOOTPROTO=static
NM_CONTROLLED=no
IPADDR=172.17.0.126
NETMASK=255.255.255.0
GATEWAY=172.17.0.254
DNS1=172.17.0.121
DNS2=8.8.8.8
NAME=ens192
UUID=c9375e0b-eb5b-4908-baee-f86ffc457265
DEVICE=ens192
ONBOOT=yes

```

Figure 3: Note that the IP Address is just temporary

12. Save by entering :wq!
13. Next, **disable** Security-Enhanced Linux by editing the configuration file located in **/etc/selinux/config**
14. Then, install and configure SSH by entering the commands below:
 - > yum install -y openssh openssh-server openssh-clients openssl-libs
 - > vi /etc/ssh/sshd_config and uncomment Port 22, and change it to **3489**
15. Disable Firewall by entering the command **systemctl disable firewalld**
16. Now, install clamav by following the [Installation and Configuration of ClamAV on Linux Servers](#) KB Article.
17. Next, install SNMP for Cacti/Nagios monitoring by following the commands below:
 - > yum install -y net-snmp net-snmp-utils
 - > systemctl enable snmpd
18. Next, enter the commands below to start installation and configuration of Samba 4.10.5:
 - > yum install attr bind-utils docbook-style-xsl gcc gdb krb5-workstation \
 libsemanage-python libxslt perl perl-ExtUtils-MakeMaker \
 perl-Parse-Yapp perl-Test-Base pkgconfig policycoreutils-python \
 python2-crypto gnutls-devel libattr-devel keyutils-libs-devel \
 libacl-devel libaio-devel libblkid-devel libxml2-devel openldap-devel \
 pam-devel popt-devel python-devel readline-devel zlib-devel systemd-devel \
 lmdb-devel jansson-devel gpgme-devel pygpgme libarchive-devel
 - > wget https://download.samba.org/pub/samba/stable/samba-4.10.5.tar.gz
 - > tar -xzf samba-4.10.5.tar.gz
 - > cd samba-4.10.5.tar.gz
 - > ./configure
 - > ./configure ... --without-ad-dc
 - > ./configure ... --sbindir=/sbin
 - > ./configure ... --sysconfdir=/etc/samba
 - > ./configure ... --mandir=/usr/share/man/

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

- > make
- > make -j 2
- > make install
- 19. Next, copy the configuration file of JKA-VLIN-FNP01 located at /etc/samba/smb.conf to the same path in JKA-VLIN-FNP02.
- 20. Next, start copying the files using the commands below:
 - > cd /home/
 - > rsync -avz -e "ssh -p3489" --progress <username>@172.17.0.124:/home/SHARE_* .
- 21. Next, create user accounts by referring to the File Share Users list in the [JKA-VLIN-FNP01 baseline](#).
 - > useradd -a -G <groupname> <username>
 - > enter password as listed on the baseline

```
711 useradd -a -G oamadmin jbuenavidez
```

Figure 4

- 22. Once all files have been transferred and users have been created, swap the IP Addresses of JKA-VLIN-FNP01 and JKA-VLIN-FNP02.
 - > JKA-VLIN-FNP02 – 172.17.0.124
 - > JKA-VLIN-FNP01 – 172.17.0.126
 - > you'll have to navigate to /etc/sysconfig/network-scripts/ to edit this
- 23. Then, install the wazuh agent by following the command below:
 - > vi /etc/yum.repos.d/wazuh.repo

```
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=Wazuh repository
baseurl=https://packages.wazuh.com/3.x/yum/
protect=1
```

 - > yum install wazuh-agent
 - > sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/wazuh.repo
- 24. Finally, set the management IP by entering the commands below:
 - > from the SSH of JKA-VLIN-FNP01, enter: ifdown /etc/sysconfig/network-scripts/ifcfg-eth1
 - > from the SSH of JKA-VLIN-FNP02, enter: ifup /etc/sysconfig/network-scripts/ifcfg-ens224
- 25. Still in JKA-VLIN-FNP02, set the management IP to static by entering the command below:
 - > vi /etc/sysconfig/network-scripts/ifcfg-ens224
 - > then edit the line IPADDR to 172.17.3.24
- 26. Next, enter the command below:
 - > vi /etc/hosts.deny
 - > enter the line at the bottom as shown in Figure 5

```
# See 'man tcpd'
#
sshd : ALL EXCEPT 172.17.*.*
~
~
```

Figure 5

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

27. Save the settings by entering the command **:wq!** then restart the ssh service by sending:
> **systemctl restart sshd.service**

Verification Procedures

1. Logon to the root environment using your own credentials and send the commands below:
> ip a

```
[[root@pelops ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop
    link/ether 00:25:90:60:c9:52 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    link/ether 00:25:90:60:c9:53 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/24 brd 172.17.0.255 scope global eth1
    inet6 fe80::225:90ff:fe60:c953/64 scope link
        valid_lft forever preferred_lft forever
```

Figure 6: It should show the server name as JKA-VLIN-FNP02, and the IPs should be 172.17.0.124 and 172.17.3.24

2. Send the command **freshclam**
> it should show that freshclam is running and updates as shown in Figure 7

```
Wed Jun 19 23:58:47 2019 -> ClamAV update process started at Wed Jun 19 23:58:47 2019
Wed Jun 19 23:59:00 2019 -> Downloading main.cvd [100%]
Wed Jun 19 23:59:10 2019 -> main.cvd updated (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Wed Jun 19 23:59:15 2019 -> Downloading daily.cvd [100%]
Wed Jun 19 23:59:36 2019 -> daily.cvd updated (version: 25485, sigs: 1596921, f-level: 63, builder: raynman)
Wed Jun 19 23:59:36 2019 -> Downloading bytecode.cvd [100%]
Wed Jun 19 23:59:36 2019 -> bytecode.cvd updated (version: 328, sigs: 94, f-level: 63, builder: neo)
Wed Jun 19 23:59:41 2019 -> Database updated (6163264 signatures) from database.clamav.net (IP: 104.16.218.84)
```

Figure 7

3. Navigate to the home folder, and it show all the folders that were migrated from the previous server.

Process Owner: IT Operations	FORM	F-CMG-3.1
	Create New Linux Samba Share for JAKA Site	

```

drwxrwxr-x 21 root      1009    4096 Dec 25 22:05 SHARE_adminassistant
drwxrwxr-x  2 root      1142    4096 Jul  4  2018 SHARE_another
drwxrwxr-x 13 root      1012    4096 Sep 24  2018 SHARE_avawomen
drwxrwxr-x  7 root      1564    4096 Mar 19 12:42 SHARE_bird
drwxrwxr-x  6 root      1016    4096 Apr 16 19:23 SHARE_circleslife
drwxrwxr-x  9 root root    4096 Aug 31  2018 SHARE_dmopc
drwxrwxr-x 24 root hr      4096 Nov 29  2018 SHARE_DTR
drwxrwxr-x  4 root      1010    4096 Jun  6 23:54 SHARE_DWARFS
drwxrwxr-x  4 root root    4096 Aug 31  2018 SHARE_engineering
drwxrwxr-x 19 root finance 4096 Mar 28 14:22 SHARE_finance
drwxrwx--  2 root      1644    4096 May  1 15:38 SHARE_formulal
drwxrwsr-x 45 root hr      4096 Apr 12 11:11 SHARE_hr
drwxrwxr-x 42 root      1006    4096 Apr 12 21:09 SHARE_hr-er
drwxrwxr-x 18 root oamadmin 4096 Apr  3 15:07 SHARE_idprinting
drwxrwxr-x  8 root      1013    4096 Dec 27 13:44 SHARE_ismt
drwxrwsr-x 34 root      1011    4096 Apr  2 16:56 SHARE_marketing
drwxrwxr-x  6 root      1501    4096 Dec  4  2018 SHARE_mavie
drwxrwxr-x  9 root      1005    4096 Dec 26 02:51 SHARE_nurse
drwxrwsr-x 34 root      1010    4096 May 28 23:30 SHARE_performancemanagement
drwxrwxr-x  2 root      1002    4096 Sep  7  2018 SHARE_pmtraining
drwxrwxr-x 19 root      1002    4096 Jun 14 09:10 SHARE_postmates
drwxrwxr-x 17 root      1002    4096 Oct 30  2018 SHARE_postmatesreports
drwxrwxr-x 14 root group1  4096 Mar  2  2015 SHARE_qa
drwxrwxr-x  2 root      781     4096 Jul  6  2018 SHARE_sku
drwxrwxr-x 31 root      1004    4096 Aug 31  2018 SHARE_training
drwxrwxr-x 30 root      1003    4096 Jun 18 09:22 SHARE_workforce
drwxrwxr-x 28 root      1014    4096 Mar 26 09:36 SHARE_worldventures
drwxrwxr-x  5 root      1014    4096 Aug 31  2018 SHARE_wvvp
drwxrwxr-x 14 root      1015    4096 Apr  5 04:03 SHARE_zenefits

```

Figure 8

- Send the command **smbd -b** to check the build, and it should show the Samba version as 4.10.5.
- Advise any user to login by pressing Windows + R simultaneously, then entering [\\172.17.0.124](https://172.17.0.124), and user should be able to login and navigate to their campaign/department folder.
> note that all their current files should be present and full migrated
- Ultimately, scan the server using Nessus, and it should no longer show any vulnerability.

Back-out Procedures

- Log on to JKA-PESX-HV01 at <https://jka-pesx-hv01.openaccess.bpo/ui/#/login> using the root account.
- Click on Virtual Machines > select JKA-VLIN-FNP02.
- Right click on it then select Power Off, then select Delete.