

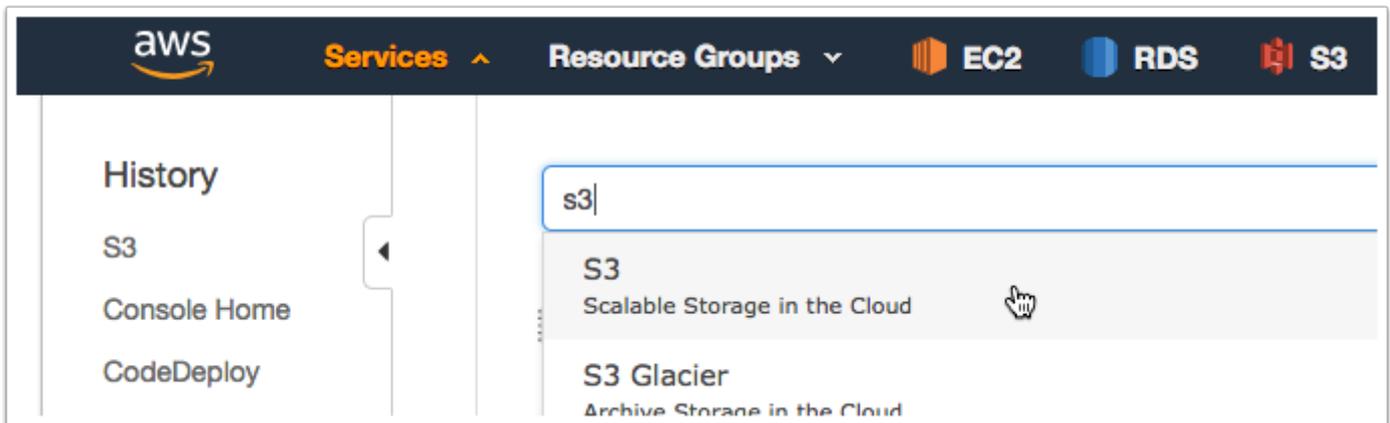
Setting Up an Amazon S3™ Bucket for WHMCS

If you want to use Amazon S3™ as the storage provider for your WHMCS installation, you will need to create an S3 bucket.

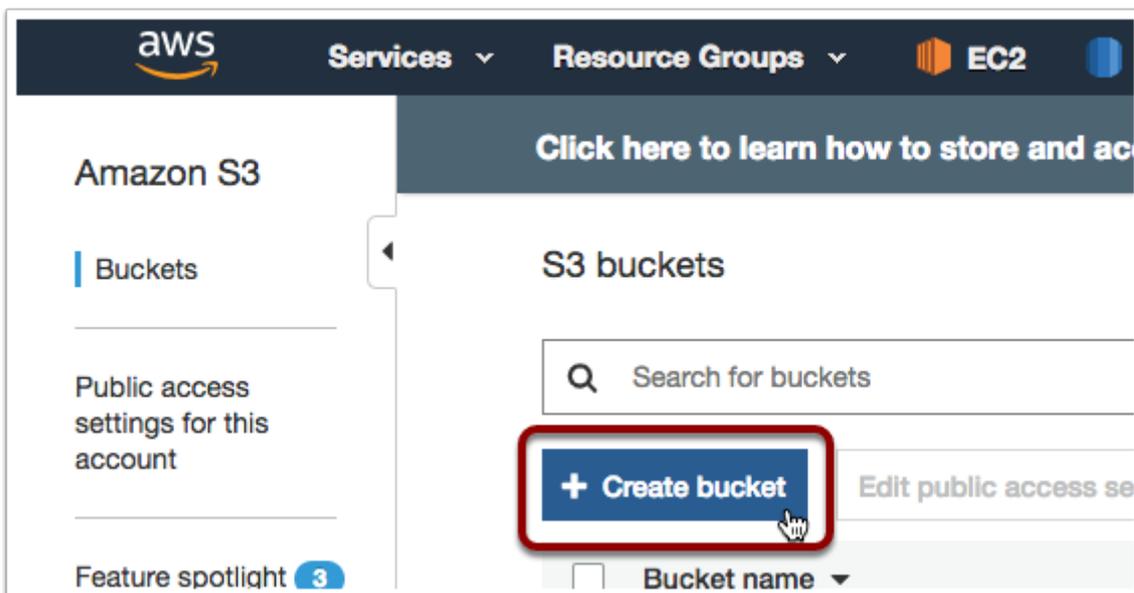
Create an S3 Bucket

To create an Amazon S3 bucket:

1. Log in to your Amazon account at <https://aws.amazon.com/>.
2. Go to S3.

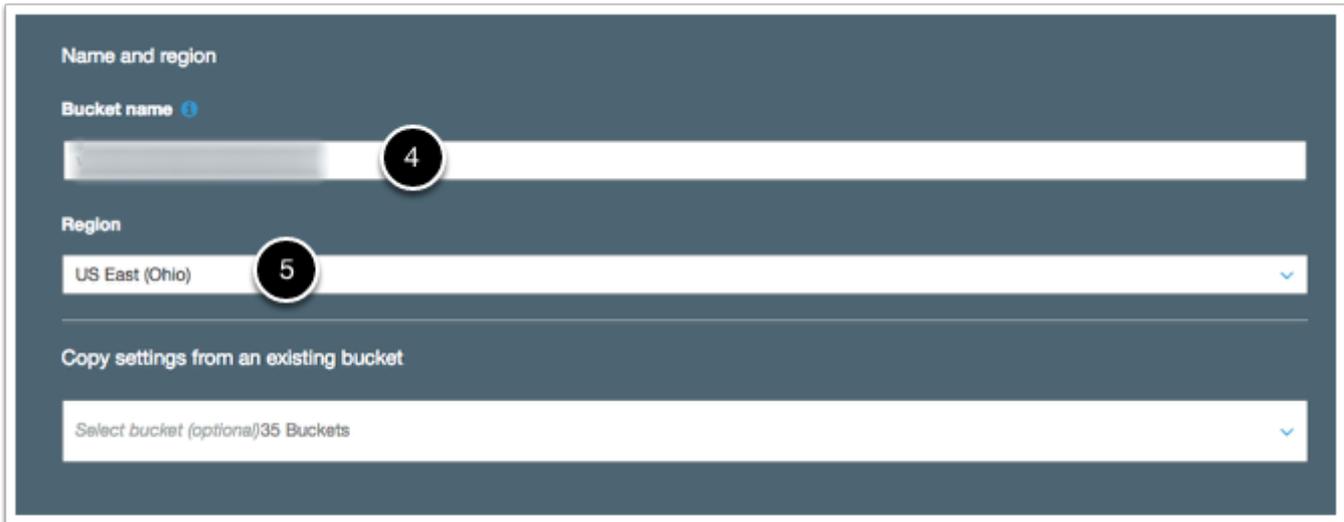


3. Click **Create bucket**.



4. Enter a name for your bucket.

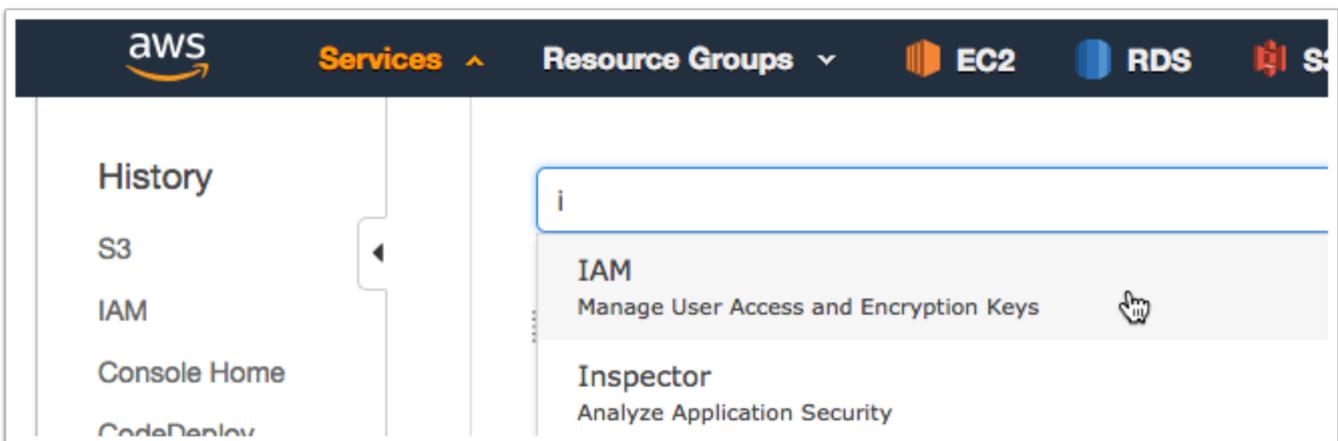
5. Choose your desired region.



The screenshot shows the 'Name and region' section of the AWS S3 console. It includes a 'Bucket name' input field with a circled '4' and a 'Region' dropdown menu with a circled '5'. The region is currently set to 'US East (Ohio)'. Below these fields is a section for 'Copy settings from an existing bucket' with a dropdown menu showing 'Select bucket (optional) 35 Buckets'.

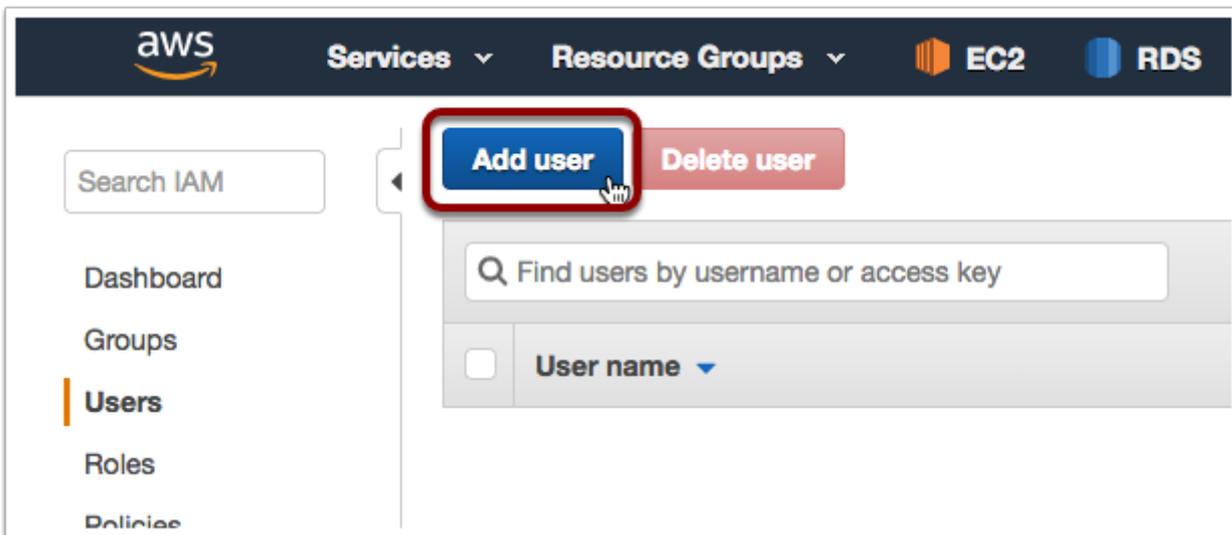
6. Configure the other bucket settings according to your needs. In most cases, for private buckets, you use the default settings.

7. Go to IAM.



8. Select **Users** in the left side menu.

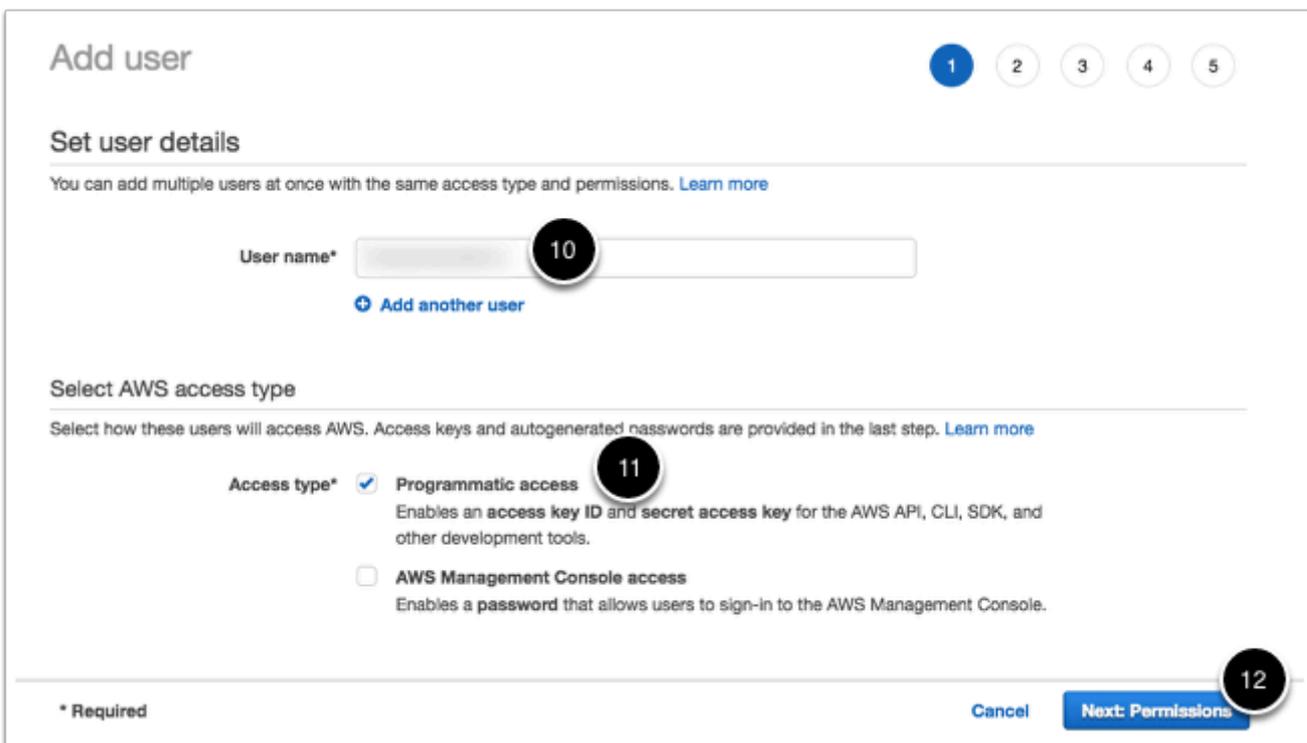
9. Click **Add user**.



10. Enter a username.

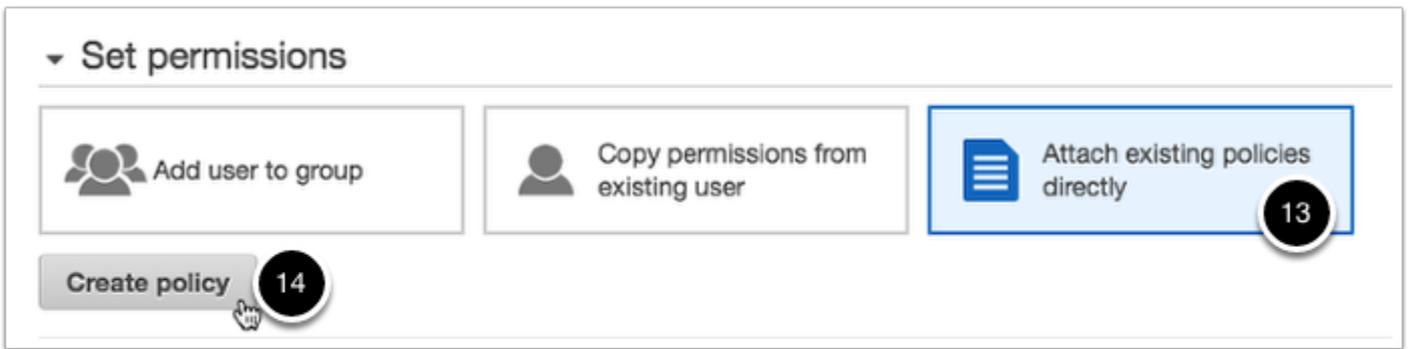
11. Check *Programmatic access* for **Access Type**.

12. Click **Next**.



13. Select **Attach existing policies directly**.

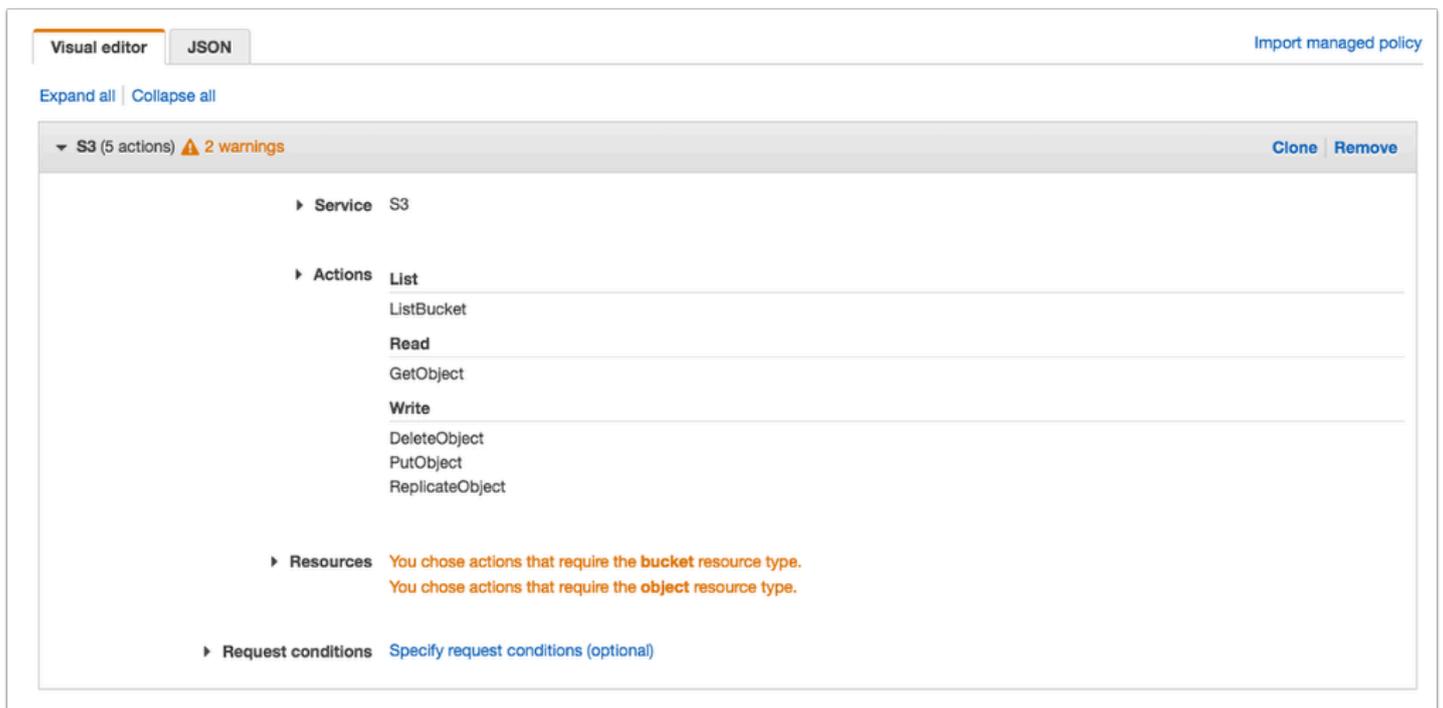
14. Click **Create policy**. The visual policy editor will load.



15. Select **S3** for **Service**.

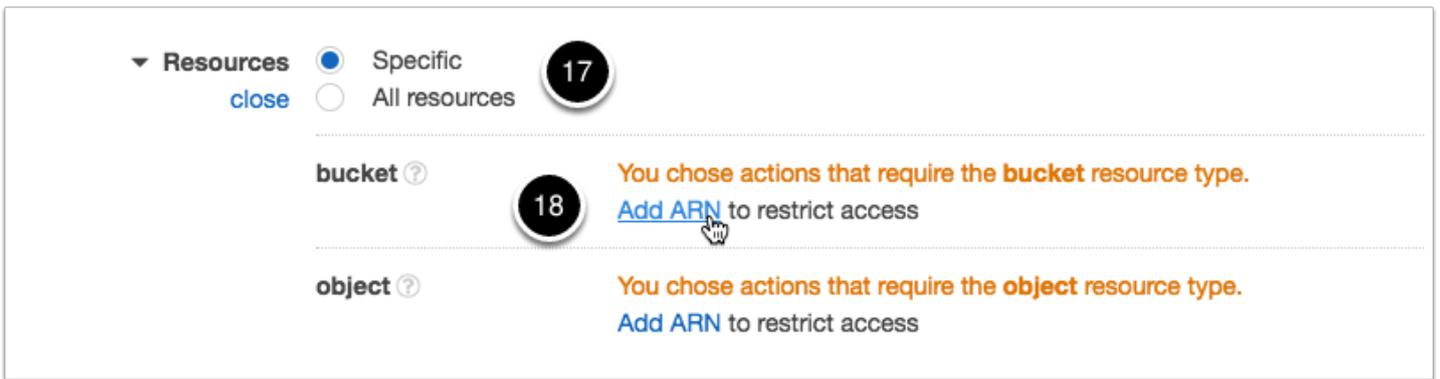
16. Select all of the following S3-related permissions:

- *ListBucket*
- *GetObject*
- *PutObject*
- *ReplicateObject*
- *DeleteObject*



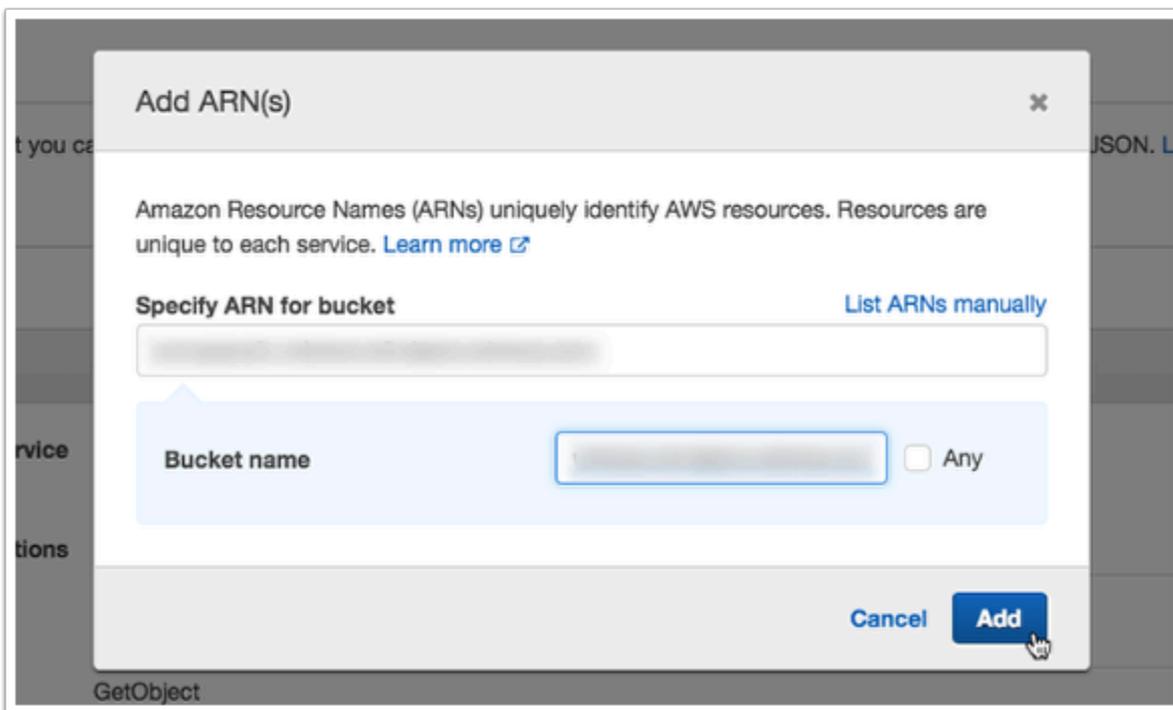
17. Under **Resources**, select *Specific*.

18. Click **Add ARN** under **bucket**.



19. Enter the name of the bucket that you created earlier.

20. Click **Add**.



21. Click **Add ARN** under **object**.

▼ Resources Specific All resources
[close](#)

bucket ?

[Add ARN](#) to restrict access

object ? You chose actions that require the object resource type.

[Add ARN](#) to restrict access

22. Enter the name of the bucket that you created earlier for **Bucket name**.

23. Check **Any**.

24. Click **Add**.

Add ARN(s) ✕

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more](#)

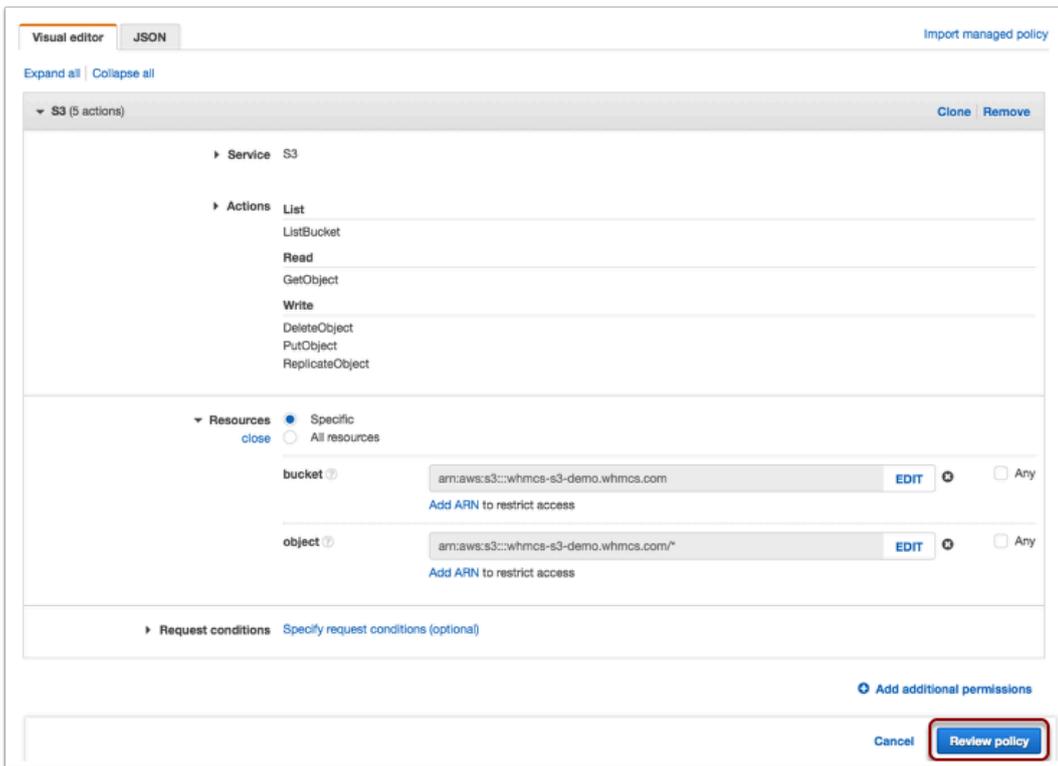
Specify ARN for object [List ARNs manually](#)

Bucket name Any

Object name Any

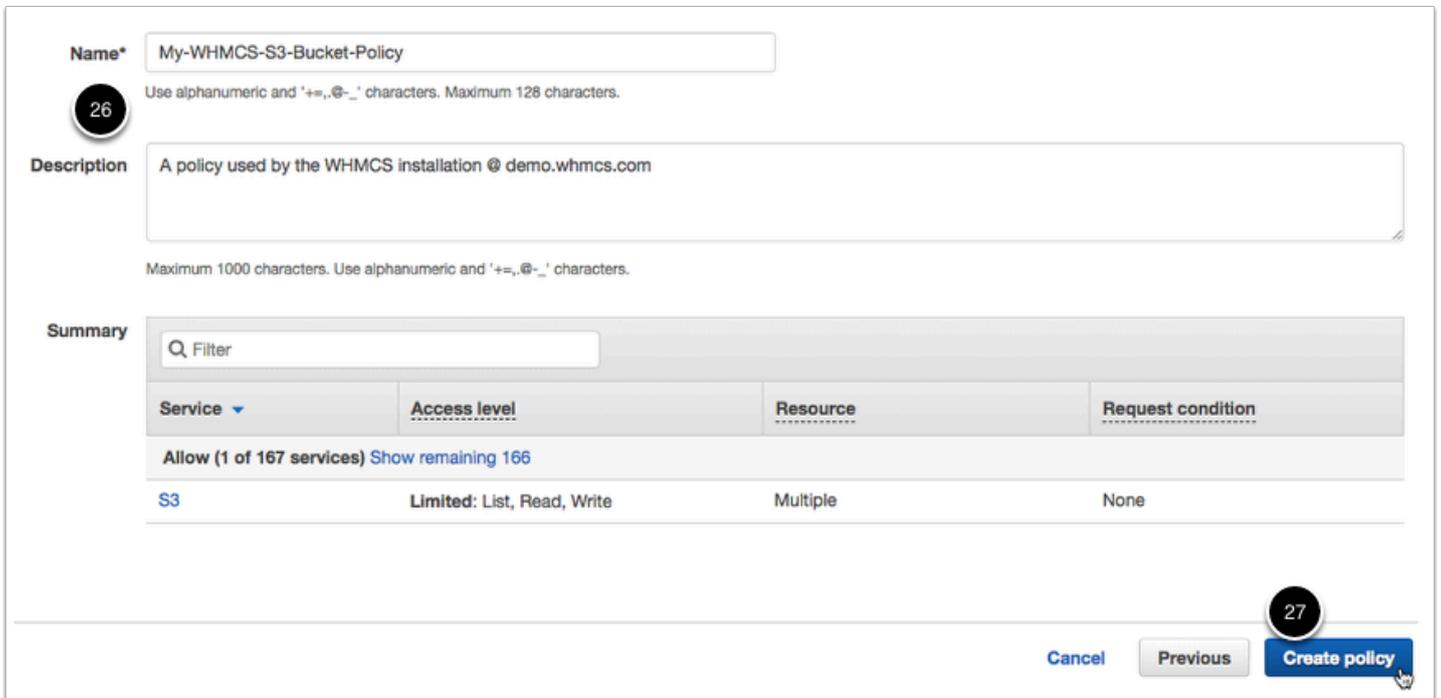
[Cancel](#) [Add](#)

25. Click **Review Policy**.

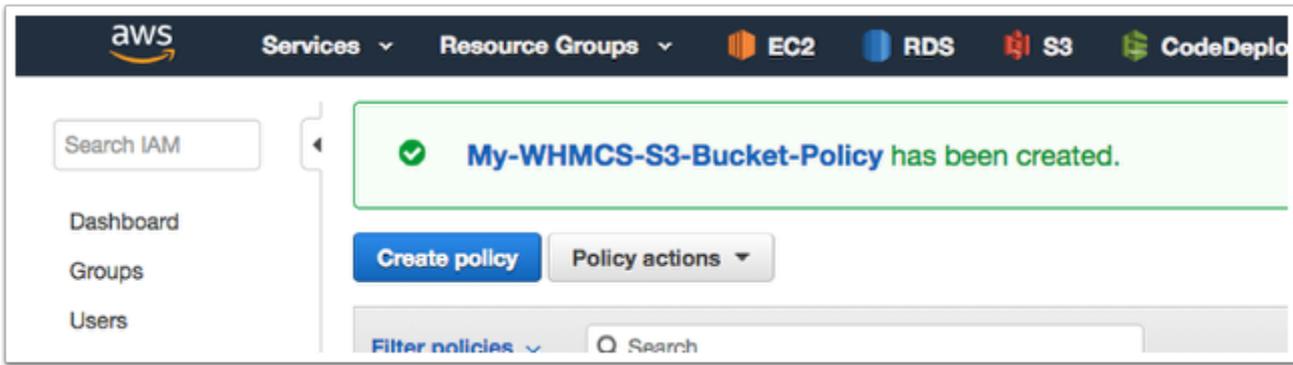


26. Enter a name for the new policy and, optionally, a description to help you identify it later.

27. Click **Create Policy**.



A success message will appear:

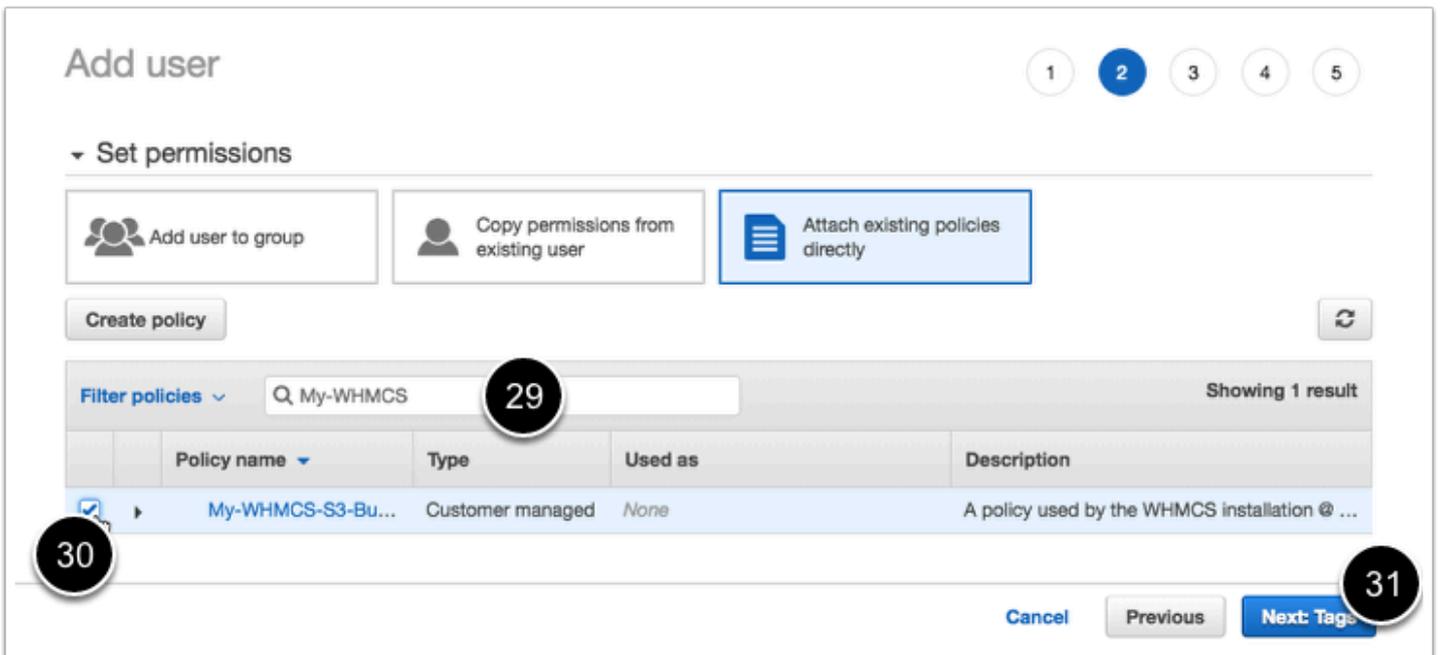


28. Return to the previous tab and refresh the list of policies.

29. Search for the name of the policy that you created.

30. Select the policy in the search results.

31. Click **Next: Tags**.



32. Optionally, assign tags to the policy.

33. Click **Next: Review** and review the details.

34. Click **Create user**. A programmatic access key ID and secret will display.

35. Copy and store the displayed ID and secret. You will need them in order to configure the bucket in WHMCS.

Add user

1 2 3 4 5

✔ Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://yourcompanyname.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	✔ whmcs-s3-demo	AKIAJWW2Y76GBL0LCT3A	***** Show

Close