AWS Notes

# Introduction

We’re going to use this document for holding information about neonKUBE and AWS that will likely turn into formal documentation when we ultimately release this thing to the public.

# Prerequisites

You’ll need to do some preparation before you’ll be able to deploy a neonKUBE cluster to AWS. This section will walk you through simplified steps to get up and running quickly. Advanced users may need to customize this process.

1. Password Manager: We highly recommend that you install and use a password manager to record your Azure credentials as well as the neonKUBE application related credentials we’ll be provisioning below. We currently use Dashlane ourselves but there are several alternatives that all look reasonable.  
     
   In leu of a password manager, you’ll need to write these credentials down on paper or to a file that you’ll keep secure some other way.
2. **AWS Account:** You’ll need and AWS account if you don’t already have one. You can open a free account [here](https://aws.amazon.com/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc).
3. neon-manager IAM user: You’ll need to create the Identity and Access Management (IAM) user neonKUBE will use to create and manage your cluster. The steps below give this user full administrative access to your AWS account. Advanced users may wish to lock this account down more.  
   1. Login: to <https://aws.amazon.com>
   2. Type IAM into the Find Services box and click on the link returned.
   3. Click Users in the left panel.
   4. Click the Add user button
   5. Enter neon-manager as the user name.
   6. Check Programmatic access
   7. Click Next Permissions on the bottom-right.
   8. Check the Administrators group
   9. Click Next Tags, Next: Review, and then Create user
   10. **IMPORTANT:** Before you close the last page of the Add user wizard:  
         
       Save the Access key ID and Secret access key to your password manager.  
         
       If you forget to do this, you’ll need to need to create a new access key in the user’s Security credentials tab and then save that.