…configure SSSD authentication & SUDO configuration

Mosaic macros cannot be exported to PDF.

Application specific "root" SUDO Configuration

In the event that there are specific root commands which need to be run in relation to an application start/stop or checks, then a separate SUDO configuration can be created.

The implementation or update of any SUDO configuration which allows the running of commands under the root user must be vetted and approved by the FA & Kyndryl teams. If individual commands cannot be uniquely stated, then the commands may need to be run via script (owned and modifiable by the root usercode only), and that script added to the SUDO configuration.

Required SUDO Active Directory group: GG_<Application AL Code>_FA_ADMIN

If required, this new AD Group should be requested and added to the Service Account as part of the Service Account creation (See Confluence Section 1.1.5).

Once the service account and group have been created, the SUDO configuration can be requested from the Tooling Services team.

The root SUDO configuration object in ALDS (this object should have a Class of sudoRole) should be configured as follows:

sudoHost : ALL

sudoUser : %SRVAPP<Application AL Code>R01

sudoOption : EXEC

sudoRunAsUser : root

sudoCommand : <full directory path to command>/<command> <parameters>

NB. Multiple sudoCommand entries can be applied to the same object i.e. 1 for each command/parameter combination

Application specific non root SUDO Configuration

The non root SUDO configuration is to allow the service account to run commands under the application owning Linux account.

It is preferable that application commands (stop/start/restart/checks etc) are run via a bash script owned and maintained by the application team. This means that any changes required due to application upgrades etc can be carried out by the application team without any changes to the non root SUDO configuration, or the related DR Pipelines.

Required SUDO Active Directory group: GG_<Application AL Code>_FA_ADMIN

If required, this new AD Group should be requested and added to the Service Account as part of the Service Account creation.

The root SUDO configuration object in ALDS (this object should have a Class of sudoRole) should be configured as follows:

sudoHost : ALL

sudoUser : %SRVAPP<Application AL Code>R01

sudoOption : EXEC

sudoRunAsUser : <Local Linux Application User>

sudoCommand : <full directory path to command/script> <parameters>

Where <Local Linux User> is the local, non root, linux account on the server under which the command should be run. This is probably the account under which the application is installed/run.

NB. Multiple sudoCommand entries can be applied to the same object i.e. 1 for each command/parameter combination

There are 2 ways to run the non root linux commands/scripts and your sudoCommand rules may be different depending on your requirements.

Simple Linux Application Script

The Simple Application Script template runs the command as the target user. All that is returned is success/failure and the console output text from the command script

In this case each individual command/script (and preferably the specific parameters) should be defined in separate the sudoCommand lines

Complex Linux Application Script

The Complex Linux Application Script template has the capability to return up to 5 output variables from the application script. Any output variables must be exported as environment variables which can then be returned via the templated stage.

To utilise this capability a "wrapper" script must be deployed to the application server and the line "sudoCommand: /opt/fa/scripts/faWrapper.sh" should be added to the sudo configuration. The wrapper script will be run under the target application user, will run the required scripting and will

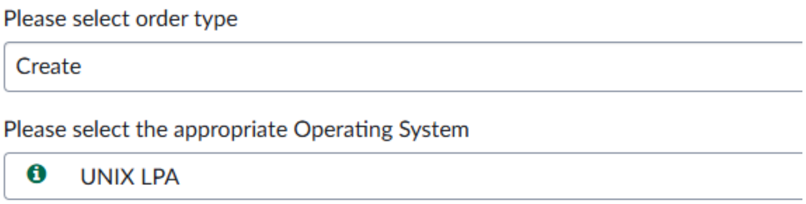
Requesting Initial SUDO configuration Rules (dev/iaglobal)

Configuration of SUDO rules in ADLDS is performed by the Unix Identity and Access Management team via the Least Privileged Access form on IT@LBG.

A request will be required for each environment, but these should be submitted as they are required/validated (see section 1.2.5)

NB. The rules are defined the same across the route to live.

The form should be completed as follows



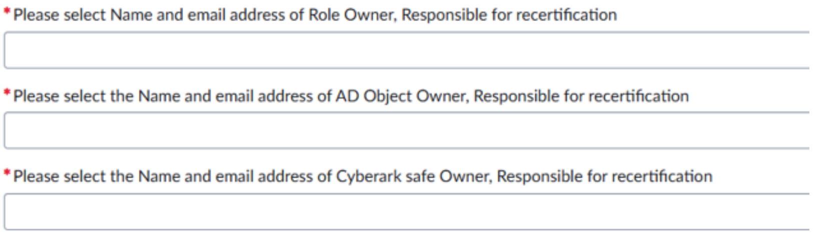
Please select order type

Create

Please select the appropriate Operating System

UNIX LPA

The next section will probably be Application specific, but will probably be populated with the Failover Automation Service Account owner



*Please select Name and email address of Role Owner, Responsible for recertification

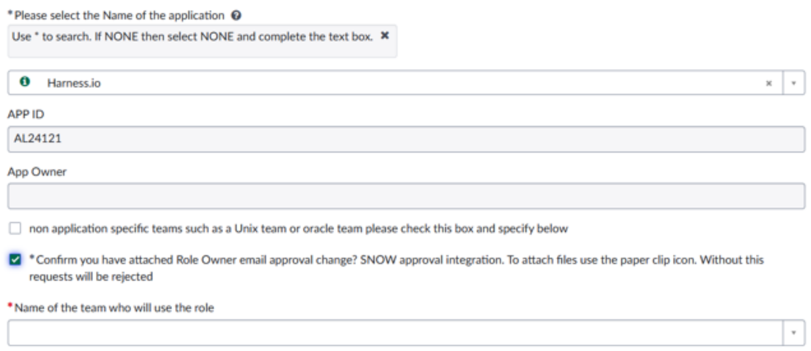
*Please select the Name and email address of AD Object Owner, Responsible for recertification

*Please select the Name and email address of Cyberark safe Owner, Responsible for recertification

Select your application as required.

You should attach an approval e-mail from the failover automation service account owner for the creation of the new LPAU Role (configuration).

For the name of the team who will use the role, please select the ServiceNow team for the application run/support team.



*Please select the Name of the application

Use * to search. If NONE then select NONE and complete the text box.

Harness.io

APP ID

AL24121

App Owner

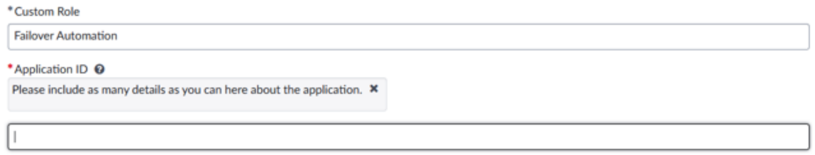
□ non application specific teams such as a Unix team or oracle team please check this box and specify below

☑ *Confirm you have attached Role Owner email approval change? SNOW approval integration. To attach files use the paper clip icon. Without this requests will be rejected

*Name of the team who will use the role

In custom role enter Failover Automation

And the application ID in the Application ID field (it should be displayed in the previous section)



*Custom Role

Failover Automation

*Application ID

Please include as many details as you can here about the application.

Finally the Role entitlements should contain the

The request should specify

- Covering Summary including the doman (IAGLOBAL)
- The development servers the rules should be applied to (Full FQDNs should be included)
- The separate configuration objects required as per Sections 1.2.1 & 1.2.2

e.g.

This request is for the configuration of SUDO rules in IAGLOBAL.

These rules are for utilisation of the Failover Automation framework to automate DR failover tasks.

Application Servers

appduv12345.onprem.cloud.test.group

appduv12346.ibmsl.cloud.test.group

The following 2 sudoRule class objects are required

sudoHost : ALL

sudoUser : %SRVAPPAL12345R01

sudoOption : EXEC

sudoRunAsUser : root

sudoCommand : /bin/systemctl start application.service

sudoCommand : /bin/systemctl stop application.service

sudoHost : ALL

sudoUser : %SRVAPPAL12345R01

sudoOption : EXEC

sudoRunAsUser : appuser

sudoCommand : /opt/fa/scripts/faWrapper.sh

sudoCommand : /opt/application/scripts/app_start.sh

sudoCommand : /opt/application/scripts/app_stop.sh

Adding the configuration to a server

In order for the configurations to be applied to a server, the UNIX configuration must be updated with the create AD Groups

NB. This should be carried out as part of the LPA request and is only included here for completeness

This AD Group must be added to the Linux Server configuration by the Unix Identity Services team as per the following instructions

Edit /etc/sssd/sssd.conf

Find line which begins simple_allow_groups (probably the last line in the file)

Go to the end of the line add the required group as part of the comma separated list

GG_<App AL Code>_FA_ADMIN

Update /etc/nsswitch.conf to enable Active Directory for sudoers configuration.

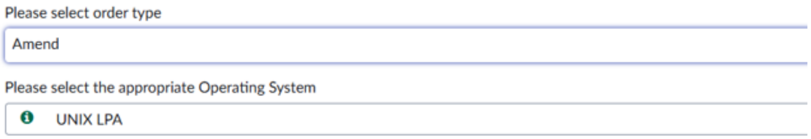
This file should not be updated manually, instead the following command as the root user

authselect enable-feature with-sudo

Amending the SUDO configuration (Including pushing to the other domains)

Amendments to the SUDO rules, or requesting them to be rolled out across the domains uses the same Least Privileged Access form on IT@LBG

Complete the form as follows



Please select order type

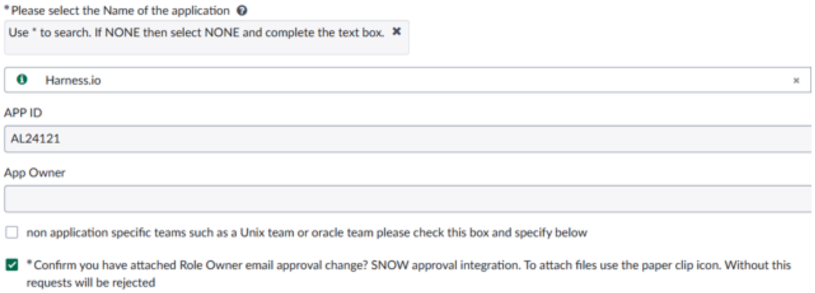
Amend

Please select the appropriate Operating System

UNIX LPA

Select your application as required.

You should attach an approval e-mail from the failover automation service account owner for the creation of the new LPAU Role (configuration).



*Please select the Name of the application

Use * to search. If NONE then select NONE and complete the text box.

Harness.io

APP ID

AL24121

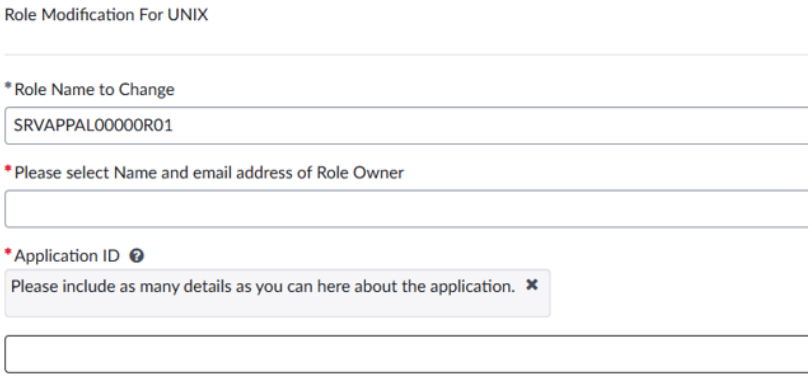
App Owner

□ non application specific teams such as a Unix team or oracle team please check this box and specify below

☑ *Confirm you have attached Role Owner email approval change? SNOW approval integration. To attach files use the paper clip icon. Without this requests will be rejected

In custom role enter the Failover Automation Service Account for your application (This will be the role name)

And the application ID in the Application ID field (it should be displayed in the previous section)



Role Modification For UNIX

*Role Name to Change

SRVAPPAL00000R01

*Please select Name and email address of Role Owner

*Application ID

Please include as many details as you can here about the application.