

AWS Compute Permissions

Policy Name "PrismaCloud-Compute-<feature_name>-Policy"	Onboarded account Protection Mode	Required Permissions
Registry Scan (Existing)	Monitor AND Monitor & Protect	Both read-only & read-write templates ecr:GetAuthorizationToken ecr:BatchCheckLayerAvailability ecr:GetDownloadUrlForLayer ecr:GetRepositoryPolicy ecr:DescribeRepositories ecr:ListImages ecr:DescribeImages ecr:BatchGetImage ecr:GetLifecyclePolicy ecr:GetLifecyclePolicyPreview ecr:ListTagsForResource ecr:DescribeImageScanFindings
Serverless Scan (Existing)	Monitor AND Monitor & Protect	Both read-only & read-write templates lambda:ListFunctions lambda:GetFunction iam:GetPolicy iam:GetPolicyVersion iam:GetRole iam:GetRolePolicy iam:ListAttachedRolePolicies iam:ListRolePolicies lambda:GetLayerVersion
Serverless Auto Defend (Existing)	Monitor & Protect ONLY	read-write templates ONLY lambda:PublishLayerVersion lambda:UpdateFunctionConfiguration lambda:GetLayerVersion lambda:GetFunctionConfiguration iam:SimulatePrincipalPolicy lambda:GetFunction lambda:ListFunctions iam:GetPolicyVersion iam:GetRole iam:ListRolePolicies iam:ListAttachedRolePolicies iam:GetRolePolicy iam:GetPolicy lambda:ListLayerVersions lambda:ListLayers lambda>DeleteLayerVersion
Serverless Radar (Existing)	Monitor & Protect ONLY	read-write templates ONLY cloudwatch:DescribeAlarms iam:GetPolicyVersion iam:GetRole iam:GetPolicy iam:GetRolePolicy iam:ListRolePolicies iam:ListAttachedRolePolicies lambda:ListFunctions lambda:GetFunction lambda:ListAliases lambda:ListEventSourceMappings lambda:GetPolicy kms:Decrypt logs:DescribeSubscriptionFilters s3:GetBucketNotification elasticloadbalancing:DescribeListeners

		elasticloadbalancing:DescribeTargetGroups							
		elasticloadbalancing:DescribeListenerCertificates							
		elasticloadbalancing:DescribeRules							
		cloudfront:ListDistributions							
		events:ListRules							
		apigateway:GET							
VM Tags Discovery (Existing)	Monitor AND Monitor & Protect	Both read-only & read-write templates							
		ec2:DescribeTags							
AMI Scan (NEW)	Monitor & Protect ONLY	read-write templates ONLY							
		ec2:CreateSecurityGroup							
		ec2:DescribeSecurityGroups							
		ec2:RevokeSecurityGroupEgress							
		ec2:AuthorizeSecurityGroupIngress							
		ec2>DeleteSecurityGroup							
		ec2:RunInstances							
		ec2:DescribeInstances							
		ec2:TerminateInstances							
		ec2:DescribeImages							
		ec2:CreateTags							
		ec2:AuthorizeSecurityGroupEgress							
		ec2:DescribeSubnets							
		ec2:DescribeVpcs							
		ec2:DescribeInstanceTypeOfferings							
Host Auto-Defend (NEW)	Monitor & Protect ONLY	read-write templates ONLY							
		ec2:DescribeImages							
		ec2:DescribeInstances							
		ssm:SendCommand							
		ssm:DescribeInstanceInformation							
		ssm:ListCommandInvocations							
		ssm:CancelCommand							
		ssm:CreateAssociation							
Alert Provider (NEW)	Monitor AND Monitor & Protect	Both read-only & read-write templates							
		securityhub:BatchImportFindings							

GCP Compute Permissions

GCP Compute Permissions							
Feature	Protection Mode	Required Permissions					
Host Discovery	Monitor	compute.zones.list, compute.projects.get instances.list, zones.list, projects.get compute.instances.list,					
Host Auto Defend	Protect	osconfig.patchJobs.exec osconfig.patchJobs.list osconfig.patchJobs.get storage.buckets.create storage.buckets.delete storage.objects.create storage.objects.delete storage.objects.get storage.objects.list compute.disks.get					

