

Q5: SecurityContext Implementation - Non-Root Deployment

Overview

This document demonstrates the implementation of SecurityContext to prevent root privileges in Kubernetes deployments.

Modified Deployment

SecurityContext Configuration

File: manifests/aks-store-quickstart-secure.yaml

The product-service deployment now includes:

```
securityContext:
  runAsNonRoot: true
  runAsUser: 1000
  runAsGroup: 1000
  fsGroup: 1000
containers:
- name: product-service
  securityContext:
    allowPrivilegeEscalation: false
    readOnlyRootFilesystem: false
    runAsNonRoot: true
    runAsUser: 1000
  capabilities:
    drop:
      - ALL
```

Screenshots

1. AKS Store Deployment with Security

```
munachiernest-eze@Munachis-MacBook-Pro BCDV4034-FinalExam % kubectl get po
&& kubectl get services -n aks-store-demo && echo "----" && kubectl get po
&& kubectl get services -n aks-store-demo && echo "----" && kubectl get de
NAME                                READY    STATUS    RESTARTS   AGE
order-service-5c85f45984-956bv      1/1      Running   0           10m
product-service-5db5645fb7-lpgbz    1/1      Running   0           2m39s
rabbitmq-0                           1/1      Running   0           10m
store-front-6ff78d4f79-6nj4w        1/1      Running   0           2m38s
----
NAME                                TYPE                CLUSTER-IP    EXTERNAL-IP    PORT(S)
order-service                       ClusterIP           10.0.196.199  <none>         3000/TCP
product-service                     ClusterIP           10.0.111.1    <none>         3002/TCP
rabbitmq                            ClusterIP           10.0.123.245  <none>         5672/TCP,156
store-front                         LoadBalancer       10.0.15.153   <pending>      80:30520/TCP
----
NAME                                READY    UP-TO-DATE    AVAILABLE    AGE
order-service                       1/1      1              1            10m
product-service                     1/1      1              1            10m
store-front                         1/1      1              1            10m
munachiernest-eze@Munachis-MacBook-Pro BCDV4034-FinalExam % █
```


ask every time ▾ Move to background


2. SecurityContext Verification

```
munachiernest-eze@Munachis-MacBook-Pro BCDV4034-FinalExam % kubectl get pod product-service-5db5645fb7-lpgbz -n aks-store-demo -o yaml | grep -A 20 securityContext
securityContext:
  allowPrivilegeEscalation: false
  capabilities:
    drop:
      - ALL
  readOnlyRootFilesystem: false
  runAsNonRoot: true
  runAsUser: 1000
  terminationMessagePath: /dev/termination-log
  terminationMessagePolicy: File
  volumeMounts:
  - mountPath: /var/run/secrets/kubernetes.io/serviceaccount
    name: kube-api-access-zvdzp
    readOnly: true
  dnsPolicy: ClusterFirst
  enableServiceLinks: true
  nodeName: aks-default-39692054-vmss000002
  nodeSelector:
    kubernetes.io/os: linux
  preemptionPolicy: PreemptLowerPriority
  priority: 0

securityContext:
  fsGroup: 1000
  runAsGroup: 1000
  runAsNonRoot: true
  runAsUser: 1000
serviceAccount: default
serviceAccountName: default
terminationGracePeriodSeconds: 30
tolerations:
- effect: NoExecute
  key: node.kubernetes.io/not-ready
  operator: Exists
  tolerationSeconds: 300
- effect: NoExecute
  key: node.kubernetes.io/unreachable
  operator: Exists
  tolerationSeconds: 300
- effect: NoSchedule
  key: node.kubernetes.io/memory-pressure
  operator: Exists
volumes:
```

3. Application Running with Non-Root User

Products Cart (0)




Contoso Catnip's Friend

Watch your feline friend embark on a fishing adventure with Contoso Catnip's Friend toy. Packed with irresistible catnip and dangling fish lure.

9.99

Add to Cart




Salty Sailor's Squeaky Squid

Let your dog set sail with the Salty Sailor's Squeaky Squid. This interactive toy provides hours of fun, featuring multiple squeakers and crinkle tentacles.

6.99

Add to Cart




Mermaid's Mice Trio

Entertain your kitty with the Mermaid's Mice Trio. These adorable plush mice are dressed as mermaids and filled with catnip to captivate their curiosity.

12.99

Add to Cart




Ocean Explorer's Puzzle Ball

Challenge your pet's problem-solving skills with the Ocean Explorer's Puzzle Ball. This interactive toy features hidden compartments and treats, providing mental stimulation and entertainment.

11.99

Add to Cart




Pirate Parrot Teaser Wand

Engage your cat in a playful pursuit with the Pirate Parrot Teaser Wand. The colorful feathers and jingling bells mimic the mischievous charm of a pirate's parrot.

8.99

Add to Cart





Seafarer's Tug Rope


Tug-of-war meets nautical adventure with the Seafarer's Tug Rope. Made from marine-grade rope, it's perfect for interactive play and promoting dental health in dogs.


14.99

Add to Cart









4. Cluster with Deployments

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

101464377@georgebro...
GEORGE BROWN COLLEGE

Home > Resource groups > rg-aks-store-demo >

aks-store-cluster

Kubernetes service

Search

Overview

Activity log

Access control (IAM)

Tags

Monitor

Diagnose and solve problems

Microsoft Defender for Cloud (preview)

Cost analysis

Resource visualizer

Kubernetes resources

Namespaces

Workloads

Services and ingresses

Storage

Configuration

Custom resources

Events

Run command

Settings

Node pools

Upgrades

Security configuration

Application scaling

Networking

Essentials

Resource group : rg-aks-store-demo

Power state : Running

Cluster operation status : Succeeded

Subscription : Azure for Students

Location : East US

Subscription ID : 69a0ceb2-4ba6-4cd4-bb7f-a35a58b1be1e

Fleet Manager : Click here to assign

Tags (edit) : Add tags

Kubernetes version : 1.30.12

API server address : aks-store--rg-aks-store-demo-69a0ce-ns1v3yp7.hcp.eastus.azurek8s.io

Network configuration : Azure CNI Overlay

Node pools : 1 node pool

Container registries : Attach a registry

Get started

Properties

Monitoring

Recommendations

Kubernetes services

Encryption type : Encryption at-rest with a platform-managed key

Virtual node pools : Not enabled

Node pools

Node pools : 1 node pool

Kubernetes versions : 1.30.12

Node sizes : Standard_B2s

Upgrades

Kubernetes version : 1.30.12

Auto Upgrade Type : -

Automatic upgrade scheduler : -

Node upgrade channel type : Node Image

Node upgrade channel scheduler : -

Security configuration

Networking

API server address : aks-store--rg-aks-store-demo-69a0ce-ns1v3yp7.hcp.eastus.azurek8s.io

Network configuration : Azure CNI Overlay

Pod CIDR : 10.244.0.0/16

Service CIDR : 10.0.0.0/16

DNS service IP : 10.0.0.10

Cilium dataplane : Not enabled

Network Policy : None

Load balancer : standard

Private cluster : Not enabled

Authorized IP ranges : Not enabled

Application Gateway ingress controller : Not enabled

Integrations

Container insights : Not enabled

Workspace resource ID : -

Service Mesh - Istio : Not enabled

5. Deployment Status

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

101464377@georgebro...
GEORGE BROWN COLLEGE

Home > All resources >

All resources

George Brown College

Create

Manage view

You are viewing a new version of Browse experience. Click here to access the old experience.

Name ↑

kubernetes

kubernetes

kubernetes-a0a198bbffd0242c1a0...

kubernetes-a43137dfd540c4d091f...

kubernetes-a85fecb84f6941f1a01

kubernetes-ac263d121efab49ec89

KubernetesRecordingRulesRuleGro...

MSProm-westus2-aks-cluster-5q07

MSProm-westus2-aks-cluster-5q07

NetworkWatcher_eastus

NetworkWatcher_westus2

NodeAndKubernetesRecordingRule...

NodeRecordingRulesRuleGroup - a...

NodeRecordingRulesRuleGroup-W

staks5q074gff

UXRecordingRulesRuleGroup - aks

UXRecordingRulesRuleGroup-Win

Showing 18 - 34 of 34. auto

Display count:

kubernetes-a0a198bbffd0242c1a0d2dd542d8a2ec

Public IP address

Search

Associate

Dissociate

Delete

Move

Refresh

Open in mobile

Give feedback

JSON View

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Settings

Monitoring

Automation

Help

Essentials

Resource group (move) : mc_rg-aks-store-demo_aks-store-cluster_eastus

Location (move) : East US

Subscription (move) : Azure for Students

Subscription ID : 69a0ceb2-4ba6-4cd4-bb7f-a35a58b1be1e

SKU : Standard

Tier : Regional

IP address : 52.147.208.33

DNS name : -

Domain name label scope : -

Associated to : kubernetes

Virtual machine : -

Routing preference : Microsoft network

Tags (edit) : aks-managed-cluster-name: aks-store-cluster aks-managed-cluster-rg: rg-aks-store-demo k8s-azure-cluster-name: kubernetes k8s-azure-service: aks-store-staging/store-front

Get Started

Properties

Tutorials

Use public IP addresses for public connections to Azure resources

Associate and configure public IP addresses to various Azure resources. Learn more.

Associate to a resource

Associate your public IP address to an Azure resource such as an Azure Load Balancer or a network interface.

Associate IP

Configure a public IP address

Configure a DNS idle time, name, and alias record for your public IP address.

Configure

Protect IP address

Choose the right DDoS protection level for your IP address.

Protect

Security Features Implemented

- **runAsNonRoot**: Prevents containers from running as root

- **runAsUser:** Runs container as user ID 1000
- **allowPrivilegeEscalation:** Prevents privilege escalation
- **capabilities.drop:** Removes all Linux capabilities
- **fsGroup:** Sets file system group ownership

Files Submitted

- **manifests/aks-store-quickstart-secure.yaml** - Deployment with SecurityContext
- **deploy-aks-store-secure.sh** - Deployment script