

CIS Features

Created by Suruchi Suruchi 8 minutes ago

Below CIS Features have been included as part of Automation Toolkit. These are not part of CD3 but just included into SetUpOCI Menu "**CIS Compliance Features**".

1. Create Key/Vault, Object Storage Bucket and enable Logging for write events to bucket:

Below TF files are created:

[cis-osskeyvault-policy.auto.tfvars](#) TF variables file for allowing object storage service to use keys. This is created in Home region directory.

[cis-keyvault.auto.tfvars](#) TF variables file for creating the key/vault in the specified compartment and region. This is created under the specified region directory.

[cis-oss.auto.tfvars](#) TF variables file for creating OSS bucket using above key (instead of Oracle Managed Keys). This is also created under specified region directory.

[cis-oss-logging.auto.tfvars](#) TF variables file for enabling logging for write events of the above created bucket. This is also created under specified region directory.

2. Enable Cloud Guard

This will enable cloud guard for tenancy from home region, create Oracle Managed detector and responder recipes. Also creates a target for root compartment with the default Oracle Managed recipes.

Below TF file is created:

[cis-cloudguard.auto.tfvars](#) TF variables file for enabling cloud guard and creating target for root compartment.

3. Enable VCN Flow Logs

This will enable Flow logs for all the subnets mentioned in 'Subnets' tab of CD3 Excel sheet. Log group for each VCN is created under the specified compartment and all subnets are added as logs to this log group.

Below TF file is created:

[cis-vcnflow-logging.auto.tfvars](#) TF variables file containing log group for each VCN and logs for each subnet in that VCN.

No labels