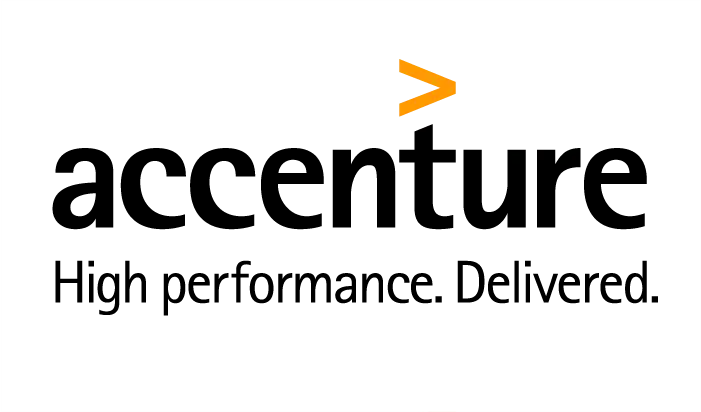
Logo

Description automatically generated 

**BHF Guide for User and SFTP setup in BODS and Apache Webserver v1.0**

Contents

[1 Introduction: 3](#_Toc98179728)

[2 Scope: 3](#_Toc98179729)

[2.1 Apache Webserver: 3](#_Toc98179730)

[2.2 BODS: 3](#_Toc98179731)

[3 ANF Mountpoints: 4](#_Toc98179732)

[4 Users: 4](#_Toc98179733)

[5 User setup: 5](#_Toc98179734)

[5.1 SFTP chroot: 5](#_Toc98179735)

[5.2 SSH key based authentication: 6](#_Toc98179736)

[5.2.1 Apache: 7](#_Toc98179737)

[5.2.2 BODS: 8](#_Toc98179738)

[6 PGP Keys: 8](#_Toc98179739)

[7 SSH Keypass: 8](#_Toc98179740)

[8 BODS Interfaces and testing: 9](#_Toc98179741)

[9 Revision History 10](#_Toc98179742)

# 1 Introduction:

The Brighthouse Financial (BHF) SAP infrastructure is hosted in Microsoft Azure cloud and amongst the various SAP application and Database servers, Apache Webservers and SAP BO Data Services (BODS) servers comprises various post deployment configurations which will be detailed in the following document.

# 2 Scope:

This document is scoped only to BHF Apache Webservers and SAP BO Data Services (BODS) servers. The document provides configuration details of the following.

* ANF mountpoints
* Local users
* SFTP configuration
* SSH key sharing
* PGP keys onboard
* Packages as on relevance

The server list is as below.

## 2.1 Apache Webserver:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **COMPONENT** | **SID** | **NAME** | **LOCATION** | **PRIVATE IP ADDRESS** |
| Apache Webserver | MFD | mfdap01use2dv | East US 2 | 10.213.37.6 |
| Apache Webserver | MFQ | mfqap01cusqa | Central US | 10.214.25.6 |
| Apache Webserver | MFP | mfpap01use2pr | East US 2 | 10.213.33.6 |

## 2.2 BODS:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **COMPONENT** | **SID** | **NAME** | **LOCATION** | **PRIVATE IP ADDRESS** |
| SAP BusinessObjects Data Services on HANA (App ) | BDD | bddap01use2dv | East US 2 | 10.213.36.24 |
| SAP BusinessObjects Data Services on HANA (App ) | BDD | bddap05use2dv | East US 2 | 10.213.36.62 |
| SAP BusinessObjects Data Services on HANA (App ) | BDD | bddap06use2dv | East US 2 | 10.213.36.64 |
| SAP BusinessObjects Data Services on HANA (App ) | BDD | bddap07use2dv | East US 2 | 10.213.36.66 |
| SAP BusinessObjects Data Services on HANA | BDQ | bdqap01cusqa | Central US | 10.214.24.5 |
| SAP BusinessObjects Data Services on HANA | BDQ | bdqap05cusqa | Central US | 10.214.24.74 |
| SAP BusinessObjects Data Services on HANA | BDQ | bdqap06cusqa | Central US | 10.214.24.76 |
| SAP BusinessObjects Data Services on HANA | BDQ | bdqap07cusqa | Central US | 10.214.24.78 |
| SAP BusinessObjects Data Services on HANA (App ) | BDP | bdpap02use2pr | East US 2 | 10.213.34.7 |
| SAP BusinessObjects Data Services on HANA (App ) | BDP | bdpap03use2pr | East US 2 | 10.213.34.9 |
| SAP BusinessObjects Data Services on HANA (App ) | BDP | bdpap04use2pr | East US 2 | 10.213.34.11 |
| SAP BusinessObjects Data Services on HANA (App ) | BDP | bdpcs01use2pr | East US 2 | 10.213.34.5 |

# 3 ANF Mountpoints:

|  |  |  |
| --- | --- | --- |
| **SERVERS** | **ANF VOLUME** | **MOUNTED AS** |
| MFP & BDP | 10.213.32.103:/MFP-SFTP/bhf | /bhf & /sftp/bhf |
| 10.213.32.103:/BDP-DATA/BHF | /BHF & /sftp/BHF |
| MFQ & BDQ | 10.214.25.100:/BHF-MFQ/MFQ\_SFTP | /bhf & /sftp/bhf |
| 10.214.25.102:/BHF-BDQ | /BHF & /sftp/BHF |
| MFD & BDD | 10.213.39.37:/BHF-MFD/MFD\_SFTP | /bhf & /sftp/bhf |
| 10.213.39.37:/BHF-SFTP/BHF | /BHF & /sftp/BHF |

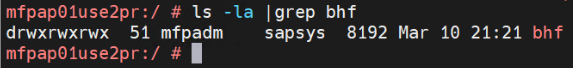
# 4 Users:

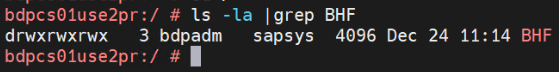
Apache Webservers houses external/3rd party SFTP users and an SFTP chroot configuration is in place for these users. BODS servers also house ETL users with ssh key based authentication. The list of users can be found below.

|  |  |  |
| --- | --- | --- |
| **SERVERS** | **USER TYPE** | **USERNAME** |
| Apache Webserver | OS | mfpadm (MFP) |
| SFTP | axway |
| aladdin |
| aon\_pathwise |
| bhf\_hr\_dev |
| bhf\_sftp\_dev |
| bloomberg |
| bondedge |
| ceridian |
| efa |
| gaalm |
| gep |
| ihs\_markets |
| kyriba |
| metlife |
| metlife\_dxc |
| metlife\_actuarial |
| metlife\_investment |
| metlife\_policyadmin |
| metlife\_treasury |
| murex |
| ofac |
| prophet |
| vaalm |
| vertex |
| bhf\_IIAM |
| bhf\_passport |
| corptax |
| madison |
| mmae |
| metlife\_essex |
| moodys |
| reged |
| SalesReporting |
| ETL | etlprocuser |
| OS | mfqadm (MFQ) |
| mfdadm (MFD) |
| BODS | OS | EIMBDP (BDP) |
| ETL | etlprocuser |
| eipdxcuser |
| SFTP | XP9585S377 |
| XP9585S464 |
| OS | EIMBDQ (BDQ) |
| EIMBDD (BDD) |

For the Apache Web servers, the mounts /bhf and /sftp/bhf should be owned by ‘sid’adm (mfpadm, mfqadm and mfdadm for the respective environments) and the user axway should posses CRUD privileges. Users should be part of the group “sapsys”.

For the BODS servers, the mounts /BHF and /sftp/BHF should be owned by ‘sid’adm (bdpadm, bdqadm and bddadm for the respective environments). The user should be part of the group “sapsys”.

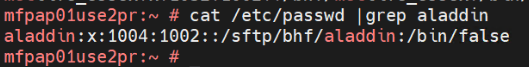


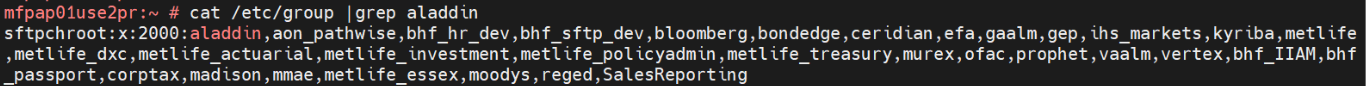


# 5 User setup:

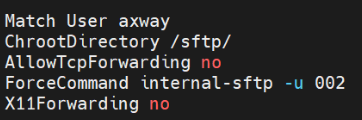
## 5.1 SFTP chroot:

The Apache Webservers were configured for SFTP access for the external users so as they access the SFTP directory and perform file transfers but cannot ssh into the server to access the OS. The “aladdin” is one such user that is created in the OS level as below. The user shell is defined as “bin/false” hence the ssh session will be denied.

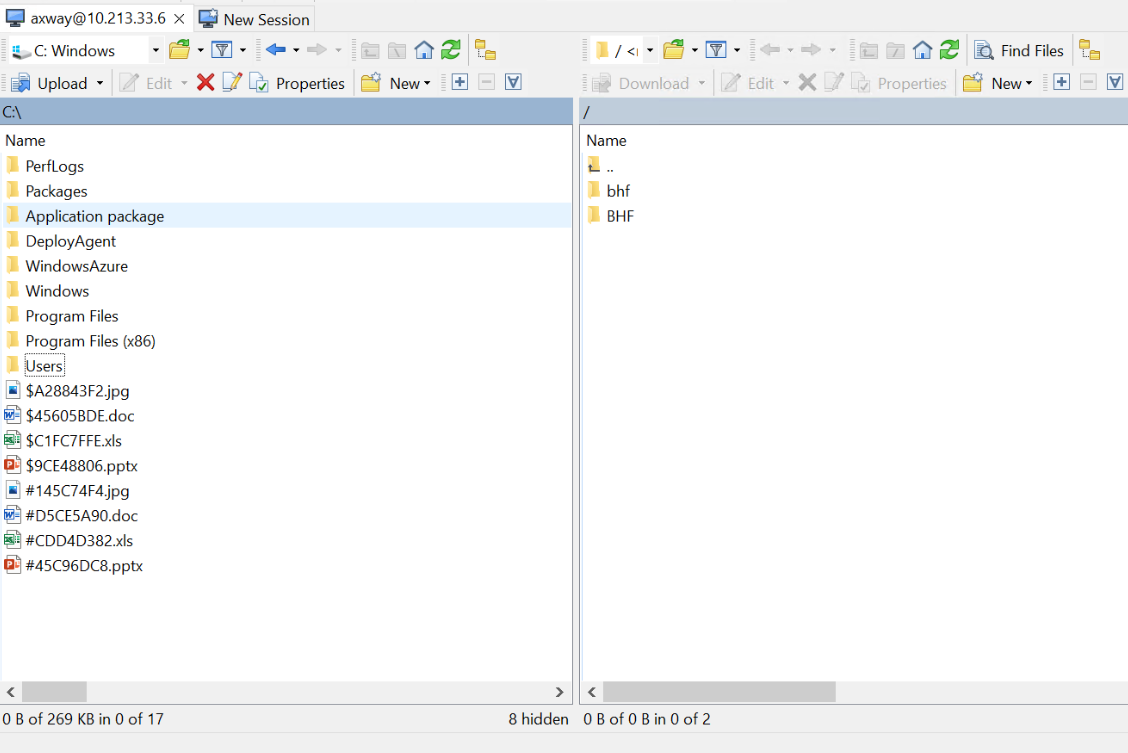




The users are added to the user group “sapsys” with gid 1002 as displayed above. For the SFTP setup, a separate group “sftpchroot” is created and the external sftp users are added to it. The sshd configuration must be updated to allow the setup to work as expected. The “axway” is one such user and the subsequent sshd configuration for the user is as below. The user will be landing on the /sftp directory and can only access its child directories. It will not be able to navigate outside of this directory.



This setup will ensure the axway user will only land on the folder /sftp which has both bhf and BHF folders that the user should be needing. The SFTP exhibit below shows the navigation pane on the right side which only shows the folders that it should access. The user cannot navigate to the root of the OS folders.



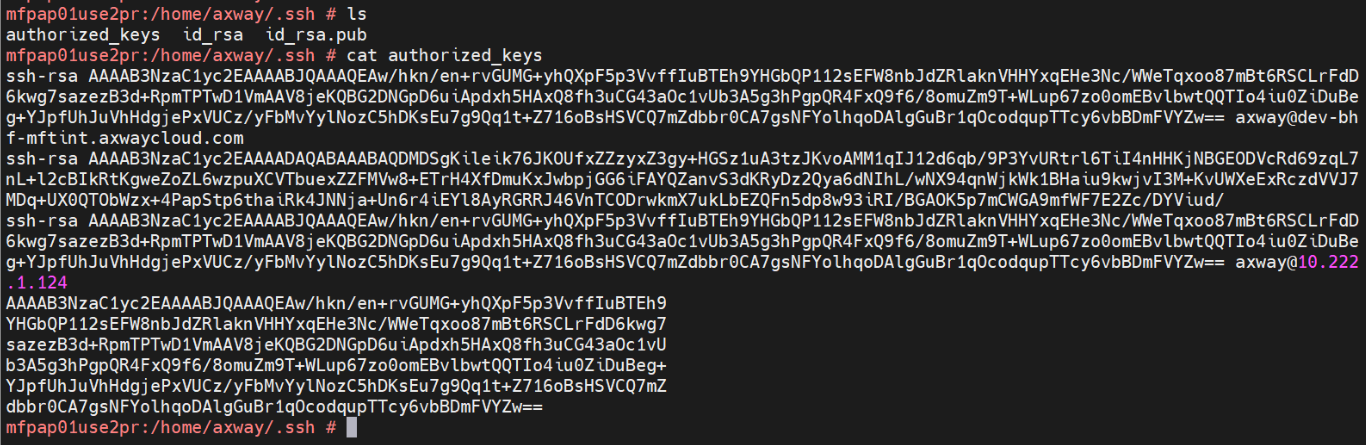
## 5.2 SSH key based authentication:

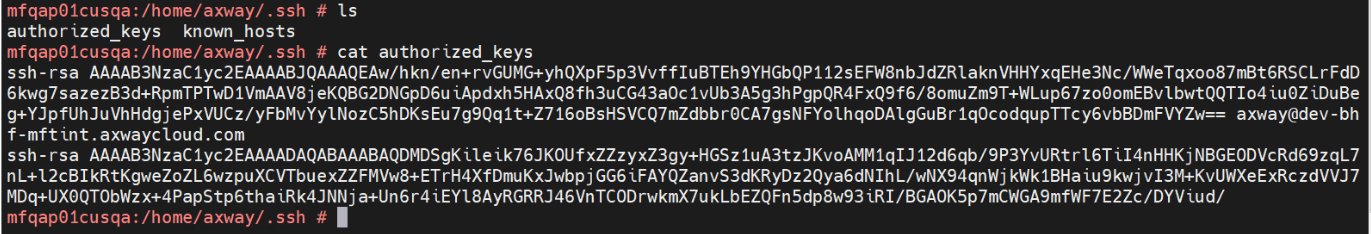
Both Apache Webservers and the BODS servers were configured with users to authenticate external hosts using ssh key based authentication. The users axway and ‘sid’adm are local users with passwords to access the server. The users etlprocuser and eipdxcuser are external vendor usernames for ETL loads.

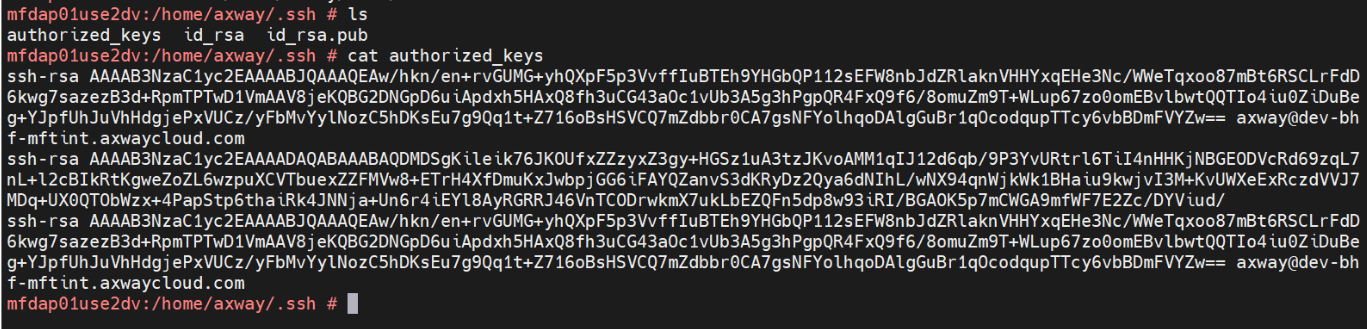
|  |  |  |
| --- | --- | --- |
| Server | Username |  |
| Apache | axway | Local |
| mfpadm | Local |
| mfqadm | Local |
| mfdadm | Local |
| BODS | etlprocuser | ETL |
| eipdxcuser | ETL |
| bddadm | Local |
| bdqadm | Local |
| bdpadm | Local |

### 5.2.1 Apache:

The user “axway” is locally created using password and has SSH keys exchanged from the vendor Axway from their respective Development, Quality and Production hosts which is imported into the respective servers in BHF.







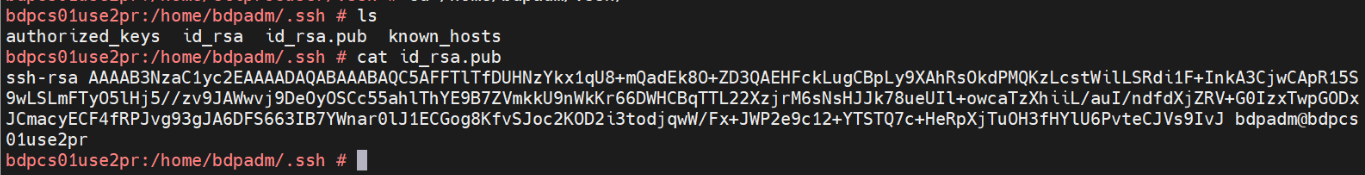
### 5.2.2 BODS:

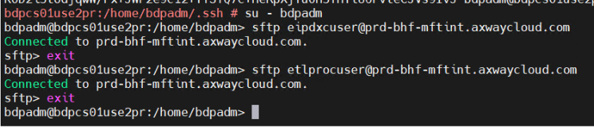
The ssh public keys for all the ‘sid’adm users and ETL users above were exchanged with the vendors. For MFT (Managed File Transfer) operations the ETL users are used and in this case the keys were exchanged with Axway.

SSH keys can be generated using the below command.

**#ssh-keygen**

The keys can be found in the following directory. Only the public key should be shared. Similarly the keys for etlprocuser and eipdxcuser can be shared with the vendor for password less authentication from the BHF servers to the external host. An example is also show below where the sftp connectivity is established without password prompt.





# 6 PGP Keys:

External vendor connectivity to Apache and BODS servers were authenticated using PGP keys. The list of PGP keys shared and imported on to BHF servers are listed in the below attachments.



# 7 SSH Keypass:

# 8 BODS Interfaces and testing:

Apart from axway, BODS needs external interface connectivity and the list of external vendors, and their hosts used for interfacing is as below. These interfaces were tested after the cutover window and tested to be working. Every connection has to be executed from the ‘sid’adm user prompt and not from the root prompt.

|  |  |  |
| --- | --- | --- |
| **External Interface** | **Interface Testing** | **Auth Type** |
| Blackrock | [sftp  bhfftp@199.242.7.3](mailto:bhfuat@199.242.7.3) | Password access |
| Ceridian | [sftp  CTS\_BRIGHTHOUSE@filemanagement.dayforcehcm.com](mailto:CTS_BRIGHTHOUSE@filemanagementtest.dayforcehcm.com) | Password access |
| Exterro | [sftp brightsftp@sftp.exterro.net](mailto:brightsftp@sftp.exterro.net) | Password access |
| Passport Pro | [sftp hac005s02@69.20.6.4](mailto:hac005s01@69.20.6.5) | Password access |
| Bondedge | [sftp BRIGHTHSFTPH1@ftpprod.icedataservices.com](mailto:BRIGHTHSFTPH1@ftpprod.icedataservices.com) | Password access |
| Bloomberg | [sftp dl790874@sftp.bloomberg.com](mailto:dl790874@sftp.bloomberg.com) | Password access |
| KBRA | [sftp brighthouse\_sftp@kbra.brickftp.com](mailto:brighthouse_sftp@kbra.brickftp.com) | Password access |
| Azure\_TAI\_SAMBA | sftp BHFWORKS\\\tai\_prod\_samba@azuresamba.bhfworks.net | Password access |
| Metlife | sftp [XP9585S482@extftp.metlife.com](mailto:XP9585S482@extftp.metlife.com) | Password access |
| Metlife | sftp [XP9585S393@extftp.metlife.com](mailto:XP9585S393@extftp.metlife.com) | Password access |
| Blackline | [sftp  brighthouse@192.188.251.35](mailto:brighthouse@192.188.251.35) | SSH |
| Blackline | [https://blprod.brighthousefinancial.com:7443](https://urldefense.proofpoint.com/v2/url?u=https-3A__blprod.brighthousefinancial.com-3A7443&d=DwMFAg&c=eIGjsITfXP_y-DLLX0uEHXJvU8nOHrUK8IrwNKOtkVU&r=sNjxB9dz37qu43Qjxbi-EoBHjYVZdtEdQPKGUi8Jj-4&m=0elx0iV8JTJWJExmtsHrXEMebCxEcmIyHDuAPlIHfHhfrhsJhYYhMXa4ytrc7Mfm&s=Kr24EwN0oCtZG9QuMpyfXvjG1caRJWQI_E-0BnnJ8Sg&e=) |  |
| Pathwise | [sftp  svcbhf103@10.224.7.13](mailto:svcbhf103@10.224.7.13) | SSH |
| ADP | sftp [BHFinGL@sdgcl.adp.com](mailto:BHFinGL@sdgcl.adp.com) | SSH |
| Informatica | EIP (sapeipdb01pr.bhfworks.net:30215) | SSH |

# 9 Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Approvers** | **Changes** |
| **1.0** | 14/3/2022 | N.Senthil Vel Murugan | Sasikumar Sampath | Initial Draft |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |