Amazon Web Services

Set up and administration

NetApp
April 01, 2022

Table of Contents

Amazon Web Services

Required permissions for the Connector in AWS

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in the policies provided by NetApp. You might want to understand what Cloud Manager does with these permissions.

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Security Token Service (STS), and the Key Management Service (KMS).

Actions	Purpose
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors the instance.
"ec2:DescribeInstanceAttribute",	Verifies that enhanced networking is enabled for supported instance types.
"ec2:DescribeRouteTables", "ec2:DescribeImages",	Launches a Cloud Volumes ONTAP HA configuration.
"ec2:CreateTags",	Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation.
"ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage.
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Creates predefined security groups for Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.

Actions	Purpose
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP.
"ec2:DescribeDhcpOptions",	Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshots",	Takes snapshots of EBS volumes during initial setup and whenever a Cloud Volumes ONTAP instance is stopped.
"ec2:GetConsoleOutput",	Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages.
"ec2:DescribeKeyPairs",	Obtains the list of available key pairs when launching instances.
"ec2:DescribeRegions",	Gets a list of available AWS regions.
"ec2:DeleteTags", "ec2:DescribeTags",	Manages tags for resources associated with Cloud Volumes ONTAP instances.
"cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Launches Cloud Volumes ONTAP instances.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Launches a Cloud Volumes ONTAP HA configuration.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Manages instance profiles for Cloud Volumes ONTAP instances.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets", "s3:ListBucket"	Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.

Actions	Purpose
"s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering.
"kms:List*", "kms:ReEncrypt*", "kms:Describe*", "kms:CreateGrant",	Enables data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtains AWS cost data for Cloud Volumes ONTAP.
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	When you deploy an HA configuration in a single AWS Availability Zone, Cloud Manager launches the two HA nodes and the mediator in an AWS spread placement group.
"ec2:DescribeReservedInstancesOfferings"	Cloud Manager uses the permission as part of Cloud Data Sense deployment to choose which instance type to use.
"ec2:CreateTags", "ec2:DeleteTags", "ec2:DescribeTags", "tag:getResources", "tag:getTagKeys", "tag:getTagValues", "tag:TagResources", "tag:UntagResources"	Enables you to manage tags on your AWS resources using the Cloud Manager Tagging service.

Actions	Purpose
"s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetObject", "s3:ListBucket", "s3:ListAllMyBuckets", "s3:GetBucketTagging", "s3:GetBucketLocation" "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Cloud Manager uses these permissions when you enable the Backup to S3 service.
"eks:ListClusters", "eks:DescribeCluster", "iam:GetInstanceProfile"	Enables discovery of Amazon EKS clusters.

Create a Connector in AWS from Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager features. Learn when a Connector is required. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

This page describes how to create a Connector in AWS directly from Cloud Manager. Learn about other ways to deploy a Connector.

These steps must be completed by a user who has the Account Admin role. A Workspace Admin can't create a Connector.

When you create your first Cloud Volumes ONTAP working environment, Cloud Manager will prompt you to create a Connector if you don't have one yet.

Setting up AWS permissions to create a Connector

Before you can deploy a Connector from Cloud Manager, you need to ensure that your AWS account has the correct permissions.

Steps

1. Download the Connector IAM policy from the following location:

   NetApp Cloud Manager: AWS, Azure, and GCP Policies

   For IAM user permissions for Amazon FSx for ONTAP, see Create an FSx for ONTAP working environment.

2. From the AWS IAM console, create your own policy by copying and pasting the text from the Connector IAM policy.

3. Attach the policy that you created in the previous step to the IAM user who will create the Connector from Cloud Manager.

Result

The AWS user now has the permissions required to create the Connector from Cloud Manager. You'll need to specify AWS access keys for this user when you're prompted by Cloud Manager.

Creating a Connector in AWS

Cloud Manager enables you to create a Connector in AWS directly from its user interface.

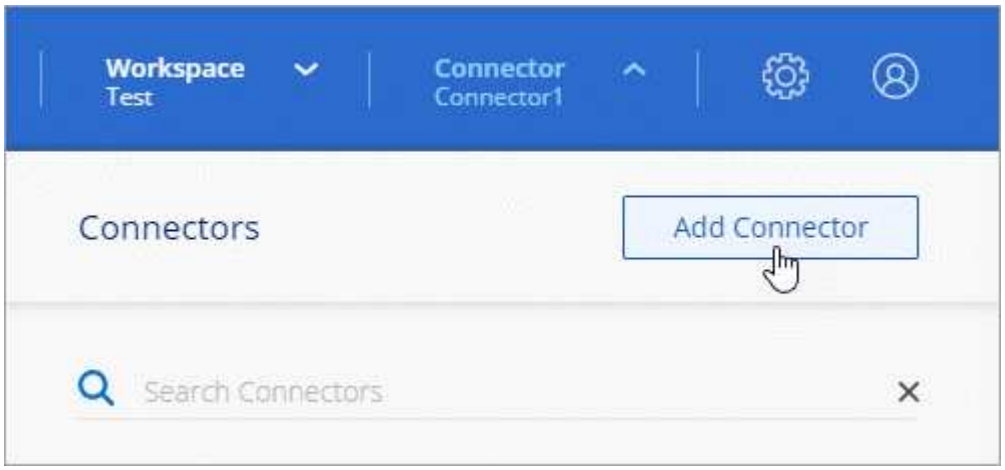
What you'll need

- An AWS access key and secret key for an IAM user who has the required permissions to create a Connector.
- A VPC, subnet, and keypair in your AWS region of choice.
- If you don't want Cloud Manager to automatically create an IAM role for the Connector, then you'll need to create your own using this policy.

  These permissions are for the Connector instance. It's a different set of permissions than what's provided in the first bullet above.

Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Choose **Amazon Web Services** as your cloud provider and click **Continue**.

   Remember that the Connector must have a network connection to the type of working environment that you're creating and the services that you're planning to enable.

   Learn more about networking requirements for the Connector.

3. Follow the steps in the wizard to create the Connector:
   - **Get Ready**: Review what you'll need.
   - **AWS Credentials**: Specify the AWS access key and secret key that meet permissions requirements and then select your region.

- **Details**: Provide details about the Connector.
  - Enter a name for the instance.
  - Add custom tags (metadata) to the instance.
  - Choose whether you want Cloud Manager to create a new role that has the required permissions, or if you want to select an existing role that you set up with the required permissions.
  - Choose whether you want to encrypt the Connector's EBS disks. You have the option to use the default encryption key or to use a custom key.
- **Network**: Specify a VPC, subnet, and key pair for the instance, choose whether to enable a public IP address, and optionally specify a proxy configuration.
- **Security Group**: Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.

  There's no incoming traffic to the Connector, unless you initiate it. HTTP and HTTPS provide access to the local UI, which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

- **Review**: Review your selections to verify that your set up is correct.

4. Click **Add**.

   The instance should be ready in about 7 minutes. You should stay on the page until the process is complete.

After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default. Learn more.

Create a Connector from the AWS Marketplace

It's best to create a Connector directly from Cloud Manager, but you can launch a Connector from the AWS Marketplace, if you'd rather not specify AWS access keys. After you create and set up the Connector, Cloud Manager will automatically use it when you create new working environments.

Steps

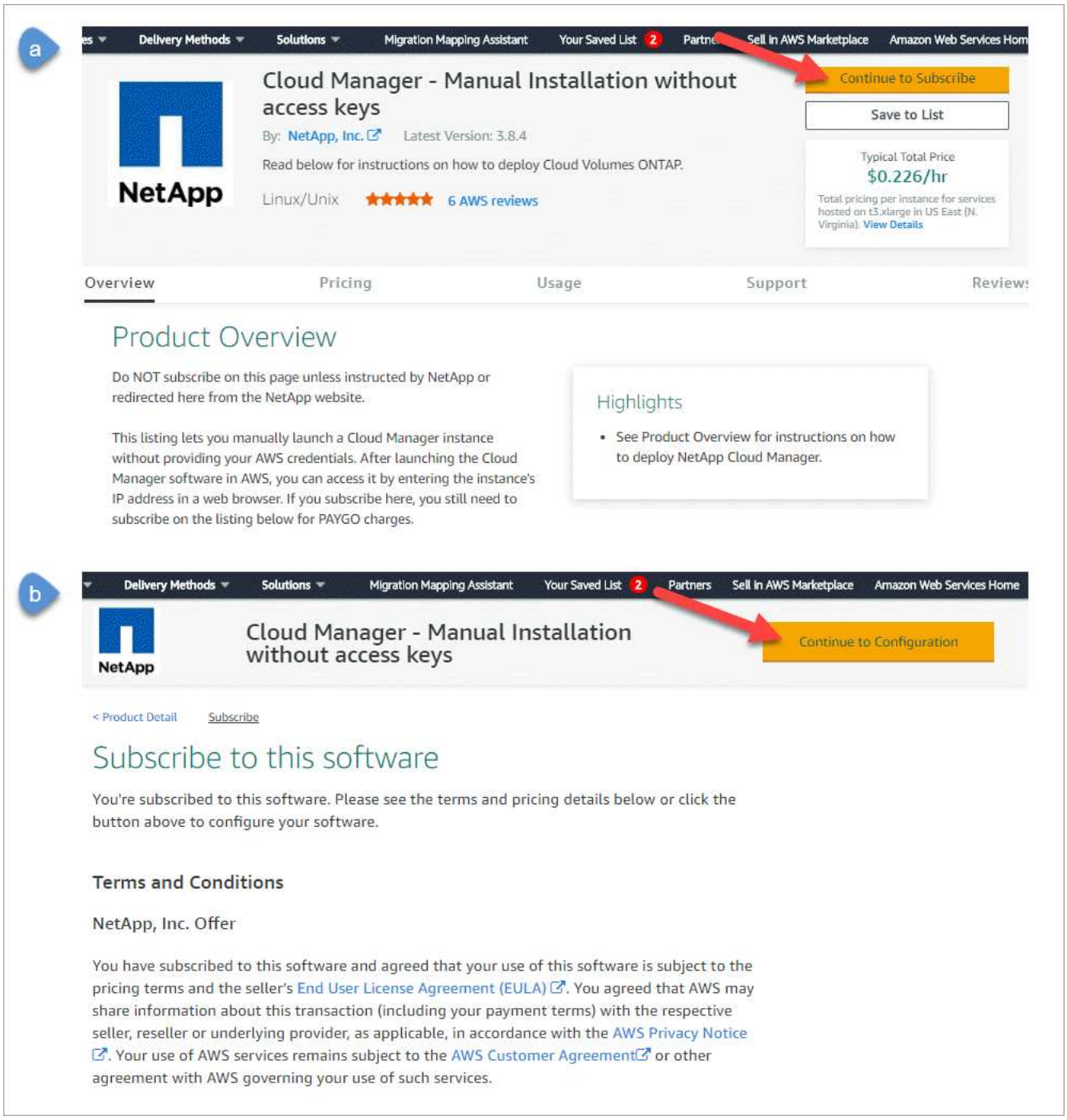
1. Create an IAM policy and role for the EC2 instance:
   a. Download the Cloud Manager IAM policy from the following location:

      NetApp Cloud Manager: AWS, Azure, and GCP Policies

   b. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
   c. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.
2. Now go to the Cloud Manager page on the AWS Marketplace to deploy Cloud Manager from an AMI.

The IAM user must have AWS Marketplace permissions to subscribe and unsubscribe.

3. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.



4. Change any of the default options and click **Continue to Launch**.
5. Under **Choose Action**, select **Launch through EC2** and then click **Launch**.

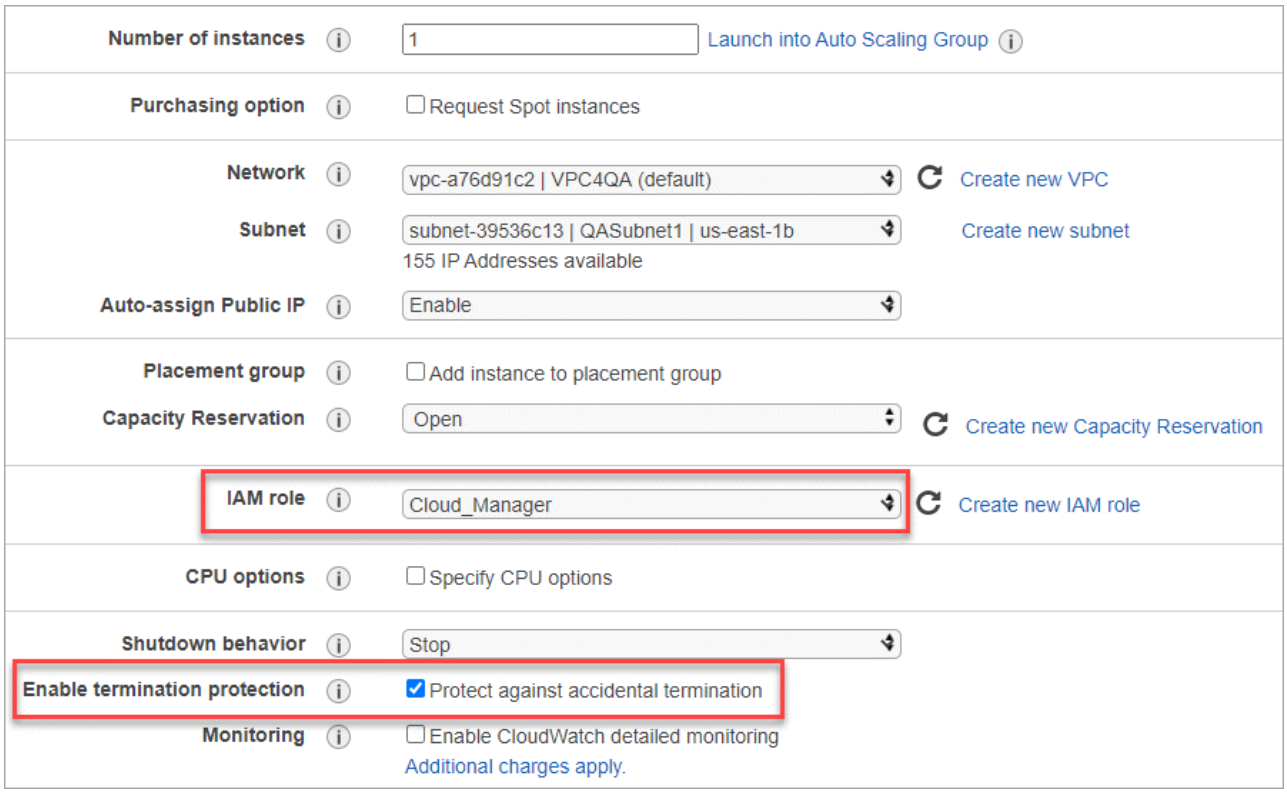
   These steps describe how to launch the instance from the EC2 Console because the console enables you to attach an IAM role to the Cloud Manager instance. This isn't possible using the **Launch from Website** action.

6. Follow the prompts to configure and deploy the instance:

- **Choose Instance Type**: Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

  Review the instance requirements.

- **Configure Instance**: Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.



- **Add Storage**: Keep the default storage options.
- **Add Tags**: Enter tags for the instance, if desired.
- **Configure Security Group**: Specify the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Review**: Review your selections and click **Launch**.

  AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

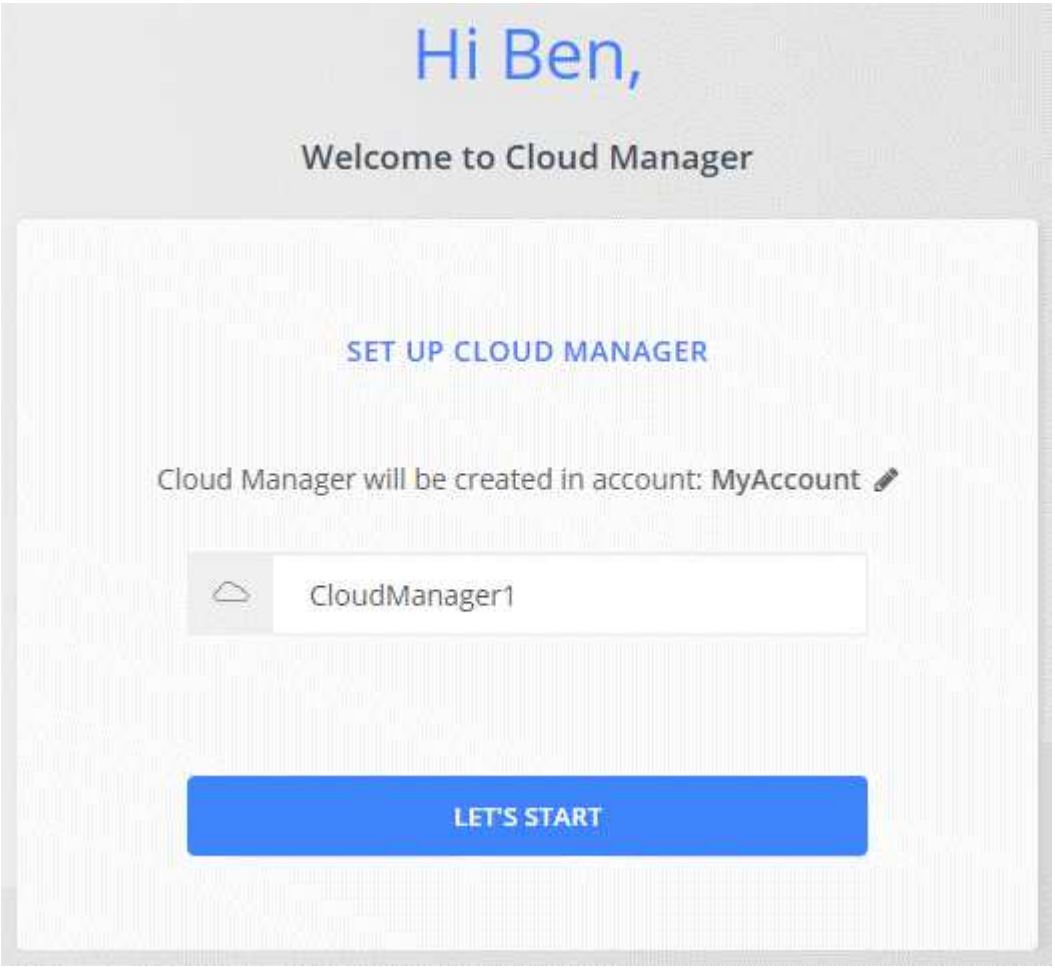
7. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

   http://*ipaddress*:80

8. After you log in, set up the Connector:
   a. Specify the NetApp account to associate with the Connector.

      Learn about NetApp accounts.

   b. Enter a name for the system.



Result

The Connector is now installed and set up with your NetApp account. Cloud Manager will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to switch between them.