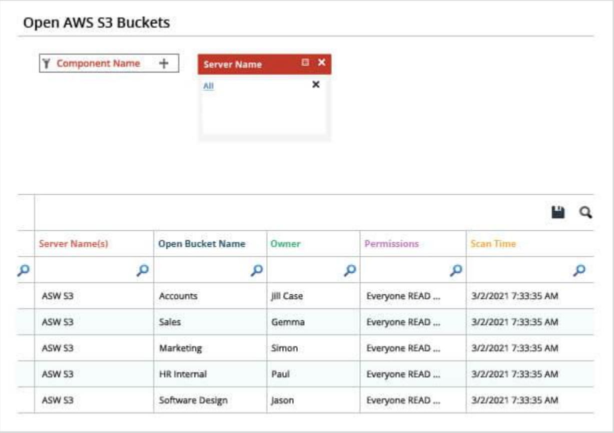
Amazon S3 Buckets

AWS buckets are a logical unit of storage in Amazon Web Services (AWS) object storage service, Simple Storage Solution S3. Buckets are used to store objects, which consist of data and metadata. S3 Customers create buckets to share data amongst users and privileges are controlled through the AWS Policy Generator. It's important for your IT security and compliance posture to not only understand who is accessing the data but also any changes to the security settings surrounding the content of the buckets. This is where Lepide Amazon S3 Auditor comes in.


Open AWS S3 Buckets

Server Name(s)	Open Bucket Name	Owner	Permissions	Scan Time
ASW S3	Accounts	Jill Case	Everyone READ ...	3/2/2021 7:33:35 AM
ASW S3	Sales	Gemma	Everyone READ ...	3/2/2021 7:33:35 AM
ASW S3	Marketing	Simon	Everyone READ ...	3/2/2021 7:33:35 AM
ASW S3	HR Internal	Paul	Everyone READ ...	3/2/2021 7:33:35 AM
ASW S3	Software Design	Jason	Everyone READ ...	3/2/2021 7:33:35 AM

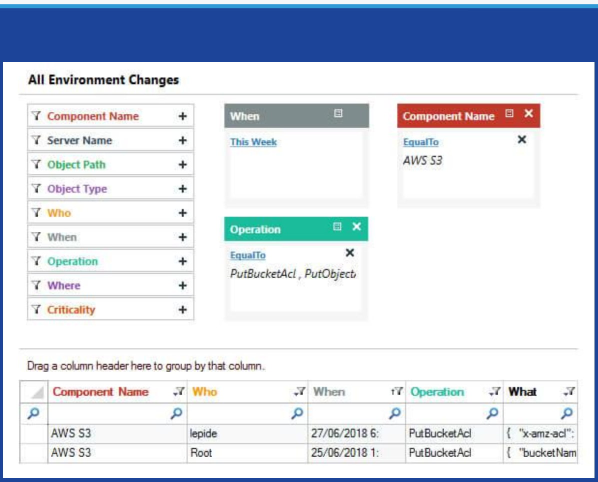
Report on AWS S3 Open Buckets.

Obviously, open buckets pose a huge risk to any organization storing sensitive data in AWS S3, so identifying the buckets that are open to "EVERYONE" is of paramount importance.

The Lepide solution includes an open bucket scanner that will scan AWS S3 storage to find these high-risk and vulnerable buckets and report on them. This will then give you a conclusive list of the buckets that need securing first.

Who's accessing critical data within the Buckets?

Understand how users are interacting with the data shared within the buckets. As well as being able to identify if new files are added and removed to the storage buckets you will also be able to gain insight into who's accessing the data, and how frequently, to help in determining unauthorized access or privilege abuse.


All Environment Changes

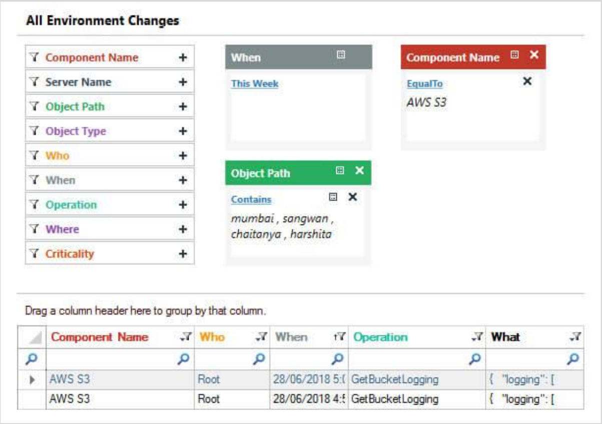
When: This Week

Component Name: EqualTo AWS S3

Operation: EqualTo PutBucketAcl , PutObject

Drag a column header here to group by that column.

Component Name	Who	When	Operation	What
AWS S3	lepide	27/06/2018 6:	PutBucketAcl	{ "x-amz-acl":
AWS S3	Root	25/06/2018 1:	PutBucketAcl	{ "bucketNam



When
This Week

Component Name
EqualTo
AWS S3

Object Path
Contains
mumbai , sangwan , chaitanya , harshita

Drag a column header here to group by that column.

	Component Name	Who	When	Operation	What
	AWS S3	Root	28/06/2018 5:(	GetBucketLogging	{ "logging": [
	AWS S3	Root	28/06/2018 4:!	GetBucketLogging	{ "logging": [

Who's making configuration changes?

To prevent privilege abuse in the first place, it's important to design a stringent security model around access management to the storage buckets. With Lepide Amazon S3 Auditor, you will be able to see if there are any unauthorized changed to the Access Control Lists surrounding the data. This will help in ensuring permissions are not granted to those who don't need them and also help to prevent privilege sprawl across the unstructured data.

Start your 20-day free trial of Lepide today!

Start free trial