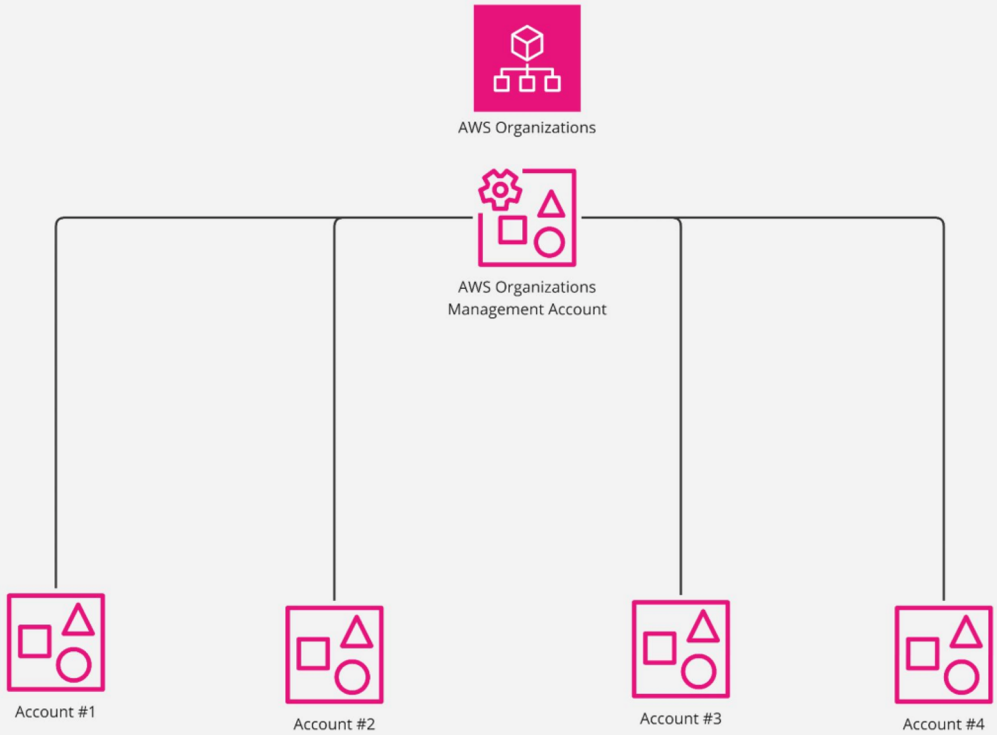
Automating AWS Organizational Management

University of Wisconsin - Madison

Key Concepts



Q: What is an organization?

An organization is a collection of AWS accounts that you can organize into a hierarchy and manage centrally.

Q: What is an AWS account?

An AWS account is a container for your AWS resources. You create and manage your AWS resources in an AWS account, and the AWS account provides administrative capabilities for access and billing.

You or a technical person you love may have asked yourself...

Is my configuration consistent?

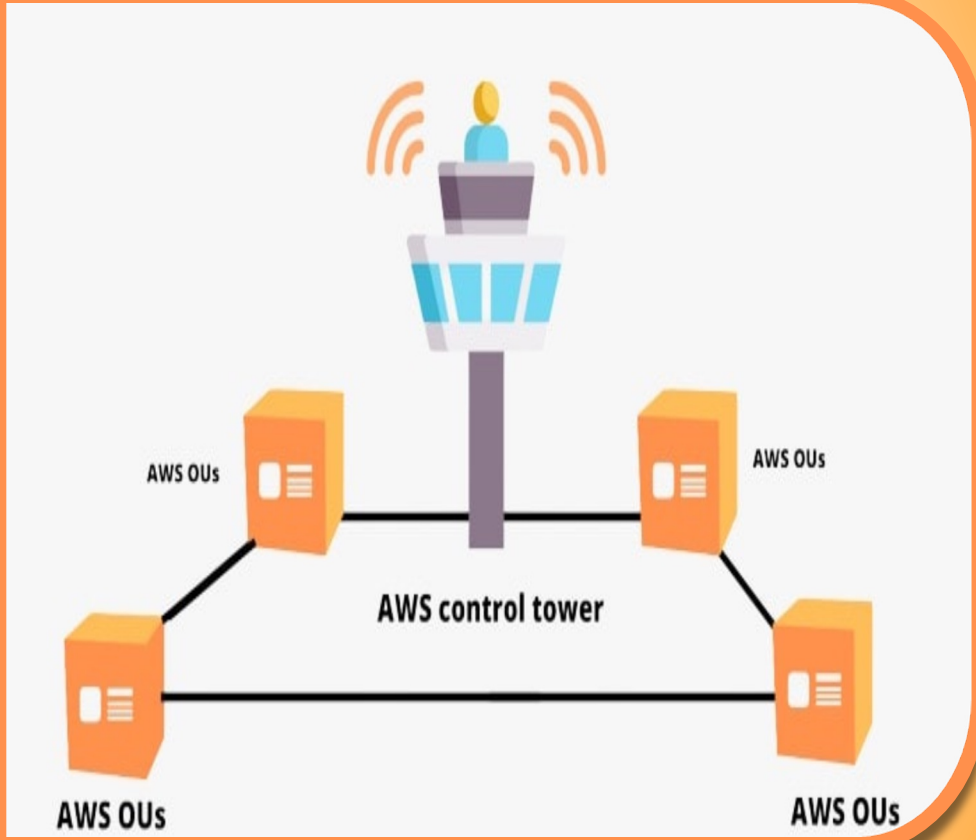
How do I audit my configurations?

How can I apply a change to all of my accounts?

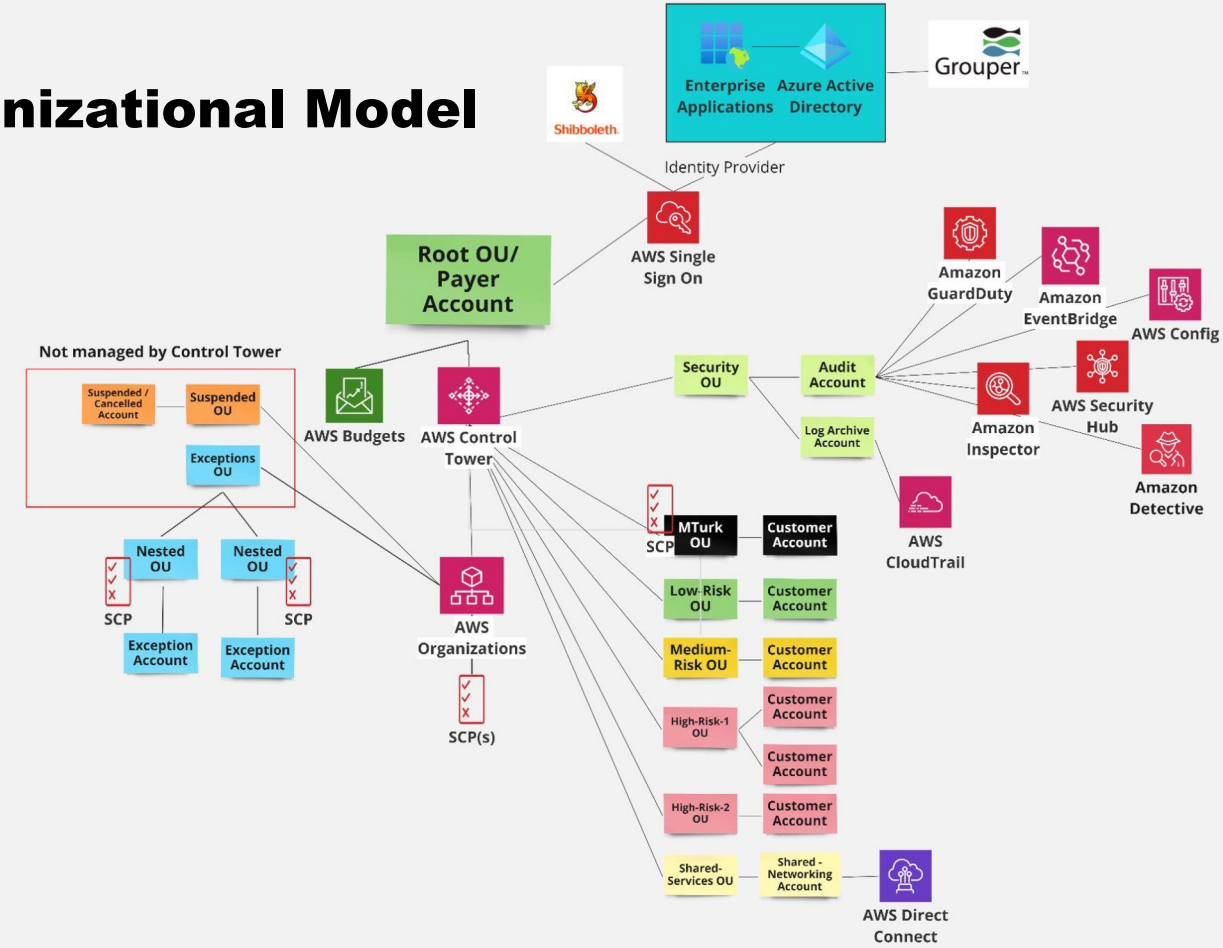
How will I know if someone changes the configuration?

AWS Control Tower

AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment, following prescriptive best practices. AWS Control Tower *orchestrates* the capabilities of several other AWS services, including AWS Organizations, AWS Service Catalog, and AWS IAM Identity Center. AWS Control Tower orchestration extends the capabilities of AWS Organizations.



Our Organizational Model



Security Posture Management

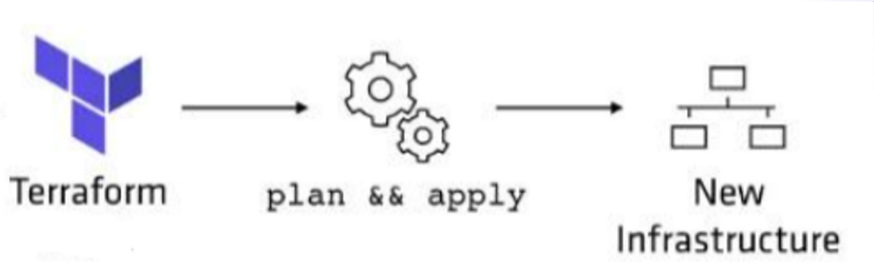
Security Tools

Centralized Alerting

Centralized Logging

Security Control Policies

HashiCorp Terraform



HashiCorp Terraform is an infrastructure as code tool that lets you define both cloud and on-prem resources in human-readable configuration files that you can version, reuse, and share

You can then use a consistent workflow to provision and manage all of your infrastructure throughout its lifecycle. Terraform can manage low-level components like compute, storage, and networking resources, as well as high-level components like DNS entries and SaaS features.

Create New Accounts Quickly

1. Create Account Email Address and User Groups for SSO
2. Add Email Address, Account Name and OU to accounts.csv file and run Terraform
3.
4.

Create New Accounts Quickly

```
: Refreshing state... [id=subnet-0ee068b042e30070b]

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
  + create

Terraform will perform the following actions:

  # module.aws_accounts.aws_organizations_account.account["hallah-fake"] will be created
  + resource "aws_organizations_account" "account" {
      + arn               = (known after apply)
      + close_on_deletion = false
      + create_govcloud   = false
      + email             = "hjhussien@wisc.edu"
      + govcloud_id       = (known after apply)
      + id                = (known after apply)
      + joined_method     = (known after apply)
      + joined_timestamp  = (known after apply)
      + name              = "hallah-fake"
      + parent_id         = "ou-nfly-rpu6hthf"
      + status            = (known after apply)
      + tags_all          = (known after apply)
    }

Plan: 1 to add, 0 to change, 0 to destroy.
```

Create New Accounts Quickly

Quickly New Acco

```
+ ipv6_cidr_blocks = [
    + "::/0",
  ]
+ prefix_list_ids  = []
+ protocol         = "-1"
+ security_groups  = []
```

environments > dlt-university-of-wisconsin-madison-3 > main.tf > ...

```
779  # account doit-at-trad
780  module "aws_account_baseline_doit-at-trad" {
781    source     = "../../modules/modules-complex/modules-complex-standard/aws-account-baseline-standard/regions"
782    account_id = "465281859793"
783  }
```

```
+ ipv6_cidr_blocks = []
+ prefix_list_ids  = (known after apply)
+ protocol         = "tcp"
+ security_groups  = []
+ self             = false
+ to_port          = 22
    },
  ]
+ name                   = "uw_ssh_allowed_list"
+ name_prefix            = (known after apply)
+ owner_id               = (known after apply)
+ revoke_rules_on_delete = false
+ tags                   = {
    + "Name"       = "uw_ssh_allowed_list"
    + "created_by" = "public_cloud_team_read_only"
  }
+ tags_all               = {
    + "Name"       = "uw_ssh_allowed_list"
    + "created_by" = "public_cloud_team_read_only"
  }
+ vpc_id                 = (known after apply)
}

Plan: 55 to add, 0 to change, 0 to destroy.
```

4

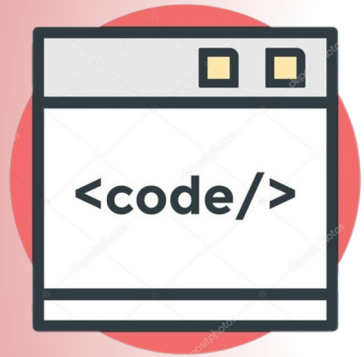
Change Management Made Easy

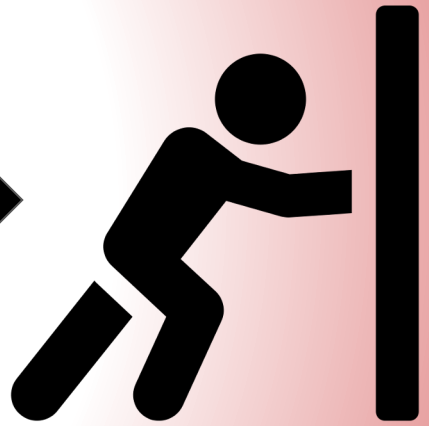
Infrastructure as code allows for peer reviews before merging the branch of code into main

It also ensures that everyone is running the same code when making infrastructure changes.

```
PS C:\Users\hjhussien\Documents\Code\AWS\aws-accounts\environments\dlt-university-of-wisconsin-madison-3> terraform plan

Error: Provider configuration not present

To work with
module.aws_iam_service_accounts.module.aws_programatic_user_833435016045_calabrio_user.module.aws_iam_attach_custom_policy[0].aws_iam_policy.policy
(orphan) its original provider configuration at
module.aws_iam_service_accounts.module.aws_programatic_user_833435016045_calabrio_user.provider["registry.terraform.io/hashicorp/aws"] is required,
but it has been removed. This occurs when a provider configuration is removed while objects created by that provider still exist in the state. Re-add
```

What happens when we need to roll out a change to all of our accounts?





1 **Update Modules**

2 **Terraform Plan & Apply**

3 **Push and Merge to team code repo**

Tracking Changes to Infrastructure With Daily Update

Back UWCLOUD-581

Terraform Plan Results

Link issue

automated-terraform@cloud-services.wisc.edu raised this request via Email

Hide details

View request in portal

Description

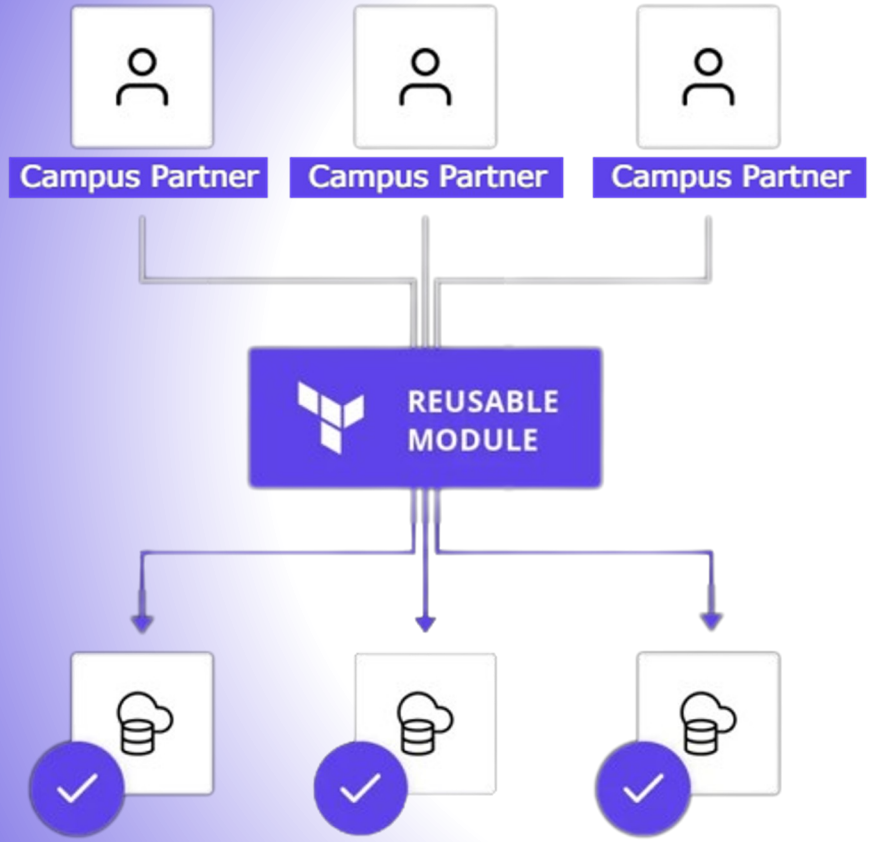
aws-organizationdlt-university-of-wisconsin-madison-3

```
"module.aws_organizational_baseline_standard.module.aws_security_hub.module.aws_secur
module.aws_organizational_baseline_standard.module.aws_guardduty.module.aws_guardduty

No changes. Your infrastructure matches the configuration.

Terraform has compared your real infrastructure against your configuration
and found no differences, so no changes are needed."
```

aws-organization/fourpoint-uw-madison-strides

```
"module.aws_organizational_baseline_standard.module.aws_organization_scps.module.aws_

No changes. Your infrastructure matches the configuration.
```

Reusable Custom Modules



Service Account User - AWS IAM User with secret stored in AWS Secrets Manager

S3 Bucket - Best practice settings applied for replication, backup, and security

VPC - AWS VPC with private and public subnets, route tables, security groups, etc

Speaker Bio

Kelly Rivera - Lead Cloud Engineer

University of Wisconsin - Madison

Kelly Rivera is the Lead Cloud Engineer of the UW Madison DoIT Public Cloud Team. She graduated from Madison College with a degree in Web Software development. After graduation, Kelly worked in private industry for a local software company as a Cloud Engineer where she honed her skills in cloud management, automation, and infrastructure as code including Terraform.

When she was looking for her next opportunity she wanted to find an organization which would allow her to make a positive difference in the world using technology. The University's commitment to research and educating the next generation drew her to take a position on the Cloud Team at DoIT.

As Lead Cloud Engineer, Kelly helps researchers, educators, administrators, and other university partners design projects in the cloud. With a background in training, she provides partners not only a solution but also the tools necessary to educate themselves about cloud. She empowers researchers to use the cloud as a tool to enable their research and make changes in the world around us.

Hallah Hussien
University of Wisconsin - Madison

Hallah Hussien is a dynamic and accomplished tech professional with a passion for all things cloud. She has dedicated the past 7 years to mastering the intricacies of cloud technologies and their real-world applications in both private industry and academia.

As a Cloud Engineer at the University of Wisconsin-Madison, Hallah plays a pivotal role in architecting and optimizing cloud solutions that drive innovation and efficiency. Her expertise encompasses a wide range of cloud platforms and services, and she possesses a unique ability to distill complex technical concepts into accessible insights for both technical and non-technical audiences.

Beyond her professional pursuits, Hallah is an avid advocate for diversity and inclusion in the tech industry. She believes in fostering an environment where individuals from all backgrounds can thrive and contribute their unique perspectives to the ever-evolving tech landscape.