Check Point Cloud Guard Dome9 Provider

The Check Point Cloud Guard Dome9 provider is used to interact with the many resources supported by Check Point Cloud Guard Dome9 (https://www.dome9.com).

Use the navigation to the left to read about the available resources.

Authentication

This provider requires a Dome9 API access ID and secret key in order to manage the resources.

To manage the full selection of resources, provide a Dome9 access id & secret key (https://secure.dome9.com/v2/settings/credentials) from an account with admin access permissions.

Dome9 API documentation (/docs/cloud/api/index.html) for more details about access to specific resources.

There are three ways to provide the required access key and secret:

- On the CLI, omit the `provider` block from your tf file, the CLI will ask for proper credentials. CLI config file (/docs/commands/cli-config.html#credentials).
- Set the `DOME9_ACCESS_ID` and `DOME9_SECRET_KEY` environment variable.
- Fill the provider block with the appropriate arguments:

Example Usage

```
# Configure the Dome9 Provider
provider "dome9" {
  dome9_access_id     = "${var.access_id}"
  dome9_secret_key    = "${var.secret_key}"
}

# Create an organization
resource "dome9_cloudaccount_aws" "account" {
  # ...
}
```

Argument Reference

The following arguments are supported:

- `dome9_access_id` - (Required) Dome9 access ID.
- `dome9_secret_key` - (Required) Dome9 access key.

Data Source: dome9_cloudaccount_aws

Use this data source to get information about AWS cloud account.

Example Usage

```
data "dome9_cloudaccount_aws" "test" {
  id = "my-dome9-id"
}
```

Argument Reference

The following arguments are supported:

- `id` - (Required) The Dome9 id

Attributes Reference

In addition to all arguments above, the following attributes are exported:

- `vendor` - The cloud provider (AWS).
- `name` - The cloud account name.
- `external_account_number` - The AWS account number.
- `error` - Credentials error status.
- `is_fetching_suspended` - Fetching suspending status.
- `creation_date` - Account creation date.
- `full_protection` - The tamper Protection mode for current security groups.
- `allow_read_only` - The AWS cloud account operation mode. true for "Manage", false for "Readonly".
- `net_sec` - The network security configuration for the AWS cloud account.

Data Source: dome9_cloudaccount_azure

Use this data source to get information about Azure cloud account.

Example Usage

```
data "dome9_cloudaccount_azure" "test" {
  account_id         = "my-dome9-id"
}
```

Argument Reference

The following arguments are supported:

- `account_id` - (Required) Account id in Dome9.

Attributes Reference

In addition to all arguments above, the following attributes are exported:

- `name` - Account name (in Dome9).
- `subscription_id` - Azure subscription id for account.
- `tenant_id` - Azure tenant id.
- `operation_mode` - Dome9 operation mode for the Azure account (Read-Only or Managed).
- `vendor` - The cloud provider (Azure).
- `creation_date` - Date Azure account was onboarded to a Dome9 account.
- `organizational_unit_id` - Organizational unit id.
- `organizational_unit_path` - Organizational unit path.
- `organizational_unit_name` - Organizational unit name.

Data Source: dome9_cloudaccount_gcp

Use this data source to get information about GCP cloud account.

Example Usage

```
data "dome9_cloudaccount_gcp" "test" {
  account_id         = "my-dome9-id"
}
```

Argument Reference

The following arguments are supported:

- `account_id` - (Required) Account id in Dome9.

Attributes Reference

In addition to all arguments above, the following attributes are exported:

- `name` - Google account name in Dome9.
- `project_id` - the Google project id (that will be onboarded).
- `creation_date` - creation date for project in Google.
- `organizational_unit_id` - Organizational unit id.
- `organizational_unit_path` - Organizational unit path.
- `organizational_unit_name` - Organizational unit name.
- `gsuite_user` - Gsuite user.
- `domain_name` - Domain name.
- `domain_name` - Azure tenant id.
- `vendor` - The cloud provider (gcp).

Data Source: dome9_continuous_compliance_policy

Use this data source to get information about continuous compliance policy.

Example Usage

```
data "dome9_continuous_compliance_policy" "test" {
  id = "${%s.id}"
}
```

Argument Reference

The following arguments are supported:

- `id` - (Required) The cloud account id.

Attributes Reference

In addition to all arguments above, the following attributes are exported:

- `cloud_account_id` - Google account name in Dome9.
- `external_account_id` - The account number.
- `cloud_account_type` - creation date for project in Google.
- `bundle_id` - Organizational unit id.
- `notification_ids` - Organizational unit path.

Data Source: dome9_iplist

Use this data source to get an IP list.

Example Usage

```
data "dome9_iplist" "test" {
  id        = "IP List Id"
}
```

Argument Reference

The following arguments are supported:

- `id` - (Required) The IP List Id.

Attributes Reference

In addition to all arguments above, the following attributes are exported:

- `name` - IP List Name.
- `description` - IP List Description.
- `items` - Items in the IP list.

dome9_cloudaccount_aws

The AWS cloud accounts resource has methods to onboard AWS cloud accounts to Dome9 and to manage some of their settings.

Example Usage

Basic usage:

```
resource "dome9_cloudaccount_aws" "test" {
  name  = "ACCOUNT NAME"

  credentials = {
    arn    = "ARN"
    secret = "SECRET"
    type   = "RoleBased"
  }
}
```

Argument Reference

The following arguments are supported:

- `name` - (Required) The AWS account name.
- `credentials` - (Required) The information needed for Dome9 System in order to connect to the AWS cloud account.
- `net_sec` - (Optional) The network security configuration for the AWS cloud account. If given, must pass all 16 regions. Otherwise, sets to default.

Credentials

`credentials` supports the following arguments:

- `arn` - (Required) AWS Role ARN (to be assumed by Dome9 System)
- `secret` - (Required) The AWS role External ID (Dome9 System will have to use this secret in order to assume the role)
- `type` - (Required) The cloud account onboarding method. Should be set to "RoleBased" as other methods are deprecated.

Network security configuration

`net_sec` supports the following arguments:

- `Region` - (Required) list of the supported regions, and their configuration:
  - `new_group_behavior` - (Required) The network security configuration. Can be "ReadOnly", "FullManage" or

"Reset".

- `region` - (Required) AWS region.

Attributes Reference

- `vendor` - The cloud provider (AWS).
- `external_account_number` - The AWS account number.
- `is_fetching_suspended` - Fetching suspending status.
- `creation_date` - Account creation date.
- `full_protection` - The tamper Protection mode for current security groups.
- `allow_read_only` - The AWS cloud account operation mode. true for "Manage", false for "Readonly".
- `net_sec` - The network security configuration for the AWS cloud account. If not given, sets to default value.

Import

AWS cloud account can be imported; use `<AWS CLOUD ACCOUNT ID>` as the import ID. For example:

```
terraform import dome9_cloudaccount_aws.test 00000000-0000-0000-0000-000000000000
```

dome9_cloudaccount_azure

The AzureCloudAccounts resource has methods to onboard Azure cloud accounts to Dome9 and to manage some of their settings.

Example Usage

Basic usage:

```
resource "dome9_cloudaccount_azure" "test" {
  name            = "NAME"
  operation_mode  = "OPERATION MODE"
  subscription_id = "SUBSCRIPTION ID"
  tenant_id       = "TENANT ID"
  credentials = {
    client_id       = "CLIENT ID"
    client_password = "CLIENT PASSWORD"
  }
  organizational_unit_id = "ORGANIZATIONAL UNIT ID"
}
```

Argument Reference

The following arguments are supported:

- `name` - (Required) The Azure account number.
- `subscription_id` - (Required) Azure subscription id for account.
- `tenant_id` - (Required) Azure tenant id.
- `operation_mode` - (Required) Dome9 operation mode for the Azure account (Read-Only or Managed).
- `credentials` - (Required) Azure account credentials.
- `organizational_unit_id` - Organizational unit id, will apply on update state.

Credentials

The `credentials` block supports:

- `client_id` - (Required) Azure account id.
- `client_password` - (Required) Password for account.

Attributes Reference

- `id` - The ID of the Azure cloud account.

- `vendor` - The cloud provider (Azure).
- `creation_date` - Date Azure account was onboarded to a Dome9 account.
- `organizational_unit_path` - Organizational unit path.
- `organizational_unit_name` - Organizational unit name.

Import

Azure cloud account can be imported; use `<Azure CLOUD ACCOUNT ID>` as the import ID. For example:

```
terraform import dome9_cloudaccount_Azure.test 00000000-0000-0000-0000-000000000000
```

dome9_cloudaccount_gcp

The GoogleCloudAccount resource has methods to onboard Google cloud accounts to a Dome9 account, and to get details for a Google accounts Dome9.

Example Usage

Basic usage:

```
resource "dome9_cloudaccount_gcp" "gcp_ca" {
  name = "sandbox"

  service_account_credentials = {
    auth_provider_x509_cert_url = "https://www.googleapis.com/oauth2/v1/certs"
    auth_uri                    = "https://accounts.google.com/o/oauth2/auth"
    client_email                = "EMAIL@ADDRESS.COM"
    client_id                   = "CID"
    client_x509_cert_url        = "CERT URL"
    private_key                 = "KEY"
    private_key_id              = "PRIVATE"
    project_id                  = "ID"
    token_uri                   = "https://oauth2.googleapis.com/token"
    type                        = "service_account"
  }
  gsuite_user = "GSUITE USER"
  domain_name = "DOMAIN NAME"
  organizational_unit_id = "ORGANIZATIONAL UNIT ID"
}
```

Argument Reference

The following arguments are supported:

- `name` - (Required) Google account name in Dome9.
- `gsuite_user` - (Optional) The gsuite user.
- `service_account_credentials` - (Required) The service account JSON block (from the GCP console).
- `domain_name` - (Optional) The domain name.
- `organizational_unit_id` - (Optional) Organizational unit id, Will apply on update state.

Service Account Credentials

The `service_account_credentials` block supports:

- `type` - (Required) type. i.e "service_account"

- `project_id` - (Required) Project ID
- `private_key_id` - (Required) Private key ID
- `private_key` - (Required) Private key
- `client_email` - (Required) GCP client email
- `client_id` - (Required) Client id
- `auth_uri` - (Required) Auth URI. i.e "https://accounts.google.com/o/oauth2/auth (https://accounts.google.com/o/oauth2/auth)"
- `token_uri` - (Required) Token URI. i.e "https://oauth2.googleapis.com/token (https://oauth2.googleapis.com/token)"
- `auth_provider_x509_cert_url` - (Required) auth_provider_x509_cert_url. i.e "https://www.googleapis.com/oauth2/v1/certs (https://www.googleapis.com/oauth2/v1/certs)"
- `client_x509_cert_url` - (Required) client_x509_cert_url

Attributes Reference

- `id` - The ID of the GCP cloud account.
- `creation_date` - creation date for project in Google.
- `vendor` - The cloud provider (gcp).
- `organizational_unit_path` - Organizational unit path.
- `organizational_unit_name` - Organizational unit name.

Import

GCP cloud account can be imported; use `<GCP CLOUD ACCOUNT ID>` as the import ID. For example:

```
terraform import dome9_cloudaccount_gcp.test 00000000-0000-0000-0000-000000000000
```

dome9_continuous_compliance_policy

The ContinuousCompliancePolicy resource has methods to create and modify compliance policies for continuous compliance assessments. A continuous compliance policy is the combination of a Rule Bundle applied to a specific cloud account. With continuous compliance, compliance policies are assessed continuously and autonomously, and the results are issued to designated recipients as emails or SNS notifications, according to notification policies.

Example Usage

Basic usage:

```
resource "dome9_continuouscompliance_policy" "test_policy" {
  cloud_account_id    = "CLOUD ACCOUNT ID"
  external_account_id = "EXTERNAL ACCOUNT ID"
  bundle_id           = 00000
  cloud_account_type  = "CLOUD ACCOUNT TYPE"
  notification_ids    = ["NOTIFICATION IDS"]
}
```

Argument Reference

The following arguments are supported:

- `cloud_account_id` - (Required) The cloud account id.
- `external_account_id` - (Required) The account number.
- `bundle_id` - (Required) The bundle id for the policy.
- `cloud_account_type` - (Required) The cloud account provider (AWS/Azure/Google).
- `notification_ids` - (Required) The notifications id's for the policy.

Attributes Reference

- `id` - ID of the policy.

Import

The policy can be imported; use `<POLICY ID>` as the import ID. For example:

```
terraform import dome9_continuouscompliance_policy.test 00000000-0000-0000-0000-000000000000
```

dome9_iplist

The IpList resource has methods to create and manage IP lists in Dome9. IP lists are groups of IP addresses (typically in customer cloud environments), on which common actions are applied. For example, a Security Group could be applied to a list, instead of applying it to each IP address in the list individually.

Example Usage

Basic usage:

```
resource "dome9_iplist" "iplist" {
  name        = "NAME"
  description = "DESCRIPTION"

  items = [
    {
      ip      = "1.1.1.1"
      comment = "COMMENT1"
    },
    {
      ip      = "2.2.2.2"
      comment = "COMMENT2"
    },
  ]
}
```

Argument Reference

The following arguments are supported:

- `name` - (Required) The IP list name.
- `description` - (Optional) IP list description, defaults to empty string.
- `items` - (Optional) Items for IP list, defaults to empty list.

Items

The `items` supports the following arguments:

- `ip` - (Optional) IP.
- `comment` - (Optional) Comment.

Attributes Reference

- `id` - IP list Id.

Import

IP list can be imported; use `<IP LIST ID>` as the import ID. For example:

```
terraform import dome9_iplist.test 00000
```