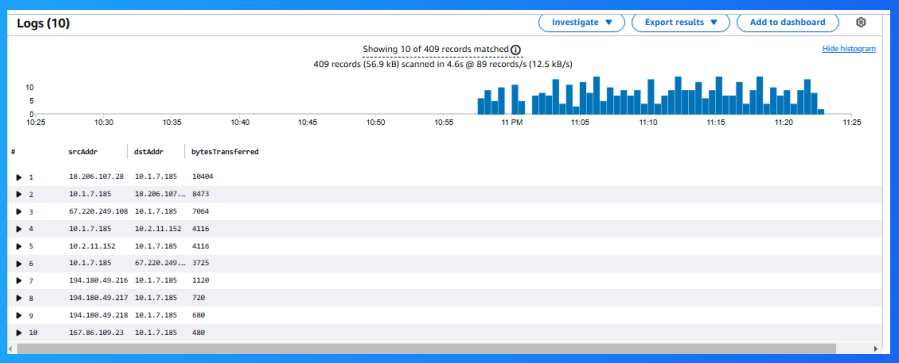
NextWork.org

VPC Monitoring with Flow Logs

Gloria



Gloria
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a secure, isolated network in AWS where you can launch resources like EC2 instances. It’s useful because it gives control over networking, such as IP ranges, subnets and security.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to set up two VPCs, configure a peering connection, and enable VPC Flow Logs to monitor network traffic. This allowed me to analyze traffic patterns, troubleshoot issues, and ensure secure communication routes

One thing I didn't expect in this project was...

One thing I didn't expect in this project was the level of detail provided by VPC Flow Logs, which made it easy to analyze specific traffic patterns and identify potential issues, like missing routes or successful connections, with precision.

This project took me...

This project took me about 40-50 minutes, including setting up the VPCs, configuring the peering connection, enabling Flow Logs, setting up IAM roles and policies and analyzing the network traffic using CloudWatch Logs Insights.

G
Gloria
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will create two VPCs from scratch using the VPC wizard. This setup will allow me to revise key concepts from the VPC peering project while also preparing for network monitoring with VPC Flow Logs and CloudWatch.

Step 2 - Launch EC2 instances

In this step, we're launching an EC2 instance in each VPC to prepare for testing the VPC peering connection. This allows us to confirm that the instances can communicate with each other across the peered VPCs, ensuring the connection is working.

Step 3 - Set up Logs

In this step, I am setting up VPC Flow Logs to monitor all inbound and outbound network traffic within my VPCs. This will allow me to track, analyze, and store records of network activity, helping identify issues and optimize performance

Step 4 - Set IAM permissions for Logs

In this step, I am granting VPC Flow Logs the necessary permissions to write network traffic data to CloudWatch. This ensures that logs from my subnet are captured and sent to a central location, where they can be monitored and analyzed

Gloria
NextWork Student

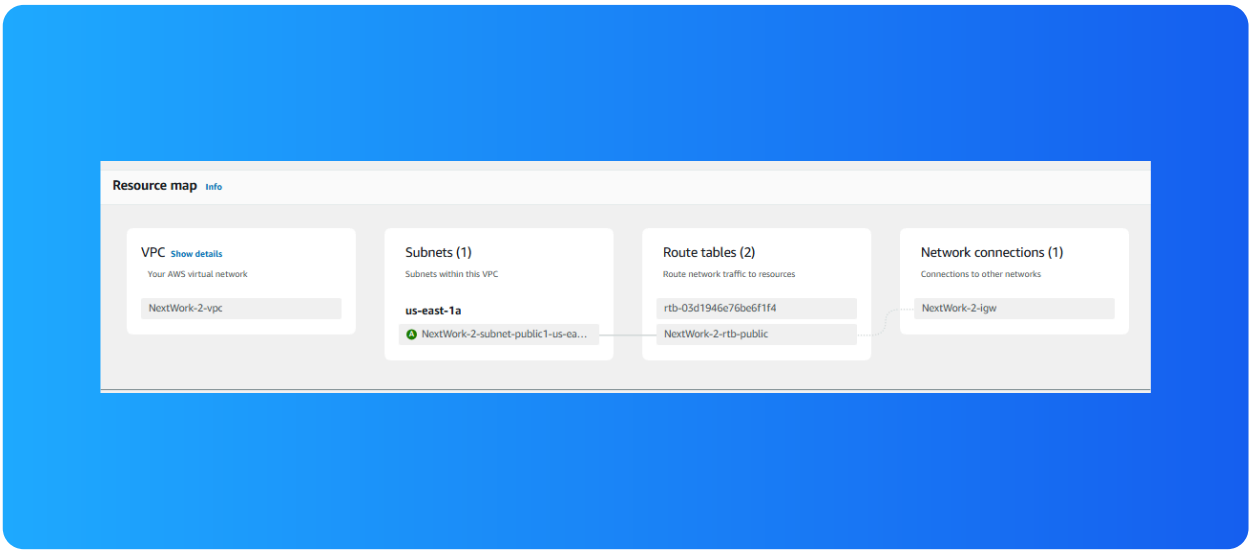
Multi-VPC Architecture

I launched a second VPC named "NextWork-2" with a unique IPv4 CIDR block of 10.2.0.0/16. It includes 1 public subnet in a single Availability Zone with no private subnets, NAT gateways, or VPC endpoints.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16. They have to be unique because overlapping IP ranges can lead to routing conflicts, ensuring smooth communication between resources in each VPC.

I also launched EC2 instances in each subnet

My EC2 instances security groups allow ICMP traffic from all IP addresses. This is because it enables ping tests and ensures connectivity for troubleshooting and communication between instances across VPCs.

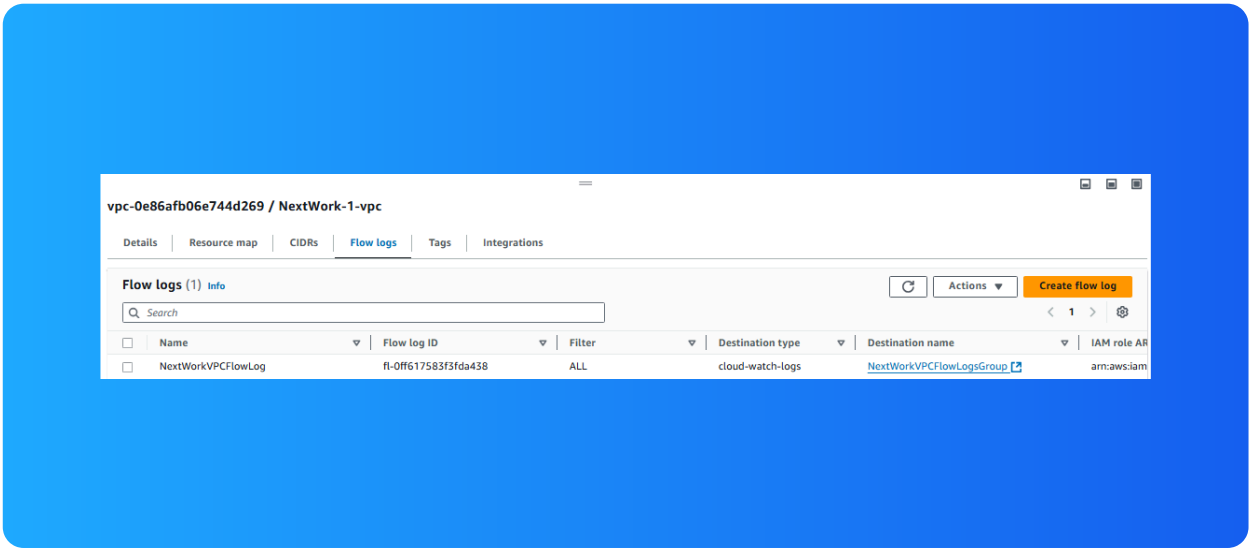


Gloria
NextWork Student

Logs

Logs are records of events or activities that occur within a system or application, capturing details such as actions taken, traffic data, errors, or system behavior. They help in monitoring, troubleshooting, and analyzing system performance.

Log groups are containers in Amazon CloudWatch where related log streams are organized and stored. They help manage and categorize logs from multiple sources, making it easier to monitor and analyze specific sets of data for your applications.



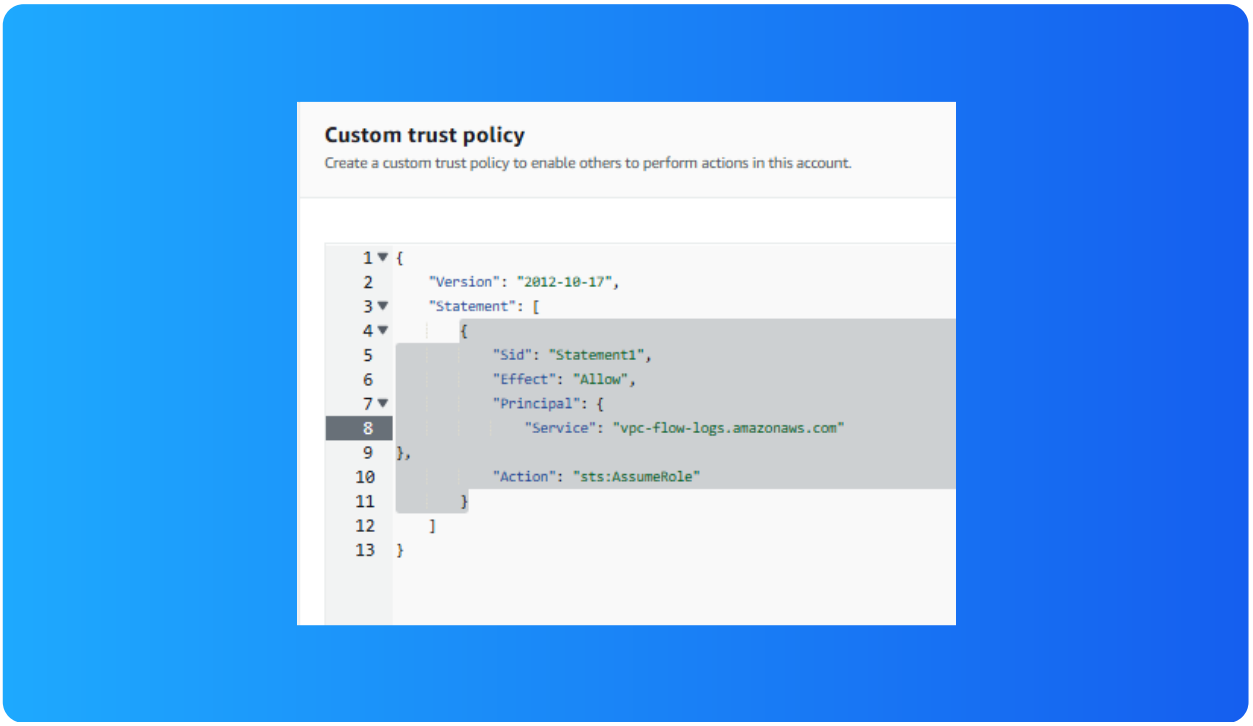
Gloria
NextWork Student

IAM Policy and Roles

I created an IAM policy because it grants VPC Flow Logs the necessary permissions to write network traffic data to CloudWatch, ensuring the logs are securely and accurately stored for monitoring and analysis.

I also created an IAM role because it allows VPC Flow Logs to assume the permissions defined in the IAM policy, enabling it to securely send network traffic data to CloudWatch on behalf of my AWS account.

A custom trust policy is a set of permissions that defines which AWS service or account is allowed to assume a specific IAM role. It specifies trusted entities and ensures secure access to resources for authorized services or users.



G
Gloria
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I am generating network traffic by sending test messages from Instance 1 in VPC 1 to Instance 2 in VPC 2. This will help test the VPC peering connection and verify that the flow logs are capturing the network activity as expected.

Step 6 - Set up a peering connection

In this step, I am setting up a peering connection between VPC 1 and VPC 2 to create a direct link for communication. This will allow instances in the two VPCs to communicate using their private IP addresses securely, avoiding traffic exposure to

Step 7 - Analyze flow logs

In this step, I am reviewing the flow logs recorded for VPC 1's public subnet to analyze network traffic. This will help me gain insights into traffic patterns, identify any blocked traffic, and understand how the network is being utilized.

Gloria
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means the network traffic was blocked, likely due to incorrect security group rules, routing issues, or a misconfigured VPC peering connection.

I could receive ping replies if I ran the ping test using the other instance's public IP address, which means the instances are able to communicate over the public internet.

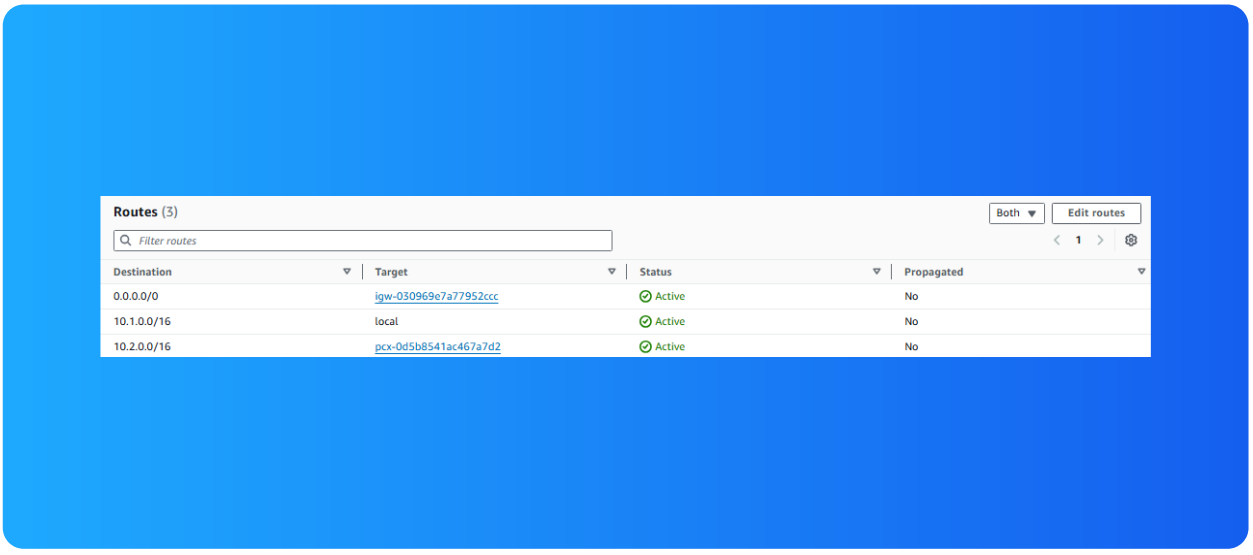
Gloria
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because there was no direct route to VPC 2 via the VPC peering connection. The traffic was not routed through the peering connection.

To solve this, I set up a peering connection between my VPCs

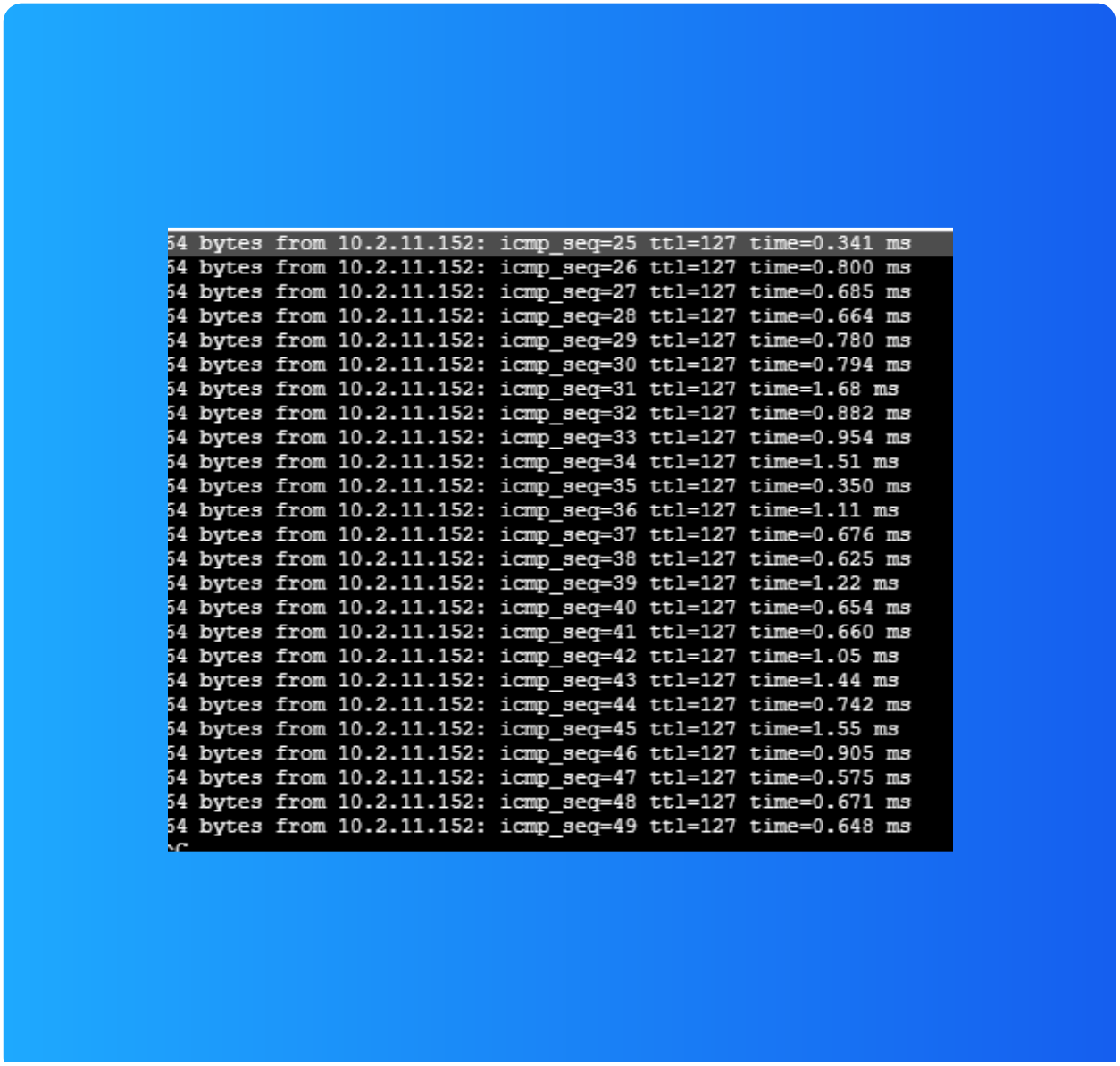
I also updated both VPCs' route tables so that traffic destined for the other VPC's private IP range is routed through the VPC peering connection, enabling direct and secure communication between the instances.



G
Gloria
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means the VPC peering connection is working correctly, the route tables are properly updated, and both instances can now communicate directly using their private IP addresses.



G
Gloria
NextWork Student

Analyzing flow logs

Flow logs tell us about various aspects of network traffic, including the source and destination IP addresses, ports, protocol used, traffic status (accepted or rejected), timestamps, and the amount of data transferred.

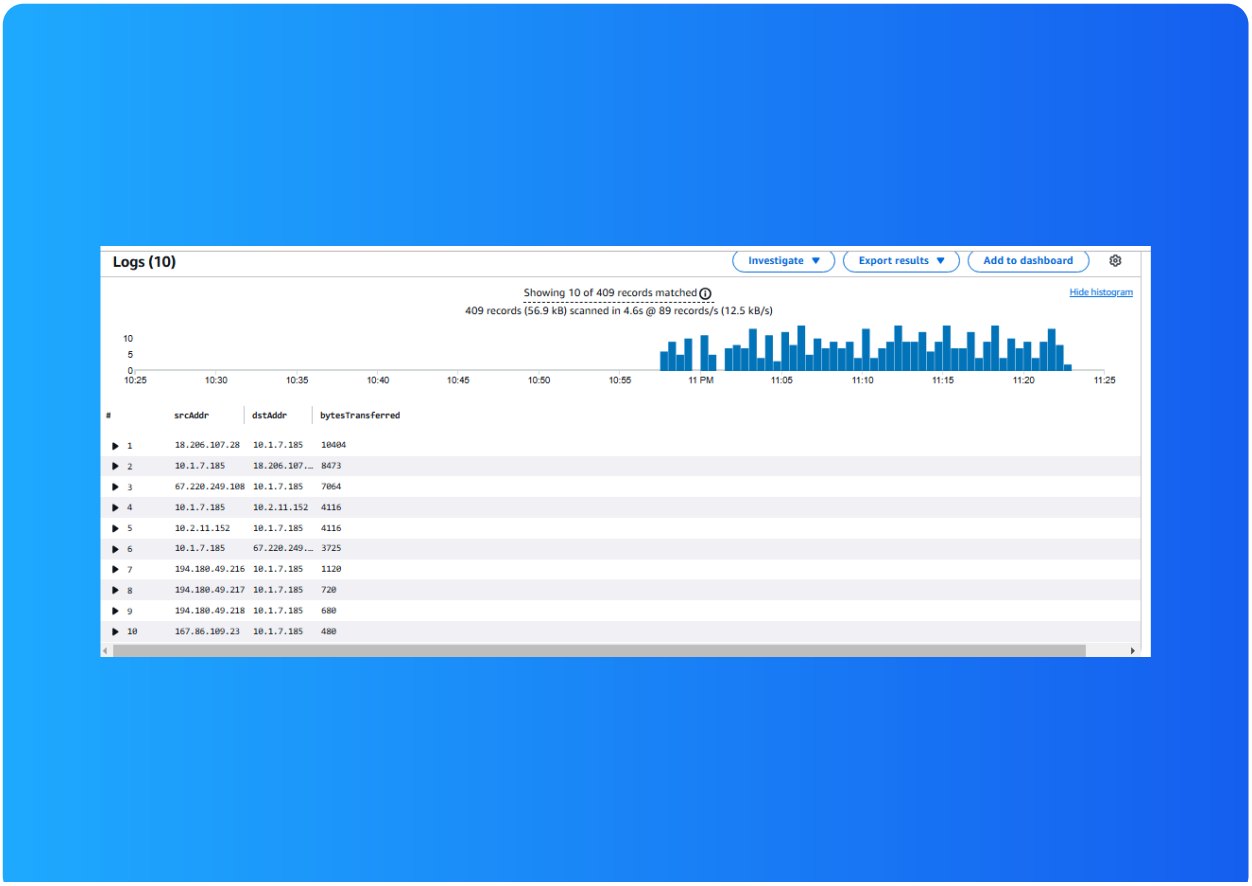
For example, the flow log I've captured tells us that traffic originated from the private IP address `10.1.7.185` and was sent to the destination `18.206.107.28` on port 22 (SSH). The traffic was accepted, indicating successful communication.

Gloria
NextWork Student

Logs Insights

Logs Insights is a powerful tool in Amazon CloudWatch that allows you to analyze, search, and visualize log data. It helps identify trends, troubleshoot issues, and gain insights from your logs using queries, making it easier to monitor applications.

I ran the query select Top 10 byte transfers by source and destination IP address This query analyzes the flow logs to identify the top 10 network traffic flows with the highest data transfer, showing the source IP, destination IP address etc.



Everyone should be in a job they love.

Check out nextwork.org for more projects