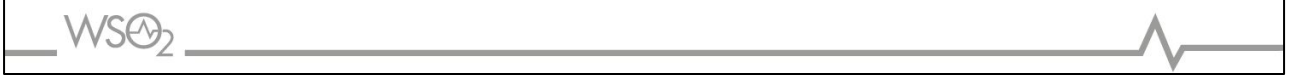

WSO2
WSO2 Product Administration
WSO2 Training
Module 09 - Backups and Disaster Recovery
CC BY 4.0

Backup What?

- Configurations
- Functional artifacts
- System data / Business data

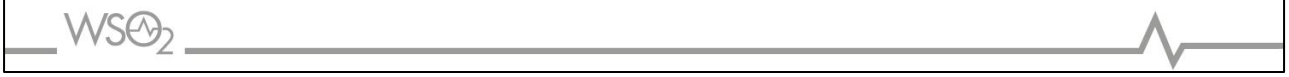


In a deployment, we need to backup Configuration files , Functional artifacts, Patches and Databases.
Let's see what these artifacts are and why we need to backup them.

Configurations

- File system based
    - conf directory configuration files
    - carbon.xml, axis2.xml, identity.xml
    - KeyStores
    - wso2carbon.jks, client-trust.store.jks
    - Startup script
    - wso2server.sh, JVM options and params etc
- Normal file backup

  or
- Automation Scripts



Configuration files directly affect deployment as they contain server specific details and tuning parameters of a setup.

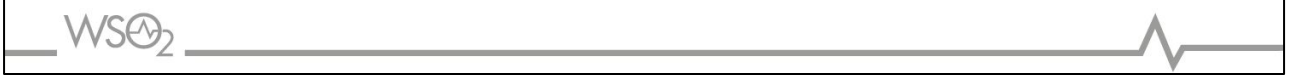
product_home/repository/conf/ directory contains all the configuration files. Keystores are located in /product_home/repository/resources/security/ folder. We also sometimes add various parameters and change parameter values in the startup scripts such as JVM options. Therefore this too needs to have a backup.

When configuration backups are available it is easy to simply replace the configurations rather than making the changes manually.

You can either manually copy them to a backup location or have automated scripts to copy the entire set of configuration files or to make the configuration changes on a new deployment.

Configuring Backup Techniques, Tools and Procedures

- Create templates of configuration files
- Maintain files with Key-Value pairs
- Use Automation Scripts (dynamic)
- To compile actual configuration files



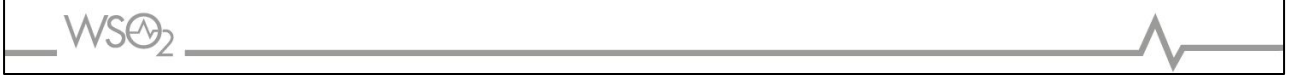
You can utilize various techniques to backup configurations.

You can maintain configuration files or templates of configuration files. Configuration file templates would be XML files with placeholders within elements. Key-value pairs of configurations can be maintained along with these XML templates.
Using these templates, configuration changes can be applied easily.
This is also useful during migrations, since configuration file changes could exists among versions.
In such cases the correct approach is to replace the relevant values rather than replacing the entire configuration file.

You can also involve automation scripts to backup configuration changes and apply them on new deployments.
It is also important to compile configuration files after making changes to ensure that there are no mistakes made while applying changes.

Functional Artifacts

- File system based
- Artifact repository
- Automated deployment



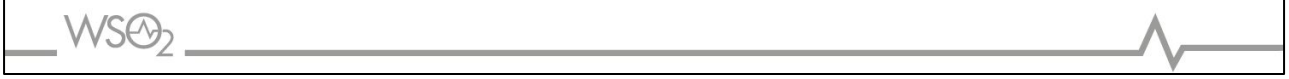
Functional artifacts are file based.

You can maintain an artifact repository, from which you can copy the artifacts to the new deployment.

You can also packed these in composite archive applications, which will be an easy way to re-deploy artifacts. This will be useful in automated artifact deployment as well.

Functional Artifact Backup Techniques, Tools, Procedure

- Compiled into archive file called Composite Application Archive
- Store in a subversion repository
- Replicated across servers
- Use automation scripts (dynamic) to automate deployment of artifacts



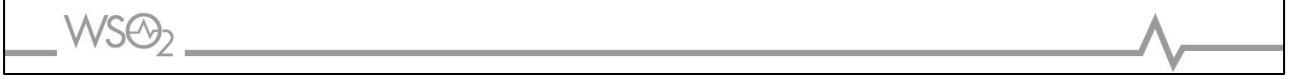
The recommended approach to deploy functional artifacts is to have them packed in a Composite Application Archive.

This will make it easier to redeploy, rather than deploying each artifact separately.

You can make use of automation scripts to backup these artifacts, and pack them in composite application archies and also to re-deploy them when required.

Updates

- Update the product using WUM
- WUM will contain the previous updated pack



Patches contains code level changes which directly affect the functionality.

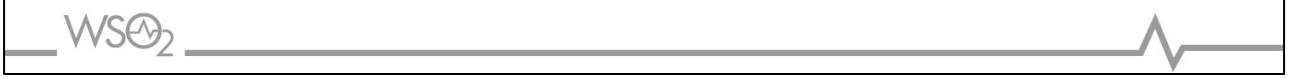
Therefore backups of a patches applied on each server type needs to be maintained.

To backup patches , you can take a backup of
<product_home>/repository/components/patches/ directory.
This will contain all the patches.

Patches may also be associated with configuration changes.
Ideally this will not be a problem, since configuration backups will also be taken.

Update Techniques, Tools, Procedures

- Use automation scripts
- Replace the old pack with the new updated pack using WUM



Patch restoration can be easily automated to replace the patch/ directory of the intended server with a backup of the patch/ directory of a certain WSO2 server.

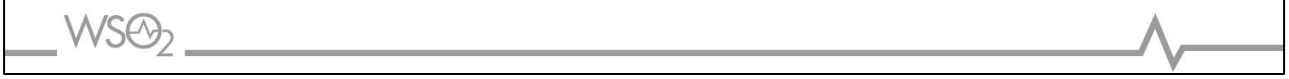
System/Business Data

System Data

- Registry based,
- Utilizes an RDBMS.
- Periodical database backup

Business Data

- Independent of WSO2 context
- Normal data backup



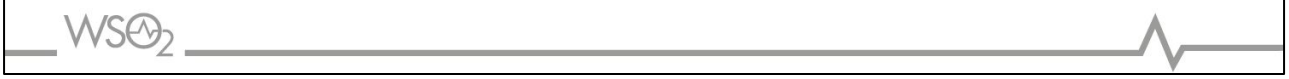
System data will be maintained in the registry and databases.

Business data will be maintained in documents and other artifacts which may be outside the WSO2 context.

The recommended practise is to take periodical database and system data backups.

System/Business Data, Techniques, Tools, Procedure

- Backups procedures may be vendor specific
- Periodically executed



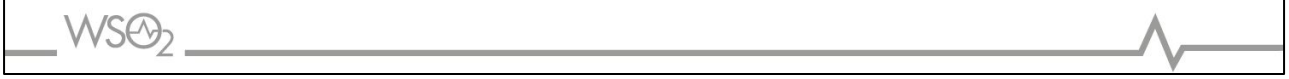
System and Business Data is independent of WSO2 context as mentioned earlier.

These are maintained in RDBMS.

Backup procedures for these can be vendor specific and periodically executed.

Disaster Recovery

- Routine backups / restoration drills
  - For DBs / artifacts
  - Restore to a last well known state
- Multi-site replication
  - Across different regions
- Automated recovery tools
  - Puppet as a service recovery tool
  - Boto as an EC2 and RDS recovery tool



In the case of disaster recovery, there are a number of procedures we can follow.

Backup availability is the most crucial factor in order to recover from a disaster. You can also restore systems to a last known stable state if possible. Deployments can be replicated across different regions to avoid failures in a specific region impacting another.
In addition you can use automated recovery tools such a Puppet and Boto depending on the deployment.

THANK YOU

wso2.com