AWS Organisation Setup

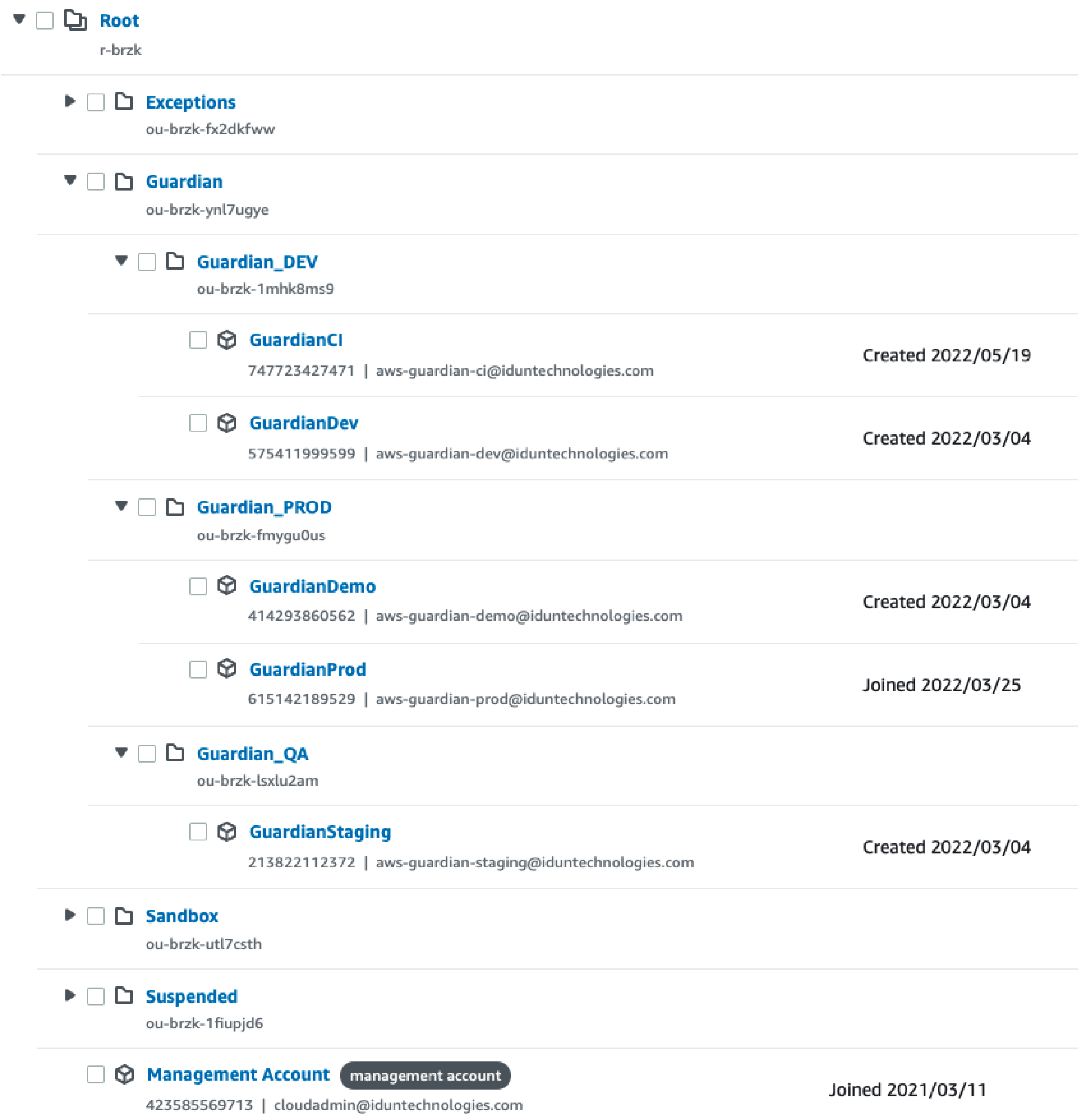
We use one AWS organisation with multiple accounts for all our cloud activities here at IDUN. We have followed the official AWS best-practice documentation when setting up our cloud accounts:

Establishing your best practice AWS environment - Amazon Web Services

AWS enables you to experiment, innovate, and scale more quickly, all while providing the most flexible and secure cloud environment. An important means through which AWS ensures security of your applications is the AWS account. An

https://aws.amazon.com/organizations/getting-started/best-practices/

The documentation points out that you should use different organisational units (OUs) for different technical teams and tasks like security, infrastructure, etc. We decided to build organization units based on application lifecycle stages (Sandbox, DEV, QA, PROD), letting us easily control access rights, if needed, based on the stage. Typically almost anything is allowed on sandbox environments, but on production environments changes are typically allowed only trought pre-defined process. Here is a screenshot of the current organisational structure with OUs and separate AWS accounts:



- ▼ □ **Root**
  r-brzk
  - ▶ □ **Exceptions**
    ou-brzk-fx2dkfww
  - ▼ □ **Guardian**
    ou-brzk-ynl7ugye
    - ▼ □ **Guardian_DEV**
      ou-brzk-1mhk8ms9
      - □ **GuardianCI**
        747723427471 | aws-guardian-ci@iduntechnologies.com — Created 2022/05/19
      - □ **GuardianDev**
        575411999599 | aws-guardian-dev@iduntechnologies.com — Created 2022/03/04
    - ▼ □ **Guardian_PROD**
      ou-brzk-fmygu0us
      - □ **GuardianDemo**
        414293860562 | aws-guardian-demo@iduntechnologies.com — Created 2022/03/04
      - □ **GuardianProd**
        615142189529 | aws-guardian-prod@iduntechnologies.com — Joined 2022/03/25
    - ▼ □ **Guardian_QA**
      ou-brzk-lsxlu2am
      - □ **GuardianStaging**
        213822112372 | aws-guardian-staging@iduntechnologies.com — Created 2022/03/04
  - ▶ □ **Sandbox**
    ou-brzk-utl7csth
  - ▶ □ **Suspended**
    ou-brzk-1fiupjd6
  - □ **Management Account** management account
    423585569713 | cloudadmin@iduntechnologies.com — Joined 2021/03/11

What the different hierarchical items mean

- **Root:** This is the root directory of the organisation. It does not contain a user or an individual AWS account. It is basically the root directory of the entire organisation from the management account that this organisation originally created.
- **Exceptions:** Everything that is not part of our core development efforts belongs here. If we use Infrastructure as Code (IaS), we can simply copy entire cloud setups to another AWS locations, for example, and start working on them there.
- **Guardian:** Our Guardian product and its application lifecycle environments belong here. Each organization unit under Guardian OU has one or more AWS accounts.
  - **Guardian_DEV:** Developers have access to the accounts under this OU via the graphical user interface (AWS Console) and command line interface (AWS CLI, SDK,

    API, etc.). Even if developers have broad access rights to these accounts, it is highly recommended that developers do not make changes to the environments manually. Instead, changes should be applied only through Github repository with automated actions.

        - **GuardianCI:** This account is used to test automatic deployment of infrastructure changes. The infrastructure deployment is automatically triggered by a Github Action when a PR is opened to merge infrastructure changes or new infrastructure feature from feature development branches to the **develop** branch
        - **GuardianDev:** This account is the first one where developers merge their different development tasks into to be able to test the solution from end-to-end. Deployments to this account are made automatically by Github Actions after merging the PR to the **develop** branch.

    - **Guardian_QA:** This organization unit contains accounts used for quality assurance and pre-production testing of the Guardian solution. DevOps have access to these accounts via the graphical user interface (AWS Console) and CLI (SDK, API, etc.). Again, even if DevOps have access to these accounts, it is highly recommended that no changes are made to the environments manually. Instead, changes should be applied only through Github repository with automated actions.
        - **Staging:** This account is used for quality assurance and pre-production testing. Changes to this account is deployed automatically by Github Actions when changes are merged to the **staging** branch.
    - **Guardian_PROD:** This organization unit contains all production accounts. Only the super admin role has access to the AWS Console of these accounts. Again, not even the super admin should do any changes to these accounts manually. All changes should be applied only through Github repository with automated actions.
        - **Prod:** Production environment. Changes to this account is deployed automatically by Github Actions when changes are merged to the **production** branch.
        - **Demo:** A replica of the production environment for demo purposes. Changes to this account is deployed automatically by Github Actions when changes are merged to the **demo** branch.
- **Sandbox:** This OU includes all sandbox accounts of developers or others who want to play and test with AWS without providing any payment information. These accounts have access to our AWS credits, but with a limited budget. If you would also like to have a sandbox account, please contact a cloud administrator (@Daniel Burger or @Andy).
- **Suspended:** All accounts that are currently blocked (90 days default) belong to this OU and will be deleted once they have been successfully blocked.
- **Management Account:** This is the account that this organisation has created. It is linked to the AWS credits and is responsible for accounting.

> 💡 For historical reasons, we created the first version 1.0 of the Cloud and Web App in the management account. Since you can't change the management account in an AWS organisation, we have to stick to it. **Once our new version is deployed in the appropriate environment (ergo AWS account), we can get rid of the resources in that AWS account.**

IAM Setup

https://viewer.diagrams.net/?border=0&tags=%7B%7D&highlight=0000ff&edit=_blank&layers=1&nav=1&open=R%3Cmxfile%3E%3Cdiagram%20id%3D%22MkyzM2U7BuFslQKI_Bwn%22%20name%3D%22Page-1%22%3E5Zpbc6IwGIZ%2FjZfOyFG4VOu2nW27u3W6h97spCRCpiGxIZ766zdIUCE4daYK6uqF8IZDeN6PL%2FkytqxBvLjmYBLdM4hIy%2BzARcu6apmm6fmW%2FEmVZaYYhudmSsgxVNpGGOF3pMSOUqcYoqRwoGCMCDwpigGjFAWioAHO2bx42JiR4l0nIESaMAoA0dVfGIooUz2zu9FvEA6j%2FM6G62ctMcgPVk%2BSRACy%2BZZkDVvWgDMmsq14MUAkpZdzyc77sqN13TGOqNjnhNHb8vrv8Ped2XaTRWAn7Gr01M4xzwCZqidWvRXLHAFnUwpRepVOy%2BrPIyzQaAKCtHUuXZdaJGIi9wy5qfdKdXSGuECLLUn18hqxGAm%2BlIeo1ralOjXfADc6vhKjLdpOLgLlcri%2B2AaE3FAsqrkk3d6zf3e%2FjH7MXP58w27%2BJLRtaFgeU6NMl8hb91%2B43ArTrV4QSDpCY%2FYBJZBMsmAd40VKtj%2FGhAwYYXx1ujX2AhQEUk8EZ69oq%2BXFc2yncxjQtqfwrV9OWwPvVWD3DkC9Oho16qvX4yzhltharh7UtbI1K150Fc15MEM0yzV5i7X8uYRQhu%2Bk31RnVGzp2afKFHf1OYwpbtEU06%2FINGaFK%2B6xXLE%2BdiURIMQ0vHBn7JOzxt7nhYnZhfvinpwvzse%2BTDiDF%2B6L55yaL%2B4FDd7lmVHjo3f3guC6pwbXuyC4XvfE4Poa3HtAZdUcp89odnYVUHUXnbZd5GbrpZDh1plODb0Y0sY5DKe0LVAQyeMYDwHF70BgRvca%2ByQYUcRYDEzKKCpFsZIAwSGVuwSN0yukkHEASE%2FJMYYwvUmla0VfD2DcGlRexO5pnHU04%2FQJymg6QbwHY0xvafsKzYZ0dtipyBi51akFdv2XznEqWnvPzHK8N0TP2xvQZ8i3PNOuiGTfqBNwPn3cFcmjrDI9z2guT%2FEaD2dTT%2FilvBGz80RdnvA1j3qP2v6REZTUNJAGki3ijQ%2BlRsmmrqPZZNc5kpp61aPZ9JRIcP%2BzS3JQaNYlS3epkLe%2BcwbPM2%2BVa6k685Y%2FTW6XXx%2Fgz4c56zn918e7b2%2F7rOEH%2BPQXvjQHKnzaaYrZ5MJXpSv6Gn6jywefo9vg8kElXH2kLiSXwW1jqeWgnI%2BYWuTu5k8Gq7at%2F2pYw38%3D%3C%2Fdiagram%3E%3Cdiagram%20id%3D%22LjBHnL4FIQbr7x8Ty_Sl%22%20name%3D%22Page-2%22%3E7VrLdtowEP0alumxLdmYJYG0XTSvsmi7FJawlcqWI0SAfn1lLOPnIScEYudgNkjX0kiaO%2BOrSRiASbj5JlAc3HJM2MAy8GYApgNLfVxTfSXINkVMA8IU8QXFGsuBGf1HsoEaXVFMlqWBknMmaVwGPR5FxJMlDAnB1%2BVhC87Kq8bIJzVg5iFWR39RLIMUda1hjn8n1A%2ByIU1nlD4JUTZYn2QZIMzXBQjcDMBEcC7TVriZEJZ4L%2FMLe767Xz%2FGz%2FP78ROe3j%2BEj%2FO7q9TY17dM2R9BkEie1nTmnhfEVtph%2BrBym3lQ8FWESWLFGIDrdUAlmcXIS56uVdAoLJAhUz1TNbU5IiTZVAh4Zffm3qUqGAkPiRRbNU9bARkLOg6h7q5zTvdYUODTcjWIdBz5e9O5r1RDu%2BstrrNqrvuZxILlMLX29VyoIp%2B0xp6nPChrfn3Fk2gZp%2FmwoJvE%2B9cLytiEMy5208HC9YjnKXwpBf9LCk%2Fmrg1t44xkQKNMhmnaNTbcBjLOxwVoCGPNQ0bDLYpUrofJuS1jz0k6SC26H1fjSTlPlqkpezziEanQoyHEqB%2BprqcWJQq%2FTqig6t001g9CinGyTGNWlfPubIk1LHM5rFNpNiUWOBeX0K0xQLB6pesuFzLgPo8Qu8nRiq%2FyMT84jzVpT0TKrdYntJK8TKIyodj%2BTuZ%2FsbPuH21u15IuSr1tiZZkg0eQog7JV8IjhyJb0yGR8Mkhg8BoplkQhiR9KW%2Fv9KSNetKOIQ2%2Bk7Td1LEQaFsYEHMayWXB8kMCFFK%2B8vq2oF0JgNRiHg77rR0fIbbRR8gxEeK2ESG220aEmH2EHBEh0GrzxZ9ts3Dzmq1iIhquwTik0ckvwQviNF%2BC8XA0Nz7yEmwZLV%2BCsxtZ52u5K7PiOuC0Xs2BeiF8KdXcVbW0Bm0Hcr2yrlVzU%2FLSl3FFEu1KSo3aruNAvSY%2FrAxV%2BCdXPj1xmmGbuBg2pZlrzYHjfGCa2VbbaQY%2FiV6Ybvfkon7tuRS5sJyuyYXzulzMJPJp5PeSUSQSdE4yhr1kHEq19iXD%2FSSSAZ3uScboYiXDhh2TjGw%2FhyuMkPd6UWTR7JpewHrRftF6Uc2z1vUCNlXy79ELjJbBbuw5xWMIOycesF5MX4p4uF

378xRsqpsr4vEgOO7Fo5hTo86JR19sHMyzM4qH6uY%2Fm0v%2FfZj%2F%2BhDc%2FAc%3D%3C%2Fdiagram%3E%3C%2Fmxfile%3E

Each of the accounts for the application lifecycle environment within the Guardian OU has its own root account, secured via a separate email address and MFA authentication. The `SuperAdmin` account in the management account is an IAM admin user and can access the resources of the other AWS accounts via IAM roles for a maximum of 1 hour each. Both the SuperAdmin account and the root account of the management account should never be used for anything despite deep organisational changes to our AWS setup or risky security modifications. Otherwise, developers are invited to the management account via IAM and then given IAM roles to work on the various application lifecycle environments/AWS accounts with appropriate restrictions.

💡 All passwords and MFA codes are handled by the cloud admins @Daniel Burger and @Andy. Ask them if you need any help regarding security, questions about authentication and authorisation.