GitLab Reference docs

07 January 2025 11:18

https://gitlab.com/gitlab-org/incubation-engineering/mobile-devops/download-secure-files

https://docs.gitlab.com/api/secure_files/#create-secure-file

```
Running with gitlab-runner 17.8.3 (690ce25c)
on MSFT RUNNER t1_H4XxH, system ID: s_7a03fa826079
Preparing the "docker" executor00:00
Using Docker executor with image tlsexpimages.azurecr.io/bapi-gitlab/dotnetcli:8.0.407 ...
ERROR: Job failed: invalid pull policy for image "tlsexpimages.azurecr.io/bapi-gitlab/dotnetcli:8.0.407": pull_policy ([always]) defined in GitLab pipeline config is not one of the allowed_pull_policies ([if-not-present])
```

From <https://gitlab-italent.com/italentdev/microsoft-middleware-functionapps/Microsoft-Middleware-FunctionApps/-/jobs/85061>

Mongo DB

13 January 2025 12:28

Create ROOT USER using Enviroment Variables:

```
MONGO_INITDB_ROOT_USERNAME

MONGO_INITDB_ROOT_PASSWORD
```

```
use admin
Show users
```

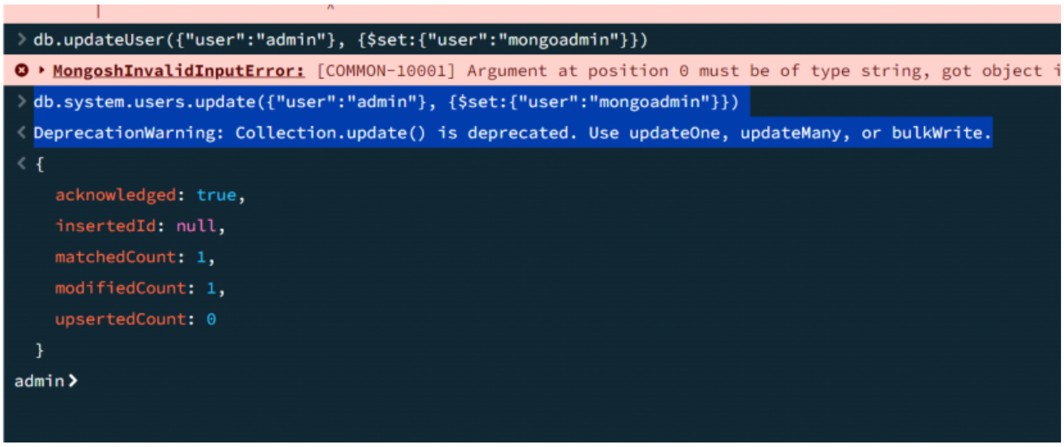
```
[
  {
    _id: 'admin.admin',
    userId: UUID('83a5e267-af71-4658-a511-82ad48545129'),
    user: 'admin',
    db: 'admin',
    roles: [
      {
        role: 'root',
        db: 'admin'
      }
    ],
    mechanisms: [
      'SCRAM-SHA-1',
      'SCRAM-SHA-256'
    ]
  }
]
```

Note: No need to Add any Other or Specific Permissions to ROOT USER

Update Password for existing user:

```
db.changeUserPassword("<USERNAME>", "NEWPASSWORD")
```

Update UserName in Admin DB



```
> db.updateUser({"user":"admin"}, {$set:{"user":"mongoadmin"}})
✖ ▸ MongoshInvalidInputError: [COMMON-10001] Argument at position 0 must be of type string, got object i
> db.system.users.update({"user":"admin"}, {$set:{"user":"mongoadmin"}})
< DeprecationWarning: Collection.update() is deprecated. Use updateOne, updateMany, or bulkWrite.
< {
    acknowledged: true,
    insertedId: null,
    matchedCount: 1,
    modifiedCount: 1,
    upsertedCount: 0
  }
admin>
```

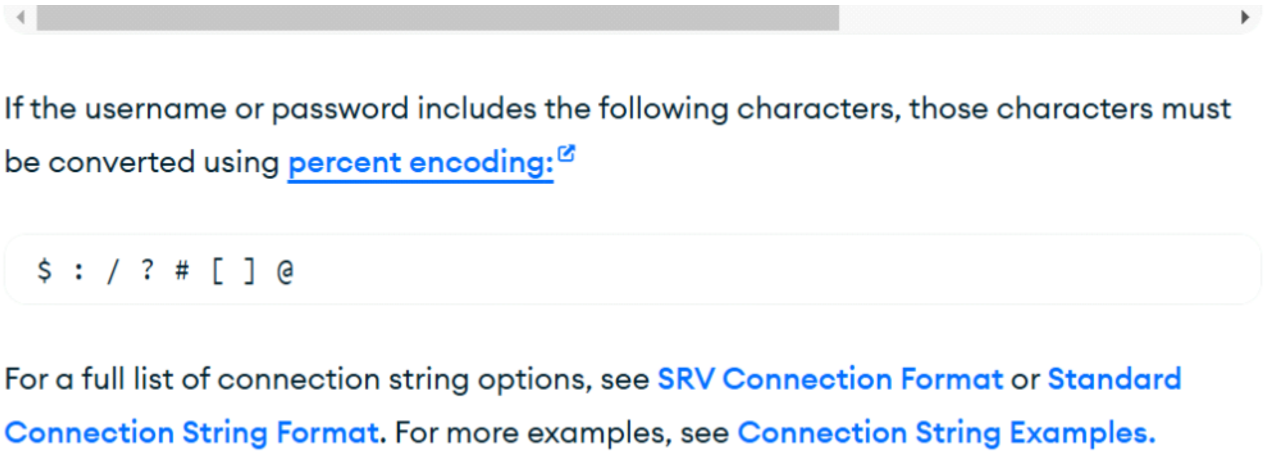
`db.system.users.update({"user":"existing_USER"}, {$set:{"user":"NEW_USERNAME"}})`

DeprecationWarning: Collection.update() is deprecated. Use updateOne, updateMany, or bulkWrite.

To List Current Logged in User

`db.runCommand({connectionStatus : 1}).authInfo.authenticatedUsers[0]`

`db.runCommand({connectionStatus : 1})`
`db.runCommand({connectionStatus : 1}).authInfo.authenticatedUserRoles[0]`



If the username or password includes the following characters, those characters must be converted using percent encoding:

```
$ : / ? # [ ] @
```

For a full list of connection string options, see SRV Connection Format or Standard Connection String Format. For more examples, see Connection String Examples.

Lifecycle:
postStartHook: logs are seen from kubelet in node level where the pod is running using command
`journalctl -u kubelet`

Access Tokens

28 November 2024 20:34

Gcloud login cli commands:

1. `gcloud auth application-default login`
2. `gcloud auth activate-service-account --key-file=${SAKEY_SECUREFILEPATH}`

Docker Configurations

```
gcloud auth configure-docker europe-west2-docker.pkg.dev --quiet
```

```
echo "Installing auth Plugin"

 sudo apt-get update -y

sudo apt-get install apt-transport-https ca-certificates gnupg curl sudo -y

curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo gpg --dearmor -o /usr/share/keyrings/cloud.google.gpg

echo "deb [signed-by=/usr/share/keyrings/cloud.google.gpg] https://packages.cloud.google.com/apt cloud-sdk main" | sudo tee -a /etc/apt/sources.list.d/google-cloud-sdk.list

sudo apt-get update && sudo apt-get install google-cloud-cli -y

sudo apt-get install google-cloud-sdk-gke-gcloud-auth-plugin -y

echo "Authenticating with SA key"

gcloud auth activate-service-account --key-file=${SAKEY_SECUREFILEPATH}

echo "set project"

gcloud config set project smartconx-dev-400910

echo "connect to cluster"

gcloud container clusters get-credentials smartconx-dev-gke1-clone-1 --zone us-central1-c --project smartconx-dev-400910
```

3. Revoke login credentials:

```
gcloud auth revoke --all
```

GOOGLE LOCATION AND ZONES:

Global Locations - Regions & Zones | Google Cloud

Regions and zones | Compute Engine Documentation | Google Cloud

Set Terraform Debug Log for windows:

```
$env:TF_LOG="DEBUG"
```

Service Availability Using Synthectic Monitoring with Cloud Run

ERRORS:

```
google_artifact_registry_repository.my_repository: Creating...
google_compute_global_address.ip_address: Creating...
google_container_cluster.primary: Creating...
│
│ Error: Error creating Repository: googleapi: Error 403: Permission denied on 'locations/europe-west-2' (or it may not exist).
│ Details:
│ [
│   {
│     "@type": "type.googleapis.com/google.rpc.ErrorInfo",
│     "domain": "googleapis.com",
│     "metadata": {
│       "consumer": "projects/smartconx-dev-400910",
│       "location": "europe-west-2",
│       "service": "artifactregistry.googleapis.com"
│     },
│     "reason": "LOCATION_POLICY_VIOLATED"
│   },
│   {
│     "@type": "type.googleapis.com/google.rpc.LocalizedMessage",
│     "locale": "en-US",
│     "message": "Permission denied on 'locations/europe-west-2' (or it may not exist)."
│   }
│ ]
│
```

```
│   with google_artifact_registry_repository.my_repository,
│   on ArtifactRegistry.tf line 1, in resource "google_artifact_registry_repository" "my_repository":



╵

╷
│ Error: when using a multi-zonal cluster, node_locations should not contain the original 'zone'
│
│   with google_container_cluster.primary,
│   on gke.tf line 8, in resource "google_container_cluster" "primary":
│    8: resource "google_container_cluster" "primary" {
│
╵

╷
│ Error: Error creating GlobalAddress: googleapi: Error 403: Required 'compute.globalAddresses.create' permission for 'projects/smartconx-dev-400910/global/addresses/smartconx-stati-ip-test', forbidden
│
│   with google_compute_global_address.ip_address,
│   on ipstaticaddress.tf line 1, in resource "google_compute_global_address" "ip_address":
│    1: resource "google_compute_global_address" "ip_address" {
│
╵



│ Error: googleapi: Error 400: Specified location "europe-west2-1" is not a valid zone in the cluster's region "europe-west2".
│ Details:
│ [
│   {
│     "@type": "type.googleapis.com/google.rpc.RequestInfo",
│     "requestId": "0xfece5160c38f0861"
│   }
│ ]
│ , badRequest
│
│   with google_container_cluster.primary,
│   on gke.tf line 8, in resource "google_container_cluster" "primary":
│    8: resource "google_container_cluster" "primary" {



╷
│ Error: googleapi: Error 400: The user does not have access to service account "468197716595-compute@developer.gserviceaccount.com". Ask a project owner to grant you the iam.serviceAccountUser role on the service account.
│ Details:
│ [
│   {
```

```
│     "@type": "type.googleapis.com/google.rpc.RequestInfo",
│     "requestId": "0x482f43ad16ff6d89"
│   }
│ ]
│ , badRequest
│
│   with google_container_cluster.primary,
│   on gke.tf line 8, in resource "google_container_cluster" "primary":
│    8: resource "google_container_cluster" "primary" {
│
╵
```

Fix:

As we are using "secretserviceacc@smartconx-dev-400910.iam.gserviceaccount.com" to create infra or cluster we got above error. So we have added "iam.serviceAccountUser" perrmission to secretserviceacc service account.

```
╷
│ Error: Error creating GlobalAddress: googleapi: Error 403: Required 'compute.globalAddresses.create'
permission for 'projects/smartconx-dev-400910/global/addresses/smartconx-stati-ip-test', forbidden
│
```

```
 Error: Error creating GlobalAddress: googleapi: Error 403: Required
'compute.globalAddresses.setLabels' permission for 'projects/smartconx-
dev-400910/global/addresses/smartconx-stati-ip-test', forbidden
```

```
kubernetes_namespace.syndication: Refreshing state... [id=syndication]

Planning failed. Terraform encountered an error while generating this plan.

╷
│ Error: Output refers to sensitive values
│
│   on gke.tf line 99:
│   99: output "service_account_access_token" {
│
│ To reduce the risk of accidentally exporting sensitive data that was intended to be only internal,
Terraform requires that any
│ root module output containing sensitive data be explicitly marked as sensitive, to confirm your intent.
│
│ If you do intend to export this data, annotate the output value as sensitive by adding the following
argument:
│     sensitive = true
```

```
Error: Error when reading or editing ComputeRegionNetworkEndpointGroup "projects/smartconx-
dev-400910/regions/europe-west2/networkEndpointGroups/test-neg-dev":
googleapi: Error 403: Required 'compute.regionNetworkEndpointGroups.get' permission for
```

```
'projects/smartconx-dev-400910/regions/europe-west2/networkEndpointGroups/test-neg-dev',
forbidden
```

```
PS D:\gitlab-smartconx\smartconxterraform\GCP\gcp-dev-test> terraform apply
╷
│ Error: Ephemeral output not allowed
│
│   on gke.tf line 99:
│   99: output "service_account_access_token" {
│
│ Ephemeral outputs are not allowed in context of a root module
```

VPC Native Cluster GKE

https://registry.terraform.io/providers/hashicorp/google/4.9.0/docs/guides/using_gke_with_terraform

```
ip_allocation_policy {
    cluster_secondary_range_name  = "pod-ranges"
    services_secondary_range_name =
google_compute_subnetwork.custom.secondary_ip_range.0.range_name
  }
```

From <https://registry.terraform.io/providers/hashicorp/google/6.24.0/docs/guides/using_gke_with_terraform>

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field
'resource.healthChecks[0]': 'projects/smartconx-dev-400910/regions/europe-
west1/healthChecks/terraform-hc'. Global backend service can not use a regional health check, invalid
```

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field
'resource.backends[0].balancingMode': 'UTILIZATION'. UTILIZATION balancing mode is not supported for
network endpoint groups., invalid
│
│   with google_compute_backend_service.alb-backend,
│   on Applicationloadbalancer.tf line 71, in resource "google_compute_backend_service" "alb-
backend":
│   71: resource "google_compute_backend_service" "alb-backend" {
```

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field
'resource.backends[0].balancingMode': 'RATE'. Either maxRate or maxRatePerEndpoint should be set
```

```
with RATE mode., invalid
│
│   with google_compute_backend_service.alb-backend,
│   on Applicationloadbalancer.tf line 71, in resource "google_compute_backend_service" "alb-
backend":
│   71: resource "google_compute_backend_service" "alb-backend" {



google_compute_backend_service.alb-backend: Creating...

╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field
'resource.backends[0]': '{  "group": "projects/smartconx-dev-400910/zones/europe-west2-
a/networkEndpointGroups/ingress-dev-te...'. Both maxConnections[PerEndpoint] and
maxRate[PerEndpoint] cannot be set., invalid



╷
│ Error: Error when reading or editing ComputeBackendService "projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg": googleapi: Error 403: Required
'compute.backendServices.get' permission for 'projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg', forbidden



╷
│ Error: Error when reading or editing BackendService: googleapi: Error 403: Required
'compute.backendServices.delete' permission for 'projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg', forbidden



google_compute_region_url_map.alb-url_map: Creating...

╷
│ Error: Error creating RegionUrlMap: googleapi: Error 403: Required
'compute.regionBackendServices.use' permission for 'projects/smartconx-dev-400910/regions/europe-
west2/backendServices/terraform-backend-neg'


Reason: forbidden, Message: Required 'compute.regionUrlMaps.create' permission for
'projects/smartconx-dev-400910/regions/europe-west2/urlMaps/terraform-regional-url-map'


compute.backendServices.update



╷
│ Error: Error when reading or editing ComputeUrlMap "projects/smartconx-
dev-400910/global/urlMaps/terraform-url-map": googleapi: Error 403: Required 'compute.urlMaps.get'
permission for 'projects/smartconx-dev-400910/global/urlMaps/terraform-url-map', forbidden
│
│   with google_compute_url_map.alb-url_map,
│   on Applicationloadbalancer.tf line 49, in resource "google_compute_url_map" "alb-url_map":
│   49: resource "google_compute_url_map" "alb-url_map" {
```

```
google_compute_backend_service.alb-backend: Creation complete after 46s [id=projects/smartconx-dev-400910/global/backendServices/terraform-backend-neg]
google_compute_url_map.alb-url_map: Creating...
╷
│ Error: Error creating UrlMap: googleapi: Error 403: Required 'compute.backendServices.use' permission for 'projects/smartconx-dev-400910/global/backendServices/terraform-backend-neg'
│ More details:
│ Reason: forbidden, Message: Required 'compute.backendServices.use' permission for 'projects/smartconx-dev-400910/global/backendServices/terraform-backend-neg'
│ Reason: forbidden, Message: Required 'compute.urlMaps.create' permission for 'projects/smartconx-dev-400910/global/urlMaps/terraform-url-map'


google_compute_global_forwarding_rule.alb: Creating...
╷
│ Error: Error creating GlobalForwardingRule: googleapi: Error 400: Invalid value for field 'resource.target': 'projects/smartconx-dev-400910/global/targetHttpsProxies/terraform-target-https'. Invalid target type TARGET_HTTPS_PROXY for forwarding rule with IPProtocol TCP with no port specified, invalid
│
│   with google_compute_global_forwarding_rule.alb,
│   on Applicationloadbalancer.tf line 31, in resource "google_compute_global_forwarding_rule" "alb":
│   31: resource "google_compute_global_forwarding_rule" "alb" {
│



╷
│ Error: Error creating Service: googleapi: Error 403: Permission 'monitoring.services.create' denied on resource 'projects/smartconx-dev-400910' (or resource may not exist).
│
│   with google_monitoring_custom_service.custom-synthetic-montoring,
│   on serviceavailability.tf line 6, in resource "google_monitoring_custom_service" "custom-synthetic-montoring":
│    6: resource "google_monitoring_custom_service" "custom-synthetic-montoring" {



│ Error: Error waiting to create Service: Error waiting for Creating Service: error while retrieving operation: googleapi: Error 403: Permission 'run.operations.get' denied on resource 'projects/smartconx-dev-400910/locations/europe-west2/operations/716ca1d4-314a-42a7-8072-21a18430b3d4' (or resource may not exist).
│
│   with google_cloud_run_v2_service.cloud_run_testing,
│   on serviceavailability.tf line 60, in resource "google_cloud_run_v2_service" "cloud_run_testing":
│   60: resource "google_cloud_run_v2_service" "cloud_run_testing" {


2025-07-18T15:45:24.135+0530 [ERROR] provider.terraform-provider-google_v6.38.0_x5.exe: Response
```

```
contains error diagnostic: diagnostic_severity=ERROR tf_proto_version=5.8
tf_provider_addr=registry.terraform.io/hashicorp/google tf_rpc=ApplyResourceChange
@caller=github.com/hashicorp/terraform-plugin-go@v0.26.0/tfprotov5/internal/diag/diagnostics.go:58
@module=sdk.proto diagnostic_detail="" diagnostic_summary="Error creating function: googleapi:
Error 400: Repository name `us-docker.pkg.dev/cloudrun/container/hello` has an invalid format. It
should match the pattern `projects/{project}/locations/{location}/repositories/{repository}`." tf_req_id=
9a15aaaf-4c80-d8bc-d8bf-fcaafd032d50 tf_resource_type=google_cloudfunctions2_function
timestamp="2025-07-18T15:45:24.135+0530"
2025-07-18T15:45:24.163+0530 [ERROR] vertex "google_cloudfunctions2_function.cloudfunction"
error: Error creating function: googleapi: Error 400: Repository name `us-
docker.pkg.dev/cloudrun/container/hello` has an invalid format. It should match the pattern
`projects/{project}/locations/{location}/repositories/{repository}`.

╷
│ Error: Error creating function: googleapi: Error 400: Repository name `us-
docker.pkg.dev/cloudrun/container/hello` has an invalid format. It should match the pattern
`projects/{project}/locations/{location}/repositories/{repository}`.
│
│   with google_cloudfunctions2_function.cloudfunction,
│   on serviceavailability.tf line 35, in resource "google_cloudfunctions2_function" "cloudfunction":
│   35: resource "google_cloudfunctions2_function" "cloudfunction" {
```

```
2025-07-18T18:48:50.978+0530 [ERROR] vertex "google_cloudfunctions2_function.cloudfunction"
error: Error waiting to create function: Error waiting for Creating function: error while retrieving
operation: googleapi: Error 403: Permission 'cloudfunctions.operations.get' denied on
'projects/smartconx-dev-400910/locations/europe-
west2/operations/operation-1752844727446-63a33f7536a67-307022bc-b77b52d5'

╷
│ Error: Error waiting to create function: Error waiting for Creating function: error while retrieving
operation: googleapi: Error 403: Permission 'cloudfunctions.operations.get' denied on
'projects/smartconx-dev-400910/locations/europe-
west2/operations/operation-1752844727446-63a33f7536a67-307022bc-b77b52d5'
│
│   with google_cloudfunctions2_function.cloudfunction,
│   on serviceavailability.tf line 21, in resource "google_cloudfunctions2_function" "cloudfunction":
│   21: resource "google_cloudfunctions2_function" "cloudfunction" {
```

Deploying Cloud Run Function using nodejs from google bucket

[Terraform Tutorial | Cloud Run functions Documentation | Google Cloud](https://cloud.google.com/functions/docs/tutorials/terraform)

```
curl -H "Authorization: Bearer $(gcloud auth print-identity-token)" YOUR_FUNCTION_URL
```

From <https://cloud.google.com/functions/docs/tutorials/terraform>

Docker Image Pull using Kubelet service account

- Assign service account either the custom or provide scopes for default service account(PROJECT_NUMBER-compute@developer.gserviceaccount.com)

  Update the below block in vmss_pools
  node_config {

```
            Scopes = [
            "",
            ""
            ]
            service_account = ""
        }
```

Compute Engine default service account	No	• https://www.googleapis.com/auth/devstorage.read_only • https://www.googleapis.com/auth/service.management.readonly • https://www.googleapis.com/auth/servicecontrol • https://www.googleapis.com/auth/trace.append • https://www.googleapis.com/auth/logging.write: added if Cloud Logging is enabled • https://www.googleapis.com/auth/monitoring: added if Cloud Monitoring is enabled

Compute Engine default service account

From <https://cloud.google.com/compute/docs/access/service-accounts>

PROJECT_NUMBER-compute@developer.gserviceaccount.com

From <https://cloud.google.com/compute/docs/access/service-accounts>

```
... 14 more
Caused by: java.io.IOException: Unexpected Error code 403 trying to get security access
token from Compute Engine metadata for the default service account: Unable to generate
access token; IAM returned 403 Forbidden: Permission 'iam.serviceAccounts.getAccessToken'
denied on resource (or it may not exist).
This error could be caused by a missing IAM policy binding on the target IAM service
account.
For more information, refer to the Workload Identity documentation:
https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity#authenticating_to
```

From <https://lens.app:57760/>

```
t java.lang.Thread.run(Thread.java:833) [?:?]
Caused by: io.grpc.StatusRuntimeException: UNAUTHENTICATED: Failed computing credential
metadata
at io.grpc.Status.asRuntimeException(Status.java:533) ~[grpc-api-1.66.0.jar!/:1.66.0]
... 14 more
Caused by: java.io.IOException: Unexpected Error code 403 trying to get security access
token from Compute Engine metadata for the default service account: Unable to generate
access token; IAM returned 403 Forbidden: Permission 'iam.serviceAccounts.getAccessToken'
denied on resource (or it may not exist).
This error could be caused by a missing IAM policy binding on the target IAM service
account.
For more information, refer to the Workload Identity documentation:
https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity#authenticating_to
```

From <https://lens.app:57760/>

Add Artificate Read Permissions to SA

```
gcloud artifacts repositories remove-iam-policy-binding REPOSITORY_NAME \
   --location=REPOSITORY_LOCATION \
--member='principal://iam.googleapis.com/projects/PROJECT_NUMBER/locations/global/workloadIdentityPools/PROJECT_ID.svc.id.goog/subject/ns/NAMESPACE/sa/KSA_NAME' \
   --role='roles/artifactregistry.reader' \
   --all
```

From <https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity>

```
# data "google_service_account" "workload-identity-service-account-name" {
#   account_id = var.wl_serviceaccount_name
#   project    = var.project_id
# }

# resource "google_service_account_iam_binding" "workload-identity-policy-binding" {
#   members            = ["serviceAccount:smartconx-dev-400910.svc.id.goog[syndication/secretmanagerdevtest]"]
#   role               = "roles/iam.workloadIdentityUser"
#   service_account_id = data.google_service_account.workload-identity-service-account-name.id
# }
```

Terraform output variables

```
Changes to Outputs:
  ~ kubernetes_cluster_api_server = [
      - {
          - client_certificate        = ""
          - client_certificate_config = [
              - {
                  - issue_client_certificate = false
                },
            ]
          - client_key                = ""
          - cluster_ca_certificate    =
"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUVMRENDQXBTZ0F3SUJBZ0lRZjNXR0JST0orNmtCYTdBUjl4b1dOVEFOQmdrcWhraUc5dzBCQVFzRkFEQXYKTVMwd0t3WURWUVFERXlRNFpqTmlNemM0T0Mxak1UUmxMVFJsTVRZdE9UVTNNaTAzT0dSbU56WTNNMk01WWpjdwpJQmNOTWpVd056RXhNRFF3TnpJMldoZ1BNakExTlRBM01EUXdOVEEzTWpaYU1DOHhMVEFyQmdOVkJBTVRKRGhtCk0ySXpOemc0TFdNeE5HVXROR1V4TmkwNU5UY3lMVGM0WkdZM05qY3pZemxpTnpDQ0FhSXdEUVlKS29aSWh2Y04KQVFFQkJRQURnZ0dQQURDQ0FZb0NnZ0dCQUoyQllOYzl1bUJCSkxZeEhmd0drNFhZNkVKaVI2L3pXeTAwOUNiTgo0d0xDUGdJclVJNmxQbGtYYjl3WUFjT2I4UFo0SThRU0x4YklPYlNld2ZNcWFDRUNnNklSNGJ3cFg4RjF2cEVNClI4KzlOcG85aXJqUkdVVWtkSEtpeUNSNGE0dFd1RDBxTVV2WWVWcmJZL0EzdHRndDJWaDY2ZU9uRFM0THVnaTgKN1k0SEhFQ0JCalB1V3VYUHYyQ1ZlR29wYk9nZXpnR1hHS1BEcE4yRTNIdnZBNTN0UGZaRDVHcmhhL2tURHgrUQpDTDdKQmZJV2tkTDFrQzBhaVpoMnFiYnM1dVFROG1PWWl2dHlzVXk2OFQxQzlJQ1lTajNpdFg5d2RBbGFIaTlHCkd1T0xsRkxacGovVERlRG5FZVRkMUorbGtPc3FsS3ZKTFpxZG83VlhSbk40YzZMVURmdEd1U0M3UGV4NlpjSTMKN002d0ZBenkvMGQvY1FtY2hXQlNsazhlSEFiaVR6Sk9UelB4aG5jTmJ2RmNXaG9aR2RlaERIRFl2N3pZMUJsVgordHJQdGVZUFN2bTA4UDA2TDJ2TlpMVnE0akp3OEZZN2JJTjdQQTFZVndac1k
4ay91UU16Ky8rRTRJSzdRMCt1ClBnNU9uL2xjRVM1WkdBT2RzbTlwc1c1SGt3SURBUUFCbzBJd1FEQU9CZ0
5WSFE4QkFmOEVCQU1DQWdRd0R3WUQKVlIwVEFRSC9CQVV3QXdFQi96QWRCZ05WSFE0RUZnUVU0T
HJ5TC8xWlp2MHdqZUJiSjlJMmhRRVN1U2d3RFFZSgpLb1pJaHZjTkFRRUxCUUFEZ2dHQkFDbHowTk5IWDB
pRmMvVWY5UHNiNWpnMlhXN3NkSnY2WWMzTDcremdLRVpRCkF6d2EvSlRrelVQOFk2NUEwaWExZXBT
MTBVN0p1MTVIbEhlYVltU085MEhYRGdmVnNNZVpyMnovQmVBOUk4VDQKRG85OU5MNVJCVGhzVWw
zKytmTVRjaUxwYytUVG5ud0h1RWc2S1QxeFBXSERiSmJzdlp1Mzd0S210cWtnOFdMSgpsVE1hVFAzMHJE
WWVqYTVKRTRMZmhqY25CTVVJMUUrUGdYclZ5aCtZd2h0VXZkaWxpenFvbmJ5d1ZOUWQxRWxLCjNTZ3
pVejNFdWZDditKcTFxSUlUOHQ2emFhaHFlOW9HdHU4NlNQQ3M4alVMS1Z3UkM5RUp0QnB2Rjc0QVZ3
UkEKTzVTdzVDMEZER25lVnVxRGtCS2p0UkdtQjNkVG9rZm1iRHBNRCtRZCs0M1RMZUE2YkNKT3ZMaWV
WRUNxWEpXdQp2TUxpS3pEQlk3WEM4TmIxZ0xJTjRnZ2F2WG5HQUlIbmlVbTdNcWlrK3pFTmdCcldiS3Bh
bFNRRlRONWdjNTJ3Cld2UWJrZHpBTFB0dithTHEvamVMVVRPaG50bTJYM1h3WVdkWnhmZkhLUFMyN2F
qelozSmppYkpRalhwRHd1Y2wKOHdsWXhuREIya1QwUG5XdEJBTW4wQT09Ci0tLS0tRU5EIENFUlRJRklDQ
VRFLS0tLS0K"
       },
   ] -
```

Access Tokens

28 November 2024 20:34

Gcloud login cli commands:

1.
   ```
   gcloud auth application-default login
   ```

2.
   ```
   gcloud auth activate-service-account --key-file=${SAKEY_SECUREFILEPATH}
   ```

Docker Configurations

```
gcloud auth configure-docker europe-west2-docker.pkg.dev --quiet
```

```
echo "Installing auth Plugin"

 sudo apt-get update -y

sudo apt-get install apt-transport-https ca-certificates gnupg curl sudo -y

curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo gpg --dearmor -o /usr/share/keyrings/cloud.google.gpg

echo "deb [signed-by=/usr/share/keyrings/cloud.google.gpg] https://packages.cloud.google.com/apt cloud-sdk main" | sudo tee -a /etc/apt/sources.list.d/google-cloud-sdk.list

sudo apt-get update && sudo apt-get install google-cloud-cli -y

sudo apt-get install google-cloud-sdk-gke-gcloud-auth-plugin -y

echo "Authenticating with SA key"

gcloud auth activate-service-account --key-file=${SAKEY_SECUREFILEPATH}

echo "set project"

gcloud config set project smartconx-dev-400910

echo "connect to cluster"

gcloud container clusters get-credentials smartconx-dev-gke1-clone-1 --zone us-central1-c --project smartconx-dev-400910
```

3. Revoke login credentials:

   ```
   gcloud auth revoke --all
   ```

GOOGLE LOCATION AND ZONES:

Global Locations - Regions & Zones | Google Cloud

Regions and zones | Compute Engine Documentation | Google Cloud

Service Availability Using Synthectic Monitoring with Cloud Run

ERRORS:

```
google_artifact_registry_repository.my_repository: Creating...
google_compute_global_address.ip_address: Creating...
google_container_cluster.primary: Creating...
╷
│ Error: Error creating Repository: googleapi: Error 403: Permission denied on 'locations/europe-west-2' (or it may not exist).
│ Details:
│ [
│   {
│     "@type": "type.googleapis.com/google.rpc.ErrorInfo",
│     "domain": "googleapis.com",
│     "metadata": {
│       "consumer": "projects/smartconx-dev-400910",
│       "location": "europe-west-2",
│       "service": "artifactregistry.googleapis.com"
│     },
│     "reason": "LOCATION_POLICY_VIOLATED"
│   },
│   {
│     "@type": "type.googleapis.com/google.rpc.LocalizedMessage",
│     "locale": "en-US",
│     "message": "Permission denied on 'locations/europe-west-2' (or it may not exist)."
│   }
│ ]
│
│   with google_artifact_registry_repository.my_repository,
│   on ArtifactRegistry.tf line 1, in resource "google_artifact_registry_repository" "my_repository":


╵

╷
```

```
│ Error: when using a multi-zonal cluster, node_locations should not contain the original 'zone'
│
│   with google_container_cluster.primary,
│   on gke.tf line 8, in resource "google_container_cluster" "primary":
│    8: resource "google_container_cluster" "primary" {
│
╵
```

```
╷
│ Error: Error creating GlobalAddress: googleapi: Error 403: Required 'compute.globalAddresses.create'
permission for 'projects/smartconx-dev-400910/global/addresses/smartconx-stati-ip-test', forbidden
│
│   with google_compute_global_address.ip_address,
│   on ipstaticaddress.tf line 1, in resource "google_compute_global_address" "ip_address":
│    1: resource "google_compute_global_address" "ip_address" {
│
╵
```

```
│ Error: googleapi: Error 400: Specified location "europe-west2-1" is not a valid zone in the cluster's
region "europe-west2".
│ Details:
│ [
│   {
│     "@type": "type.googleapis.com/google.rpc.RequestInfo",
│     "requestId": "0xfece5160c38f0861"
│   }
│ ]
│ , badRequest
│
│   with google_container_cluster.primary,
│   on gke.tf line 8, in resource "google_container_cluster" "primary":
│    8: resource "google_container_cluster" "primary" {
```

```
╷
│ Error: googleapi: Error 400: The user does not have access to service account "468197716595-
compute@developer.gserviceaccount.com". Ask a project owner to grant you the
iam.serviceAccountUser role on the service account.
│ Details:
│ [
│   {
│     "@type": "type.googleapis.com/google.rpc.RequestInfo",
│     "requestId": "0x482f43ad16ff6d89"
│   }
│ ]
│ , badRequest
│
│   with google_container_cluster.primary,
│   on gke.tf line 8, in resource "google_container_cluster" "primary":
```

```
│   8: resource "google_container_cluster" "primary" {
│
╵
```

Fix:

As we are using "secretserviceacc@smartconx-dev-400910.iam.gserviceaccount.com" to create infra or cluster we got above error. So we have added "iam.serviceAccountUser" perrmission to secretserviceacc service account.

```
╷
│ Error: Error creating GlobalAddress: googleapi: Error 403: Required 'compute.globalAddresses.create' permission for 'projects/smartconx-dev-400910/global/addresses/smartconx-stati-ip-test', forbidden
│
```

```
 Error: Error creating GlobalAddress: googleapi: Error 403: Required 'compute.globalAddresses.setLabels' permission for 'projects/smartconx-dev-400910/global/addresses/smartconx-stati-ip-test', forbidden
```

```
kubernetes_namespace.syndication: Refreshing state... [id=syndication]

Planning failed. Terraform encountered an error while generating this plan.

╷
│ Error: Output refers to sensitive values
│
│   on gke.tf line 99:
│   99: output "service_account_access_token" {
│
│ To reduce the risk of accidentally exporting sensitive data that was intended to be only internal, Terraform requires that any
│ root module output containing sensitive data be explicitly marked as sensitive, to confirm your intent.
│
│ If you do intend to export this data, annotate the output value as sensitive by adding the following argument:
│     sensitive = true
```

```
Error: Error when reading or editing ComputeRegionNetworkEndpointGroup "projects/smartconx-dev-400910/regions/europe-west2/networkEndpointGroups/test-neg-dev": googleapi: Error 403: Required 'compute.regionNetworkEndpointGroups.get' permission for 'projects/smartconx-dev-400910/regions/europe-west2/networkEndpointGroups/test-neg-dev', forbidden
```

```
PS D:\gitlab-smartconx\smartconxterraform\GCP\gcp-dev-test> terraform apply
╷
│ Error: Ephemeral output not allowed
│
```

```
│  on gke.tf line 99:
│  99: output "service_account_access_token" {
│
│ Ephemeral outputs are not allowed in context of a root module
```

VPC Native Cluster GKE

https://registry.terraform.io/providers/hashicorp/google/4.9.0/docs/guides/using_gke_with_terraform

```
ip_allocation_policy {
    cluster_secondary_range_name  = "pod-ranges"
    services_secondary_range_name = google_compute_subnetwork.custom.secondary_ip_range.0.range_name
  }
```

From <https://registry.terraform.io/providers/hashicorp/google/6.24.0/docs/guides/using_gke_with_terraform>

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field 'resource.healthChecks[0]': 'projects/smartconx-dev-400910/regions/europe-west1/healthChecks/terraform-hc'. Global backend service can not use a regional health check, invalid
```

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field 'resource.backends[0].balancingMode': 'UTILIZATION'. UTILIZATION balancing mode is not supported for network endpoint groups., invalid
│
│  with google_compute_backend_service.alb-backend,
│  on Applicationloadbalancer.tf line 71, in resource "google_compute_backend_service" "alb-backend":
│  71: resource "google_compute_backend_service" "alb-backend" {
```

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field 'resource.backends[0].balancingMode': 'RATE'. Either maxRate or maxRatePerEndpoint should be set with RATE mode., invalid
│
│  with google_compute_backend_service.alb-backend,
│  on Applicationloadbalancer.tf line 71, in resource "google_compute_backend_service" "alb-backend":
│  71: resource "google_compute_backend_service" "alb-backend" {
```

```
google_compute_backend_service.alb-backend: Creating...
╷
│ Error: Error creating BackendService: googleapi: Error 400: Invalid value for field
'resource.backends[0]': '{  "group": "projects/smartconx-dev-400910/zones/europe-west2-
a/networkEndpointGroups/ingress-dev-te...'. Both maxConnections[PerEndpoint] and
maxRate[PerEndpoint] cannot be set., invalid
```

```
╷
│ Error: Error when reading or editing ComputeBackendService "projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg": googleapi: Error 403: Required
'compute.backendServices.get' permission for 'projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg', forbidden
```

```
╷
│ Error: Error when reading or editing BackendService: googleapi: Error 403: Required
'compute.backendServices.delete' permission for 'projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg', forbidden
```

```
google_compute_region_url_map.alb-url_map: Creating...
╷
│ Error: Error creating RegionUrlMap: googleapi: Error 403: Required
'compute.regionBackendServices.use' permission for 'projects/smartconx-dev-400910/regions/europe-
west2/backendServices/terraform-backend-neg'
```

```
Reason: forbidden, Message: Required 'compute.regionUrlMaps.create' permission for
'projects/smartconx-dev-400910/regions/europe-west2/urlMaps/terraform-regional-url-map'
```

```
compute.backendServices.update
```

```
╷
│ Error: Error when reading or editing ComputeUrlMap "projects/smartconx-
dev-400910/global/urlMaps/terraform-url-map": googleapi: Error 403: Required 'compute.urlMaps.get'
permission for 'projects/smartconx-dev-400910/global/urlMaps/terraform-url-map', forbidden
│
│   with google_compute_url_map.alb-url_map,
│   on Applicationloadbalancer.tf line 49, in resource "google_compute_url_map" "alb-url_map":
│   49: resource "google_compute_url_map" "alb-url_map" {
```

```
google_compute_backend_service.alb-backend: Creation complete after 46s [id=projects/smartconx-
dev-400910/global/backendServices/terraform-backend-neg]
google_compute_url_map.alb-url_map: Creating...
╷
│ Error: Error creating UrlMap: googleapi: Error 403: Required 'compute.backendServices.use'
permission for 'projects/smartconx-dev-400910/global/backendServices/terraform-backend-neg'
```

```
│ More details:
│ Reason: forbidden, Message: Required 'compute.backendServices.use' permission for 'projects/smartconx-dev-400910/global/backendServices/terraform-backend-neg'
│ Reason: forbidden, Message: Required 'compute.urlMaps.create' permission for 'projects/smartconx-dev-400910/global/urlMaps/terraform-url-map'
```

```
google_compute_global_forwarding_rule.alb: Creating...

╷
│ Error: Error creating GlobalForwardingRule: googleapi: Error 400: Invalid value for field 'resource.target': 'projects/smartconx-dev-400910/global/targetHttpsProxies/terraform-target-https'. Invalid target type TARGET_HTTPS_PROXY for forwarding rule with IPProtocol TCP with no port specified, invalid
│
│   with google_compute_global_forwarding_rule.alb,
│   on Applicationloadbalancer.tf line 31, in resource "google_compute_global_forwarding_rule" "alb":
│   31: resource "google_compute_global_forwarding_rule" "alb" {
│
```

```
╷
│ Error: Error creating Service: googleapi: Error 403: Permission 'monitoring.services.create' denied on resource 'projects/smartconx-dev-400910' (or resource may not exist).
│
│   with google_monitoring_custom_service.custom-synthetic-montoring,
│   on serviceavailability.tf line 6, in resource "google_monitoring_custom_service" "custom-synthetic-montoring":
│    6: resource "google_monitoring_custom_service" "custom-synthetic-montoring" {
```

Compute Engine default service account

From <https://cloud.google.com/compute/docs/access/service-accounts>

PROJECT_NUMBER-compute@developer.gserviceaccount.com

From <https://cloud.google.com/compute/docs/access/service-accounts>

Terraform output variables

```
Changes to Outputs:
  ~ kubernetes_cluster_api_server = [
      - {
          - client_certificate        = ""
          - client_certificate_config = [
          - {
              - issue_client_certificate = false
            },
        ]
      - client_key              = ""
      - cluster_ca_certificate    =
"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUVMRENDQXBTZ0F3SUJBZ0lRZjNXR0JST0orNmtCYTdB
Ujl4b1dOVEFOQmdrcWhraUc5dzBCQVFzRkFEQXYKTVMwd0t3WURWUVFERXlRNFpqTmlNemM0T0Mxak
1UUmxMVFJsTVRZdE9UVTNNaTAzT0dSbU56WTNNMk01WWpjdwpJQmNOTWpVd056RXhNRFF3TnpJMl
doZ1BNakExTlRBM01EUXdOVEEzTWpaYU1DOHhMVEFyQmdOVkJBTVRKRGhtCk0ySXpOemc0TFdNeE5H
VXROR1V4TmkwNU5UY3lMVGM0WkdZM05qY3pZemxpTnpDQ0FhSXdEUVlKS29aSWh2Y04KQVFFQkJRQ
URnZ0dQQURDQ0FZb0NnZ0dCQUoyQllOYzl1bUJCSkxZeEhmd0drNFhZNkVKaVI2L3pXeTAwOUNiTgo0d0x
DUGdJclVJNmxQbGtYYjl3WUFjT2I4UFo0SThRU0x4YklPYlNld2ZNcWFDRUNnNklSNGJ3cFg4RjF2cEVNClI4K
zlOcG85aXJqUkdVVWtkSEtpeUNSNGE0dFd1RDBxTVV2WWVWcmJZL0EzdHRndDJWaDY2ZU9uRFM0THV
naTgKN1k0SEhFQ0JCalB1V3VYUHYyQ1ZlR29wYk9nZXpnR1hHS1BEcE4yRTNIdnZBNTN0UGZaRDVHcmhhL
2tURHgrUQpDTDdKQmZJV2tkTDFrQzBhaVpoMnFiYnM1dVFROG1PWWl2dHlzVXk2OFQxQzlJQ1lTajNpdF
g5d2RBbGFIaTlHCkd1T0xsRkxacGovVERlRG5FZVRkMUorbGtPc3FsS3ZKTFpxZG83VlhSbk40YzZMVURmdE
d1U0M3UGV4NlpjSTMKN002d0ZBenkvMGQvY1FtY2hXQlNsazhlSEFiaVR6Sk9UelB4aG5jTmJ2RmNXaG9a
R2RlaERIRFl2N3pZMUJsVgordHJQdGVZUFN2bTA4UDA2TDJ2TlpMVnE0akp3OEZZN2JJTjdQQTFZVndac1k
4ay91UU16Ky8rRTRJSzdRMCt1ClBnNU9uL2xjRVM1WkdBT2RzbTlwc1c1SGt3SURBUUFCbzBJd1FEQU9CZ0
5WSFE4QkFmOEVCQU1DQWdRd0R3WUQKVlIwVEFRSC9CQVV3QXdFQi96QWRCZ05WSFE0RUZnUVU0T
HJ5TC8xWlp2MHdqZUJiSjlJMmhRRVN1U2d3RFFZSgpLb1pJaHZjTkFRRUxCUUFEZ2dHQkFDbHowTk5IWDB
pRmMvVWY5UHNiNWpnMlhXN3NkSnY2WWMzTDcremdLRVpRCkF6d2EvSlRrelVQOFk2NUEwaWExZXBT
MTBVN0p1MTVIbEhlYVltU085MEhYRGdmVnNNZVpyMnovQmVBOUk4VDQKRG85OU5MNVJCVGhzVWw
zKytmTVRjaUxwYytUVG5ud0h1RWc2S1QxeFBXSERiSmJzdlp1Mzd0S210cWtnOFdMSgpsVE1hVFAzMHJE
WWVqYTVKRTRMZmhqY25CTVVJMUUrUGdYclZ5aCtZd2h0VXZkaWxpenFvbmJ5d1ZOUWQxRWxLCjNTZ3
pVejNFdWZDditKcTFxSUlUOHQ2emFhaHFlOW9HdHU4NlNQQ3M4alVMS1Z3UkM5RUp0QnB2Rjc0QVZ3
UkEKTzVTdzVDMEZER25lVnVxRGtCS2p0UkdtQjNkVG9rZm1iRHBNRCtRZCs0M1RMZUE2YkNKT3ZMaWV
WRUNxWEpXdQp2TUxpS3pEQlk3WEM4TmIxZ0xJTjRnZ2F2WG5HQUlIbmlVbTdNcWlrK3pFTmdDcldiS3Bh
bFNRRlRONWdjNTJ3Cld2UWJrZHpBTFB0dithTHEvamVMVVRPaG50bTJYM1h3WVdkWnhmZkhLUFMyN2F
qelozSmppYkpRalhwRHd1Y2wKOHdsWXhuREIya1QwUG5XdEJBTW4wQT09Ci0tLS0tRU5EIENFUlRJRklDQ
VRFLS0tLS0K"
      },
   ] -
```

21 March 2024 14:49

GET 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://management.azure.com/' HTTP/1.1 Metadata: true

Expand table

From <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-to-use-vm-token#get-a-token-using-http>

https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=portal%2Chttp#rest-endpoint-reference

http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://management.azure.com/&client_id=3343d0b1-08f4-43ee-bd12-aee63794aae7

```
variables('AARP_TENTANT_OBJECT')['value'][0]['count_']
@{string(variables('myArrayVariable'))}
```

```
"@body('Parse_JSON_response')?['access_token']",
```

From <https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-create-variables-store-values?tabs=consumption>

SAAS Accelerator

13 March 2023 10:36

Create a APP Registration, add the Redirect URI of Both the App Services URI,
Eg: https://sdkcoustmerprovisioning.azurewebsites.net/
https://sdkcoustmerprovisioning.azurewebsites.net/signin-oidc
https://sdkcoustmerprovisioning.azurewebsites.net/Home/Index

Need to Modify the "appsettings.json" for both the App services or can be passed as a parameter while running Script
Make sure to use KeyVault to pass Azure AAD APP Secret.
Also pass connection String of Database. Update the password of User, at password field.

At Partner Login Page, Go to Technical Configuration add the URI of Coustmer Provisioning App service
Eg: https://sdkcoustmerprovisioning.azurewebsites.net/
And for WebHook:
https://sdkcoustmerprovisioning.azurewebsites.net/api/AzureWebhook
Add pass Tentant ID and Client ID of AAD

Create SQL Database using Script file, make sure to configure Firewall settings open or allow to access. Also create Azure APP services for Coustomer Provisioning, Publisher Solution.

Add a user at the KnownUsers table in DataBase, so that the user can only login to the admin pages and Landing Pages.

ICS_DEVOPS_TASKS

27 February 2023 17:58

Tasks Assigned:

1. Static Public IP Address for Ingress-Controller
2. Setup of Grafana for Clusters
3. Configured AAD login for Grafana
4. Created Alerts using Grafana Managed Alerting
5. "Origin Not Allowed" issue for Grafana when access behind Ingress Proxy
6. Configured /grafana for Front Door URL
7. Written Shell Script for Running all Pipelines within a Project
8. Added WAF Polices for Grafana To access without any Restrictions
9. Created Custom Dashboards for Memory and CPU metrics for Pods
10. CDCC-2309 - LM-42 - Move Label Manager VMs
11. Log Exception alert where Logs Files are Attached to Mail
12. TLS automation for patching tls.crt file replacement in Secret
13. Python script to automate Jira version numbers

Things to learn DevOps:

Setup Dynamic runners for pipeline agents
Lock terraform state using DynmoDB and store the state using AWS S3 or any euqivalent
Refercne links: https://medium.com/dlt-labs-publication/remote-state-and-locking-using-terraform-cff38241a548

Need to send mails when an 5XX errors Triggers
New version of Terraform 1.25V generate automated code for imported Resources

Java Open Telemetry Api https://learn.microsoft.com/en-us/azure/azure-monitor/app/opentelemetry-add-modify?tabs=java#modify-telemetry

26 January 2023 15:02

Grafana Alerting Reference

https://grafana.com/docs/grafana/latest/alerting/set-up/provision-alerting-resources/file-provisioning/

Api Grafana:

https://editor.swagger.io/?url=https://raw.githubusercontent.com/grafana/grafana/main/pkg/services/ngalert/api/tooling/post.json

ModelsL

GettableGrafanaRule:

https://italenticsstg.azurefd.net((/[a-zA-Z0-9-_.]*.(js|css|jpg|png|ico|woff|woff2|gif))|(/grafana/.*)|($))

https://italenticsstg.azurefd.net((/[a-zA-Z0-9-_.]*.(js|css|jpg|png|ico|woff|woff2|gif))|(/ui-service/.*)|(/collabservice/.*)|(/assets/.*)|(/xcommunityui/.*)|(/xcommunityaad/.*)|(/higher.*)|(/wrmsdc.*)|(/lithiumservice.*)|(/swagger-ui.html)|(/aarp.*)|(/grafana/.*)|($))

https://italenticsstg.azurefd.net((/[a-zA-Z0-9-_.]*.(js|css|jpg|png|ico|woff|woff2|gif))|(/ui-service/.*)|(/collabservice/.*)|(/assets/.*)|(/xcommunityui/.*)|(/xcommunityaad/.*)|(/higher.*)|(/wrmsdc.*)|(/lithiumservice.*)|(/swagger-ui.html)|(/aarp.*)|($))

Grafana DataBase is Locked

https://opsverse.io/2022/12/15/grafana-sqlite-and-database-is-locked/

https://iximiuz.com/en/posts/kubernetes-ephemeral-containers/

```
 extraInitContainers:
    - name: grafana-db-clone-replace
      image: keinos/sqlite3
      command:
        - "/bin/sh"
        - "-c"
        - "/usr/bin/sqlite3 /var/lib/grafana/grafana.db '.clone
/var/lib/grafana/grafana.db.clone'; mv /var/lib/grafana/grafana.db.clone
/var/lib/grafana/grafana-old.db; mv /var/lib/grafana/grafana.db.clone
/var/lib/grafana/grafana.db; chmod a+w /var/lib/grafana/grafana.db"
      imagePullPolicy: IfNotPresent
      securityContext:
        runAsUser: 0
      volumeMounts:
       - name: storage
         mountPath: "/var/lib/grafana"
```

Working Configuration Alerts using helm values:

Adding another Rule to same Group and folder:

```
test_pod:
  image: bats/bats:v1.1.0
  pullPolicy: IfNotPresent
loki:
  enabled: true
  isDefault: true
  url: http://{{(include "loki.serviceName" .)}}:{{ .Values.loki.service.port }}
  gateway:
    enabled: true
  persistence:
    type: pvc
    enabled: true
    size: 20Gi
    storageClassName: grafana
    existingClaim: loki-pvc
  existingSecretForConfig: loki
  config:
    server:
      log_level: "error"
    ruler:
      storage:
        type: local
        local:
          directory: /data/loki/rules
      rule_path: /tmp/loki/rules
      alertmanager_url: http://loki-prometheus-alertmanager:80
      enable_alertmanager_discovery: false
      ring:
        kvstore:
          store: inmemory
      enable_api: true
      enable_alertmanager_v2: true
  readinessProbe:
    httpGet:
      path: /ready
      port: http-metrics
    initialDelaySeconds: 45
  livenessProbe:
    httpGet:
      path: /ready
      port: http-metrics
    initialDelaySeconds: 45
  datasource:
    jsonData: {}
    uid: ""

promtail:
  enabled: true
  config:
    logLevel: info
    serverPort: 3101
    clients:
      - url: http://{{ .Release.Name }}:3100/loki/api/v1/push
fluent-bit:
  enabled: false
grafana:
  enabled: true
  sidecar:
    datasources:
      label: ""
      labelValue: ""
      enabled: true
      maxLines: 1000
  image:
    tag: 9.3.1
  admin:
    existingSecret: azure-aad
    userKey: admin-user
    passwordKey: admin-password
  env:
    GF_SERVER_DOMAIN: italenticsstg.azurefd.net
    GF_SERVER_ROOT_URL: https://italenticsstg.azurefd.net/grafana/
    GF_SERVER_SERVE_FROM_SUB_PATH: true
  envValueFrom:
    GF_AUTH_AZUREAD_CLIENT_ID:
        secretKeyRef:
          name: azure-aad
          key: client_id
    GF_AUTH_AZUREAD_CLIENT_SECRET:
        secretKeyRef:
          name: azure-aad
          key: client_secret
            #GF_SECURITY_ADMIN_USER:
            #secretKeyRef:
            # key: admin-user
            #name: azure-aad
            #GF_SECURITY_ADMIN_PASSWORD:
            #secretKeyRef:
            #key: admin-password
            #name: azure-aad
  persistence:
    type: pvc
    enabled: true
    size: 10Gi
    storageClassName: grafana
    existingClaim: grafana-pvc

  alerting:
     delete_rules.yaml:
       apiVersion: 1
       deleteRules:
       - orgId: 1
         uid: helm_alert_id
       - orgId: 1
         uid: my_id_1
     rules.yaml:
       apiVersion: 1
       groups:
       - orgId: 1
         name: Volume
         folder: Volume
         interval: 40s
         rules:
          - uid: dummy_alertid
            title: Crash Loop Back Off
            condition: B
            data:
            - refId: A
              queryType: ''
              relativeTimeRange:
                from: 1800
                to: 0
              datasourceUid: PBFA97CFB590B2093
              model:
                datasource:
                  type: prometheus
                  uid: PBFA97CFB590B2093
                editorMode: code
                expr:
kube_pod_container_status_waiting_reason{reason=~"CrashLoopBackOff"}
                format: time_series
                interval: ''
                intervalMs: 15000
                legendFormat: __auto
                maxDataPoints: 43200
                range: true
                refId: A
            - refId: B
              datasourceUid: "-100"
              relativeTimeRange:
                form: 1800
                to: 0
              model:
                datasource:
                  type: __expr__
                  uid: __expr__
                  name: Expression
                type: reduce
                hide: false
                reducer: last
                expression: A
                intervalMs: 15000
                maxDataPoints: 43200
                window: ''
                refId: B
            dashboardUid: helm_uid
            panelId: 2
            execErrState: OK
            noDataState: OK
            for: 2m
            labels:
              helm: alerts
            description: Hi, the Pod in Namespace syndication has been in
crashloopbackoff
          - uid: dummy_alertid2
            title: Pod Failure
            condition: B
            data:
            - refId: A
              queryType: ''
              relativeTimeRange:
                from: 300
                to: 0
              datasourceUid: PBFA97CFB590B2093
              model:
                datasource:
                  type: prometheus
                  uid: PBFA97CFB590B2093
                editorMode: code
                expr: kube_pod_status_phase{phase=~"Failed|Pending|Unknown"}
                format: time_series
                interval: ''
                intervalMs: 15000
                legendFormat: __auto
                maxDataPoints: 43200
                range: true
                refId: A
            - refId: B
              datasourceUid: "-100"
              relativeTimeRange:
                form: 300
                to: 0
              model:
                datasource:
                  type: __expr__
                  uid: __expr__
                  name: Expression
                type: reduce
                hide: false
                reducer: last
                expression: A
                intervalMs: 15000
                maxDataPoints: 43200
                window: ''
                refId: B
            interval: 30s
            dashboardUid: helm_uid
            panelId: 2
            execErrState: OK
            noDataState: OK
            for: 3m
            labels:
              helm: alerts
              pod: failure
```

Contacts Points Refence:

https://github.com/grafana/grafana/tree/main/pkg/services/provisioning/alerting/testdata/contact_points

Multiple Rules Reference:

https://github.com/grafana/grafana/blob/main/pkg/services/provisioning/alerting/testdata/alert_rules/multiple-rules/rules.yml

180472
To Reset Polices:

```
notifiers.yaml:
       apiVersion: 1
       resetPolicies:
       - 1
```

Default Microsoft User has viewer role:
can see only firing alerts

/ui-service
/aarp
/wrmsdc
/higherlogic

https://italenticsstg.azurefd.net((/[a-zA-Z0-9-_.]*.(js|css|jpg|png|ico|woff|woff2|gif))|(/ui-service/.*)|(/collabservice/.*)|(/assets/.*)|(/xcommunityui/.*)|(/xcommunityaad/.*)|(/higher.*)|(/wrmsdc.*)|(/lithiumservice.*)|(/swagger-ui.html)|(/aarp.*)|($))
smartconx

https://italenticsstg.azurefd.net((/[a-zA-Z0-9-_.]*.(js|css|jpg|png|ico|woff|woff2|gif))|(/ui-service/.*)|(/collabservice/.*)|(/assets/.*)|(/xcommunityui/.*)|(/xcommunityaad/.*)|(/lithiumservice.*)|(/swagger-ui.html)|($))

https://italenticsstg.azurefd.net((/[a-zA-Z0-9-_.]*.(js|css|jpg|png|ico|woff|woff2|gif))|(/higher.*)|(/wrmsdc.*)|(/aarp.*)|(/grafana/.*)|($))
Raise Support ticket for Azure Front Door
RBAC Grafana using Terraform:

https://grafana.com/docs/grafana/latest/administration/roles-and-permissions/access-control/rbac-terraform-provisioning/

Error while running Terraform apply:

```
This could be caused by your reverse proxy settings.<br/><br/>2. If you host grafana under subpath make sure your grafana.ini root_url setting includes subpath. If not using a reverse proxy make sure to set serve_from_sub_path to true.<br/><br/>3. If you have a local dev build make sure you build frontend using: yarn start, yarn start:hot, or yarn build<br/><br/>4. Sometimes restarting grafana-server can help<br/><br/>5. Check if you are using a non-supported browser. For more information, refer to the list of <a href="https://grafana.com/docs/grafana/latest/installation/requirements/#supported-web-browsers">supported browsers</a>.</p></div><script nonce="">
```

Your browser is not fully supported, please try newer version

```
function checkBrowserCompatibility() {
|         var isIE = navigator.userAgent.indexOf('MSIE') > -1;
|         var isEdge = navigator.userAgent.indexOf('Edge/') > -1 ||
navigator.userAgent.indexOf('Edg/') > -1;
|         var isFirefox = navigator.userAgent.toLowerCase().indexOf('firefox') > -1;
|         var isChrome = /Chrome/.test(navigator.userAgent) && /Google Inc/.test(navigator.vendor);
|
|
|
|         var isEdgeVersion = /Edge\/([0-9.]+)/.exec(navigator.userAgent);
|
|         if (isIE && parseFloat(/Trident\/([0-9.]+)/.exec(navigator.userAgent)[1]) <= 7) {
|           return false;
|         } else if (
|           isEdge &&
|           ((isEdgeVersion && parseFloat(isEdgeVersion[1]) <= 16) ||
|             parseFloat(/Edg\/([0-9.]+)/.exec(navigator.userAgent)[1]) <= 16)
|         ) {
|           return false;
|         } else if (isFirefox && parseFloat(/Firefox\/([0-9.]+)/.exec(navigator.userAgent)[1]) <= 64) {
|           return false;
|         } else if (isChrome && parseFloat(/Chrome\/([0-9.]+)/.exec(navigator.userAgent)[1]) <= 54) {
|           return false;
|         }
|
|         return true;
|       }
|
|       if (!checkBrowserCompatibility()) {
|         alert('Your browser is not fully supported, please try newer version.');
```

Custom roles

If you are a Grafana Enterprise customer, you can create custom roles to manage user permissions in a way that meets your security requirements.

From <https://grafana.com/docs/grafana/latest/administration/roles-and-permissions/access-control/>

```
grafana_user.terraformuser: Creating...
```

| Error: status: 403, body: {"accessErrorId":"ACE6688662271","message":"You'll need additional permissions to perform this action. Permissions needed: users:create","title":"Access denied"}

Error: status: 403, body: {"accessErrorId":"ACE5679533616","message":"You'll need additional permissions to perform this action. Permissions needed: users:create","title":"Access denied"}

Ppfd dev Vul id b8ff83e3b49d1ee5205cdd07ae0823f9b9a67d6b76c7fea9558260fff196ce68

Ppfd stg Vul id 9cc7a3546e36063f5b9f9cd103b7076ad735641187a30d73b128251afc08dcc9
Grafana Loki Retention:

By default, when `table_manager.retention_deletes_enabled` or `compactor.retention_enabled` flags are not set, then logs sent to Loki live forever.

Retention through the Table Manager is achieved by relying on the object store TTL feature, and will work for both boltdb-shipper store and chunk/index store. However retention through the Compactor is supported only with the boltdb-shipper store.

The Compactor can deduplicate index entries. It can also apply granular retention. When applying retention with the Compactor, the Table Manager is unnecessary.

Run the compactor as a singleton (a single instance).

The Compactor loops to apply compaction and retention at every `compaction_interval`, or as soon as possible if running behind.

Marker files (containing chunks to delete) should be stored on a persistent disk, since the disk will be the sole reference to them.

Configuration:

```
compactor:
  working_directory:/data/retention
  shared_store:gcs
  compaction_interval:10m
  retention_enabled:true
  retention_delete_delay:2h
  retention_delete_worker_count:150
schema_config:
  configs:
    - from:"2020-07-31"
      index:
        period:24h
        prefix:loki_index_
      object_store:gcs
      schema:v11
      store:boltdb-shipper
storage_config:
  boltdb_shipper:
     active_index_directory:/data/index
     cache_location:/data/boltdb-cache
     shared_store:gcs
  gcs:
    bucket_name:loki
```

From <https://grafana.com/docs/loki/latest/operations/storage/retention/>

Note that retention is only available if the index period is 24h.

```
limits_config:
  retention_period:744h
  retention_stream:
   - selector:'{namespace="dev"}'
   - priority:1
   - period:24h
  per_tenant_override_config:/etc/overrides.yaml
```

From <https://grafana.com/docs/loki/latest/operations/storage/retention/>

```
overrides:
  "29":
    retention_period:168h
    retention_stream:
    - selector:'{namespace="prod"}'
      priority:2
      period:336h
    - selector:'{container="loki"}'
      priority:1
      period:72h
  "30":
    retention_stream:
   - selector:'{container="nginx"}'
   - priority:1
   - period:24h
```

From <https://grafana.com/docs/loki/latest/operations/storage/retention/>

```
retention_stream:
 - selector: '{namespace="dev"}'
   priority: 1
   period: 24h
 - selector: '{container="nginx"}'
   priority: 1
   period: 744h


Selector is a Prometheus labels matchers that will apply the `period` retention
only if# the stream is matching. In case multiple stream are matching, the
highest# priority will be picked. If no rule is matched the `retention_period` is
used.
```

Retention Test:

Deployed pod rentention-test at 5.00 pm(1-02-2023)
Set retention_period for 24h

Promtail logs exclusion:

```
client_config:
 scrape_config:
  - job_name: prometheus
    entry_parser: raw
    relabel_configs:
    - source_labels: [__meta_kubernetes_pod_label_app]
      action: keep
      regex: ^(?!excluded-pod)$
```

Logs from pod with labels app=excluded-pod

explain this regex: ^(?!excluded-pod)$

Go re2 (?m)^(?!kube-system)$

```
line 87: cannot unmarshal !!map into discovery.StaticConfig

line 86: field entry_parser not found in type scrapeconfig.plain
```

```
level=info ts=2023-02-01T18:05:14.044963171Z caller=promtail.go:123 msg="Reloading configuration
file" md5sum=db4fc73a5da48ee869c19d4e6f3dd8d1
level=error ts=2023-02-01T18:05:14.045174088Z caller=main.go:167 msg="error creating promtail"
error="no valid target scrape config defined for \"namespace-exclude\""
```

This regular expression is used to match a string that is not equal to "excluded-pod".
Here is a breakdown of the expression:

1. ^ - Matches the start of a line.
2. (?!excluded-pod) - This is a negative lookahead assertion. It means that the regular expression should fail the match if the string "excluded-pod" appears immediately after the start of the line.
3. $ - Matches the end of a line.

Therefore, this regular expression will only match a string that starts and ends with anything other than "excluded-pod".

Existing config Promtail:

```
server:
 log_level: info
 http_listen_port: 3101


clients:
 - url: http://loki:3100/loki/api/v1/push

positions:
 filename: /run/promtail/positions.yaml
```

```
scrape_configs:
  # See also
https://github.com/grafana/loki/blob/master/production/ksonnet/promtail/scrape_config.libsonnet for
reference
  - job_name: kubernetes-pods
    pipeline_stages:
      - cri: {}
    kubernetes_sd_configs:
      - role: pod
    relabel_configs:
      - source_labels:
          - __meta_kubernetes_pod_controller_name
        regex: ([0-9a-z-.]+?)(-[0-9a-f]{8,10})?
        action: replace
        target_label: __tmp_controller_name
      - source_labels:
          - __meta_kubernetes_pod_label_app_kubernetes_io_name
          - __meta_kubernetes_pod_label_app
          - __tmp_controller_name
          - __meta_kubernetes_pod_name
        regex: ^;*([^;]+)(;.*)?$
        action: replace
        target_label: app
      - source_labels:
          - __meta_kubernetes_pod_label_app_kubernetes_io_instance
          - __meta_kubernetes_pod_label_release
        regex: ^;*([^;]+)(;.*)?$
        action: replace
        target_label: instance
      - source_labels:
          - __meta_kubernetes_pod_label_app_kubernetes_io_component
          - __meta_kubernetes_pod_label_component
        regex: ^;*([^;]+)(;.*)?$
        action: replace
        target_label: component
      - action: replace
        source_labels:
        - __meta_kubernetes_pod_node_name
        target_label: node_name
      - action: replace
        source_labels:
        - __meta_kubernetes_namespace
        target_label: namespace
      - action: replace
        replacement: $1
        separator: /
        source_labels:
        - namespace
        - app
        target_label: job
      - action: replace
        source_labels:
        - __meta_kubernetes_pod_name
        target_label: pod
      - action: replace
        source_labels:
        - __meta_kubernetes_pod_container_name
        target_label: container
      - action: replace
        replacement: /var/log/pods/*$1/*.log
        separator: /
        source_labels:
        - __meta_kubernetes_pod_uid
        - __meta_kubernetes_pod_container_name
        target_label: __path__
      - action: replace
        regex: true/(.*)
        replacement: /var/log/pods/*$1/*.log
        separator: /
        source_labels:
        - __meta_kubernetes_pod_annotationpresent_kubernetes_io_config_hash
        - __meta_kubernetes_pod_annotation_kubernetes_io_config_hash
        - __meta_kubernetes_pod_container_name
        target_label: __path__



limits_config:
```

Data 30m aletname coveo Data(dur) For

For: 1m   coveo

Values C and B

Modifying one alert

```
sum(rate({namespace="syndication"} |= "coveo connector error occured" [5m])) by (pod)
```

This query calculates the rate of log messages containing the string "coveo connector error occured" in a 5-minute time window, aggregated by pod, in the "syndication" namespace.
The sum function is used to calculate the total rate of log messages containing the specified string.
The rate function calculates the per-second occurrence rate of log messages matching a certain condition. The condition in this case is "coveo connector error occured".
The [5m] argument to the rate function specifies the time window over which to calculate the rate, in this case, 5 minutes.
The by (pod) clause groups the result by the pod label, meaning that the rate of log messages containing the specified string will be calculated separately for each pod.
The final result of this query is a time series of the total rate of log messages containing the string "coveo connector error occured", aggregated by pod in the "syndication" namespac

From <https://chat.openai.com/chat>

Coveo
Sum internal or rate interval 5m
query evaluate interval 5m
For 0s

Log entry 14.47   for every 5m

First Mail recevied 14.51

Applied notification policies:

10 seconds group wait
5 min
5 min

Frequency Mail received: time: 14.51, 15:13, 15:19, 15:29, 15:39, 15:49, 15:59, 16:12, 16:27, 16:42, 16:57

2nd attempt

Coveo
Sum internal or rate interval 5m
query evaluate interval 5m
For 0s

Log entry: 17.04 for every 10 minutes
Notification policy:
10 seconds group wait
5 min group interval
5 min repeat interval

First Mail recevied time: 17.05

Freqency mail received time: 17:15, 17:25, 17:35, 17:45

Logger pod deleted at 17:36

NO DATA at 17:45

Khoros:

Sum internal or rate interval 5m

query evaluate interval 5m
For 0s

Log entry: 17:55 for every 10 minutes

Notification Policy

10 seconds group wait
5 min group interval
5 min repeat interval

Added to two same strings

First Mail recevied time: 18:00
Logger pod deleted : 18:13

Freqency mail received time: 18:04, 18:08, 18:12, 18:16, 18:20. 18:24

Server Too Busy:
Evluate interval: 2m
For: 30m

Sum internal or rate interval 1m

Log entry: 20:29
Notification policy:

Group wait: 5s
Group interval: 5s
Repeat interval: 5m

After 11 minutes of pending state it went to Normal state
21.00 from pending state

String prints for every 30 minutes
First mail : 21:16
Frequency mail: 21:46, 22:16

Coevo connector error:

Notification polices:
Group wait: 10s
Group interval: 15m
Reapeat interval: 1h

First mail 11:20
Fequeny: 12:45, 14:00, 13:00

Coveo 30m
Khoros 30m
Cron job 30m
Db connection 5m
Pod failure
Read Connection time out 5m
Coveo limit as exceed 5m
Server too busy 15m

Helm Charts:

Chart failed to download

sol: helm repo update or helm repo add chart or network issue

Every alert rules get modified or gets back to normal state because, it happens if we change evaluate interval value is changed, this value is by default changed to git alerts in a group.

The frequency at which alerts queries are run in Grafana is determined by the "Evaluation interval" setting in the alert rule. The evaluation interval is the frequency at which Grafana will evaluate the alert conditions and determine whether to trigger the alert.
By default, the evaluation interval is set to 1 minute, which means Grafana will run the alert queries every minute and check if the conditions are met. If the conditions are met, Grafana will send out the notifications.
However, you can customize the evaluation interval to meet your specific needs. For example, if you have a critical metric that needs to be monitored more frequently, you could set the evaluation interval to 30 seconds. On the other hand, if you have a less critical metric that changes infrequently, you could set the evaluation interval to a longer time, such as 5 minutes.
In summary, the evaluation interval determines how often Grafana will run the alert queries and check the conditions. You can customize it to match the specific requirements of your use case.

Notification Policy

Group Wait: This is the time Grafana will wait before sending out notifications after the first alert condition is met. The purpose of this wait is to allow for other alert conditions to be met, which can reduce the number of notifications sent. For example, if you have two alerts that trigger at the same time and the group wait is set to 5 minutes, Grafana will wait 5 minutes before sending out a single combined notification for both alerts.

Group Interval: This is the time that Grafana will wait before sending another notification after the first notification has been sent. The purpose of this interval is to prevent an excessive number of notifications from being sent if the alert condition persists. For example, if the group interval is set to 30 minutes and the alert condition persists, Grafana will send notifications every 30 minutes.

Repeat Interval: This is the time that Grafana will wait before retrying to send a notification if the previous attempt failed. For example, if the repeat interval is set to 5 minutes and a notification attempt fails, Grafana will retry the notification 5 minutes later.

BackOffLimit Reached:

BackOffLimt:3

Failures are considered even if container restarts when RestartPolicy is set "OnFailure".
If restartPolicy set to "Never", then BackOffLimt is calculated based on the pod restarts.

```
Regex experssion to filert specific labels from values:

Eg:   pod=sample-pod, namespace=alet, node=node-first, labels=app,

/.*pod="([^"]*).*/
```

```
Cpu usage of container:
```

100 - (avg by(container_name) (irate(node_cpu_seconds_total{container_name!="",mode="idle"}[5m])) * 100)

Pod memory :

avg by(pod_name) (node_memory_MemTotal_bytes - node_memory_MemFree_bytes) / node_memory_MemTotal_bytes

```
container_memory_working_set_bytes{container="${container_name.values}", name=~".*", pod=~".*", namespace="${namespace.values}"}
```

```
avg by(container)
(container_memory_working_set_bytes{container="${container_name.values}",
name=~".*", pod=~".*", namespace="${namespace.values}"})
```

```
kubectl get deployments.apps -n kube-system italentstg-ingress-nginx-controller -o
jsonpath='{.spec.template.spec.containers[].resources.requests.memory}'
```

```
avg by(container)(rate(container_cpu_usage_seconds_total{cpu="total",
container="${container_name.values}",pod=~".*", id=~".*",
namespace="${namespace.values}", name=~".*"}[5m]))
```

```
container_spec_cpu_period{container="grafana"}
```

Nginx avg memory:

```
avg(nginx_ingress_controller_nginx_process_resident_memory_bytes{controller_pod=~"$controller",controller_class=~"$controller_class",controller_namespace=~"$namespace"})
```

Nignx avg CPU:

```
sum (rate
(nginx_ingress_controller_nginx_process_cpu_seconds_total{controller_pod=~"$controller",controller_class=~"$controller_class",controller_namespace=~"$namespace"}
[2m]))
```

The cpu label is set to "total" to filter the data based on the total CPU usage of the container, rather than the usage of a specific CPU core.

The "container_cpu_user_seconds_total" is a metric that measures the total amount of CPU time the container has spent executing user-level processes and applications.

The "container_cpu_system_seconds_total" is a metric that measures the total amount of CPU time the container has spent on system calls

The "container_cpu_usage_seconds_total" is a metric that measures the total amount of CPU time used by a container. This metric is the sum of the container's user-level CPU time (container_cpu_user_seconds_total) and system-level CPU time (container_cpu_system_seconds_total).

Exclude Logs Form Namespace:

https://itnext.io/grafana-logging-using-loki-45665916aec9

Excludeed Logs from Namespace [Kube-System] Feb 6th 15:25 for iTalent STG

Configuration for dropping logs from specific Namespace.

```yaml
promtail:
  enabled: true
  config:
    logLevel: info
    serverPort: 3101
    clients:
      - url: http://{{ .Release.Name }}:3100/loki/api/v1/push
    snippets:
      extraRelabelConfigs:
      - source_labels:
        - __meta_kubernetes_namespace
        action: drop
        regex: kube-system
```

```
level=warn ts=2023-02-06T11:35:10.763021638Z caller=logging.go:86 traceID=36342eb2fa4be0ea
msg="GET /ready (500) 64.819µs Response: \"Not ready: Unable to find any logs to tail. Please verify
permissions, volumes, scrape_config, etc.\\n\" ws: false; Accept: */*; Connection: close; User-Agent:
kube-probe/1.24; "
```

```
attached volumes=[kube-api-access-grrcq sc-datasources-volume config storage]: timed out waiting for
the condition
  Warning  FailedAttachVolume  94s (x13 over 11m)     attachdetach-controller  AttachVolume.Attach
failed for volume "grafana-pv" : rpc error: code = NotFound desc = Volume not found, failed with error:
Retriable: false, RetryAfter: 0s, HTTPStatusCode: 403, RawError:
{"error":{"code":"AuthorizationFailed","message":"The client
'bae6a6b9-1593-4339-8a5e-94baac8653ab' with object id 'bae6a6b9-1593-4339-8a5e-94baac8653ab'
does not have authorization to perform action 'Microsoft.Compute/disks/read' over scope
'/subscriptions/5cd41c92-754a-486e-95ff-f1fc311c0fa2/resourceGroups/ICS-iTalent-QA-
RG/providers/Microsoft.Compute/disks/pvc-46fa8dae-4f8e-4f13-a407-76bb463c1bb9' or the scope is
invalid. If access was recently granted, please refresh your credentials."}}
```

Retention Pod in syndication created on 10-02-2023 6:25pm

And also same Logger pod which does not have retention policy set.

Roles:

On every login the user organization role will be reset to match AzureAD's application role and their organization membership will be reset to the default organization.

By default, the users' organization and role is reset on every new login.

https://stackoverflow.com/questions/58952293/grafana-role-assignment-using-azure-ad-oauth

Coveo and Khoros Connector Exception: 30m
PANW Coveo Limit: 15m
PANW Khoros server busy 15m
Read Connection Timeout (nested exception) 30m
DB connection Exception(unable to acquire) 5m

MSFT:

Read Connection: 5m
Power query one time syndication failed 15m
Exception mails 1d
Bulk Data CSV 1d
DB Connection Exception: 5m

Email Templating:

https://community.grafana.com/t/create-a-custom-template-grafana-9-3/79055/7

https://grafana.com/docs/grafana/next/alerting/manage-notifications/template-notifications/create-notification-templates/

https://community.grafana.com/t/how-to-use-alert-message-templates-in-grafana/67537/98?page=2

https://grafana.com/docs/grafana/next/alerting/manage-notifications/template-notifications/create-notification-templates/

```
{{ range $key, $value := .Labels }}
{{ if or (eq $key "alertname") (eq $key "instance") }}
{{ $key }}={{ $value }}
{{ end }}
{{ end }}
```

Labels:

```
{{ range .Labels.SortedPairs }}
{{ if ne .Name "release" }}
- {{ .Name }} = {{ .Value }}
{{ end }}
{{ end }}
```

Removed Values and Labels:

```
{{ define "__text_alert_list" }}
{{ range . }}
Annotations:
{{ range .Annotations.SortedPairs }} - {{ .Name }} = {{ .Value }}
{{ end }}{{ if gt (len .GeneratorURL) 0 }}Source: {{ .GeneratorURL }}
{{ end }}{{ if gt (len .SilenceURL) 0 }}Silence: {{ .SilenceURL }}
{{ end }}{{ if gt (len .DashboardURL) 0 }}Dashboard: {{ .DashboardURL }}
{{ end }}{{ if gt (len .PanelURL) 0 }}Panel: {{ .PanelURL }}
{{ end }}
{{ end }}
```

Modifying Subject Template:

```
{{ define "__subject" }}[{{ .Status | toUpper }}{{ if eq .Status "firing" }}:{{ .Alerts.Firing | len }}{{ if gt
(.Alerts.Resolved | len) 0 }}, RESOLVED:{{ .Alerts.Resolved | len }}{{ end }}{{ end }}] Custom Subject
Text{{ end }}
```

```
{{ define "default.title" }}{{ if eq .Status "firing" }}[{{ .Status | toUpper }}:{{ .Alerts.Firing | len }}]{{ else }}
[{{ .Status | toUpper }}]{{ end }} {{ .GroupLabels.SortedPairs.Values | join " " }}{{ end }}

{{ define "default.message" }}
{{ if gt (len .Alerts.Firing) 0 }}**Firing**
{{ range .Alerts.Firing }}
- {{ .Annotations.summary }}
{{ end }}
{{ if gt (len .Alerts.Resolved) 0 }}
{{ end }}
{{ end }}
{{ if gt (len .Alerts.Resolved) 0 }}**Resolved**
{{ range .Alerts.Resolved }}
- {{ .Annotations.summary }}
{{ end }}
{{ end }}{{ end }}
```

```
import requests

# Set Loki API URL and headers
url = "http://your-loki-instance/loki/api/v1/query_range"
headers = {"Authorization": "Bearer <your-api-key>"}

# Set query parameters
params = {
    "query": "{job=\"my-job\"} |= \"error\" | count_over_time[5m]",
    "start": "2023-03-01T00:00:00Z",
    "end": "2023-03-05T23:59:59Z",
    "step": "60s",
}

# Send API request and get response
response = requests.get(url, headers=headers, params=params)

# Process and save the data to a file in your desired format
# For example, you can save the data as CSV
with open("logs.csv", "w") as f:
    f.write(response.content.decode())
```

CPU usage

```
(
  (1 - sum without (mode) (rate(node_cpu_seconds_total{mode=~"idle|iowait|steal",
node="aks-agentpool-44999582-vmss000008"}[5m])))
/ ignoring(cpu) group_left
  count without (cpu, mode) (node_cpu_seconds_total{mode="idle"})
)
```

```
Memory Usage:


100 -
(
  avg(node_memory_MemAvailable_bytes{job="node", instance="aks-
agentpool-44999582-vmss000008", cluster="ics-msft-stg"}) /
  avg(node_memory_MemTotal_bytes{job="node", instance="aks-agentpool-44999582-
vmss000008", cluster="ics-msft-stg"})
* 100
)



(
  node_memory_MemTotal_bytes{job="node", instance="aks-agentpool-44999582-
vmss000008", cluster="ics-msft-stg"}
-
  node_memory_MemFree_bytes{job="node", instance="aks-agentpool-44999582-
vmss000008", cluster="ics-msft-stg"}
-
  node_memory_Buffers_bytes{job="node", instance="aks-agentpool-44999582-
vmss000008", cluster="ics-msft-stg"}
-
  node_memory_Cached_bytes{job="node", instance="aks-agentpool-44999582-
vmss000008", cluster="ics-msft-stg"}
)


Network received :



rate(node_network_receive_bytes_total{job="node", instance="aks-
agentpool-44999582-vmss000008", device!="lo", cluster="ics-msft-stg"}
[$__rate_interval]) * 8


Network Transmitted:


rate(node_network_transmit_bytes_total{job="node", instance="aks-
agentpool-44999582-vmss000008", device!="lo", cluster="ics-msft-stg"}
[$__rate_interval]) * 8
```

```
{__name__="kubelet_node_name", agentpool="agentpool", beta_kubernetes_io_arch="amd64",
beta_kubernetes_io_instance_type="Standard_D2as_v4", beta_kubernetes_io_os="linux",
failure_domain_beta_kubernetes_io_region="eastus",
failure_domain_beta_kubernetes_io_zone="eastus-1", instance="aks-agentpool-21137216-
vmss000000", job="kubernetes-nodes", kubernetes_azure_com_agentpool="agentpool",
kubernetes_azure_com_cluster="MC_ICS-iTalent-QA-RG_ics-aks-qa_eastus",
kubernetes_azure_com_kubelet_identity_client_id="eefcce8c-759c-45c1-b4ad-5158b01c1d30",
kubernetes_azure_com_mode="system",
kubernetes_azure_com_node_image_version="AKSUbuntu-1804gen2containerd-2023.01.20",
kubernetes_azure_com_os_sku="Ubuntu", kubernetes_azure_com_role="agent",
kubernetes_azure_com_storageprofile="managed",
kubernetes_azure_com_storagetier="Premium_LRS", kubernetes_io_arch="amd64",
kubernetes_io_hostname="aks-agentpool-21137216-vmss000000", kubernetes_io_os="linux",
kubernetes_io_role="agent", node="aks-agentpool-21137216-vmss000000",
node_kubernetes_io_instance_type="Standard_D2as_v4", storageprofile="managed",
storagetier="Premium_LRS", topology_disk_csi_azure_com_zone="eastus-1",
topology_kubernetes_io_region="eastus", topology_kubernetes_io_zone="eastus-1"}
```

From <https://italenticsstg.azurefd.net/grafana/d/e1-PSJxVz/cluster-info?editPanel=12>

```
/.*pod="([^"]*).*/
```

```
kubelet_node_name{instance="${nodename}"}
```

```
PS D:\kubernetes-yamls> kubectl logs -n logging loki-dev-prometheus-server-b46dd5bbc-t2cmq -c
prometheus-server
ts=2023-03-15T04:58:58.753Z caller=main.go:516 level=info msg="Starting Prometheus"
version="(version=2.34.0, branch=HEAD, revision=881111fec4332c33094a6fb2680c71fffc427275)"
ts=2023-03-15T04:58:58.753Z caller=main.go:521 level=info build_context="(go=go1.17.8, user=root@
121ad7ea5487, date=20220315-15:18:00)"
ts=2023-03-15T04:58:58.753Z caller=main.go:522 level=info host_details="(Linux 5.4.0-1103-azure #109
~18.04.1-Ubuntu SMP Wed Jan 25 20:53:00 UTC 2023 x86_64 loki-dev-prometheus-server-b46dd5bbc-
t2cmq (none))"
ts=2023-03-15T04:58:58.753Z caller=main.go:523 level=info fd_limits="(soft=1048576, hard=1048576)"
ts=2023-03-15T04:58:58.753Z caller=main.go:524 level=info vm_limits="(soft=unlimited,
hard=unlimited)"
ts=2023-03-15T04:58:58.754Z caller=query_logger.go:90 level=error component=activeQueryTracker
msg="Error opening query log file" file=/data/queries.active err="open /data/queries.active: read-only
file system"
panic: Unable to create mmap-ed active query log

goroutine 1 [running]:
github.com/prometheus/prometheus/promql.NewActiveQueryTracker({0x7ffddf249327, 0x5}, 0x14,
{0x3637a40, 0xc0006bd4f0})
        /app/promql/query_logger.go:120 +0x3d7
main.main()
        /app/cmd/prometheus/main.go:569 +0x6049
```

```
Error: UPGRADE FAILED: cannot patch "loki-dev-promtail" with kind DaemonSet: DaemonSet.apps "loki-
dev-promtail" is invalid: spec.template.spec.tolerations[0].operator: Invalid value:
core.Toleration{Key:"service", Operator:"Exists", Value:"aarp", Effect:"NoSchedule",
TolerationSeconds:(*int64)(nil)}: value must be empty when `operator` is 'Exists'
```

```
KubePodInventory
| where ClusterName contains "ICS-MSFT-STG" | summarize count() by Namespace | project
Namespace
```

Using Terraform

[azurerm_monitor_scheduled_query_rules_alert | Resources | hashicorp/azurerm | Terraform Registry]

Log analytics query:

To list logs for a pod

```
KubePodInventory
| where TimeGenerated >= ago(1d)
| where Name == "my-pod-name" and Namespace == "my-namespace"
| project PodUID
| join kind=inner (ContainerLog
    | where TimeGenerated >= ago(1d)
    | where LogEntry contains "my-search-term"
    | project PodUID, LogEntry
) on PodUID
| project TimeGenerated, LogEntry, Name, Namespace
```

To list Namespace in a Cluster:

```
KubePodInventory | where ClusterName == "ics-aks-qa" | summarize count() by Namespace | project
Namespace
```

To list pods in a Namespace:

```
KubePodInventory
```

```
| where Namespace contains "syndication"
| where ContainerStatus contains "Running"
| summarize count() by Name | project Name
```

Query where time span is ignored incase of Grafana:

```
ContainerLog
| where LogEntry contains "Tomcat"
```

Query where time span is provided manually:

```
ContainerLog
| where LogEntry contains " Stopping service [Tomcat]" and TimeGenerated between
(

(2023-03-27)..datetime(2023-03-28))
```

To print Container Name or Pod name:

```
let containerID = toscalar(ContainerLog | where LogEntry contains "sheetId" | take 1 | project
ContainerID);
ContainerInventory
| where ContainerID  == containerID
| project ContainerHostname
```

```
ContainerLog
| where LogEntry contains "$string"
| where TimeGenerated > ago($time_span)
```

```
let containerID = toscalar(ContainerLog | where LogEntry contains "sheetId" | take 1 | project
ContainerID);
ContainerInventory
| where ContainerID  == containerID
| project ContainerHostname
```

```
ContainerLog
| where LogEntry  contains "sheetId"
| where TimeGenerated > ago(10h)
| project ContainerID, LogEntry
```

To list containerHostname == Pod Name:

```
ContainerInventory
| where ContainerState contains "Running"
| project ContainerHostname
```

To list Pods in Namespace:

```
KubePodInventory
| where Namespace contains "syndication"
```

```
KubePodInventory
| where Name contains "crossxui-549f49759f-dflq9"
| project ContainerID
```

To list container name:

```
KubePodInventory
| where ContainerID contains "$containerid"
| where ContainerStatus == "running"
| where TimeGenerated > ago(5m)
| summarize count() by ServiceName
| project ServiceName
```

Regex :
To extract after /   in 3f5b4013-a196-4e52-979f-4ba40ac9ea7d/xcommunityconnector-service

From <https://chat.openai.com/chat>

```
/.*\/([^\/]*)$/
```

From <https://chat.openai.com/chat>

Pod Failure Alert Query:

```
let endDateTime = (datetime(2023-03-29T12:36:38.0000000Z));
let startDateTime = (datetime(2023-03-29T12:36:38.0000000Z) - 5m);
let trendBinSize = 1m;

let clusterName = 'ics-aks-qa';

let nameSpace = 'syndication';

KubePodInventory

| where TimeGenerated < endDateTime

| where TimeGenerated >= startDateTime

| where ClusterName == clusterName

| distinct ClusterName, TimeGenerated

| summarize ClusterSnapshotCount = count() by bin_at(TimeGenerated, trendBinSize, datetime(2023-03-29T12:36:38.0000000Z)), ClusterName

| join

hint.strategy=broadcast (KubePodInventory

| where TimeGenerated < endDateTime

| where TimeGenerated >= startDateTime

| where Namespace == nameSpace

| distinct ClusterName, Namespace, Computer, PodUid, TimeGenerated, PodStatus

| summarize TotalCount = count(), PendingCount = sumif(1, PodStatus =~ 'Pending'), RunningCount = sumif(1, PodStatus =~ 'Running'), SucceededCount = sumif(1, PodStatus =~ 'Succeeded'), FailedCount = sumif(1, PodStatus =~ 'Failed') by ClusterName, bin_at(TimeGenerated, trendBinSize, datetime(2023-03-29T12:36:38.0000000Z))

)

on ClusterName, TimeGenerated

| extend UnknownCount = TotalCount - PendingCount - RunningCount - SucceededCount - FailedCount

| project TimeGenerated, TotalCount = todouble(TotalCount) / ClusterSnapshotCount, PendingCount = todouble(PendingCount) / ClusterSnapshotCount, RunningCount = todouble(RunningCount) / ClusterSnapshotCount, SucceededCount = todouble(SucceededCount) / ClusterSnapshotCount, FailedCount = todouble(FailedCount) / ClusterSnapshotCount, UnknownCount = todouble(UnknownCount) / ClusterSnapshotCount

| where (FailedCount +PendingCount + UnknownCount) > 0
```

To get Log Analytics Workspace resource id:

```
Resources
| where type == 'microsoft.containerservice/managedclusters'
| project name, properties["addonProfiles"]["omsagent"]["config"]
["logAnalyticsWorkspaceResourceID"]
// Microsoft.ContainerService/managedClusters
```

```
Resources
| where type == 'microsoft.containerservice/managedclusters'
| extend workspaceid = tostring(properties["addonProfiles"]["omsagent"]["config"]
["logAnalyticsWorkspaceResourceID"])
| project name, workspaceid
```

```
// Microsoft.ContainerService/managedClusters
```

```
Resources
| where type == 'microsoft.containerservice/managedclusters'
| extend workspaceid =
tostring(properties.addonProfiles.omsagent.config.logAnalyticsWorkspaceResourceID
)
| project workspaceid
// Microsoft.ContainerService/managedClusters
```

```
Resources
| where type == 'microsoft.containerservice/managedclusters'
| where name ==  "ics-italent-dev-aks"
| project subscriptionId
// Microsoft.ContainerService/managedClusters
```

```
resourcecontainers
 | where type == "microsoft.resources/subscriptions"
 | where subscriptionId == "ea490839-c54c-4ba8-8160-45d78dcf94a7"
 | project name
```

```
KubePodInventory
| where ClusterName contains "italent-ics-prod-aks"
| where Name contains "aarp"
| where TimeGenerated > ago(30d)
| summarize count() by Name, PodCreationTimeStamp
| project PodCreationTimeStamp, Name
// | summarize count() by Name
```

Enhancements:

- To print logs from all pods and also need to add a PodName column

```
ContainerLog
| where ContainerID contains
"27cc0d3f86819c17ed761329d845f883e2bd6ab38c67a2aa1e84135370c51792"
| join kind=inner (
KubePodInventory
| where ContainerID contains
"27cc0d3f86819c17ed761329d845f883e2bd6ab38c67a2aa1e84135370c51792"
)on ContainerID
| project Name1, LogEntry, LogEntrySource
```

To modify the Display Value to Custom Name

```
ContainerLog
| where ContainerID contains
"27cc0d3f86819c17ed761329d845f883e2bd6ab38c67a2aa1e84135370c51792"
| join kind=inner (
KubePodInventory
| where ContainerID contains
"27cc0d3f86819c17ed761329d845f883e2bd6ab38c67a2aa1e84135370c51792"
)on ContainerID
| project PodName=Name1, LogEntry, LogEntrySource
```

A datetime value in Kusto is always in the UTC time zone. If displaying datetime values in other time zones is required, please use datetime_utc_to_local() or its counterpart, datetime_local_to_utc(), to convert to a different time zone.

From <https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/scalar-data-types/datetime>

About variables
https://grafana.com/docs/grafana/latest/dashboards/variables/add-template-variables/

Using Grafana drop down time Ranges:

```
$__timeFilter(TimeGenerated)
```

```
let start_date = "${__from:date:iso}";
let end_date = "${__to:date:iso}";
print date_today_start = start_date, date_today_end = end_date
```

```
ContainerLog
| where ContainerID contains "bb76d4d1a58dbcd49a2543873703981a712c261f8b5af553c5ca4086415edde2"
| where TimeGenerated between (datetime(${__from:date:iso}) .. datetime(${__to:date:iso}))
```

For Exception Dashboard:

```
ContainerLog
| where LogEntry matches regex ".Exception"
| where TimeGenerated > ago(24h)
| summarize count() by ContainerID
| project ContainerID
```

```
KubePodInventory
| where ContainerID contains "bb76d4d1a58dbcd49a2543873703981a712c261f8b5af553c5ca4086415edde2"
|summarize count() by Name
| project Name
```

Logs based on Time Generate Variables:

```
let myTimes = toscalar(ContainerLog
| where TimeGenerated > ago(1h)
| where LogEntry matches regex ".Exception"
| summarize make_list(TimeGenerated));

ContainerLog
| where TimeGenerated in (myTimes)
| where LogEntry matches regex ".Exception"
| project TimeGenerated, LogEntry
```

Dealing with JSON Objects using KQL

https://stackoverflow.com/questions/67198867/kusto-query-json-array-values

```
Resources
| where type == "microsoft.compute/virtualmachinescalesets"
| where resourceGroup == "mc_ics-italent-qa-rg_ics-aks-qa_eastus"
| project NodeNames = name
```

Below Vmsize is list

```
// Microsoft.ContainerService/managedClusters
Resources
| where type == 'microsoft.containerservice/managedclusters'
| where name == "ics-aks-qa"
| project VMsize = properties.agentPoolProfiles
| mv-expand VMsize
| project Mode = VMsize.name
```

Matching Regex patterns:

```
// // Microsoft.ContainerService/managedClusters
// Resources
// | where type == 'microsoft.containerservice/managedclusters'
// | where name == "italent-ics-prod-aks"
// | project ObjectID = properties.["addonProfiles"].["omsAgent"].["identity"].["objectId"]
// // | mv-expand VMsize
// // | project ProvisionState = VMsize
Resources
| where type == "microsoft.network/loadbalancers"
| where tags["aks-managed-cluster-name"] == "ics-aks-qa"
| project LoadBalancer_Properties = properties["backendAddressPools"]
| mv-expand LoadBalancer_Properties
| project VM_Backends = LoadBalancer_Properties["properties"]["backendIPConfigurations"]
| mv-expand VM_Backends
// | project VirtualMachineScaleSet = substring(VM_Backends["id"], indexof(VM_Backends["id"], "virtualMachineScaleSets/") +
strlen("virtualMachineScaleSets/"))
| project VirtualMachineScaleSet = substring(VM_Backends["id"], indexof(VM_Backends["id"], "virtualMachineScaleSets/") +
strlen("virtualMachineScaleSets/"), indexof(VM_Backends["id"], "/virtualMachines/") - (indexof(VM_Backends["id"],
"virtualMachineScaleSets/") + strlen("virtualMachineScaleSets/")))
```

```
Resources
| where type == "microsoft.compute/disks"
| where resourceGroup contains "$noderg"
| project name, location, resourceGroup, PVCname = tostring(tags["kubernetes.io-created-for-pvc-name"]), AttachedVM =
substring(managedBy, indexof(managedBy, "virtualMachineScaleSets/") + strlen("virtualMachineScaleSets/"), indexof(managedBy,
"/virtualMachines/") - (indexof(managedBy, "virtualMachineScaleSets/") + strlen("virtualMachineScaleSets/")))
```

Vnet and subnets:

```
properties["virtualMachineProfile"]["networkProfile"]["networkInterfaceConfigurations"][0]["properties"]["ipConfigurations"][0]
["properties"]["subnet"]
```

```
Resources
| where type == "microsoft.compute/virtualmachinescalesets"
| project VMSubnet = properties["virtualMachineProfile"]["networkProfile"]["networkInterfaceConfigurations"][0]["properties"]
["ipConfigurations"][0]["properties"]["subnet"]
| project VMSubnet = substring(VMSubnet, indexof(VMSubnet, "virtualNetworks/") + strlen("virtualNetworks/"), indexof(VMSubnet,
"/subnets/") - (indexof(VMSubnet, "virtualNetworks/") + strlen("virtualNetworks/")))
```

```
Resources
| where type == "microsoft.sql/servers"
|
```

```
Resources
| where type == "microsoft.sql/servers/databases"
```

To add Variables:

SubcrptionId:
Namespace: Microsoft.Sql/servers/databases
Resource Name: ics-prod-mssql-srvr/ics-prod-mssql-db
Resource Group: ICS-Prod-RG
Region: eastus2

$subsid
microsoft.sql/servers/databases
$resourcegp
$sqlservers/$sqldatabase

To list Kubernetes services:

```
Resources
 | where type == 'microsoft.containerservice/managedclusters'
```

To list SQL Servers

```
Resources
| where type == "microsoft.sql/servers"
|
```

To list SQL Databases

```
Resources
| where type == "microsoft.sql/servers/databases"
```

To List Resources of Load Balancers:

```
Resources
| where type == "microsoft.network/loadbalancers"
```

To list Resources of VNET:

```
Resources
| where type == "microsoft.network/virtualnetworks"
```

To list Resources of Disk:

```
Resources
| where type == "microsoft.compute/disks"
```

To list VMSS:

```
Resources
| where type == "microsoft.compute/virtualmachinescalesets"
```

To list Front Doors:

```
Resources
| where type == 'microsoft.network/frontdoors'
```

To list Storage Accounts:

```
Resources
| where type == 'microsoft.storage/storageaccounts'
```

To list KeyVaults:

```
Resources
| where type == 'microsoft.keyvault/vaults'
```

```
ContainerLog
| where LogEntry contains "$string"
| where TimeGenerated between (datetime(${__from:date:iso}) ..
datetime(${__to:date:iso}))
| join kind=inner (
KubePodInventory
| where ContainerID contains ""
)on ContainerID
| project LogEntry, PodName=Name1, LogEntrySource, ContainerID
```

```
ContainerLog
| where TimeGenerated >= ago(1h) // select logs from the last hour
| take 1
| extend NewTimeGenerated = TimeGenerated - 5m // add 5 minutes to TimeGenerated
| project TimeGenerated, NewTimeGenerated // display both original and new
timestamps
```

```
ContainerLog
| where LogEntry matches regex ".Exception"
| take 1
| project TimeGenerated, UpdatedTime = TimeGenerated-5m
| join kind=inner ContainerLog on TimeGenerated
| where TimeGenerated  between (UpdatedTime .. TimeGenerated)
```

```
az aks update --disable-azuremonitormetrics -n <cluster-name> -g <cluster-resource-group>
```

```
let endDateTime = now();
let startDateTime = ago(5m);
let trendBinSize = 1m;

let clusterName = 'ics-aks-qa';

let nameSpace = 'syndication';

KubePodInventory

| where TimeGenerated < endDateTime

| where TimeGenerated >= startDateTime

| where ClusterName == clusterName

| distinct ClusterName,TimeGenerated

| summarize ClusterSnapshotCount = count() by bin(TimeGenerated, trendBinSize),ClusterName

| join

hint.strategy=broadcast ( KubePodInventory

| where TimeGenerated < endDateTime

| where TimeGenerated >= startDateTime

| where Namespace == nameSpace

| distinct ClusterName, Namespace ,Computer, PodUid, TimeGenerated, PodStatus

| summarize TotalCount = count(), PendingCount = sumif(1, PodStatus =~ 'Pending'), RunningCount =
sumif(1, PodStatus =~ 'Running'), SucceededCount = sumif(1, PodStatus =~ 'Succeeded'), FailedCount =
sumif(1, PodStatus =~ 'Failed') by ClusterName, bin(TimeGenerated, trendBinSize)

)

on ClusterName, TimeGenerated

| extend UnknownCount = TotalCount - PendingCount - RunningCount - SucceededCount - FailedCount

| project TimeGenerated, TotalCount = todouble(TotalCount) / ClusterSnapshotCount,PendingCount =
todouble(PendingCount) / ClusterSnapshotCount, RunningCount = todouble(RunningCount) /
ClusterSnapshotCount, SucceededCount = todouble(SucceededCount) / ClusterSnapshotCount,
FailedCount = todouble(FailedCount) / ClusterSnapshotCount, UnknownCount =
todouble(UnknownCount) / ClusterSnapshotCount
```

```
| where (FailedCount +PendingCount + UnknownCount) > 0
```

```
(datetime(2023-05-01 13:08:16.880) .. datetime(2023-05-01 13:11:16.880))
```

```
ContainerLog
| where LogEntry contains ""
| where ContainerID contains
"ae1e51a8dcaad4f8f1e120d5f15700079810e75efc7ab492127681df52eac820"
// | where TimeGenerated > ago(5m)
| where TimeGenerated between (datetime(2023-05-01 07:41:16.880) ..
datetime(2023-05-01 07:46:16.880))   // UTC TIME
| project TimeGenerated,LogEntry
```

UTC TIME

Working Query to Get Logs from last 5min Based on Exception Logs:

```
ContainerLog
| where LogEntry contains ""
| where ContainerID contains
"ae1e51a8dcaad4f8f1e120d5f15700079810e75efc7ab492127681df52eac820"
| take 1
| project TimeGenerated
| join kind=inner (ContainerLog
| where TimeGenerated <= TimeGenerated and TimeGenerated >= TimeGenerated-5m) on
TimeGenerated
| project LogEntry
```

Log Analytics Workspace:

https://learn.microsoft.com/en-us/azure/azure-monitor/service-limits#user-query-throttling

Log Analytics Workspace : Python SDK

https://learn.microsoft.com/en-us/python/api/overview/azure/monitor-query-readme?view=azure-python

Log Analytics Workspace Alerts:

Crash Loop Back Alert:

```
KubePodInventory
| where ClusterName contains "smartconx-dev-aks"
| where TimeGenerated > ago(5m)
| where ControllerKind contains "ReplicaSet"
| where ContainerRestartCount > 2
| where ContainerStatusReason contains "CrashLoopBackOff"
| summarize count() by Name
| project Name
```

```
foridinrequired_container_ids:
ifidnotindeDuplicated_container_ids:
deDuplicated_container_ids.append(id)
print("printafterDeDuplicatingcontainersids")
print(deDuplicated_container_ids)
```

```
tsmanohar@italentdigital.com","akunam@italentdigital.com","divyak@italentdigital.com","yeshwanth@italentdigital.com","vinayt@italentdigital.com","bhanub@italentdigital.com","lnarayana@italentdigital.com","ramesh@italentdigital.com"
```

Escape Characters :

```
| where LogEntry matches regex  "com.microsoft.aad.adal4j.AuthenticationException:
{\"error_description\":\"AADSTS7000222: The provided client secret"
```

Log Exception alert:

```
forrequired_stringsinlogentry.values:
pattern=r'(\S+Exception:)((?:\s*\S+){0,5})'
matches=re.search(pattern,required_strings)
ifmatches:
extracted_string=matches.group(0)
print("Extractedstring:",extracted_string)
extracted_logentries.append(extracted_string)
```

To get Data size:

```
ContainerLog
// | where ContainerID contains
"76f4630f3b3259e4ad8418e79dba752dfc9f9117e537ca510a06df3c215d20a1"
| summarize  Size = sum(_BilledSize) by  _IsBillable | sort by Size desc | extend Size2 =
format_bytes(Size, 2)
```

```
ContainerLog
// | where LogEntry matches regex ".Exception"
| where TimeGenerated between (datetime('2023-06-19 04:36:00') ..
datetime('2023-06-19 04:37:00'))
|where ContainerID contains
"7af40239aaaaf4e18a095640ea483352e651a49067dbce9a08e24f6013853116"
// | project LogEntry
| summarize  Size = sum(_BilledSize) by  _IsBillable | sort by Size desc | extend
Size2 = format_bytes(Size, 2)
```

```
KubePodInventory
| where Name contains $podname
| where TimeGenerated between (datetime(${__from:date:iso}) ..
datetime(${__to:date:iso}))
| project Time=PodCreationStamp
| project format_datetime(Time, 'MM-dd-yyyy [H:mm:ss]')
```

```
| project Time = datetime_add('minute',330, make_datetime(PodCreationTimeStamp))
```

```
KubePodInventory
| where Name contains $podname
| where TimeGenerated between (datetime(${__from:date:iso}) ..
datetime(${__to:date:iso}))
| project Time = datetime_add('minute',330, make_datetime(PodCreationTimeStamp))
| project format_datetime(Time, 'MM-dd-yyyy [hh:mm:ss:tt]')
```

T oget array of lists

```
| where Name in ($podnames)
```

Use variables :

```
let mylist = toscalar(
   KubePodInventory
   | where Namespace contains "syndication"
   | where ServiceName contains "chama"
   | where TimeGenerated > ago(240h)
   | summarize mylist = make_list(Name)
   | project mylist
);
KubePodInventory
| where Name in (mylist)
| summarize count() by ContainerID
| project ContainerID
```

Log Analyrics Workspace:

/subscriptions/5cd41c92-754a-486e-95ff-f1fc311c0fa2/resourceGroups/ics-prod-rg/providers/Microsoft.OperationalInsights/workspaces/icsitalentprodlogspace

Variable Service-Name

```
KubePodInventory
| where Namespace contains "syndication"
| where ControllerKind contains "ReplicaSet"
| where TimeGenerated between (datetime(${__from:date:iso}) ..
datetime(${__to:date:iso}))
| summarize count() by ServiceName
| project ServiceName
```

italent-ics-prod-aks

Variable PodNames

```
KubePodInventory
// | where Namespace contains "$namespace"
| where ServiceName contains "$serivcename"
| where TimeGenerated between (datetime(${__from:date:iso}) .. datetime(${__to:date:iso}))
| where ControllerKind contains "ReplicaSet"
| where ContainerStatus contains "running"
| where PodStatus contains "Running"
| summarize count() by Name
| project Name
```

Variable container_id

```
KubePodInventory
| where Name in ($podnames)
| where TimeGenerated between (datetime(${__from:date:iso}) .. datetime(${__to:date:iso}))
| project ContainerID
```

Variable podCreatedAt

```
KubePodInventory
| where Name in ($podnames)
| where TimeGenerated between (datetime(${__from:date:iso}) ..
datetime(${__to:date:iso}))
| project Time = datetime_add('minute',330, make_datetime(PodCreationTimeStamp))
| project format_datetime(Time, 'MM-dd-yyyy [hh:mm:ss:tt]')
```

Log Query:

```
ContainerLog
| where ContainerID in ($containerid)
| where LogEntry contains "$string"
| where TimeGenerated between (datetime(${__from:date:iso}) ..
datetime(${__to:date:iso}))
| project LogEntry, LogEntrySource, ContainerID, TimeGenerated
```

Alert Azures Schema: https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-common-schema

generate Access tokens: AAD

https://stackoverflow.com/questions/64217464/valid-authentication-was-not-provided

Kusto query are allowed to return max 500000 rows or 64MB, as default parameters.

From <https://community.fabric.microsoft.com/t5/Desktop/Kusto-query-limits/td-p/1593686>

25 January 2023 14:42

Rest API

Azure DevOps API Module for python

Rest API reference:

https://stackoverflow.com/questions/66185420/azure-devops-rest-api-run-pipeline-with-variables

Azure Pipelines Stream Lining

https://techcommunity.microsoft.com/t5/azure-devops-blog/just-in-time-privilege-s-access-to-azure-devops/ba-p/3062589

Azure DevOps Pipeline Stream Lining:

Providing access to a User for specific period of time

Refenrece for registering AAD:

https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

```
import adal
import os
from azure.devops.connection import Connection
from msrest.authentication import BasicTokenAuthentication

# Acquire an access token using adal
authority_url = "https://login.microsoftonline.com/{}".format(os.environ['AZURE_TENANT_ID'])
context = adal.AuthenticationContext(authority_url)
token = context.acquire_token_with_client_credentials("https://dev.azure.com/",
os.environ['AZURE_CLIENT_ID'], os.environ['AZURE_CLIENT_SECRET'])

# Authenticate with Azure DevOps using the access token
credentials = BasicTokenAuthentication(token["accessToken"])
connection = Connection("https://dev.azure.com/{}".format(os.environ['AZURE_ORGANIZATION']),
creds=credentials)
```

Git API for reference:

https://martinheinz.dev/blog/25

Updating and commiting a file using Github api:

```
file_path ="requirements.txt"g =Github(token)repo =g.get_repo("MartinHeinz/python-project-blueprint")
```

```
file=repo.get_contents(file_path,ref="master")# Get file from branchdata
=file.decoded_content.decode("utf-8")# Get raw string datadata +="\npytest==5.3.2"# Modify/Create
filedefpush(path,message,content,branch,update=False):author
=InputGitAuthor("MartinHeinz","martin7.heinz@gmail.com")source =repo.get_branch("master")
repo.create_git_ref(ref=f"refs/heads/{branch}",sha=source.commit.sha)# Create new branch from
masterifupdate:# If file already exists, update itcontents =repo.get_contents(path,ref=branch)#
Retrieve old file to get its SHA and
pathrepo.update_file(contents.path,message,content,contents.sha,branch=branch,author=author)#
Add, commit and push branchelse:# If file doesn't exist, create
itrepo.create_file(path,message,content,branch=branch,author=author)# Add, commit and push
branchpush(file_path,"Add pytest to dependencies.",data,"update-dependencies",update=True)
```

Appending Text or modify the text in a file:

```
with open("example.csv", "r") as file:
    lines = file.readlines()

# Modify the line that contains the field you want to update
for i, line in enumerate(lines):
    if "field_name" in line:
        field_values = line.strip().split(",")
        field_values[1] = "new_value"
        lines[i] = ",".join(field_values) + "\n"

# Write the updated content back to the file
with open("example.csv", "w") as file:
    file.writelines(lines)
```

https://stackoverflow.com/questions/4719438/editing-specific-line-in-text-file-in-python

```
import yaml
from github import Github

# Replace with your personal access token
token = "your_token_here"

# Replace with the name of the repository owner and the repository name
owner = "your_username"
repo_name = "your_repo_name"

# Replace with the path to the file you want to update
file_path = "path/to/your/file.yaml"

# Connect to GitHub using your personal access token
github = Github(token)

# Get the repository
repo = github.get_repo(f"{owner}/{repo_name}")

# Get the contents of the file
contents = repo.get_contents(file_path)

# Load the YAML data from the file contents
yaml_data = yaml.load(contents.decoded_content.decode("utf-8"), Loader=yaml.SafeLoader)

# Modify the specific field in the YAML data
yaml_data["key1"] = "new_value1"

# Dump the YAML data as a string
new_file_contents = yaml.dump(yaml_data)

# Update the file on GitHub
repo.update_file(contents.path, "Update file", new_file_contents, contents.sha)
```

Git push failed required str 0r bytes:

In your code, it seems like you are passing new_content.encode("base64") as the content argument, which will result in a bytes object. However, the github library is expecting either a string or a bytes object, not a base64-encoded bytes object.
To fix this issue, you can encode the new_content string as a utf-8 encoded bytes object instead of a base64-encoded bytes object:

```
repo.update_file(contents.path, message, new_content.encode("utf-8"), contents.sha, branch=branch)
```

Pipelines managing security reference:
https://github.com/kagarlickij/azuredevops-security-automation

https://learn.microsoft.com/en-us/azure/devops/pipelines/policies/permissions?view=azure-devops

```
from azure.devops.connection import Connection
from msrest.authentication import BasicAuthentication
from azure.devops.v6_0.security.security_client import SecurityClient
from azure.devops.v6_0.security.models import (
    AccessControlList,
    SecurityNamespace,
    GraphSubject,
    VssJsonCollectionWrapper,
    TokenAdminPolicies,
    AccessControlEntry,
    GraphUser,
)

# Set up Azure DevOps connection and authentication
personal_access_token = 'your_personal_access_token_here'
organization_url = 'https://dev.azure.com/your_organization_name_here'
credentials = BasicAuthentication('', personal_access_token)
connection = Connection(base_url=organization_url, creds=credentials)

# Get the Security client
security_client = connection.clients.get_client('azure.devops.v6_0.security.SecurityClient')

# Define the security namespace and descriptor for pipelines
namespace_id = '33344d9c-fc72-4d6f-aba5-fa317101a7e9'
descriptor = 'Microsoft.TeamFoundation.ServiceIdentity;33344d9c-fc72-4d6f-aba5-fa317101a7e9'

# Create a security group for pipelines
group_name = 'My Pipeline Security Group'
group_subject = GraphSubject(descriptor=descriptor, subject_type='ServiceIdentity')
security_namespace = SecurityNamespace(id=namespace_id)
group_access_control_list = AccessControlList(
    token=group_subject.descriptor,
    access_control_entries=[
        AccessControlEntry(
            allow_bits=31,
            deny_bits=0,
            extended_info=None,

subject_descriptor=GraphSubject(descriptor=GraphUser(uniquename='[DefaultCollection]\\Project
Collection Service Accounts').descriptor),
            allow_inherited_permissions=True,
            inherit_permissions=False
        ),
        AccessControlEntry(
            allow_bits=2,
            deny_bits=0,
            extended_info=None,

subject_descriptor=GraphSubject(descriptor=GraphUser(uniquename='[DefaultCollection]\\Project 
Collection Build Service (your_project_name)').descriptor),
            allow_inherited_permissions=True,
            inherit_permissions=False
        )
    ]
)
group = security_client.set_access_control_entries(security_namespace, group_subject, 
group_access_control_list)

# Add a user to the security group
user_email = 'user_email@example.com'
user_subject = security_client.read_identities(user_email, identity_type='user', 
query_membership=False)[0]
membership_json = VssJsonCollectionWrapper({'members': [user_subject.descriptor]})
membership_response = security_client.add_members_to_group(membership_json, 
security_namespace.id, group_subject.descriptor)

# Set pipeline security to use the security group
pipeline_id = '12345'
token_admin_policies = TokenAdminPolicies(use_groups=[group.token])
security_client.set_token_administration_policies(pipeline_id, token_admin_policies)
```

read_identities(user_email, identity_type='user', query_membership=False): A method of the SecurityClient that retrieves a list of identities matching the given email address and identity type. The identity_type parameter defaults to 'user', which means that we're looking for a user identity. The query_membership parameter is set to False, which means we're not interested in the groups or memberships the user might be part of

Sure! allow_bits=31 is a parameter that specifies the set of permissions that a user or group should be granted on an Azure DevOps resource.
Let me explain in a bit more detail:
In Azure DevOps, every resource (such as a team project, repository, build definition, or release definition) has a set of permissions that control who can perform specific actions on that resource. Each permission is represented as a bit in an integer value, where each bit corresponds to a specific permission. By combining bits, we can create a value that represents a set of permissions.
In this case, the value 31 is a bitwise OR of several permission bits, which means that the user or group being granted these permissions will have the following permissions on the resource:

- 1: View the resource
- 2: Edit the resource
- 4: Create child resources
- 8: Delete the resource
- 16: Manage permissions on the resource

By setting allow_bits to 31, we're granting the user or group all of these permissions on the specified resource.
Note that different resources may have different sets of permissions, so the meaning of allow_bits can vary depending on the resource being granted permissions. Also, be careful when assigning permissions to users or groups, as giving too many permissions can create security risks.

Points to Remember:

Data stored in security namespaces are used to determine whether an user has permissions to perform a specific action on a specific resource.
Typically, each family of resources (work items, Git repositories, etc.) is secured using a different namespace. Each security namespace contains zero or more access control lists. Each access control list contains a token, an inherit flag and a set of zero or more access control entries. Each access control entry contains an identity descriptor, an allowed permissions bitmask and an denied permissions bitmask.

Query_access_list:

```
allow': 4745, 'deny': 0, 'descriptor': 'Microsoft.TeamFoundation.ServiceIdentity;b5050f46-d077-4126-b5a7-0a6693026914:Build:cfd9df0e-df52-4228-98cd-c132aec45422', 'extended_info': None
```

CLI reference:

https://learn.microsoft.com/en-us/cli/azure/devops/security/group/membership?view=azure-cli-latest

```
az devops security permission list --namespace 52d39943-cb85-4d7f-8fa8-c6baac873819 --subject "vinaytalla20@gmail.com"
```

```
az ad app credential list --id 80fa2766-41f1-44e5-bec9-d54aa03362c2
```

```
az ad app credential list --id 80fa2766-41f1-44e5-bec9-d54aa03362c2 --query [].endDateTime --output tsv
```

```
az login --service-principal -u <app-id> -p <password-or-cert> --tenant <tenant>
```

```
az login --service-principal --username appID --tenant tenantID --password /path/to/cert
```

```
az role assignment create --assignee <service principal object ID> --role "Reader"
```

Azure AAD :

Appid:
07dd855d-e370-4a00-9fd7-4c9121292131   80fa2766-41f1-44e5-bec9-d54aa03362c2
0e6b74b1-ca2f-440c-bdab-c5f93849704e   e9a8de64-29ac-46f0-9e88-28018fa6145e

```
az vm list --resource-group QueryDemo --query "[?contains(storageProfile.osDisk.managedDisk.storageAccountType,'SSD')].{Name:name, Storage:storageProfile.osDisk.managedDisk.storageAccountType}"
```

```
az ad app credential list --id e9a8de64-29ac-46f0-9e88-28018fa6145e --query "[? contains(keyId, 'b4a6e1bd-d4f3-4051-9b01-f77bed178eb0')].{ENDDATE:endDateTime}"
```

Azure Pipelines:

To Run all pipelines:

```
az pipelines build queue --definition-name "*" --project <project-name> --org <organization-url>

az config set extension.use_dynamic_install=yes_without_prompt
```

```
repositories:
- repository: string # Required as first property. Alias for the specified repository.  ([-_A-Za-z0-9]*)
  endpoint: string # ID of the service endpoint connecting to this repository.
  trigger: trigger # CI trigger for this repository, no CI trigger if skipped (only works for Azure Repos).
  ref: string # ref name to checkout; defaults to 'refs/heads/main'. The branch checked out by default
whenever the resource trigger fires. Does not accept variables.
  name: string # repository name (format depends on `type`); does not accept variables.
  type: string # Type of repository: `git`, `github`, `githubenterprise`, and `bitbucket`.
```

Reference: https://learn.microsoft.com/en-us/azure/devops/pipelines/yaml-schema/resources-repositories-repository?view=azure-pipelines

Releases:

Need to Publish the Kubernetes manifests with latest commit Docker Tag to Artifacts Staging Directory to access them in Releases.

Pipeline Artifacts:

```
# Publish Pipeline Artifacts v1
# Publish (upload) a file or directory as a named artifact for the current run.
- task: PublishPipelineArtifact@1
  inputs:
    targetPath: '$(Pipeline.Workspace)' # string. Alias: path. Required. File or directory path. Default: $(Pipeline.Workspace).
    #artifact: # string. Alias: artifactName. Artifact name.
    publishLocation: 'pipeline' # 'pipeline' | 'filepath'. Alias: artifactType. Required. Artifact publish location. Default: pipeline.
    #fileSharePath: # string. Required when artifactType = filepath. File share path.
    #parallel: false # boolean. Optional. Use when artifactType = filepath. Parallel copy. Default: false.
    #parallelCount: '8' # string. Optional. Use when artifactType = filepath && parallel = true. Parallel count. Default: 8.
    #properties: # string. Custom properties.
```

```
- task: PublishPipelineArtifact@1
  displayName: 'Publish'
  inputs:
    targetPath: $(Build.ArtifactStagingDirectory)/**
    ${{ if eq(variables['Build.SourceBranchName'], 'main') }}:
      artifactName: 'prod'
    ${{ else }}:
      artifactName: 'dev'
    artifactType: 'pipeline'
```

Download Artifacts:

```
# Download an artifact named 'WebApp' to 'bin' in $(Build.SourcesDirectory)
- task: DownloadPipelineArtifact@2
  inputs:
```

```
  artifactName: 'WebApp'
  targetPath: $(Build.SourcesDirectory)/bin
```

```
trigger:
- main
stages:
- stage: build
 jobs:
 - job: run_build
  pool:
   vmImage: 'windows-latest'
  steps:
  - task: VSBuild@1
   inputs:
    solution: '**/*.sln'
    msbuildArgs: '/p:DeployOnBuild=true /p:WebPublishMethod=Package /p:PackageAsSingleFile=true /p:SkipInvalidConfigurations=true
/p:DesktopBuildPackageLocation="$(build.artifactStagingDirectory)\WebApp.zip" /p:DeployIisAppPath="Default Web Site"'
    platform: 'Any CPU'
    configuration: 'Release'

  - task: CopyFiles@2
   displayName: 'Copy scripts'
   inputs:
    contents: 'scripts/**'
    targetFolder: '$(Build.ArtifactStagingDirectory)'

  - publish: '$(Build.ArtifactStagingDirectory)/scripts'
   displayName: 'Publish script'
   artifact: drop

- stage: test
 dependsOn: build
 jobs:
 - job: run_test
  pool:
   vmImage: 'windows-latest'
  steps:
  - download: current
   artifact: drop
  - task: PowerShell@2
   inputs:
    filePath: '$(Pipeline.Workspace)\drop\test.ps1'
```

```
# Publish build artifacts v1
# Publish build artifacts to Azure Pipelines or a Windows file share.
- task: PublishBuildArtifacts@1
 inputs:
  PathtoPublish: '$(Build.ArtifactStagingDirectory)' # string. Required. Path to publish. Default: $(Build.ArtifactStagingDirectory).
  ArtifactName: 'drop' # string. Required. Artifact name. Default: drop.
  publishLocation: 'Container' # 'Container' | 'FilePath'. Alias: ArtifactType. Required. Artifact publish location. Default: Container.
  #TargetPath: # string. Required when ArtifactType = FilePath. File share path.
  #Parallel: false # boolean. Optional. Use when ArtifactType = FilePath. Parallel copy. Default: false.
  #ParallelCount: '8' # string. Optional. Use when ArtifactType = FilePath && Parallel = true. Parallel count. Default: 8.
 # Advanced
  #FileCopyOptions: # string. Optional. Use when ArtifactType = FilePath. File copy options.
  #StoreAsTar: false # boolean. Tar the artifact before uploading. Default: false.
```

A stage is one or more jobs, which are units of work assignable to the same machine. You can arrange both stages and jobs into dependency graphs. Examples include "Run this stage before that one" and "This job depends on the output of that job."

This hierarchy is reflected in the structure of a YAML file like:

- Pipeline
- Stage A
- Job 1
- Step 1.1
- Step 1.2
- ...
- Job 2
- Step 2.1
- Step 2.2
- ...
- Stage B
- ...

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/yaml-schema/pipeline?view=azure-pipelines>

if you have a single stage, you can omit the stages keyword and directly specify the jobs keyword:

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/yaml-schema/pipeline?view=azure-pipelines>

If you have a single stage and a single job, you can omit the stages and jobs keywords and directly specify the steps keyword:

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/yaml-schema/pipeline?view=azure-pipelines>

```
PIPELINE_WORKSPACE=/home/vsts/work/1
AGENT_BUILDDIRECTORY=/home/vsts/work/1
BUILD_SOURCESDIRECTORY=/home/vsts/work/1/s

AGENT_ROOTDIRECTORY=/home/vsts/work
BUILD_BINARIESDIRECTORY=/home/vsts/work/1/b
BUILD_STAGINGDIRECTORY=/home/vsts/work/1/a
BUILD_REPOSITORY_LOCALPATH=/home/vsts/work/1/s
SYSTEM_ARTIFACTSDIRECTORY=/home/vsts/work/r1/a
AGENT_RELEASEDIRECTORY=/home/vsts/work/r1/a
```

```
BUILD_SOURCEVERSION=a136b486bc8600ae52527f8a535b6e379d8125e7
BUILD_BUILDNUMBER=20230223.14

Image Tag = $(BUILD_SOURCEVERSION)$(BUILD_BUILDNUMBER)

 RELEASE_PRIMARYARTIFACTSOURCEALIAS=_vinaytalla20.email_integration

RELEASE_TRIGGERINGARTIFACT_ALIAS=_vinaytalla20.email_integration
SYSTEM_DEFINITIONNAME=vinaytalla20.email_integration
```

Template files need to exist on your filesystem at the start of a pipeline run. You can't reference templates in an artifact.

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops>

```
resources:
```

```
repositories:
  - repository: templates
    name: Contoso/BuildTemplates
    endpoint: myServiceConnection # Azure DevOps service connection
jobs:
- template: common.yml@templates
```

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops>

Reference for templates
[Templates - Azure Pipelines | Microsoft Learn](https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops)

Variables:

On UNIX systems (macOS and Linux), environment variables have the format `$NAME`. On Windows, the format is `%NAME%` for batch and `$env:NAME` in PowerShell.
System and user-defined variables also get injected as environment variables for your platform. When variables convert into environment variables, variable names become uppercase, and periods turn into underscores. For example, the variable name `any.variable` becomes the variable name `$ANY_VARIABLE`.

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=yaml%2Cbatch#environment-variables>

For Secrets Variables:

Each task that needs to use the secret as an environment variable does remapping. If you want to use a secret variable called `mySecret` from a script, use the `Environment` section of the scripting task's input variables. Set the environment variable name to `MYSECRET`, and set the value to `$(mySecret)`.

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=classic%2Cbatch#environment-variables>

For PAT token:

https://vssps.dev.azure.com/v-raayin/_apis/tokens/pats?api-version=7.0-preview.1

curl -H "Authorization: Bearer $TOKEN" https://vssps.dev.azure.com/v-raayin/_apis/tokens/pats?api-version=7.0-preview.1

```
az login
token = az account get-access-token --query accessToken -o tsv;
```

From <https://github.com/MicrosoftDocs/azure-devops-docs/issues/3926>

To test PAT:

https://dev.azure.com/{ORGANISATION_NAME}/_apis/connectionData.

From <https://stackoverflow.com/questions/53190769/validate-the-azure-devops-pat>

Gets a single personal access token (PAT).

GET https://vssps.dev.azure.com/{organization}/_apis/tokens/pats?authorizationId={authorizationId}&api-version=7.0-preview.1

```
object {2}

continuationToken :

patTokens [1]

0      {7}

displayName :      pipeline_script

validTo :      2023-04-23T06:34:54.26Z

scope   :      vso.build_execute vso.code_manage vso.connected_server
               vso.identity_manage vso.pipelineresources_manage
               vso.security_manage vso.tokenadministration vso.tokens
               vso.variablegroups_manage

targetAccounts [1]

0      :       6c8b9f85-572b-4b6a-9537-2b1a238ba101

validFrom :      2023-02-22T06:37:03.7833333Z

authorizationId :      33bd4ecb-d899-45c0-a50a-be830d415749

token   :      null
```

Using Golang:

Use the pipelineClient object to set permissions for a pipeline:

```
pipelineID := "<your-pipeline-id>"
acl, err := pipelineClient.GetAccessControlLists(context.Background(),
pipelines.GetAccessControlListsArgs{
   Project:  "<your-project-name>",
   Pipeline: &pipelineID,
})

if err != nil {
   fmt.Printf("Error: %v\n", err)
   return
}

// Update the ACL with the new permissions
// ...

_, err = pipelineClient.UpdateAccessControlLists(context.Background(),
pipelines.UpdateAccessControlListsArgs{
   Project:          "<your-project-name>",
   Pipeline:         &pipelineID,
   AccessControlLists:  &acl,
})

if err != nil {
   fmt.Printf("Error: %v\n", err)
   return
}
```

In this example, the GetAccessControlLists method is used to retrieve the current access control list (ACL) for the specified pipeline. You can then modify the ACL to set the required permissions, and use the UpdateAccessControlLists method to save the changes.
Note that you need to provide a Personal Access Token (PAT) to authenticate with Azure DevOps. You can create a new PAT in your Azure DevOps account settings. Also, make sure to replace the placeholder values (<your-pipeline-id>, <your-project-name>, etc.) with the actual values for your pipeline and project.

UpdateAccessControlLists method in the Azure DevOps Go client library, you can follow these steps

Retrieve the current ACL for the pipeline using the GetAccessControlLists method

```
pipelineID := "<your-pipeline-id>"
acl, err := pipelineClient.GetAccessControlLists(context.Background(),
pipelines.GetAccessControlListsArgs{
   Project:  "<your-project-name>",
   Pipeline: &pipelineID,
})
```

Create a new AccessControlEntry object for the user you want to add:

```
userEntry := pipelines.AccessControlEntry{
   Descriptor: &pipelines.IdentityDescriptor{
      Identifier: "<user-or-group-id>",
      IdentityType: pipelines.IdentityTypeUser, // or IdentityTypeGroup for groups
   },
   Role: &pipelines.RoleAssignment{
      Role: pipelines.RoleContributor, // or any other role you want to assign
   },
}
```

Replace <user-or-group-id> with the ID of the user or group you want to add to the ACL. You can find the ID by browsing to the user or group in Azure DevOps and looking at the URL, which will contain the ID.

Add the new user entry to the ACL

```
acl.AccessControlList = append(acl.AccessControlList, &userEntry)
```

Update the ACL using the UpdateAccessControlLists method:

```
_, err = pipelineClient.UpdateAccessControlLists(context.Background(),
pipelines.UpdateAccessControlListsArgs{
   Project:           "<your-project-name>",
   Pipeline:          &pipelineID,
   AccessControlLists:  &acl,
})
```

To PRINT User ID:

Here's an example of how to retrieve the user ID for a user and use it to add the user to the pipeline ACL:

```
import (
   "github.com/microsoft/azure-devops-go-api/azuredevops/pipelines"
   "github.com/microsoft/azure-devops-go-api/azuredevops/webapi"
)

// Create a new identity client to retrieve the user ID
identityClient := webapi.NewIdentitiesClient(connection)
```

```
// Retrieve the user by name
userName := "<user-name>"
user, err := identityClient.ReadIdentities(context.Background(), webapi.ReadIdentitiesArgs{
    Identities: []*webapi.IdentityDescriptor{{
        IdentityType: &pipelines.IdentityTypeUser,
        Identifier:   &userName,
    }},
})

if err != nil {
    fmt.Printf("Error: %v\n", err)
    return
}

if len(user) == 0 {
    fmt.Println("User not found")
    return
}

// Get the user ID from the returned identity descriptor
userID := *user[0].Id

// Create a new AccessControlEntry object for the user
userEntry := pipelines.AccessControlEntry{
    Descriptor: &pipelines.IdentityDescriptor{
        Identifier: userID,
        IdentityType: pipelines.IdentityTypeUser,
    },
    Role: &pipelines.RoleAssignment{
        Role: pipelines.RoleContributor, // or any other role you want to assign
    },
}

// Add the user entry to the ACL and update it
acl.AccessControlList = append(acl.AccessControlList, &userEntry)

_, err = pipelineClient.UpdateAccessControlLists(context.Background(),
pipelines.UpdateAccessControlListsArgs{
    Project:           "<your-project-name>",
    Pipeline:          &pipelineID,
    AccessControlLists: &acl,
})

if err != nil {
    fmt.Printf("Error: %v\n", err)
    return
}
```

ACL with user id:

```
import (
    "context"
    "fmt"
    "github.com/microsoft/azure-devops-go-api/azuredevops"
    "github.com/microsoft/azure-devops-go-api/azuredevops/pipelines"
    "github.com/microsoft/azure-devops-go-api/azuredevops/webapi"
)
// Create a new connection using your Azure DevOps organization URL and
personal access token
organizationURL := "https://dev.azure.com/v-raayin"
pat := ""
connection := azuredevops.NewPatConnection(organizationURL, pat)
// Create a new web client to manage identities
client := webapi.NewClient(connection)
// Retrieve the user by name
userName := "vinayt@italentdigital.com"
```

```
    users, err := client.GetIdentities(context.Background(),
    webapi.GetIdentitiesArgs{
        Identities: []string{userName},
    })
    if err != nil {
        fmt.Printf("Error: %v\n", err)
        return
    }
    if len(users) == 0 {
        fmt.Println("User not found")
        return
    }
    // Get the user ID from the returned identity descriptor
    userID := *users[0].Id
    // Create a new AccessControlEntry object for the user
    userEntry := pipelines.AccessControlEntry{
        Descriptor: &pipelines.IdentityDescriptor{
            Identifier: userID,
            IdentityType: pipelines.IdentityTypeUser,
        },
        Role: &pipelines.RoleAssignment{
            Role: pipelines.RoleContributor, // or any other role you want to
    assign
        },
    }
    // Add the user entry to the ACL and update it
    acl.AccessControlList = append(acl.AccessControlList, &userEntry)
    pipelineClient := pipelines.NewClient(connection)
    _, err = pipelineClient.UpdateAccessControlLists(context.Background(),
    pipelines.UpdateAccessControlListsArgs{
        Project:            "<your-project-name>",
        Pipeline:           &pipelineID,
        AccessControlLists: &acl,
    })
    if err != nil {
        fmt.Printf("Error: %v\n", err)
        return
    }
```

```
package main
import (
    "context"
    "fmt"
    "github.com/microsoft/azure-devops-go-api/azuredevops"
    "github.com/microsoft/azure-devops-go-api/azuredevops/location"
)
func main() {
    organizationUrl := "https://dev.azure.com/v-
raayin"                          // todo: replace value with your
organization url
    personalAccessToken := "" // todo: replace value with your PAT
    connection := azuredevops.NewPatConnection(organizationUrl,
personalAccessToken)
    ctx := context.Background()
    locationClient := location.NewClient(ctx, connection)
    conData, _ := locationClient.GetConnectionData(ctx,
location.GetConnectionDataArgs{})
    fmt.Printf("Display Name: %v",
*conData.AuthorizedUser.ProviderDisplayName)
}
```

```
package main
import (
    "context"
    "log"
    "github.com/microsoft/azure-devops-go-api/azuredevops"
    "github.com/microsoft/azure-devops-go-api/azuredevops/identity"
)
func main() {
    organizationUrl := "https://dev.azure.com/v-
raayin"                           // todo: replace value with your
organization url
    personalAccessToken :=
"n2p66lq7ojajkik5scmm6avqv7yf2s46jcw2ajixhpnwraim5nmq" // todo: replace
value with your PAT
    connection := azuredevops.NewPatConnection(organizationUrl,
personalAccessToken)
    ctx := context.Background()
    //locationClient := location.NewClient(ctx, connection)
    //conData, _ := locationClient.GetConnectionData(ctx,
location.GetConnectionDataArgs{})
    //fmt.Printf("Display Name: %v",
*conData.AuthorizedUser.ProviderDisplayName)
    UserClient, err := identity.NewClient(ctx, connection)
    if err != nil {
        log.Fatal(err)
    }
    UserInfo, err := UserClient.ListGroups(ctx, identity.ListGroupsArgs{})
    if err != nil {
        log.Fatal(err)
    }
    //fmt.Printf("Details: %v", UserInfo)
    index := 0
    for UserInfo != nil {
        for _, groupslist := range *UserInfo {
            log.Printf("Groups %v", groupslist)
            index++
        }
    }
}
```

https://stackoverflow.com/questions/56591886/how-to-add-a-user-to-azure-devops-using-its-python-client-api

Azure Pipelines Caching:

https://learn.microsoft.com/en-us/azure/devops/pipelines/release/caching?view=azure-devops

Although multiple agents can be installed per machine, we strongly suggest to only install one agent per machine. Installing two or more agents may adversely affect performance and the result of your pipelines.

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser>

In Azure Pipelines, you can run parallel jobs on Microsoft-hosted infrastructure or your own (self-hosted) infrastructure. Each parallel job allows you to run a single job at a time in your organization. You don't need to pay for parallel jobs if you're using an on-premises server. The concept of parallel jobs only applies to Azure DevOps Services.

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/licensing/concurrent-jobs?view=azure-devops&tabs=ms-hosted>

Using Self Hosted Agent as Docker Container:

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/docker?view=azure-devops

Conditions in Azure Devops pipelines :

https://learn.microsoft.com/en-us/azure/devops/pipelines/process/expressions?view=azure-devops

To run pipelines agent in Kubernetes clusters:

To use Docker in Docker bind mount the Docker socket

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/docker?view=azure-devops

Please, consider that any docker based tasks will not work on AKS 1.19 or later due to docker in docker restriction. Docker was replaced with containerd in Kubernetes 1.19, and Docker-in-Docker became unavailable.

From <https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/docker?view=azure-devops>

Scale self-hosted Agents in Azure DevOps Pipelines using VMSS

https://medium.selbstge.cloud/autoscale-self-hosted-azure-devops-agents-with-scale-sets-cdea63d73e35

Scale self-hosted Agents in Azure DevOps Pipelines using AKS
https://medium.com/@matt_89326/auto-scaling-self-hosted-azure-pipelines-agents-on-aks-996471e268bc

Scale self-hosted Agents in Azure DevOps Pipelines using AKS and KEDA

https://keda.sh/blog/2021-05-27-azure-pipelines-scaler/

download binary:

https://github.com/moby/buildkit/releases/download/v0.11.6/buildkit-v0.11.6.linux-amd64.tar.gz

using build ctl command to build docker images:

```
./bin/buildctl build --frontend=dockerfile.v0 --local context=. --local dockerfile=.
```

From another pod:

```
./buildctl --addr tcp://buildkitd.default.svc.cluster.local:1234 build  --frontend=dockerfile.v0 --local
context=. --local dockerfile=.
```

To push to private registrty:

```
/home/vinay/bin/buildctl --addr tcp://buildkitd.default.svc.cluster.local:1234 build  --
frontend=dockerfile.v0 --local context=. --local dockerfile=. --output
type=image,name=icsitalentdev.azurecr.io/test-push,push=true
```

To get pool id :

Hit below url in browser with changing organization name

https://dev.azure.com/vinaytalla20/_apis/distributedtask/pools?api-version=6.1-preview.1

To docker login for buildkitctl:

```
azAcrLogin=$(az acr login --name zylab -t) && mkdir -p ~/.docker && echo "{\"auths\": {$(echo $azAcrLogin| jq
'.loginServer'): {\"auth\": \"MDAwMDAwMDAtMDAwMC0wMDAwLTAwMDAtMDAwMDAwMDAwMDAwOg==\",
\"identitytoken\": $(echo $azAcrLogin| jq '.accessToken')}}}" > ~/.docker/config.json
trap "rm -f ~/.docker/config.json" EXIT
```

From <https://github.com/moby/buildkit/issues/565>

```
BASE64_AUTH=`echo -n "$CI_REGISTRY_USER:$CI_REGISTRY_PASSWORD" | base64`
mkdir -p ~/.docker
echo "{\"auths\": {\"$CI_REGISTRY\": {\"auth\": \"$BASE64_AUTH\"}}}" > ~/.docker/config.json

chown -R AzDevOps:AzDevOps /home/AzDevOps/.docker
```

```
{
        "auths": {
                "icsitalentdev.azurecr.io": {
                        "auth":
"MGRjYTM5MWUtMWJkMi00MDIzLTgyMmYtODQ1OWRmNWNlNmJkOm9ETzhRflJ0TUU2bWVFalkzQzZ
3VlUyM3gueUsufnhobWFuRWRjelc="
                },
                "italenticsstage.azurecr.io": {
                        "auth": "aXRhbGVudGljc3N0YWdlOkxlaVRCOG1CS3htN08zL2ttQ0ZHVmNRZFZJbDhKbUxD"
                }
        }
}
```

- context: where to perform the build.
- dockerfile: where to find the dockerfile to parse describing the build.

From <https://github.com/moby/buildkit/blob/master/docs/reference/buildctl.md>

Starting the buildkitd daemon

You need to run buildkitd as the root user on the host.

```
$ sudo buildkitd
```

To run buildkitd as a non-root user, see docs/rootless.md.

The buildkitd daemon supports two worker backends: OCI (runc) and containerd.

By default, the OCI (runc) worker is used. You can set `--oci-worker=false --containerd-worker=true` to use the containerd worker.

From <https://github.com/moby/buildkit>

Error running in pod:

```
error: failed to solve: failed to read dockerfile: failed to mount /tmp/buildkit-mount2127907715:
[{Type:bind Source:/var/lib/buildkit/runc-native/snapshots/snapshots/2 Options:[rbind ro]}]: permission
denied
```

```
ERRO[2023-06-30T16:22:44Z] /moby.buildkit.v1.Control/Solve returned error: rpc error: code =
Unknown desc = failed to read dockerfile: failed to mount /tmp/buildkit-mount2127907715: [{Type:bind
Source:/var/lib/buildkit/runc-native/snapshots/snapshots/2 Options:[rbind ro]}]: permission denied
```

ENV Variables:

URL = https://dev.azure.com/vinaytalla20
TOKEN = u6rikixjz6rjxipfcknaul4nhp4nfl7qbw6pazjhvempllnghvaa
AGENT NAME = kubernetes
POOL NAME = linux

```
export AZP_URL=https://dev.azure.com/vinaytalla20
export AZP_TOKEN=u6rikixjz6rjxipfcknaul4nhp4nfl7qbw6pazjhvempllnghvaa
export AZP_AGENT_NAME=linux-agent
export AZP_POOL=kubernetes
Export TARGETARCH=linux-x64
```

Terraform

03 January 2023 17:42

Kubernetes Resource Creation:

```
AKS
  |__ main.tf
```

```
resource "azurerm_kubernetes_cluster" "terraform_k8s"

module "nodepool" {
  source = "../NodePools"
  cluster_id = azurerm_kubernetes_cluster.terraform_k8s.id
  rg-name = "terraform-rg"
}
```

```
Nodepools
  |__ zonetest.tf
```

```
resource "azurerm_kubernetes_cluster_node_pool" "zonetest" {
  kubernetes_cluster_id = var.cluster_id
  os_type = "Linux"
  vm_size = "Standard_D2_v3"
  zones = [ "1","2" ]
  mode = "User"
  name = "zonetest"
}
```

Terraform import command worked successfully

By adding resource to main.tf file in "NodePools" module

```
Terrraform  import  -var-file  variables.tfvars  module.nodepool.azurerm_kubernetes_cluster_node_pool.zonetest
```

To Apply Specific Resource

```
Terraform apply -var-file variables.tfvars  -target module.nodepool.azurerm_kubernetes_cluster_node_pool.test
```

Terraform KT Questions

23 May 2025 15:29

1. Diff between .terraform.local.hcl vs .terrraform?
2. Will terraform apply command recreate resources which are tainted?
3. Will terraform destroy deletes resources which are tainted?
4. Ignore_changes related to fields which are within the resource?
5. Provisioners- Local-Exec , File-Exec, Remote-Exec

Notes:

1. locals variables defined in the file are available within the file
2. Lifecycle:
3. a. create_before_destroy
4. b. prevent_destroy
5. c. ignore_changes

Remote GITLAB Modules

Setup sshkeys for the gitlab project

- Generate ssh public and private keys

```
ssh-keygen -t rsa -b 2048 -C "<comment>"
```

```
vinaytalla@ITD-584:~/Terraform-Labs$ cat $HOME/.ssh/config
Host gitlab-italent.com
    PreferredAuthentications publickey
    IdentityFile /home/vinaytalla/Terraform-Labs/terraform-module
```

- Add ssh pub key to gitlab under user profile at ssh_keys section

Test connection

```
ssh -T git@gitlab.example.com
```

Modules in Package Sub-directories

When the source of a module is a version control repository or archive file (generically, a "package"), the module itself may be in a sub-directory relative to the root of the package.

A special double-slash syntax `//` is interpreted by Terraform to indicate that the remaining path after that point is a sub-directory within the package. For example:

- hashicorp/consul/aws//modules/consul-cluster
- git::https://example.com/network.git//modules/vpc
- https://example.com/network-module.zip//modules/vpc

If the source address has arguments, such as the `ref` argument supported for the version control sources, the sub-directory portion must be *before* those arguments:

- git::https://example.com/network.git//modules/vpc?ref=v1.2.0
- github.com/hashicorp/example//modules/vpc?ref=v1.2.0

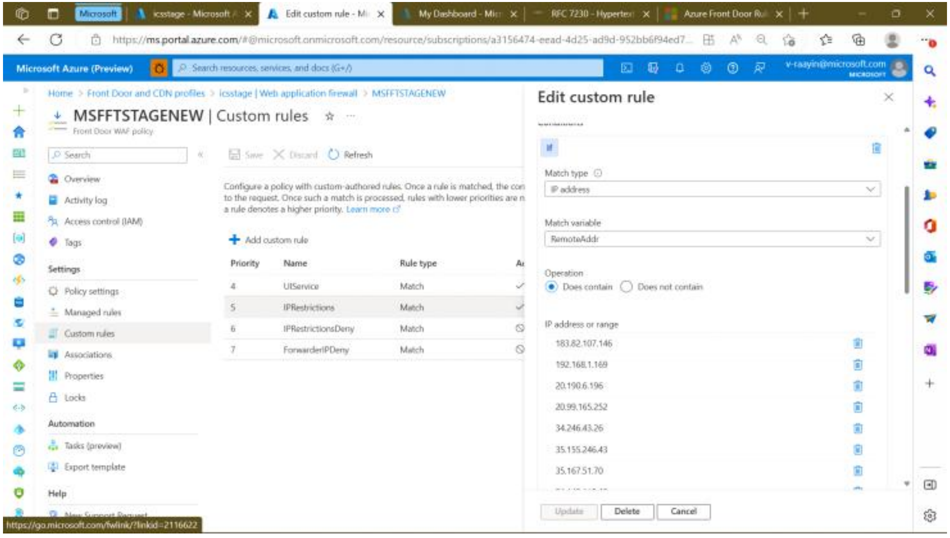
Terraform will still extract the entire package to local disk, but will read the module from the subdirectory. As a result, it is safe for a module in a sub-directory of a package to use a local path to another module as long as it is in the *same* package.

Azure Front Door

02 January 2023 11:13

Access was blocked for Grafana From Azure Front Door from on-premises IP Address(what is my IP)

To Allow Access add WAF Rules pointing the IP Address



Home > Front Door and CDN profiles > icsstage | Web application firewall > MSFFTSTAGENEW

MSFFTSTAGENEW | Custom rules

Front Door WAF policy

Configure a policy with custom-authored rules. Once a rule is matched, the con
to the request. Once such a match is processed, rules with lower priorities are n
a rule denotes a higher priority. Learn more

Priority	Name	Rule type	A
4	UIService	Match	✓
5	IPRestrictions	Match	✓
6	IPRestrictionsDeny	Match	⃠
7	ForwarderIPDeny	Match	⃠

Edit custom rule

Match type: IP address

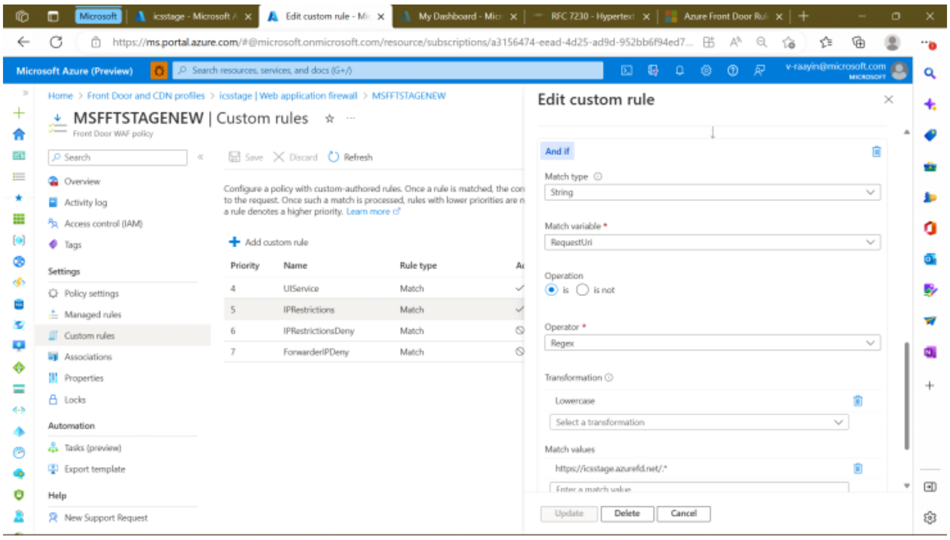
Match variable: RemoteAddr

Operation: ● Does contain ○ Does not contain

IP address or range

183.82.107.146
192.168.1.169
20.190.6.196
20.99.165.252
34.246.43.26
35.155.246.43
35.167.51.70

https://go.microsoft.com/fwlink/?linkid=2116622



Edit custom rule

And if

Match type: String

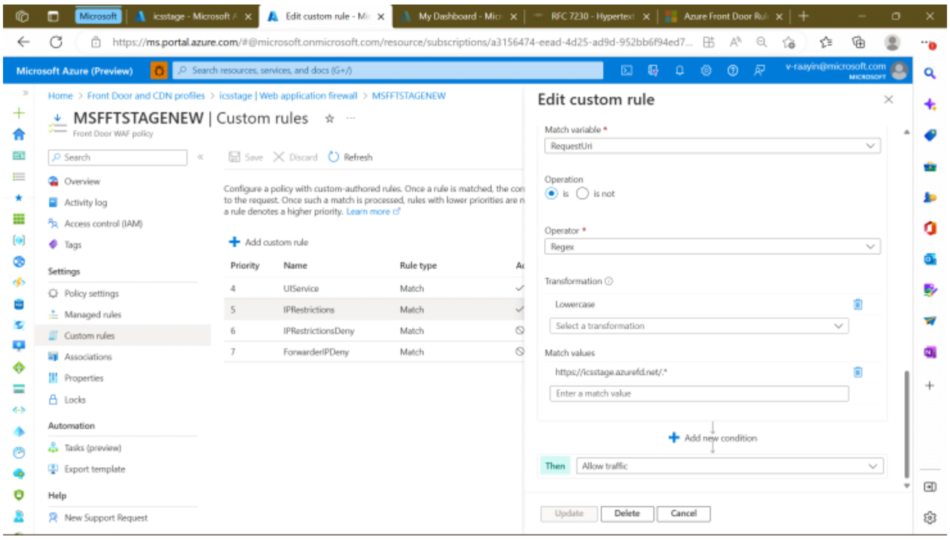
Match variable *: RequestUri

Operation: ● is ○ is not

Operator *: Regex

Transformation: Lowercase

Match values: https://icsstage.azurefd.net/.*



Edit custom rule

Match variable *: RequestUri

Operation: ● is ○ is not

Operator *: Regex

Transformation: Lowercase

Match values: https://icsstage.azurefd.net/.*

Then: Allow traffic

Accessing Grafana UI from Azure Front Door Host(hostname.azurefd.net/grafana/login)

403 Forbiden Error
302 Redirection
308 Permanent Redirection
404 File Not Found

URL or its content (such as files or images) was either **deleted** or **moved**

https://github.com/grafana/grafana/issues/46321The

CNAME RECORD:

Basically CNAME record should be created for Azure Front Door Frontend Host with the Custom Domain.

1. Sign into DNS Provider, find the DNS Records create a CNAME record entry for your custom domain

Source	Type	Destination
example.dev	CNAME	exampledev.azurefd.net

Azure Front Door Design:

Frontend Host/Domain	Backend Pool	Route Rule
italenticsstg.azurefd.net	public-ingress-host-with-tls italenticsstg.com	Match Request; /* From Frontend to Ingress-Backend
	public-host-grafana-loadbalancerIP grafanaui.eastus.cloudapp.azure.com	Accept Only Https /grafana/* Forward Rule : Http only From Frontend to Grafana-Backend

Grafana version 8.55, 8.3.5, 9.0.4, 9.3.1(stable)

"Origin not allowed"

DNS Configuration:

dig italenticsdev.azurefd.net

;; ANSWER SECTION:

italenticsdev.azurefd.net. 30 IN CNAME star-azurefd-prod.trafficmanager.net.

star-azurefd-prod.trafficmanager.net. 38 IN CNAME shed.dual-low.part-0030.t-0009.fdv2-t-msedge.net.

shed.dual-low.part-0030.t-0009.fdv2-t-msedge.net. 60 IN CNAME part-0030.t-0009.fdv2-t-msedge.net.

part-0030.t-0009.fdv2-t-msedge.net. 56 IN A 13.107.237.58

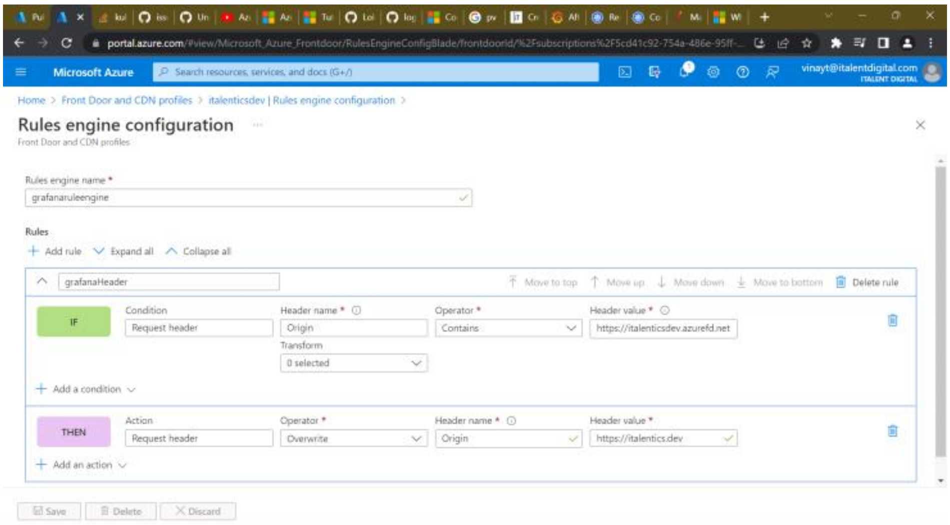
part-0030.t-0009.fdv2-t-msedge.net. 56 IN A 13.107.238.58

```
[security]

csrf_additional_headers X-FORWARDED-HOST
csrf_trusted_origins https://<frontdoor>.azurefd.net
```

From <https://github.com/grafana/grafana/issues/46321>

Solution to "Origin Not Allowed" in Grafana

Make sure you add custom rule engine to Azure Front Door Backend Pool and Route Rule



portal.azure.com/#view/Microsoft_Azure_Frontdoor/RulesEngineConfigBlade/frontdoorId/%2Fsubscriptions%2F5cd41c92-754a-486e-95ff-...

vinayt@italentdigital.com

Home > Front Door and CDN profiles > italenticsdev | Rules engine configuration >

Rules engine configuration

Front Door and CDN profiles

Rules engine name *: grafanaruleengine

Rules

grafanaHeader

IF — Condition: Request header; Header name *: Origin; Operator *: Contains; Header value *: https://italenticsdev.azurefd.net; Transform: 0 selected

THEN — Action: Request header; Operator *: Overwrite; Header name *: Origin; Header value *: https://italentics.dev

No need to add Proxy_set_Header in ingress rules
No need to add CSRF_TRUSTED_ORIGINS in Grafana.ini Configuration.

As a result second rule worked fine while accessing Grafana with the host(italenticsstg.azurefd.net/grafana/login)
Grafana Configuration:

```
Grafana.ini:
  server:
   serve_from_sub_path: true
   root_url: https://italenticsstg.azurefd.net/grafana/
   domain: italenticsstg.azurefd.net
```

Basically this Front Door Rule Redirects HTTPS request to HTTP, with TLS Encrption at Front Door Level. Point to be noted here is Grafana UI is Still Accessible from LoadBalancerIP and LoadBalancerDNS-label. As a fix to this issue for Stg ENV Grafana need to be proxied behind ingress using ClusterIP Service.

Ingress rule for Grafana UI:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 annotations:
  kubernetes.io/ingress.class: nginx
  nginx.ingress.kubernetes.io/backend-protocol: HTTP
  nginx.ingress.kubernetes.io/cors-allow-credentials: "true"
  nginx.ingress.kubernetes.io/cors-allow-headers: X-Forwarded-For, X-Forwarded-Proto,
   X-Forwarded-Port, X-Forwarded-Prefix,Content-Type, X-Forwarded-Host
  nginx.ingress.kubernetes.io/cors-allow-methods: PUT, GET, POST, OPTIONS, DELETE
  nginx.ingress.kubernetes.io/cors-allow-origin: "https://italenticsstg.azurefd.net"
  nginx.ingress.kubernetes.io/enable-cors: "true"
  nginx.ingress.kubernetes.io/proxy-body-size: 4m
  labels:
  name: grafana
 name: grafana-ingress
 namespace: syndication
spec:
 rules:
 - host: italenticsstg.com
  http:
   paths:
   - backend:
     service:
      name: grafana-ui-cname
      port:
       number: 80
    path: /grafana/
    pathType: Prefix
 tls:
 - hosts:
  - italenticsstg.com
  secretName:
```

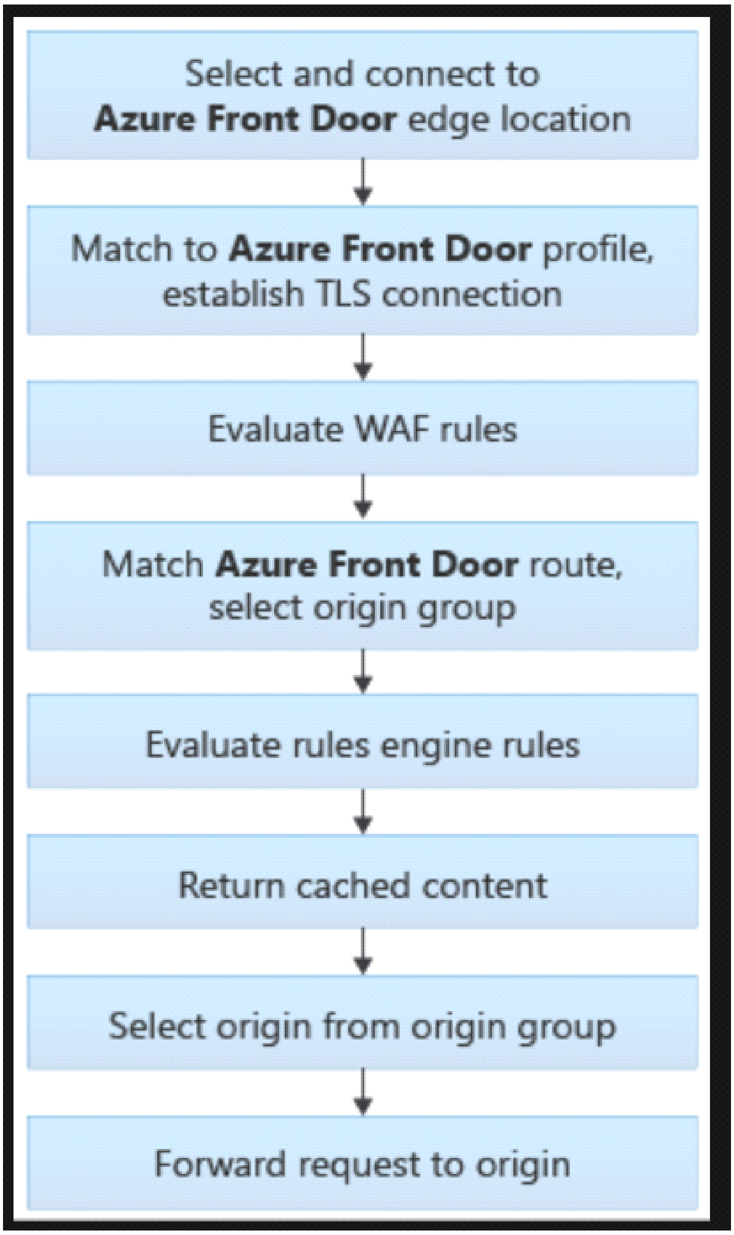
Web Application Firewall(WAF):

Modes:

1. Detection Mode: WAF rules only validates the rules and doesn't block incoming request. Logs the information in Log Analytics Workspace.
2. Prevention Mode: WAF rules are validated and incoming request is blocked based on the rules set.

Custom Rules has highest priority when compared to Managed Rules.

Azure Front Door Architecture:


Select and connect to **Azure Front Door** edge location
Match to **Azure Front Door** profile, establish TLS connection
Evaluate WAF rules
Match **Azure Front Door** route, select origin group
Evaluate rules engine rules
Return cached content
Select origin from origin group
Forward request to origin

Health Check Failed:

```
{
    "channels": "Admin, Operation",
    "correlationId": "7c7a1924-15e2-445b-acf6-d34c2ba0bb0c",
    "description": "",
    "eventDataId": "f1ae5c59-9056-464f-b2c5-28dcd674e7b0",
    "eventName": {
        "value": "",
        "localizedValue": ""
    },
    "category": {
        "value": "ResourceHealth",
        "localizedValue": "Resource Health"
    },
    "eventTimestamp": "2023-02-02T21:44:46.68Z",
    "id": "/subscriptions/5cd41c92-754a-486e-95ff-f1fc311c0fa2/resourcegroups/ICS-iTalent-QA-RG/providers/Microsoft.Network/frontdoors/italenticsstg/events/f1ae5c59-9056-464f-b2c5-28dcd674e7b0/ticks/638109710866800000",
    "level": "Critical",
    "operationId": "",
    "operationName": {
        "value": "Microsoft.Resourcehealth/healthevent/InProgress/action",
        "localizedValue": "Health Event InProgress"
    },
    "resourceGroupName": "ICS-iTalent-QA-RG",
    "resourceProviderName": {
        "value": "Microsoft.Resourcehealth/healthevent/action",
        "localizedValue": "Microsoft.Resourcehealth/healthevent/action"
    },
    "resourceType": {
        "value": "MICROSOFT.NETWORK/FRONTDOORS",
        "localizedValue": "MICROSOFT.NETWORK/FRONTDOORS"
    },
    "resourceId": "/subscriptions/5cd41c92-754a-486e-95ff-f1fc311c0fa2/resourcegroups/ICS-iTalent-QA-RG/providers/Microsoft.Network/frontdoors/italenticsstg",
    "status": {
        "value": "Updated",
        "localizedValue": "Updated"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2023-02-02T21:44:46.68Z",
    "subscriptionId": "5cd41c92-754a-486e-95ff-f1fc311c0fa2",
    "tenantId": "",
    "properties": {
        "title": "Unavailable Backends",
        "details": "One or more of your Front Door backends are responding with e
rrors to health probes. The backends associated with this Front Door are not resp
onding to health probes with the expected status.",
        "currentHealthStatus": "Unavailable",
        "previousHealthStatus": "Unavailable",
        "type": "Downtime",
        "cause": "PlatformInitiated"
    },
    "relatedEvents": []
}
```

```
"submissionTimestamp": "2023-02-03T01:58:28.692Z",
    "subscriptionId": "5cd41c92-754a-486e-95ff-f1fc311c0fa2",
    "tenantId": "",
    "properties": {
        "title": "Unavailable Backends",
        "details": "One or more of your Front Door backends are responding with e
rrors to health probes. The backends associated with this Front Door are not resp
onding to health probes with the expected status.",
        "currentHealthStatus": "Unavailable",
        "previousHealthStatus": "Unavailable",
        "type": "Downtime",
        "cause": "PlatformInitiated"
```

Issue around: 11:16pm IST 02-feb-2023

```
{
    "channels": "Admin, Operation",
    "correlationId": "7c7a1924-15e2-445b-acf6-d34c2ba0bb0c",
    "description": "",
    "eventDataId": "ff99ff00-6e09-44dc-9ae9-82635bcc781b",
    "eventName": {
        "value": "",
        "localizedValue": ""
    },
    "category": {
        "value": "ResourceHealth",
        "localizedValue": "Resource Health"
    },
    "eventTimestamp": "2023-02-02T21:37:25.1042239Z",
    "id": "/subscriptions/5cd41c92-754a-486e-95ff-
f1fc311c0fa2/resourcegroups/ICS-iTalent-QA-
RG/providers/Microsoft.Network/frontdoors/italenticsstg/events/ff99ff00-6e09-44dc
-9ae9-82635bcc781b/ticks/638109706451042239",
    "level": "Informational",
    "operationId": "",
    "operationName": {
        "value": "Microsoft.Resourcehealth/healthevent/Resolved/action",
        "localizedValue": "Health Event Resolved"
    },
    "resourceGroupName": "ICS-iTalent-QA-RG",
    "resourceProviderName": {
        "value": "Microsoft.Resourcehealth/healthevent/action",
        "localizedValue": "Microsoft.Resourcehealth/healthevent/action"
    },
    "resourceType": {
        "value": "MICROSOFT.NETWORK/FRONTDOORS",
        "localizedValue": "MICROSOFT.NETWORK/FRONTDOORS"
    },
    "resourceId": "/subscriptions/5cd41c92-754a-486e-95ff-
f1fc311c0fa2/resourcegroups/ICS-iTalent-QA-
RG/providers/Microsoft.Network/frontdoors/italenticsstg",
    "status": {
        "value": "Resolved",
        "localizedValue": "Resolved"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2023-02-02T21:37:25.1042239Z",
    "subscriptionId": "5cd41c92-754a-486e-95ff-f1fc311c0fa2",
    "tenantId": "",
    "properties": {
        "title": "Unknown",
        "details": "Unknown",
        "currentHealthStatus": "Available",
        "previousHealthStatus": "Unavailable",
        "type": "Unknown",
        "cause": "Unknown"
    },
    "relatedEvents": []
}
```

. you have a domain : devopsguru.com
2. You have a AzureFrontdoor named : devopsguru.azurefd.net
3. you have a cluster named: myservicefabric.northeurope.cloudapp.azure.com.
4. Create a record set :myservicefabric.devopsguru.com and www.devopsguru.com
5. Map myservicefabric.devopsguru.com to myservicefabric.northeurope.cloudapp.azure.com
6. Map www.devopsguru.com to devopsguru.azurefd.net
7. Create a FrontendHosts for www.devopsguru.com
8. Create BackendPool called frontedbackendpool.
9. Add Backends hosts with myservicefabric.devopsguru.com as Custom Host
10. Create Routing rules called frontendrules. In FrontendHosts select www.devopsguru.com and backendpool select frontedbackendpool

Private DNS Mapping to Azure Front Door:

Limitations:

1. Only certain types of domain names are supported, including root domains and subdomains.
2. The domain must be registered with a domain registrar and have appropriate DNS entries pointing to Azure Front Door.
3. The private DNS zone must be in the same Azure resource group and region as the Azure Front Door instance.
4. Private domains cannot be used for wildcard matching, path-based routing, or custom rules.
5. Azure Private DNS zones only support A and AAAA records, so other record types such as MX, CNAME, and TXT are not supported.
6. There may be additional latency introduced by resolving the domain name through the private DNS zone before it is mapped to the Front Door instance.
7. There is a cost associated with using Azure Private DNS and Azure Front Door, so be sure to consider this when planning your implementation

Resources in Node are equally divided to the underlying pods when no limits are set by pod.

```
"One or more of your Front Door backends are responding with errors to health probes. The backends associated with this Front Door are not responding to health probes with the expected status
```

If you have a single backend in your backend pool, you can choose to disable the health probes reducing the load on your application backend. Even if you have multiple backends in the backend pool but only one of them is in enabled state, you can disable health probe

From <https://learn.microsoft.com/en-us/azure/frontdoor/health-probes>

AKS thorughput

Changed timeout from 120 to 240 seconds, intially it was 120 seconds, may be default is 30 seconds

Azure Front Door Caching

Cache expiration

The following order of headers is used to determine how long an item gets stored in our cache:

1. `Cache-Control: s-maxage=<seconds>`
2. `Cache-Control: max-age=<seconds>`
3. `Expires: <http-date>`

Some `Cache-Control` response header values indicate that the response isn't cacheable. These values include `private`, `no-cache`, and `no-store`. Front Door honors these header values and doesn't cache the responses, even if you override the caching behavior by using the Rules Engine.

If the `Cache-Control` header isn't present on the response from the origin, by default Front Door randomly determines a cache duration between one and three days.

Note: Cache expiration can't be greater than 366 days.

You may see `REVALIDATED_HIT` in the `Cache-Control` response header. This indicates that the cached content in Azure Front Door was revalidated with the origin server before being served to the client. This can happen when the cached content has expired, but the origin server indicates that the content hasn't changed. In this case, the cached content is served to the client, and the cache expiration is reset.

From <https://learn.microsoft.com/en-us/azure/frontdoor/front-door-caching?pivots=front-door-classic>

Common Kubernetes Failures or Errors

30 December 2022 10:07

Reference Documentation https://learn.microsoft.com/en-us/azure/virtual-machines/disks-redundancy

When a Disk created in zone "None" can only be attached to VM from same zone. As a result the pod will be in Container Creating State.

Disk from one location cannot be attached to some other VM running in different locations.

Set "Max Share" value, when creating Disk so that different Nodes or VMs can use same Disk Concurrently.

Either Use Node Affinity to make sure Disk from same zone is attached to VM from same Zone as Disk or Create VM in the same Zone as Disk Zone.

A disk with sku 'StandardSSD_ZRS' cannot be created in an availability zone.

Local Redundant Storage(LRS):
However, the write latency for LRS disks is better than ZRS disks because LRS disks synchronously write data to three copies in a single data center.

Zone Redundant Storage(ZRS):

Zone-redundant storage (ZRS) synchronously replicates your Azure managed disk across three Azure availability zones in the region you select. Each availability zone is a separate physical location with independent power, cooling, and networking

A ZRS disk lets you recover from failures in availability zones. If a zone went down, a ZRS disk can be attached to a virtual machine (VM) in a different zone.

Persistent Volume:

An Azure disk can only be mounted with *Access mode* type *ReadWriteOnce*, which makes it available to one node in AKS. If you need to share a persistent volume across multiple nodes, use Azure Files.

If multiple pods need concurrent access to the same storage volume, you can use Azure Files to connect using the Server Message Block (SMB) protocol.

Public IP Address:

Assign contributer role to AKS objectid to the public IP Address resource.

Dealing with PV and PVC Volume

Make sure proper affinities guided with manifest
Also set maxsure parameter for storage to be '2' , so that it can be mounted on two Nodes at same time

aaduser=674dd9ac-8fe3-4ec7-ad1d-66a93e9c06f9;72f988bf-86f1-41af-91ab-2d7cd011db47

From <https://lens.msftcloudes.com/#/dashboard/3d69316d-1ec7-4a2f-98bf-731fca784f1f?_g=(ws:e36e780f-b4f7-49f6-b1c8-a426de0d20bc)&params=(filters:!((k:AssetType,v:'Container%20Host'),(k:Cloud,v:'Public'),(k:RemediationOwner,v:'65b004c8-34a6-4afe-805b-c7bd15edd15b'),(k:SubscriptionId,v:'cf931916-a75b-449e-bebe-feef88b19893'),(k:Environment,v:'Prod'),(k:IsActionable,v:'True'),(k:DueDateMonth,v:'2023-04-01T00:00:00.0000000Z'),(k:ScanType,v:'Qualys'),(k:ScanToolName,v:'ContainerImageScan')),time:(from:'2023-03-12T13:51:35.4584432Z',to:'2023-03-12T14:22:00.9346298Z'))>

Cluster Creation of V 1.24

To Resolve Node "vinay-Virtual" not found
Error getting node" err="node

Refernce link https://github.com/kubernetes/minikube/issues/4144

```
sed -i "s/cgroupDriver: systemd/cgroupDriver: cgroupfs/g"/var/lib/kubelet/config.yaml
systemctl daemon-reload
systemctl restart kubelet
```

From <https://github.com/kubernetes/minikube/issues/4144>

```
java.net.SocketException: Connection reset
        at java.base/sun.nio.ch.NioSocketImpl.implRead(NioSocketImpl.java:313)
        at java.base/sun.nio.ch.NioSocketImpl.read(NioSocketImpl.java:340)
        at java.base/sun.nio.ch.NioSocketImpl$1.read(NioSocketImpl.java:789)
        at java.base/java.net.Socket$SocketInputStream.read(Socket.java:1025)
        at java.base/sun.security.ssl.SSLSocketInputRecord.read(SSLSocketInputRecord.java:483)
        at java.base/sun.security.ssl.SSLSocketInputRecord.readHeader(SSLSocketInputRecord.java:477)
        at java.base/sun.security.ssl.SSLSocketInputRecord.decode(SSLSocketInputRecord.java:160)
        at java.base/sun.security.ssl.SSLTransport.decode(SSLTransport.java:111)
        at java.base/sun.security.ssl.SSLSocketImpl.decode(SSLSocketImpl.java:1510)
        at java.base/sun.security.ssl.SSLSocketImpl.readHandshakeRecord(SSLSocketImpl.java:1425)
        at java.base/sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:455)
        at java.base/sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:426)
        at
        org.apache.http.conn.ssl.SSLConnectionSocketFactory.createLayeredSocket(SSLConnectionSocketFactory.java:436)
        at
        org.apache.http.conn.ssl.SSLConnectionSocketFactory.connectSocket(SSLConnectionSocketFactory.java:384)
```

```
at
org.apache.jmeter.protocol.http.sampler.hc.LazyLayeredConnectionSocketFactory.connectSocket(
LazyLayeredConnectionSocketFactory.java:87)
at
org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConn
ectionOperator.java:142)
at org.apache.jmeter.protocol.http.sampler.HTTPHC4Impl
$JMeterDefaultHttpClientConnectionOperator.connect(HTTPHC4Impl.java:408)
at
org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHttpClientConn
ectionManager.java:376)
at org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.java:393)
at org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
at org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
at org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
at org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
at org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.java:185)
at org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:83)
at
org.apache.jmeter.protocol.http.sampler.HTTPHC4Impl.executeRequest(HTTPHC4Impl.java:939)
at org.apache.jmeter.protocol.http.sampler.HTTPHC4Impl.sample(HTTPHC4Impl.java:650)
at
org.apache.jmeter.protocol.http.sampler.HTTPSamplerProxy.sample(HTTPSamplerProxy.java:66)
at
org.apache.jmeter.protocol.http.sampler.HTTPSamplerBase.sample(HTTPSamplerBase.java:1301)
at
org.apache.jmeter.protocol.http.sampler.HTTPSamplerBase.sample(HTTPSamplerBase.java:1290)
at org.apache.jmeter.threads.JMeterThread.doSampling(JMeterThread.java:651)
at org.apache.jmeter.threads.JMeterThread.executeSamplePackage(JMeterThread.java:570)
at org.apache.jmeter.threads.JMeterThread.processSampler(JMeterThread.java:501)
at org.apache.jmeter.threads.JMeterThread.run(JMeterThread.java:268)
at java.base/java.lang.Thread.run(Thread.java:1589)
```

Pod to Pod communitcation using cluster domain:

```
 curl --cert icsservices.cer https://secure-gateway.syndication.svc.cluster.local:443
```

```
curl: (58) unable to set private key file: 'icsservices.cer' type PEM
root@schedular-service-786d89cc9f-c6z7d:/tmp# openssl pkcs12 -in icsservices.cer -out key.pem -
clcerts
139861398930752:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong
tag:../crypto/asn1/tasn_dec.c:1149:
139861398930752:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:../crypto/asn1/tasn_dec.c:309:Type=PKCS12
```

```
openssl x509 -inform der -in icsservices.cer -out certificate.pem
```

```
unable to load certificate
```

```
140399187612992:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong
tag:../crypto/asn1/tasn_dec.c:1149:
140399187612992:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:../crypto/asn1/tasn_dec.c:309:Type=X509
```

```
curl --cert tlstest.pem https://secure-gateway.syndication.svc.cluster.local:443

curl: (58) unable to set private key file: 'tlstest.pem' type PEM
```

```
keytool -import -alias tomcat -file /path/to/icsservices.cer -keystore /path/to/keystore.p12 -storepass
changeit -storetype PKCS12
```

- X.509 Certificate (.crt, .pem, .cer): This format contains the public key certificate, usually in Base64-encoded ASCII text format.
- PKCS12 (.p12, .pfx): This format is a binary format that can store the private key, public key certificate, and certificate chain in a single file. It is commonly used for importing/exporting certificates and private keys into Java keystores.
- Java KeyStore (JKS) (.jks): This is the default keystore format used by Java, which can store cryptographic keys and certificates.

From <https://chat.openai.com/>

Azure Cloud

30 December 2022 11:50

By Default AKS is created in the same location of Resource Group and also the Node Resource Group or Infrastructure Resource Group i.e., MC_clusterName_resourceGroupName_location.

Azure Storage Account

An Azure storage account contains all of your Azure Storage data objects, including blobs, file shares, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS.

AAD is a multi-tenant, cloud-based directory and identity management service that is provided as part of the Azure platform. AAD is used to store and manage identities and their associated information, such as user accounts and groups. AAD enables you to manage access to cloud-based resources, including Azure services and applications, based on the identities of users and groups.

Service Principals, on the other hand, are non-interactive, automated identities that are used by Azure resources and applications to access other Azure services. Service Principals are used to represent the identity of an application, and they are created in AAD. Service Principals are typically created through an application registration process, and they have their own authentication credentials, such as a

ID and secret, that are used to authenticate to Azure services

From <https://chat.openai.com/chat>

Querying Azure reosurces using az commands:

To list arrays:

```
az vm list --resource-group QueryDemo --query "[].{Name:name, OS:storageProfile.osDisk.osType, admin:osProfile.adminUsername}"
```

```
az aks show --resource-group  ICS-iTalent-QA-RG --name ics-aks-qa
```

To get Objectid of cluster which got attached to it:

```
az account set --subscription <subcritionId>
```

If

```
servicePrincipalProfile": {
    "clientId": "msi"
}
```

Get objectId by below command:

```
az aks show --resource-group  ICS-iTalent-QA-RG --name ics-aks-qa --query identity.principalId --output tsv
```

If

```
servicePrincipalProfile": {
    "clientId": "0e6b74b1-ca2f-440c-bdab-c5f93849704e"
  }
```

Must use objectId of Enterprise Application AAD

To get ClientId:

```
az aks show --resource-group  ICS-iTalent-QA-RG --name ics-italent-qa-aks --query servicePrincipalProfile.clientId --output tsv
```

To get ObjectId using clientId:

```
az ad sp show --id 0e6b74b1-ca2f-440c-bdab-c5f93849704e --query id --output tsv

az ad sp show --id clientid(above_one) --query id --output tsv
```

when you create a service principal in Azure, an associated Enterprise Application is created by default.

Cluster Name	servicePrincipalProfile	identity	identityProfile
ics-italent-qa-aks(stopped)	Clientid= 5ac10039-b35e-4e25-ad05-e7c6d4d09248	Null	Null

	ObjectId= 82548fa3-06bf-4ec6-8caf-f588ca36da4e		
ics-aks-qa	Clientid= Msi	"principalId": "bae6a6b9-1593-4339-8a5e-94baac8653ab", "type": "SystemAssigned" "userAssignedIdentities": null	Kubelet: clientId": "eefcce8c-759c-45c1-b4ad-5158b01c1d30", "objectId": "c326f962-2b1a-4d1c-94f6-369248526176" "resourceId": "/subscriptions/5cd41c92-754a-486e-95ff-f1fc311c0fa2/resourcegroups/MC_ICS-iTalent-QA-RG_ics-aks-qa_eastus/providers/Microsoft.ManagedIdentity/userAssignedIdentities/ics-aks-qa-agentpool"
ics-italent-dev-aks	"clientId": "0e6b74b1-ca2f-440c-bdab-c5f93849704e" Objectid = 345f13fd-7518-481c-a79e-45862b83a562	Null	Null
ICS-MSFT-STG	Clientid= msi	"principalId": "8fe2646f-0cf5-4580-a97d-ed20b7ab0525" type": "SystemAssigned" serAssignedIdentities": null Objectid = 8fe2646f-0cf5-4580-a97d-ed20b7ab0525	Kubelet: clientId": "6340bf4a-7f45-4828-8501-d46277068de8" "objectId": "f186a8a6-1994-491f-b5bb-f0c7d4807134" resourceId": "/subscriptions/a3156474-eead-4d25-ad9d-952bb6f94ed7/resourcegroups/MC_ICSyndicate_ICS-MSFT-STG_westus3/providers/Microsoft.ManagedIdentity/userAssignedIdentities/ICS-MSFT-STG-agentpool"
PPFD-CLUSTER-STG	Clientid= msi	principalId": "2be1562f-fd9d-40ce-88b4-2931a08fbb91" type": "SystemAssigned", userAssignedIdentities": null Objectid = 2be1562f-fd9d-40ce-88b4-2931a08fbb91	Kubelet: clientId": "d15918ac-64a4-47c1-a7c7-067afb12ffdf" objectId": "94310377-7874-4c8b-ae94-57b5ac5256a2", resourceId": "/subscriptions/b344665e-dbe2-4b8c-b187-6c04a43e6bcf/resourcegroups/MC_PPFD-RG-STG_PPFD-CLUSTER-STG_westus3/providers/Microsoft.ManagedIdentity/userAssignedIdentities/PPFD-CLUSTER-STG-agentpool"
Ics-italent-prod-aks	Clientid= msi	principalId": "667622ca-a2d1-476e-b613-8e8c8ba11b11" Objectid= 667622ca-a2d1-476e-b613-8e8c8ba11b11	

Get Objectid of AAD using

servicePrincipalProfile.clientid

Objectid and principalid(clientid) is same for MSI cluster.

The "clientid=msi" syntax in Azure AKS refers to using a managed service identity (MSI) for authentication purposes. An MSI is a feature in Azure Active Directory (AD) that allows an Azure resource to act as its own identity when requesting access to other resources. In the context of AKS, the client ID refers to the MSI identity associated with the AKS cluster, which is used to authenticate with other Azure services.

By using an MSI, you can avoid the need to store secrets or certificates within your AKS cluster, and instead rely on Azure AD to manage the authentication process. This can simplify the deployment and management of your AKS cluster, and make it easier to secure access to other Azure services.

To use an MSI with your AKS cluster, you'll need to create an MSI identity in Azure AD, and then configure your AKS cluster to use that identity. The exact steps for doing this will depend on your specific scenario and the tools you are using, but in general, you'll need to create an MSI identity in Azure AD, grant it the necessary permissions to access other Azure services, and then specify the client ID of the MSI identity when you create or update your AKS cluster.

```
az aks update-credentials \
   --resource-group ICS-iTalent-Dev-RG  \
   --name ics-italent-dev-aks \
   --reset-service-principal \
   --service-principal "0e6b74b1-ca2f-440c-bdab-c5f93849704" \
   -- client-secret
```

Alerts for AAD secret   using API:

```
import requests
import json
```

```
# Replace with your tenant ID, client ID, client secret, and service principal object ID
tenant_id = 'your-tenant-id'
client_id = 'your-client-id'
client_secret = 'your-client-secret'
object_id = 'your-service-principal-object-id'

# Authenticate and obtain a token using the client credentials flow
auth_url = 'https://login.microsoftonline.com/{}/oauth2/token'.format(tenant_id)
auth_data = {
    'grant_type': 'client_credentials',
    'client_id': client_id,
    'client_secret': client_secret,
    'resource': 'https://graph.windows.net'
}
response = requests.post(auth_url, data=auth_data)
token = response.json()['access_token']

# Send a request to the Graph API to retrieve the service principal
headers = {
    'Authorization': 'Bearer {}'.format(token),
    'Content-Type': 'application/json'
}
url = 'https://graph.windows.net/{}/servicePrincipals/{}'.format(tenant_id, object_id)
response = requests.get(url, headers=headers)
data = response.json()

# Extract the expiration time of the first secret from the response data
secrets = data.get('passwordCredentials')
if secrets:
    expiration_time = secrets[0].get('endDate')
    print('The first secret expires at: {}'.format(expiration_time))
```

```
from azure.devops.connection import Connection
from msrest.authentication import BasicAuthentication
from azure.graphrbac import GraphRbacManagementClient
from azure.common.credentials import ServicePrincipalCredentials

# Replace with your Azure AD tenant ID, client ID, client secret, and service principal object ID
tenant_id = 'your-tenant-id'
client_id = 'your-client-id'
client_secret = 'your-client-secret'
object_id = 'your-service-principal-object-id'

# Authenticate using a service principal and obtain a bearer token
credentials = ServicePrincipalCredentials(
    client_id=client_id,
    secret=client_secret,
    tenant=tenant_id
)

# Connect to Azure DevOps using the Python client library
connection = Connection(base_url='https://dev.azure.com/your-organization', creds=credentials)

# Use the Azure AD authentication helper to obtain an access token for the Graph API
aad_helper = connection.get_client('azure.devops.v6_0.aadhelper.AadHelper')
access_token = aad_helper.get_graph_access_token()

# Create a GraphRbacManagementClient object using the access token
graph_client = GraphRbacManagementClient(
    credentials=credentials,
    tenant_id=tenant_id,
    base_url='https://graph.windows.net',
    access_token={'access_token': access_token}
)

# Use the Graph API to retrieve the service principal
service_principal = graph_client.service_principals.get(object_id)

# Extract the expiration time of the first secret from the service principal object
secrets = service_principal.password_credentials
if secrets:
    expiration_time = secrets[0].end_date.isoformat()
    print('The first secret expires at: {}'.format(expiration_time))
```

```
import requests
import json
import datetime

# Replace with your Azure AD application ID and secret
app_id = 'your-application-id'
app_secret = 'your-application-secret'
```

```
# Replace with the ID of the secret you want to retrieve
secret_id = 'your-secret-id'

# Replace with your tenant ID
tenant_id = 'your-tenant-id'

# Obtain an access token for the Microsoft Graph API
token_url = f'https://login.microsoftonline.com/{tenant_id}/oauth2/v2.0/token'
payload = {
   'grant_type': 'client_credentials',
   'client_id': app_id,
   'client_secret': app_secret,
   'scope': 'https://graph.microsoft.com/.default'
}
response = requests.post(token_url, data=payload)
access_token = response.json()['access_token']

# Retrieve the secret from the Microsoft Graph API
secret_url = f'https://graph.microsoft.com/v1.0/applications/{app_id}/passwordCredentials/{secret_id}'
headers = {
   'Authorization': f'Bearer {access_token}',
   'Content-Type': 'application/json'
}
response = requests.get(secret_url, headers=headers)
secret = response.json()

# Extract the expiration time of the secret
expiration_time = secret['endDateTime']
expiration_time = datetime.datetime.strptime(expiration_time, '%Y-%m-%dT%H:%M:%S.%fZ').isoformat()
print(f'The secret expires at: {expiration_time}')
```

```
code': 'Authorization_RequestDenied', 'message': 'Insufficient privileges to complete the operation.
```

The "Authorization_RequestDenied" error with the message "Insufficient privileges to complete the operation" indicates that the user or application making the request does not have the necessary permissions to perform the requested operation.

To resolve this issue, you need to ensure that the user or application has been granted the necessary permissions to access the required resource. Specifically, you need to check the permissions associated with the Azure AD application registration that is being used to make the request.

To retrieve password credentials, you will need to have one of the following application permissions granted to your application:

- Application.ReadWrite.OwnedBy
- Application.ReadWrite.All

If you are trying to retrieve password credentials for another user's application, you will need to have one of the following delegated permissions granted to your application:

- Application.ReadWrite.OwnedBy
- Application.ReadWrite.All
- Directory.Read.All
- Directory.ReadWrite.All

You can check and manage these permissions in the "API permissions" tab of your Azure AD application registration.

Azure AAD :

Appid:
07dd855d-e370-4a00-9fd7-4c9121292131   80fa2766-41f1-44e5-bec9-d54aa03362c2
0e6b74b1-ca2f-440c-bdab-c5f93849704e   e9a8de64-29ac-46f0-9e88-28018fa6145e

Note:
Yes, both the Standard_DS2_v2 and Standard_DS3_v2 virtual machine (VM) sizes belong to the same family in Azure, which is the Dv2-series.

Operation could not be completed as it results in exceeding approved Total Regional Cores quota. Additional details - Deployment Model: Resource Manager, Location: eastus, Current Limit: 24, Current Usage: 16, Additional Required: 12, (Minimum) New Limit Required: 28. Submit a request for Quota increase at https://aka.ms/ProdportalCRP/#blade/Microsoft_Azure_Capacity/UsageAndQuota.ReactView/Parameters/%7B%22subscriptionId%22:%22ea490839-c54c-4ba8-8160-45d78dcf94a7%22,%22command%22:%22openQuotaApprovalBlade%22,%22quotas%22:[%7B%22location%22:%22eastus%22,%22providerId%22:%22Microsoft.Compute%22,%22resourceName%22:%22cores%22,%22quotaRequest%22:%7B%22properties%22:%7B%22limit%22:28,%22unit%22:%22Count%22,%22name%22:%7B%22value%22:%22cores%22%7D%7D%7D%7D]%7D by specifying parameters listed in the ‘Details’ section for deployment to succeed. Please read more about quota limits at https://docs.microsoft.com/en-us/azure/azure-supportability/regional-quota-requests

```
az aks nodepool add --name ephemeral --cluster-name myAKSCluster --resource-group
myResourceGroup -s Standard_DS3_v2 --node-osdisk-type Ephemeral
```

```
(PreconditionFailed) Provisioning of resource(s) for Agent Pool arpnodepool failed. Error: {
  "code": "InvalidTemplateDeployment",
  "message": "The template deployment '5e0a1521-96b9-4aa0-8d64-e255d4d0dab4' is not valid
according to the validation procedure. The tracking id is '59b9acbf-3269-4b73-9eb3-0424e51067bc'. See
inner errors for details.",
  "details": [
   {
    "code": "QuotaExceeded",
    "message": "Operation could not be completed as it results in exceeding approved
standardDSv2Family Cores quota. Additional details - Deployment Model: Resource Manager, Location:
eastus, Current Limit: 20, Current Usage: 12, Additional Required: 12, (Minimum) New Limit Required:
24. Submit a request for Quota increase at https://aka.ms/ProdportalCRP/
#blade/Microsoft_Azure_Capacity/UsageAndQuota.ReactView/Parameters/%7B%22subscriptionId%
22:%22ea490839-c54c-4ba8-8160-45d78dcf94a7%22,%22command%22:%
22openQuotaApprovalBlade%22,%22quotas%22:[%7B%22location%22:%22eastus%22,%22providerId%
22:%22Microsoft.Compute%22,%22resourceName%22:%22standardDSv2Family%22,%
22quotaRequest%22:%7B%22properties%22:%7B%22limit%22:24,%22unit%22:%22Count%22,%
22name%22:%7B%22value%22:%22standardDSv2Family%22%7D%7D%7D%7D]%7D by specifying
parameters listed in the ‘Details’ section for deployment to succeed. Please read more about quota
limits at https://docs.microsoft.com/en-us/azure/azure-supportability/per-vm-quota-requests"
   }
  ]
 }
Code: PreconditionFailed
Message: Provisioning of resource(s) for Agent Pool arpnodepool failed. Error: {
  "code": "InvalidTemplateDeployment",
  "message": "The template deployment '5e0a1521-96b9-4aa0-8d64-e255d4d0dab4' is not valid
according to the validation procedure. The tracking id is '59b9acbf-3269-4b73-9eb3-0424e51067bc'. See
inner errors for details.",
  "details": [
   {
    "code": "QuotaExceeded",
    "message": "Operation could not be completed as it results in exceeding approved
standardDSv2Family Cores quota. Additional details - Deployment Model: Resource Manager, Location:
eastus, Current Limit: 20, Current Usage: 12, Additional Required: 12, (Minimum) New Limit Required:
24. Submit a request for Quota increase at https://aka.ms/ProdportalCRP/
#blade/Microsoft_Azure_Capacity/UsageAndQuota.ReactView/Parameters/%7B%22subscriptionId%
22:%22ea490839-c54c-4ba8-8160-45d78dcf94a7%22,%22command%22:%
22openQuotaApprovalBlade%22,%22quotas%22:[%7B%22location%22:%22eastus%22,%22providerId%
22:%22Microsoft.Compute%22,%22resourceName%22:%22standardDSv2Family%22,%
22quotaRequest%22:%7B%22properties%22:%7B%22limit%22:24,%22unit%22:%22Count%22,%
22name%22:%7B%22value%22:%22standardDSv2Family%22%7D%7D%7D%7D]%7D by specifying
parameters listed in the ‘Details’ section for deployment to succeed. Please read more about quota
limits at https://docs.microsoft.com/en-us/azure/azure-supportability/per-vm-quota-requests"
   }
  ]
 }
```

AARP Througput

Size   DS3_v2
General purpose
  vcpu 4
  RAM   14
Data Disks 16
Max IOPS   12800
 Temp Storage 28
Permium disk Supported
Cost per month $213.89

```
az aks nodepool add --name icssmartconx  --cluster-name ics-aks-qa --resource-group ICS-iTalent-QA-RG -s  Standard_D4ads_v5  --node-osdisk-type Ephemeral  --node-count 1 --zone 1, 2,
3 --mode User
az aks nodepool add --name aarpnodepool --cluster-name ics-italent-dev-aks --resource-group ICS-iTalent-Dev-RG -s Standard_DS3_v2 --node-osdisk-type Ephemeral  --node-count 1

az aks nodepool add --name aarpnodepool  --cluster-name ics-aks-qa --resource-group ICS-iTalent-QA-RG -s  Standard_D8s_v3  --node-osdisk-type Ephemeral  --node-count 1 --zone 1, 2,
3 --mode User
```

Previous Size: icssmartconx   Standard_D4s_v3
Updated with icssmartconx   Standard_D4ads_v5

--nodepool-name can contain at most 12 characters

```
az aks scale --nodepool-name aarpnodepool --name ics-italent-dev-aks --resource-group ICS-iTalent-Dev-RG --node-count 1
```

```
{
  "availabilityZones": null,
  "count": 3,
  "creationData": null,
  "currentOrchestratorVersion": "1.24.6",
  "enableAutoScaling": false,
  "enableEncryptionAtHost": false,
  "enableFips": false,
  "enableNodePublicIp": false,
  "enableUltraSsd": false,
  "gpuInstanceProfile": null,
  "hostGroupId": null,
  "id": "/subscriptions/ea490839-c54c-4ba8-8160-45d78dcf94a7/resourcegroups/ICS-iTalent-Dev-RG/providers/Microsoft.ContainerService/managedClusters/ics-italent-dev-
aks/agentPools/aarpnodepool",
  "kubeletConfig": null,
  "kubeletDiskType": "OS",
  "linuxOsConfig": null,
  "maxCount": null,
  "maxPods": 30,
  "minCount": null,
  "mode": "User",
  "name": "aarpnodepool",
  "nodeImageVersion": "AKSUbuntu-1804gen2containerd-2023.02.15",
  "nodeLabels": null,
  "nodePublicIpPrefixId": null,
  "nodeTaints": null,
  "orchestratorVersion": "1.24.6",
  "osDiskSizeGb": 128,
  "osDiskType": "Ephemeral",
  "osSku": "Ubuntu",
  "osType": "Linux",
  "podSubnetId": null,
  "powerState": {
    "code": "Running"
  },
  "provisioningState": "Succeeded",
  "proximityPlacementGroupId": null,
  "resourceGroup": "ICS-iTalent-Dev-RG",
  "scaleDownMode": "Delete",
  "scaleSetEvictionPolicy": null,
  "scaleSetPriority": null,
  "spotMaxPrice": null,
  "tags": null,
  "type": "Microsoft.ContainerService/managedClusters/agentPools",
  "typePropertiesType": "VirtualMachineScaleSets",
  "upgradeSettings": {
    "maxSurge": null
  },
  "vmSize": "Standard_DS3_v2",
  "vnetSubnetId": "/subscriptions/ea490839-c54c-4ba8-8160-45d78dcf94a7/resourceGroups/ICS-iTalent-Dev-RG/providers/Microsoft.Network/virtualNetworks/ICS-iTalent-Dev-RG-
vnet/subnets/default",
  "workloadRuntime": null
}
```

eyJraWQiOiJmYmJRbmxHaGRqM1dzQ2pKamdlZE5hZDFxa19PcXhFMGxTVG1oUWRvSExJIiwiYWxnIjoiUlMyNTYifQ.eyJ2ZXIiOjEsImp0aSI6IkFULmdCcy1reWtlbDNZeWI2aTEzdmpsOWR2TzBudl
92anZOZ2hKMUUwZHlSMkkiLCJpc3MiOiJodHRwczovL2lkLXBpLmFhcnAub3JnL29hdXRoMi9hdXNhbHRuZHRrc1drajlkYjBoNyIsImF1ZCI6Imh0dHBzOi8vc2VydmljZXMuc2hhcmUtcGkuYWFycC5
vcmcvYXBwbGljYXRpb25zL0NvcmVBcGkvdXNlciIsImlhdCI6MTY3OTAyODY5NSwiZXhwIjoxNjc5MDcxODk1LCJjaWQiOiIwb2ExZTVld293Zk1nb2dlZDBoOCIsInVpZCI6IjAwdTE3em45ZTR6VTNLbj
A1MGg4Iiwic2NwIjpbImJtaSIsImJ1aSJdLCJhdXRoX3RpbWUiOjE2Nzg5NDU2NTYsInN1YiI6IjAwdTE3em45ZTR6VTNLbjA1MGg4IiwiZmVkZXJhdGVkSWQiOiJLT05YMjQyMzg0MjE3NzkyMzcwOTI
wNTgzIn0.hMj9YXVSnvJNcdnHPTpxXqLcYHa2QMmVQdpBul0mHI1RWriH4cyFSkLBNYSJiw5VbjwKPTHJOfkqSi9SjeQrCQAI5KTYXnBcHnqu4a8i5eXO_X7c75uPs7flpGjSR4nMS6TOmrrGZMu9sb
mkrrq3_I93uX-l0buQmareRc3_sTyLpCQ1BKHZufQFZOMwr4sXcaE_ooAeOB5O5d1TrHVtNuvKdgzbqkjlKRQ657XevcjJo_NRkhKeK3Su_ICir9AYyankkEUxpbG-
js_YiM2a19fPoqLuKfGBWkCdcMt3V-DcyEh2DnWTRGObn1kfvGmAe5hYFK2EeEjJjROg5fGj2Q

eyJraWQiOiJmYmJRbmxHaGRqM1dzQ2pKamdlZE5hZDFxa19PcXhFMGxTVG1oUWRvSExJIiwiYWxnIjoiUlMyNTYifQ.eyJ2ZXIiOjEsImp0aSI6IkFULmdCcy1reWtlbDNZeWI2aTEzdmpsOWR2TzBudl
92anZOZ2hKMUUwZHlSMkkiLCJpc3MiOiJodHRwczovL2lkLXBpLmFhcnAub3JnL29hdXRoMi9hdXNhbHRuZHRrc1drajlkYjBoNyIsImF1ZCI6Imh0dHBzOi8vc2VydmljZXMuc2hhcmUtcGkuYWFycC5
vcmcvYXBwbGljYXRpb25zL0NvcmVBcGkvdXNlciIsImlhdCI6MTY3OTAyODY5NSwiZXhwIjoxNjc5MDcxODk1LCJjaWQiOiIwb2ExZTVld293Zk1nb2dlZDBoOCIsInVpZCI6IjAwdTE3em45ZTR6VTNLbj
A1MGg4Iiwic2NwIjpbImJtaSIsImJ1aSJdLCJhdXRoX3RpbWUiOjE2Nzg5NDU2NTYsInN1YiI6IjAwdTE3em45ZTR6VTNLbjA1MGg4IiwiZmVkZXJhdGVkSWQiOiJLT05YMjQyMzg0MjE3NzkyMzcwOTI
wNTgzIn0

Song theme token:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2ZXIiOjEsImp0aSI6IkFULmdCcy1reWtlbDNZeWI2aTEzdmpsOWR2TzBudl92anZOZ2hKMUUwZHlSMkkiLCJpc3MiOiJodHRwczovL2lkLXBpLmFhcnAub
3JnL29hdXRoMi9hdXNhbHRuZHRrc1drajlkYjBoNyIsImF1ZCI6Imh0dHBzOi8vc2VydmljZXMuc2hhcmUtcGkuYWFycC5vcmcvYXBwbGljYXRpb25zL0NvcmVBcGkvdXNlciIsImlhdCI6MTY3OTAyODY
5NSwiZXhwIjoxNjc5MDcxODk1LCJjaWQiOiIwb2ExZTVld293Zk1nb2dlZDBoOCIsInVpZCI6IjAwdTE3em45ZTR6VTNLbjA1MGg4Iiwic2NwIjpbImJtaSIsImJ1aSJdLCJhdXRoX3RpbWUiOjE2Nzg5NDU
2NTYsInN1YiI6IjAwdTE3em45ZTR6VTNLbjA1MGg4IiwiZmVkZXJhdGVkSWQiOiJLT05YMjQyMzg0MjE3NzkyMzcwOTIwNTgzIn0.URAe4Py-Tu-i199X2qUyqeKXRrOl6bSMgrSrU8q1ML8

About Azure AAD authentication:

https://learn.microsoft.com/en-us/azure/active-directory/develop/reply-url

ITalent Tenent
Resource Quota:
Microsoft Partner Network
Standard DS2_V2 VCPUs used: 4 out of 16 used cluster DEV

Key Vaults Download private keys:

https://learn.microsoft.com/en-us/azure/key-vault/certificates/how-to-export-certificate?tabs=azure-cli

Azure DNS for Kubernetes Cluster:

https://www.thorsten-hans.com/external-dns-azure-kubernetes-service-azure-dns/

Caution: There is a limitation in Helm regarding values being provided via `--set`. Helm can't deal with commas (`,`) as part of a value in `--set`. Before invoking `helm install`, consider checking if your `SP_CLIENT_SECRET` contains a comma (`echo $SP_CLIENT_SECRET`). If so, update the `SP_CLIENT_SECRET` variable and replace `,` with `\,`.

From <https://www.thorsten-hans.com/external-dns-azure-kubernetes-service-azure-dns/>

Azure App Service

WEBSITE_RUN_FROM_PACKAGE https://learn.microsoft.com/en-us/azure/app-service/deploy-run-package?source=recommendations

The `WEBSITE_RUN_FROM_PACKAGE` app setting enables running from a ZIP package. To set it, run the following command with Azure CLI.

```
az webapp config appsettings set --resource-group <group-name> --name <app-name> --settings
WEBSITE_RUN_FROM_PACKAGE="1"
```

`WEBSITE_RUN_FROM_PACKAGE="1"` lets you run your app from a ZIP package local to your app. You can also run from a remote package.

Using Remote ZIP URL

By passing SAS Token

```
az webapp config appsettings set --name <app-name> --resource-group <resource-group-name> --
settings
WEBSITE_RUN_FROM_PACKAGE="https://myblobstorage.blob.core.windows.net/content/SampleCore
MVCApp.zip?st=2018-02-13T09%3A48%3A00Z&se=2044-06-14T09%3A48%3A00Z&sp=rl&sv=
2017-04-17&sr=b&sig=bNrVrEFzRHQB17GFJ7boEanetyJ9DGwBSV8OM3Mdh%2FM%3D"
```

If you publish an updated package with the same name to Blob storage, you need to restart your app so that the updated package is loaded into App Service.

Access a package in Azure Blob Storage using a managed identity

By default, the app's system-assigned identity is used. If you wish to specify a user-assigned identity, you can set the `WEBSITE_RUN_FROM_PACKAGE_BLOB_MI_RESOURCE_ID` app setting to the resource ID of that identity. The setting can also accept `SystemAssigned` as a value, which is equivalent to omitting the setting.

To enable the package to be fetched using the identity:

1. Ensure that the blob is configured for private access.
2. Grant the identity the Storage Blob Data Reader role with scope over the package blob. See Assign an Azure role for access to blob data for details on creating the role assignment.
3. Set the `WEBSITE_RUN_FROM_PACKAGE` application setting to the blob URL of the package. This URL is usually of the form `https://{storage-account-`

name}.blob.core.windows.net/{container-name}/{path-to-package} or similar.

4. If you wish to specify a user-assigned identity, you can set the `WEBSITE_RUN_FROM_PACKAGE_BLOB_MI_RESOURCE_ID` app setting to the resource ID of that identity. The setting can also accept "SystemAssigned" as a value, although this is the same as omitting the setting altogether. A resource ID is a standard representation for a resource in Azure. For a user-assigned managed identity, that is going to be `/subscriptions/subid/resourcegroups/rg-name/providers/Microsoft.ManagedIdentity/userAssignedIdentities/identity-name`. The resource ID of a user-assigned managed identity can be obtained in the Settings -> Properties -> ID for the user assigned managed identity

To enable this setting, set `WEBSITE_RUN_FROM_PACKAGE`=1 or provide the URL of the ZIP file. There are several benefits to running directly from a package:

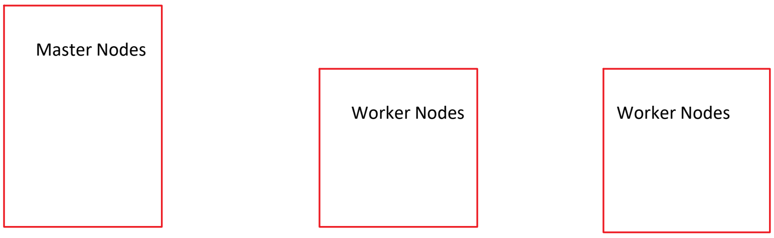
- Eliminates file lock conflicts between deployment and runtime.
- Ensures only full-deployed apps are running at any time.
- Can be deployed to a production app (with restart).
- Improves the performance of Azure Resource Manager deployments.
- May reduce cold-start times, particularly for JavaScript functions with large npm package trees.

From <https://learn.microsoft.com/en-us/azure/app-service/deploy-run-package?source=recommendations>

Startup.sh

```
#!/bin/sh

# Enter the source directory to make sure the script runs where the user expects
cd "/home/site/wwwroot"

export NODE_PATH=/usr/local/lib/node_modules:$NODE_PATH

if [ -z "$PORT" ]; then
    export PORT=8080
fi

echo "Found tar.gz based node_modules."
extractionCommand="tar -xzf node_modules.tar.gz -C /node_modules"
echo "Removing existing modules directory from root..."
rm -fr /node_modules
mkdir -p /node_modules
echo "Extracting modules..."
$extractionCommand

export NODE_PATH="/node_modules":$NODE_PATH
export PATH=/node_modules/.bin:$PATH

if [ -d node_modules ]; then
    mv -f node_modules _del_node_modules || true
fi

if [ -d /node_modules ]; then
    ln -sfn /node_modules ./node_modules
fi

echo "Done."
npm start
```

06 September 2022 12:29



For every pod we create, by default kubelet will attach service account of namespace as volume at /var/run/secrets/kubernetes.io/serviceaccount as a mount path.

Stateful Sets

Elastic search with 3 replicas

Metadata.name= es-cluster

Pod.metadata.name=es-cluster-0
Pod.metadata.name=es-cluster-1
Pod.metadata.name=es-cluster-2

Headless Service for elastic search

FOR EXAMPLE :

```
apiVersion: v1
kind: Service
metadata:
  name: head
spec:
  selector:
    app: nginx
  clusterIP: None
  ports:
    - port: 80
      targetPort: 80
```

Service.metadata.name=elasticsearch

STATEFULSET:

```
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: nginx
spec:
  serviceName: head
  replicas: 2
  selector:
    matchLabels:
        app: nginx
  template:
    metadata:
        name: nginx-pod
        labels:
          app: nginx
        namespace: default
    spec:
      hostname: appone
      subdomain: new
      containers:
        - name: cont
          image: nginx
          ports:
             - containerPort: 80
```

Kibana access elastic search DB

Hosts to point for elastic search DB

Svc.namespace.cluster.local

For Headless Service pointing selector labels of pods which contain hostname and subdomain fields in theirs specifications
Can be accessed with the FQDN i.e.., hostname.serviceName.namespace.svc.cluster.local

Because A or AAAA records are not created for Pod names, hostname is required for the Pod's A or AAAA record to be created. A Pod with no hostname but with subdomain will only create the A or AAAA record for the headless Service (default-subdomain.my-namespace.svc.cluster-domain.example), pointing to the Pod's IP address. Also, Pod needs to become ready in order to have a record unless publishNotReadyAddresses=True is set on the Service

STATEFULSETS   DNS DISCOVERY

Each Pod in a StatefulSet derives its hostname from the name of the StatefulSet and the ordinal of the Pod. The pattern for the constructed hostname is $(statefulset name)-$(ordinal). The example above will create three Pods named web-0,web-1,web-2. A StatefulSet can use a Headless Service to control the domain of its Pods. The domain managed by this Service takes the form: $(service name).$(namespace).svc.cluster.local, where "cluster.local" is the cluster domain. As each Pod is created, it gets a matching DNS subdomain, taking the form: $(podname).$(governing service domain), where the governing service is defined by the serviceName field on the StatefulSet.

Connecting Backend to Frontend

Deploying nginx server for frontend to connect with backend service using ClusterIP and DNS Discovery.

/etc/nginx/Conf.d/frontend.conf

```
upstream hello {
   server hello;
}

server {
   listen 80;

   location / {
      proxy_pass http://hello;
   }
}
```

Connecting to multiple cluster using same config file

Kubectl connect to Clusters through

--kubeconfig flag at kubectl command
KUBECONFIG env variable
~/.kube/config   path

```
Export KUBECONFIG=~/.kube/config:~/.kube/config_new
```

Adding USER to Kubernetes Cluster

Creating Certs for user

Creating private.key for a user

```
#   openssl genrsa  -out  user.key  2048(bit encryption)
```

Requesting CSR using private key

```
#  openssl  req  -new  -key user.key  -out  user.csr  -subj
"/CN=username/O=developers"
```

Signing the CSR using Authorized CA in our case Kubernetes Api-Server

```
#   openssl  x509  -req  -in user.csr  -CA=path to ca.crt  -Cakey= path to ca.key
 -CAcreateserial   -out user.crt   -days  365
```

Add user to cluster

Kubernetes knowns only the user name we defined at the time of certificates creation using CN name pointing to USERNAME

Adding user credentials to config

```
#  Kubectl config set-credentials username  ---client-certificate user.crt   -
client-key  user.key
```

Setting kubernetes context so that user can access to cluster

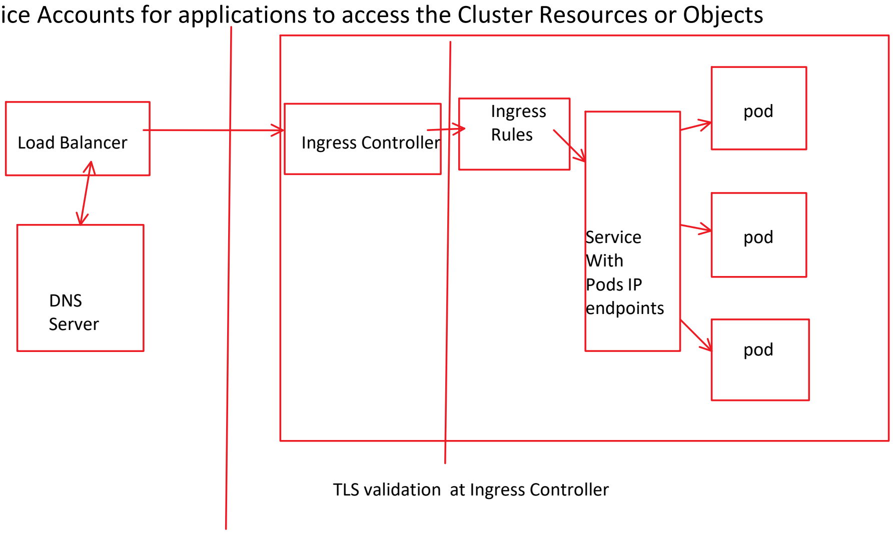
```
#  Kubectl set-context contextName --user username --cluster ClusterName
```

To set cluster entry

```
#   export KUBECONFIG=~/.kube/config_develop
```

```
#  kubectl config set-cluster   ClusterName   \
 -- server=https://masterIP:6443    --certificate-authority=path to ca.crt of
master    --embed-certs=true
```

We create Users in kubernetes for accessing kubernetes Cluster and also Service Accounts for applications to access the Cluster Resources or Objects



TLS validation at Ingress Controller

SSL Termination at Load Balancer level

Create a wildCard entry DNS for LoadBalancer Ip address
Example   *.domainName.com

Added ingress rules with subdomain or prefix hostnames
Will direct plain http request to backend service you want

For example
Incoming request from app.domain.com will validate SSL at Load Balancer Level and resolve to Ip address Using DNS server.
Load balancer will balance the incoming traffic to backends we define in our case it is Ingress-Controllers.
Ingress Controllers will resolve the hosts to matching rules defied in Ingress Objects and Divert request to backend service(ClusterIP).
From Service it will load balance in round-robin fashion the pods matching the selector labels defined.

Pods running on Nodes to be drained to other nodes
Need to change kubelet configuration on the drained nodes
Core-DNS need to rollout so no downtime for resloving existing domain
Then need to rollout the deployments so that kubelet will assign new domain

Static Public IP Address For Nginx Ingress:

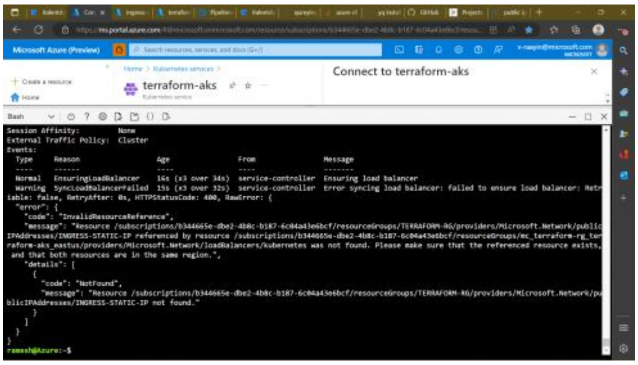
Create a Static Public IP Address in Resource Group where your cluster is created, best practice is to create in Node-Resource-Group.

Manually created Public IP Address won't be deleted when an associated service or cluster gets destroyed. Aslo make sure those IP addresses are in Disassociate state

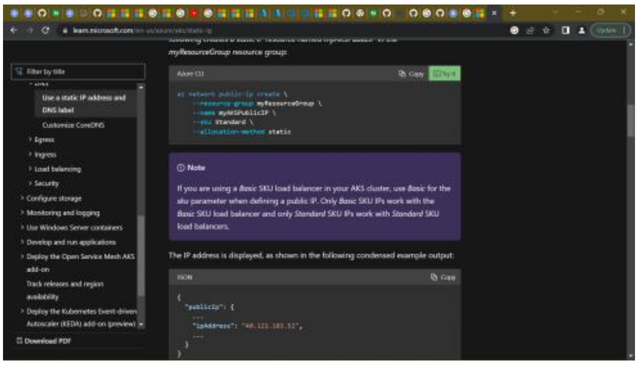
Note: Public IP Address created in Infrastructure Resource Group of Cluster will be No guraantee that it persists.

Make sure that AAD used for cluster creation should have "**Network Contributer**" Access Control over the Resource Group where your Public IP Address resides.

When you deploy a Kubernetes cluster in Azure, an Azure Load Balancer is automatically created to handle the incoming network traffic to the Kubernetes cluster. The load balancer is associated with a public IP address and can be used to expose services running in the cluster to the internet



```
Session Affinity:        None
External Traffic Policy:  Cluster
Events:
  Type     Reason                  Age                From                Message
  ----     ------                  ----               ----                -------
  Normal   EnsuringLoadBalancer    16s (x3 over 34s)  service-controller  Ensuring load balancer
  Warning  SyncLoadBalancerFailed  15s (x3 over 32s)  service-controller  Error syncing load balancer: failed to ensure load balancer: Retr
iable: false, RetryAfter: 0s, HTTPStatusCode: 400, RawError: {
  "error": {
    "code": "InvalidResourceReference",
    "message": "Resource /subscriptions/b344665e-dbe2-4b8c-b187-6c04a43e6bcf/resourceGroups/TERRAFORM-RG/providers/Microsoft.Network/public
IPAddresses/INGRESS-STATIC-IP referenced by resource /subscriptions/b344665e-dbe2-4b8c-b187-6c04a43e6bcf/resourceGroups/mc_terraform-rg_ter
raform-aks_eastus/providers/Microsoft.Network/loadBalancers/kubernetes was not found. Please make sure that the referenced resource exists,
 and that both resources are in the same region.",
    "details": [
      {
        "code": "NotFound",
        "message": "Resource /subscriptions/b344665e-dbe2-4b8c-b187-6c04a43e6bcf/resourceGroups/TERRAFORM-RG/providers/Microsoft.Network/pu
blicIPAddresses/INGRESS-STATIC-IP not found."
      }
    ]
  }
}
ramesh@Azure:~$
```


Filter by title
Use a static IP address and DNS label
Customize CoreDNS
Egress
Ingress
Load balancing
Security
Configure storage
Monitoring and logging
Use Windows Server containers
Develop and run applications
Deploy the Open Service Mesh AKS add-on
Track releases and region availability
Deploy the Kubernetes Event-driven Autoscaler (KEDA) add-on (preview)
Download PDF
Azure CLI
Copy
Try it
JSON
Copy

myResourceGroup resource group:

```
az network public-ip create \
    --resource-group myResourceGroup \
    --name myAKSPublicIP \
    --sku Standard \
    --allocation-method static
```

Note

If you are using a *Basic* SKU load balancer in your AKS cluster, use *Basic* for the sku parameter when defining a public IP. Only *Basic* SKU IPs work with the *Basic* SKU load balancer and only *Standard* SKU IPs work with *Standard* SKU load balancers.

The IP address is displayed, as shown in the following condensed example output:

```
{
  "publicIp": {
    ...
    "ipAddress": "40.121.183.52",
    ...
  }
}
```

Note: Matching SKUs are required for load balancer and public IP resources. You can't have a mixture of basic SKU resources and standard SKU resources. You can't attach standalone virtual machines, virtual machines in an availability set resource, or a virtual machine scale set resources to both SKUs simultaneously. New designs should consider using Standard SKU resources. For more information about a standard load balancer, see Standard Load Balancer.

From <https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses>

- The Global Tier allows a public IP address to be used with cross-region load balancers.

From <https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses>

The SKU of the virtual machine's public IP address must match the public IP SKU of Azure public load balancer when added to the backend pool of the load balancer

From <https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-deploy-static-pip-arm-portal>

If you customized your outbound IP, make sure your cluster identity has permissions to both the outbound public IP and the inbound public IP.

From <https://learn.microsoft.com/en-us/azure/aks/static-ip>

https://learn.microsoft.com/en-us/azure/aks/static-ip

Alternatively, you can create an IP address in a different resource group, which you can manage separately from your AKS cluster. If you create an IP address in a different resource group, ensure the following are true:

- The cluster identity used by the AKS cluster has delegated permissions to the resource group, such as *Network Contributor*.
- Add the `--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-resource-group"="<RESOURCE_GROUP>"` parameter. Replace `<RESOURCE_GROUP>` with the name of the resource group where the IP address resides.

From <https://learn.microsoft.com/en-us/azure/aks/ingress-tls?tabs=azure-cli>

Azure Load Balancer is available in two SKUs: *Basic* and *Standard*. The *Standard* SKU is used by default when you create an AKS cluster. The *Standard* SKU gives you access to added functionality, such as a larger backend pool, multiple node pools, Availability Zones, and is secure by default. It's the recommended load balancer SKU for AKS.

From <https://learn.microsoft.com/en-us/azure/aks/load-balancer-standard>

The outbound type defines the egress method for a cluster and defaults to type `LoadBalancer`.

From <https://learn.microsoft.com/en-us/azure/aks/load-balancer-standard>

Persistent Storage(PV) highly available:
SKU(StandardSSD_LRS)
max_share=0

Note: Each domain name label created must be unique within its Azure location.

From <https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses>

Persistent Volume by default it is created based on the spec attached to its storage class.
By default it resides on Node Resource Group and same location as the cluster.
PV will be created on the same zone as node for the first time it scheduled.

API-SERVER: https://ics-italent-dev-aks-dns-bcfe6c15.hcp.eastus.azmk8s.io:443

DNS_Prefix: ics-italent-dev-aks-dns

Points to be Noted:

when cluster nodes are running in specific zones without zone redundant i.e., availability zones is not set to 3. In this scenario Disk Created in one Zone cannot be attached to other zone unless both zones are matched.

Load Balancer Routing Architecture

When pods gets shifted to other Nodes, we might come across the "Multi-Attach Volume Error" means volume is already attached to a Node so it cannot attach to other node concurrently.

Frontend IP Configuration:

Solution(Reference):

1. Add your Public IP Address to the Frontend Configuration.

The disk we create should consists of "max_share" parametes set to more than "1", so that disk concurrently gets attached

You can choose to route traffic to the virtual machines in the backend pool using a different port than the one clients use to communicate with the load balancer.
Best Practices:
Without Floating IP, Azure exposes a traditional load balancing IP address mapping scheme for ease of use (the VM instances' IP). Enabling Floating IP changes the IP address mapping to the Frontend IP of the load balancer to allow for additional flexibility

Backend Pools:

1. Make Sure your Worker Nodes are added as Backend Pool with InBound and OutBound Rules Configured.
2. A backend Pool can contains Resource from one Vnet
3. Select NIC (Network Interface Card) as a Backend Pool Configuration.
4. Make sure Virtual Machines(Nodes) are in same location as LoadBalancer and VNET.

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Health Probes:

Health probes are used to check the status of a backend pool instance. If the health probe fails to get a response from a backend instance then no new connections will be sent to that backend instance until the health probe succeeds again.

For TCP ports do need to provide paths

1. Configure Health Probes for the Backend port(3000-32567) with HTTP and HTTPS as Protocols, also add "/healthz" path so that it notifies load balancer to divert traffic to live connections.

Load Balancing Rules:

1. Add Fronted IP and Backend Pool with Procotcol TCP, also add port and Backend Port same as exposed port of Kubenetes service.
2. Add Health Probe associated to port, enable TCP Reset and Floating IP .

Inbound NAT Rules:

if you are looking to do DNS based global routing and do not have requirements for Transport Layer Security (TLS) protocol termination ("SSL offload"), per-HTTP/HTTPS request or application-layer processing, review Traffic Manager.

- If you want to load balance between your servers in a region at the application layer, review Application Gateway.

Commads:

To list pods with specfic to its name(metadata.name):

```
kubectl get pods --no-headers -o custom-columns=":metadata.name" -n syndication
```

```
cat webhook.key | base64 | tr -d '\n'
```

Issues:

```
Error from server (BadRequest): error when creating "test-valida
the provided object does not match the namespace sent on the r
```

Admission Controller Webhooks:

Reference link Dynamic Admission Control | Kubernetes

1. ValidatingWebhookConfiguration
2. MutatingWebhookConfiguration

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  name: "pod-policy.example.com"
webhooks:
- name: "pod-policy.example.com"
  rules:
  - apiGroups:   [""]
    apiVersions: ["v1"]
    operations:  ["CREATE"]
    resources:   ["pods"]
    scope:       "Namespaced"
  clientConfig:
    service:
      namespace: "example-namespace"
      name: "example-service"
    caBundle: <CA_BUNDLE>
  admissionReviewVersions: ["v1"]
  sideEffects: None
  timeoutSeconds: 5
```

When an API server receives a request that matches one of the rules, the API server sends an admissionReview request to webhook as specified in the clientConfig

Cron Jobs:

```
Schedule: minutes hours day month  week
jobTemplate:
   spec:
     template:
        containers:
           - name: sample
             image: busybox
            command:
               - /bin/bash
              - c
             - echo Hello world
           imagePullyPolicy: ifNotPresent
        restartPolicy: onFailure
Backofflimit:
concurrencyPolicy:
successfulJobsHistoryLimit:
failedJobsHistoryLimit:
startingDeadlineSeconds:
```

Logger Test:

Deployed Two Replicas of Pods which prints their hostname for every 30s

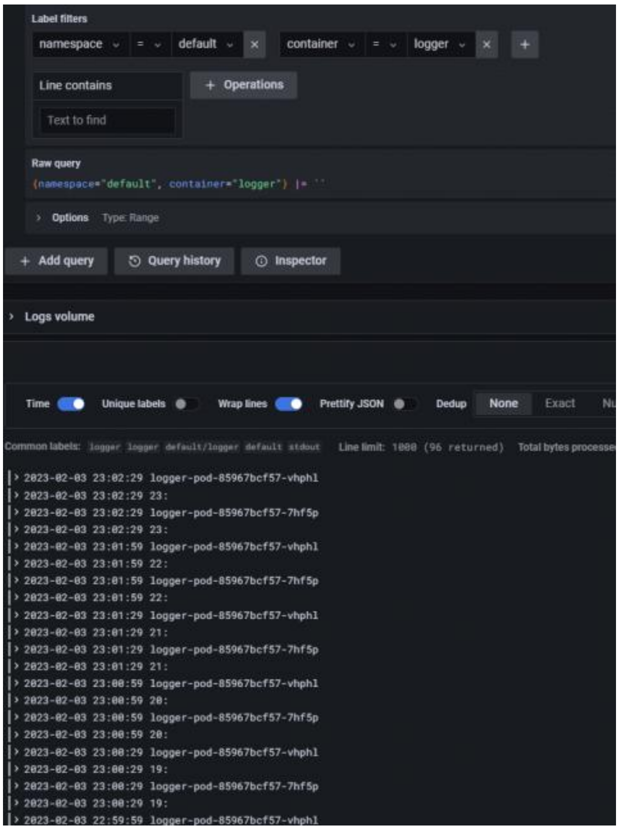
Basically we get logs from specific pods using pod names and also using container name we can get logs of two pods at once.

Note: Pods have scheduled into different Node

Reference yaml:

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: logger-pod
spec:
  replicas: 2
  selector:
    matchLabels:
      app: logger
  template:
    metadata:
      labels:
        app: logger
    spec:
      containers:
      - name: logger
        image: busybox
        args: [/bin/sh, -c, 'i=0; while true; do echo "$i:"; hostname; i=
$((i+1)); sleep 30; done']
```

Visualized in Grafana:



namespace = default, container = logger

```
{namespace="default", container="logger"} |= ``
```

Common labels: logger logger default/logger default stdout Line limit: 1000 (96 returned) Total bytes processe

```
2023-02-03 23:02:29 logger-pod-85967bcf57-vhphl
2023-02-03 23:02:29 23:
2023-02-03 23:02:29 logger-pod-85967bcf57-7hf5p
2023-02-03 23:02:29 23:
2023-02-03 23:01:59 logger-pod-85967bcf57-vhphl
2023-02-03 23:01:59 22:
2023-02-03 23:01:59 logger-pod-85967bcf57-7hf5p
2023-02-03 23:01:59 22:
2023-02-03 23:01:29 logger-pod-85967bcf57-vhphl
2023-02-03 23:01:29 21:
2023-02-03 23:01:29 logger-pod-85967bcf57-7hf5p
2023-02-03 23:01:29 21:
2023-02-03 23:00:59 logger-pod-85967bcf57-vhphl
2023-02-03 23:00:59 20:
2023-02-03 23:00:59 logger-pod-85967bcf57-7hf5p
2023-02-03 23:00:59 20:
2023-02-03 23:00:29 logger-pod-85967bcf57-vhphl
2023-02-03 23:00:29 19:
2023-02-03 23:00:29 logger-pod-85967bcf57-7hf5p
2023-02-03 23:00:29 19:
2023-02-03 22:59:59 logger-pod-85967bcf57-vhphl
```

CPU and Memory Resources:

- The Container has no upper bound on the CPU resources it can use. The Container could use all of the CPU resources available on the Node where it is running.
- The Container is running in a namespace that has a default CPU limit, and the Container is automatically assigned the default limit. Cluster administrators can use a LimitRange to specify a default value for the CPU limit.

Memory:

Memory requests and limits are associated with Containers, but it is useful to think of a Pod as having a memory request and limit. The memory request for the Pod is the sum of the memory requests for all the Containers in the Pod. Likewise, the memory limit for the Pod is the sum of the limits of all the Containers in the Pod.

Pod scheduling is based on requests. A Pod is scheduled to run on a Node only if the Node has enough available memory to satisfy the Pod's memory request.

If you do not specify a memory limit

- The Container has no upper bound on the amount of memory it uses. The Container could use all of the memory available on the Node where it is running which in turn could invoke the OOM Killer. Further, in case of an OOM Kill, a container with no resource limits will have a greater chance of being killed.

The Container is running in a namespace that has a default memory limit, and the Container is automatically assigned the default limit. Cluster administrators can use a LimitRange to specify a default value for the memory limit

```
az ad sp create-for-rbac --name <service_principal_name> --skip-assignment
```

```
kubectl create clusterrolebinding cluster-admin-binding --clusterrole=cluster-admin --
user=<service_principal_client_id>
```

```
az aks update-credentials --resource-group <resource_group_name> --name <aks_cluster_name> --
reset-service-principal --service-principal <service_principal_client_id> --client-secret
<service_principal_client_secret>
```

```
az aks update --resource-group <resource_group_name> --name <aks_cluster_name> --enable-aad
```

Managed identities are the recommended way to authenticate with other resources in Azure, and is the default authentication method for your AKS cluster

From <https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli>

MSFT_STG kubernetes.azure.com/kubelet-identity-client-id:6340bf4a-7f45-4828-8501-d46277068de8

ICS_STG kubernetes.azure.com/kubelet-identity-client-id=eefcce8c-759c-45c1-b4ad-5158b01c1d30

To list Object id or client id of AAD Attached to cluster:

```
az aks list --query [].identity
```

```
WARNING: version difference between client (1.23) and server (1.25) exceeds the supported minor
version skew of +/-1
```

Azsecpack:

```
  File "/usr/local/lib/python3.9/site-packages/azure/keyvault/secrets/_generated/v7_2/operations/
_key_vault_client_operations.py", line 292, in get_secret
    raise HttpResponseError(response=response, model=error)
azure.core.exceptions.HttpResponseError: (Forbidden) The user, group or application
'appid=d15918ac-64a4-47c1-a7c7-067afb12ffdf;oid=94310377-7874-4c8b-
ae94-57b5ac5256a2;iss=https://sts.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/' does not
```

```
have secrets get permission on key vault 'icsbagstagesecpack;location=westus2'. For help resolving this
issue, please see https://go.microsoft.com/fwlink/?linkid=2125287
Code: Forbidden
Message: The user, group or application 'appid=d15918ac-64a4-47c1-a7c7-067afb12ffdf;oid=
94310377-7874-4c8b-
ae94-57b5ac5256a2;iss=https://sts.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/' does not
have secrets get permission on key vault 'icsbagstagesecpack;location=westus2'. For help resolving this
issue, please see https://go.microsoft.com/fwlink/?linkid=2125287
Inner error: {
    "code": "AccessDenied"
}
```

Security Context:

By default, Kubernetes recursively changes ownership and permissions for the contents of each volume to match the fsGroup specified in a Pod's securityContext when that volume is mounted. For large volumes, checking and changing ownership and permissions can take a lot of time, slowing Pod startup. You can use the fsGroupChangePolicy field inside a securityContext to control the way that Kubernetes checks and manages ownership and permissions for a volume.

From <https://kubernetes.io/docs/tasks/configure-pod-container/security-context/>

To specify security settings for a Container, include the securityContext field in the Container manifest. The securityContext field is a SecurityContext object. Security settings that you specify for a Container apply only to the individual Container, and they override settings made at the Pod level when there is overlap. Container settings do not affect the Pod's Volumes.

From <https://kubernetes.io/docs/tasks/configure-pod-container/security-context/>

```
kubectl get node aks-agentnp-34161091-vmss00000a -o jsonpath='{.metadata.labels.node\.kubernetes
\.io/instance-type}{.status.capacity.cpu}'
```

```
 kubectl get nodes -o=jsonpath="{range .items[*]}{.metadata.labels.node\.kubernetes\.io/instance-type}
{.status.capacity.cpu}   {end}"
```

```
Standard_DS2_v2   2   Standard_DS2_v2   2   Standard_DS2_v2   2   Standard_DS2_v2   2   Standard_DS2
_v2   2   Standard_DS2_v2   2
```

For windows:

```
kubectl get nodes -o=jsonpath="{range .items[*]}{.metadata.labels.node\.kubernetes\.io/instance-type}
{.status.capacity.cpu}{'\n'}{end}"
```

```
Standard_DS2_v2  2
Standard_DS2_v2  2
Standard_DS2_v2  2
Standard_DS2_v2  2
Standard_DS2_v2  2
Standard_DS2_v2  2
```

A taint is a way to mark a node as unsuitable for certain pods. When a taint is set on a node, any pods that do not have a corresponding toleration cannot be scheduled on that node.

```
kubectl taint nodes <node_name> <taint_key>=<taint_value>:NoSchedule
kubectl taint nodes node-1 environment=prod:NoSchedule
```

This will prevent any pods that do not have a toleration for the environment=prod:NoSchedule taint from being scheduled on the node.

Node selector has different label from taint label

Node taints : service=aarp:NoSchedule

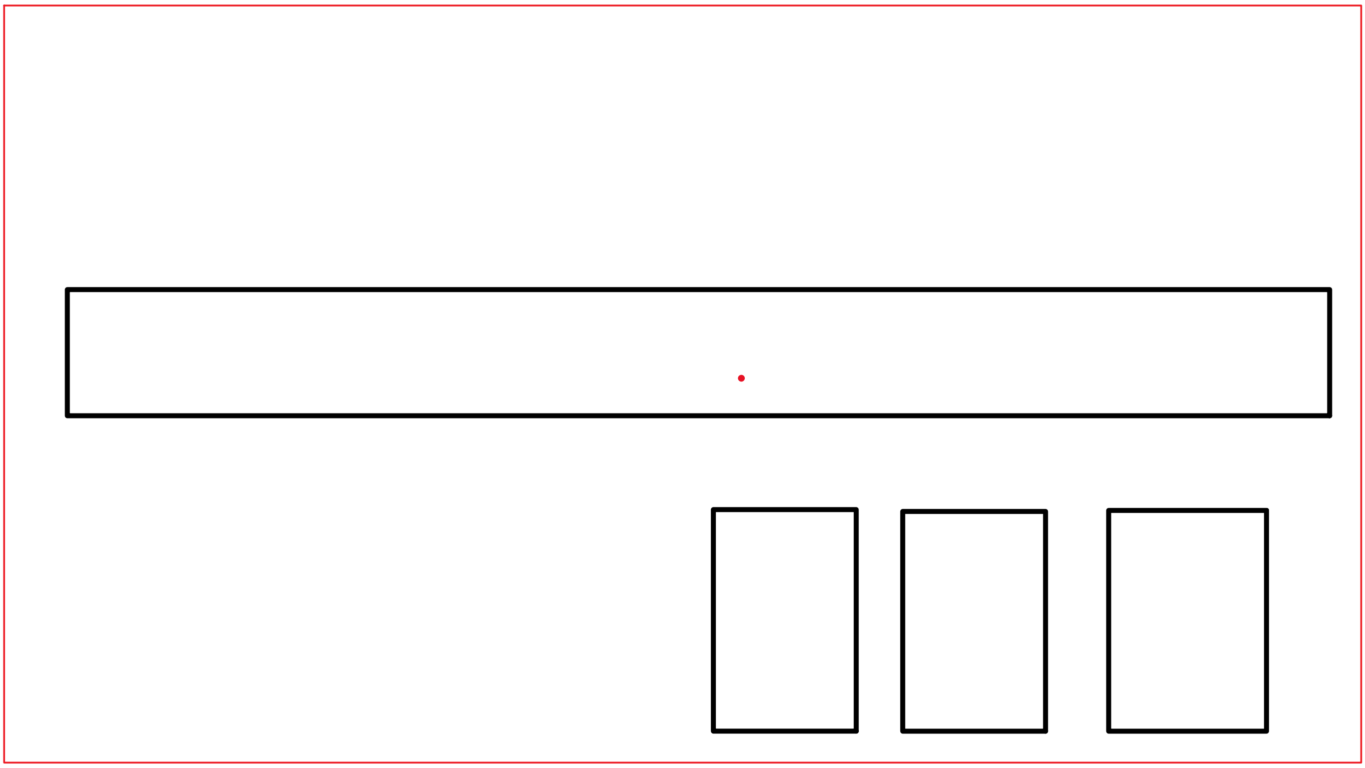
Eg: nodeserivce = aarp
Node selector took precedence over taints

ACR secret:

```
kubectl create secret docker-registry acrsecret  --namespace default  --docker-server=ppfdacrdev.azurecr.io  --docker-username=12e29e13-371f-44ec-b5e1-e515c29b9ed4 --docker-
password=OVU8Q~jDmlVMLM1PdmnIo5OlQ5gUzk_K9ad6zcP-
```

From <https://learn.microsoft.com/en-us/azure/container-registry/container-registry-auth-kubernetes>

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: aarp-service
  namespace: syndication
 spec:
  replicas: 2
  selector:
    matchLabels:
      app: aarp-service
  strategy:
    rollingUpdate:
      maxSurge: 25%
      maxUnavailable: 25%
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: aarp-service
    spec:
      containers:

      - image: icsreg.azurecr.io/dev/aarpservice:fe0e581cfb91d65cba0eb3161a7d775c0aefa24020230317.3
        imagePullPolicy: IfNotPresent
        name: aarp-service
        ports:
        - containerPort: 443
          protocol: TCP
          imagePullSecrets:
      - name: acrsecret
```



```
yarn run v1.22.19
$ yarn workspace api start
$ yarn build
$ bob-ts -f cjs --paths -i src
Circular dependency: src/fetchers/spotify.ts -> src/services/tokens.ts -> src/fetchers/spotify.ts
Entry module "src/app.ts" is using named and default exports together. Consumers of your bundle will
have to use `chunk["default"]` to access the default export, which may not be what you want. Use
`output.exports: "named"` to disable this warning
Generated an empty chunk: "spotify"
$ cross-env ENV=prod node server.js
```

```
Loading fastify.config.js undefined
/usr/src/app/apps/api/dist/db/validate.js:11
    throw new Error(`"${key}" is not configured in env variables`);
    ^

Error: "INSIGHTS_CONNECTION_STRING" is not configured in env variables
    at Object.getEnvVariable (/usr/src/app/apps/api/dist/db/validate.js:11:11)
    at Object.<anonymous> (/usr/src/app/apps/api/dist/config/appinsights.js:9:36)
    at Module._compile (node:internal/modules/cjs/loader:1254:14)
    at Module._extensions..js (node:internal/modules/cjs/loader:1308:10)
    at Module.load (node:internal/modules/cjs/loader:1117:32)
    at Module._load (node:internal/modules/cjs/loader:958:12)
    at Module.require (node:internal/modules/cjs/loader:1141:19)
    at require (node:internal/modules/cjs/helpers:110:18)
    at Object.<anonymous> (/usr/src/app/apps/api/dist/app.js:9:21)
    at Module._compile (node:internal/modules/cjs/loader:1254:14)

Node.js v18.15.0
error Command failed with exit code 1.
info Visit https://yarnpkg.com/en/docs/cli/run for documentation about this command.
error Command failed.
Exit code: 1
Command: /usr/local/bin/node
Arguments: /opt/yarn-v1.22.19/lib/cli.js start
Directory: /usr/src/app/apps/api
Output:

info Visit https://yarnpkg.com/en/docs/cli/workspace for documentation about this command.
info Visit https://yarnpkg.com/en/docs/cli/run for documentation about this command.
error Command failed with exit code 1
```

Kubernetes with Dapr:

https://gist.github.com/vfarcic/8d941690a087b0de0e2731a52cfb1f51

Estimation of Logs over a period of 24 hrs:

```
--tail=-1:
        Lines of recent log file to display. Defaults to -1 with no selector, showing all log lines otherwise 10,
if a
        selector is provided.
```

```
kubectl logs -n syndication -l app=fedaration-db --since 5h | tail -n +1 > fedrationDB_5hours_test_logs.txt
```

```
yq e '.spec.template.spec.containers[0].env[0].name | select(. == "LOG_LEVEL")' azurestorage-deployment.yaml
```

```
yq e '.spec.template.spec.containers[0].env.value' azurestorage-deployment.yaml
```

```
yq e '.spec.template.spec.containers[0].env[0].name | select(. == "LOG_LEVEL")' azurestorage-deployment.yaml

yq e '.spec.template.spec.containers[0].env[0].value| select(. == "LOG_LEVEL")' azurestorage-deployment.yaml
```

```
yq e -i '.spec.template.spec.containers[0].env[1].name = "DUMMY"' azurestorage-deployment.yaml
```

To read shell varibale:

```
yq e -i '.spec.template.spec.containers[0].env[0].value = "'$LOG_LEVEL'"' azurestorage-deployment.yaml
```

https://learn.microsoft.com/en-us/azure/aks/node-access#create-an-interactive-shell-connection-to-a-linux-node

```
yq e -i '.spec.template.spec.containers[0].env[0].value = "'${LOG_LEVEL}'"'
xcommunity_azurestorage_deployment.yml
```

eyJhbGciOiJSUzI1NiIsImtpZCI6IkdBRGpma3k4RUxEZDhsLU1ZQ3QwMlY4ZUhSR1FrRC0yYlM5UXl2OFYwY
UEifQ.eyJhdWQiOlsiaHR0cHM6Ly9rdWJlcm5ldGVzLmRlZmF1bHQuc3ZjLmNsdXN0ZXIubG9jYWwiXSwiZX
hwIjoxNjgxNTM5NzU0LCJpYXQiOjE2ODE0NTMzNTQsImlzcyI6Imh0dHBzOi8va3ViZXJuZXRlcy5kZWZhdWx
0LnN2Yy5jbHVzdGVyLmxvY2FsIiwia3ViZXJuZXRlcy5pbyI6eyJuYW1lc3BhY2UiOiJkZWZhdWx0Iiwic2Vydmlj
ZWFjY291bnQiOnsibmFtZSI6ImRlZmF1bHQiLCJ1aWQiOiIxOTIzMDM4MC00Y2ZjLTQxYjctYmI0NS0yNzhlM
zM2ZGIxOWQifX0sIm5iZiI6MTY4MTQ1MzM1NCwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW50OmRlZmF1
bHQ6ZGVmYXVsdCJ9.R7Er9H6YA95f36e4NweYwpRZU6abDfx-
JVsqqIEWcyz4YwNekShETSS7jMMC9Aj4xRlcIDc1tjmzve33a5Rw6fhEpaN5XYrvW3
_Z6ce1HlDljnLt9lgm2Z6IKeHQRK00-ZwxGAPUPDMfT_rhUEUc74-98gCFHkCPPT3G4wosEo4NH5Sf_iul-
CRoGmoDmy73S1QV6AfLTCgNlw3FidsecZtNv8_GvmjYAs3zBobtZE9
_IHzyxJe9VWts1R5Jd88TihDvFiPOsYRwSFkViC3KJCzTAiqR5oJ8BnmkaMFyQcp1qLBVi8mHesWrm2YscobU
2jzmi6MKYZKM6icpFJQC4w

```
curl --cacert ${CACERT} --header "Authorization: Bearer ${TOKEN}" -X GET
https://192.169.0.100:6443/api/v1/namespaces/default/pods
```

When you upgrade a supported AKS cluster, Kubernetes minor versions can't be skipped. All upgrades must be performed sequentially by major version number. For example, upgrades between *1.14.x* -> *1.15.x* or *1.15.x* -> *1.16.x* are allowed, however *1.14.x* -> *1.16.x* is not allowed.
Skipping multiple versions can only be done when upgrading from an *unsupported version* back to a *supported version*. For example, an upgrade from an unsupported *1.10.x* -> a supported *1.15.x* can be completed if available. When performing an upgrade from an *unsupported version* that skips two or more minor versions, the upgrade is performed without any guarantee of functionality and is excluded from the service-level agreements and limited warranty. If your version is significantly out of date, it's recommended to re-create the cluster.

From <https://learn.microsoft.com/en-us/azure/aks/upgrade-cluster?tabs=azure-cli>

Node surges require subscription quota for the requested max surge count for each upgrade operation. For example, a cluster that has 5 node pools, each with a count of 4 nodes, has a total of 20 nodes. If each node pool has a max surge value of 50%, additional compute and IP quota of 10 nodes (2 nodes * 5 pools) is required to complete the upgrade.
If using Azure CNI, validate there are available IPs in the subnet as well to [satisfy IP requirements of Azure CNI](#).

From <https://learn.microsoft.com/en-us/azure/aks/upgrade-cluster?tabs=azure-cli>

Azure RBAC:

Enable Azure AAD Authentication

GO Daddy Certs:

https://www.godaddy.com/garage/ssl-ultimate-guide/#:~:text=certificate%20for%20you.-,Go%20to%20your%20GoDaddy%20product%20page.,then%20select%20Download%20Zip%20File.

TLS for Microservices:

https://medium.com/avmconsulting-blog/how-to-secure-applications-on-kubernetes-ssl-tls-certificates-8f7f5751d788

D4sv4
100 mpbs througoput:

Insights VMSS
Metric :
operations per seconds
Throughput= bytes per seconds

TEST VM BenchMark results:

https://learn.microsoft.com/en-us/azure/virtual-machines/disks-benchmarks#fio

https://learn.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance

Attached PV storage for Mongo DB:

```
sdc    8:32   0     4G  0 disk /var/lib/kubelet/pods/df5d0a5c-727e-4444-8734-e08e78a1b032/volumes/kubernetes.io~csi/pvc-4d17469e-76ba-476b-852c-48e40fa6d903/mount
```

PATCH:

```
'{"spec":{"containers":[{"name":"kubernetes-serve-hostname","image":"new image"}]}}'
```

Azure CNI vs Kubnet:

https://inder-devops.medium.com/aks-networking-deep-dive-kubenet-vs-azure-cni-vs-azure-cni-overlay-a51709171ce9

Stress commands:

```
stress --cpu 8 --io 4 --vm 2 --vm-bytes 128M --timeout 10s
```

Ingress Gate-way Timeout:

```
2023/05/04 07:24:23 [error] 24#24: *1575643 upstream timed out (110: Operation timed out) while reading response header from upstream, client: 10.240.0.91, server: italentics.dev, request: "GET /healthcheck/availability1 HTTP/1.1", upstream: "https://10.240.0.8:8443/healthcheck/availability1", host: "italentics.dev"
```

```
10.240.0.91 - - [04/May/2023:07:24:23 +0000] "GET /healthcheck/availability1 HTTP/1.1" 499 0 "-" "Apache-HttpClient/4.5.13 (Java/19.0.2)" 524 59.825 [syndication-healthcheck-service-443] [] 10.240.0.8:8443 0 59.824 - 39107ffd60f7c6aea3eff9b4960e0c2c
```

```
{"timestamp":"2023-05-04T09:50:28.530+00:00","status":500,"error":"Internal Server
Error","path":"/healthcheck/availability2"}
```

```
4m1s       Warning   Evicted              pod/aad-service-5f445bf9b9-rzjgc               The node was low on
resource: memory. Threshold quantity: 750Mi, available: 718476Ki. Container aad-service was using
450380Ki, request is 0, has larger consumption of memory.
4m1s       Normal    Killing              pod/aad-service-5f445bf9b9-rzjgc               Stopping container aad-
service
```

```
node.kubernetes.io/memory-pressure:NoSchedule
```

```
]When using COPY with more than one source file, the destination must be a directory and end with a /
```

From <https://v-raayin.visualstudio.com/ICS_DEV_DEVOPS/_build/results?buildId=17472&view=logs&j=b5cdfb1e-c180-561f-918e-a169e451719e&t=c336def0-6bf6-5b52-4254-cbf469cc2b33>

Memory Analysis in perspective of Application:

Memory leaks: If the application has memory leaks, it means that it dynamically allocates memory but fails to release it properly. Memory leaks can occur due to coding errors, such as not deallocating memory after use or retaining references to objects unnecessarily. Even if the container restarts or a new container is created, the memory leaks in the application code will persist, leading to continued memory consumption

1. Inefficient memory management: The application might have inefficient memory management practices, such as excessive caching, redundant data structures, or inefficient algorithms. These factors can result in the application using more memory than necessary. Even if the container restarts or a new container is created, the underlying memory management issues in the application will remain, leading to persistent memory usage.
2. External resources or dependencies: The application might be relying on external resources or dependencies that hold onto memory even after the container restarts or a new container is created. For example, if the application is connected to a database or another service that caches data, the memory consumed by those resources might not be released when the container restarts.

From <https://chat.openai.com/>

https://bitbucket.org/blog/ssh-host-key-changes

Kubeadm init: 1.27

Installation reference link: https://akyriako.medium.com/install-kubernetes-on-ubuntu-20-04-

f1791e8cf799

```
You can also perform this action in beforehand using 'kubeadm config images pull'
W0531 15:29:02.247567   63820 images.go:80] could not find officially supported version of etcd for Kubernetes v1.27.2, falling back to the nearest etcd version (3.5.7-0)
W0531 15:30:01.668967   63820 checks.go:835] detected that the sandbox image "registry.k8s.io/pause:3.6" of the container runtime is inconsistent with that used by kubeadm. It is recommended that using "registry.k8s.io/pause:3.9" as the CRI sandbox image.
```

```
az login --service-principal -u http://azure-cli-2016-08-05-14-31-15 -p VerySecret --tenant contoso.onmicrosoft.com
```

Log in with a service principal using client secret. Use -p=secret if the first character of the password is '-'.

Kubernetes Schedular service:
https://developer.ibm.com/articles/creating-a-custom-kube-scheduler/

Scheduling reference:

Pod anti-affinity requires nodes to be consistently labelled, in other words, every node in the cluster must have an appropriate label matching topologyKey. If some or all nodes are missing the specified topologyKey label, it can lead to unintended behavior.

From <https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/>

Docker Login:

```
docker login registryname.azurecr.io  -u clientID -p clientpassword
```

ICS -Active MQ URL Health Check:

```
# Define the target URL
target_url="ics-activemq.syndication.svc.cluster.local:61616"


# Check if the TCP connection is successful
nc -z -w 3 $target_url

# Check the exit code of the nc command
if [ $? -eq 0 ]; then
  echo "ActiveMQ is reachable"
else
  echo "ActiveMQ is not reachable"
fi
```

PV kubernetes as Azure Files:

Reference link: https://learn.microsoft.com/en-us/azure/aks/azure-csi-files-storage-provision

ReadWriteOnce

the volume can be mounted as read-write by a single node. ReadWriteOnce access mode still can allow multiple pods to access the volume when the pods are running on the same node.

ReadOnlyMany

the volume can be mounted as read-only by many nodes.

ReadWriteMany

the volume can be mounted as read-write by many nodes.

ReadWriteOncePod

- RWO - ReadWriteOnce
- ROX - ReadOnlyMany
- RWX - ReadWriteMany
- RWOP - ReadWriteOncePod

From <https://kubernetes.io/docs/concepts/storage/persistent-volumes/>

From <https://kubernetes.io/docs/concepts/storage/persistent-volumes/>

From <https://kubernetes.io/docs/concepts/storage/persistent-volumes/>

Using same storage for multiple pods where pods are running on different Nodes.

A persistent volume represents a piece of storage that has been provisioned for use with Kubernetes pods. You can use a persistent volume with one or many pods, and it can be dynamically or statically provisioned. If multiple pods need concurrent access to the same storage volume, you can use Azure Files to connect using the Server Message Block (SMB) protocol

From <https://learn.microsoft.com/en-us/azure/aks/azure-csi-files-storage-provision>

Standard file shares are hosted on a storage system backed by hard disk drives (HDD), while premium file shares are backed by solid-state drives (SSD) for better performance

If you require large amounts of IOPS, extremely fast data transfer speeds, or very low latency, then you should choose premium Azure file shares

Caution: There is a limitation in Helm regarding values being provided via `--set`. Helm can't deal with commas (`,`) as part of a value in `--set`. Before invoking `helm install`, consider checking if your `SP_CLIENT_SECRET` contains a comma (`echo $SP_CLIENT_SECRET`). If so, update the `SP_CLIENT_SECRET` variable and replace `,` with `\,`.

From <https://www.thorsten-hans.com/external-dns-azure-kubernetes-service-azure-dns/>

Azure Kubernetes with DNS

https://learn.microsoft.com/en-us/azure/aks/ingress-tls?tabs=azure-cli

20.231.238.237

```
kubectl exec -it curl -- curl -k https://10.244.1.154:8443/healthcheck/availability
```

To restrict same replica pods scheduling in one Nodes:

```
affinity:
      podAntiAffinity:
        requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
            - key: app
              operator: In
              values:
              - web-store
          topologyKey: "kubernetes.io/hostname"
```