Continuous Security for Microsoft Azure Cloud and Containers

sysdig

Contents

Security for Microsoft Azure Cloud and Containers

The global economy moves quickly, and the only way enterprises can remain competitive is to have a technology foundation that supports their need to move fast, innovate, and be secure.

Public clouds are designed to deliver a faster, more effective way of integrating technology with business needs. The cloud provides a dynamic environment that is inherently scalable, optimized for application integration, and helps organizations take advantage of technologies that support continuous innovation.

Cloud and containers enable an entirely new way of doing business. Modern enterprises are rapidly adopting these technologies as core aspects of their growth strategies. Using DevOps approaches and container application development, cloud teams can rapidly spin up software, make adjustments, and continuously deliver solutions to meet customer and market needs.

Microsoft Azure gives enterprises the ability to take advantage of both speed and agility by integrating cloud services and container platforms to support rapid application development and deployment. Microsoft recognizes that as companies progress with cloud use, they must transform their security and compliance processes.

Containers, microservices, and hybrid cloud workloads disrupt traditional enterprise security. As enterprises move from sandbox to production deployments, they face new security dynamics and encounter challenges establishing secure processes across the lifecycle of cloud services and containers. Complex interactions among often short-lived processes, and new capabilities such as serverless computing, create a constantly changing security environment. The use of these solutions enables your business to move faster, but presents a new set of potential threats.

Enterprise DevOps, cloud, and IT teams must establish ways to balance the need for speed with effective data, application, and infrastructure security. Microsoft Azure customers need complementary security solutions that can keep pace with the speed and agility of the cloud. This duality in goals – accelerating delivery while meticulously checking security – demands an approach that both protects data and workloads, and facilitates agile application development. In other words, make it safe but don't slow it down.

How Sysdig provides a security foundation for Microsoft Azure

Azure customers use the Sysdig Secure DevOps Platform to confidently run containers, Kubernetes, and cloud workloads. With Sysdig, you can secure the build, detect and respond to threats, and continuously validate cloud posture and compliance. In addition, Sysdig solutions maximize performance and availability by monitoring and troubleshooting cloud infrastructure and services for Azure, hybrid cloud, and multicloud environments.

Sysdig operates as a SaaS platform, built on an open-source stack that includes Falco and sysdig OSS, the open standards for runtime threat detection and response. By creating a secure DevOps workflow that integrates security, compliance, and monitoring, organizations can accelerate deployment and confidently run container and cloud workloads on Azure with Sysdig. This allows you to:

- Speed deployment by validating security policies and configurations during the build process.
- Continuously assess cloud security posture and compliance.
- Stop runtime threats without impacting performance.
- Prevent issues by monitoring performance and health across infrastructure, services, and applications.
- Conduct incident response using detailed records.

This guide offers a framework for establishing comprehensive cloud and container security for Microsoft Azure environments with specific recommendations for how Sysdig can complement and enhance native Azure tools.

Why security and visibility are top of mind for Azure users

There are three key elements to Azure security that are critical to the protection of data, applications, and cloud infrastructure.

Sharing responsibility for security

In a public cloud like Azure, security is a shared responsibility. Microsoft handles the security OF the environment while the customer is responsible for everything that happens WITHIN the environment. Azure delivers out-of-the-box security features like user authentication and logging, however, users must also consider how they will identify and remediate misconfigurations, known vulnerabilities, and behavioral anomalies across their workloads.

Continuous cloud change requires continuous monitoring. That monitoring must function across all cloud and orchestration activities to provide visibility into in-use cloud assets, and audit configuration settings. It also requires continuous scanning and analysis of cloud and container activity to manage health and security risk.

Automating to move fast and scale securely

Security and DevOps teams have to validate that security controls are actually working as intended, but also aren't slowing down development efforts. Many enterprises perform manual checks for this, but that's simply not scalable. Automation is the only way to do this effectively, so companies require tools that can analyze cloud activity without manual processes to help you understand if things are operating as expected, even in the largest deployments.

With an automated approach, cloud activity can be analyzed and interpreted, and DevOps and security teams can be alerted about abnormal behavior within their Azure environment. This helps you address vulnerabilities and issues before they are exploited, slow down your development process, and impact your business applications.

Optimizing for development and container orchestration

Azure offers container services, such as Azure Kubernetes Service (AKS) and Azure Red Hat OpenShift (ARO). Each functions as a comprehensive container orchestration system. They are designed to optimize development, operations, and security processes that support the secure creation and deployment of containerized workloads, and help accelerate container application deployment.

In these orchestrated application environments, legacy security tools no longer work as they can't see inside containers, handle the dynamic nature of Kubernetes, or scale across clusters, availability zones, and regions. What's needed is a container and cloud security stack built for containers, Kubernetes, and cloud that integrates into your DevOps workflow.

Container platforms available on Azure such as Azure Kubernetes Service (AKS), help you operate containerized applications more easily by providing a fully managed Kubernetes service. AKS is designed to provide a great experience for development, operations, and security teams to build, deploy, and securely run containerized workloads, as well as accelerate container application deployment.

Across your organization, different teams and roles will have different concerns and points of view on visibility and security, as well as what processes are required to move containerized applications into production.

Developers

Azure container services help developers take advantage of containerized applications and orchestration without having to know the underlying infrastructure details. Azure DevOps developer services helps teams to plan work, collaborate on code development, and build and deploy applications. Azure Pipelines automates build and test processes, creates a container image from your source code, and pushes it to targets like Microsoft Azure Container Registry (ACR). Ensuring images are free of known vulnerabilities and follow security best practices is a major challenge that often compromises application integrity and slows down development release schedules.

Cloud/DevOps

DevOps teams are responsible for maintaining high availability, quality of service, health, and performance of applications and infrastructure. Users leverage the built-in Azure web console to manage infrastructure and platform capabilities, and also rely on playbooks and infrastructure as code (IAC) to automate application deployments. DevOps teams are increasingly expected to ensure that security is built into the platform with features like IaC scanning, runtime security, admission control, network policies, and more.

Security and compliance

To be effective at preventing threats, identifying risk, and isolating vulnerabilities, Security operations, SecOps, DevSecOps, and CSIRT teams need to continuously monitor Azure cloud and container environments to protect against anomalous behavior and zero-day attacks, as well as perform incident response if a violation occurs. Security teams must set policies based on compliance frameworks and internal requirements, and apply controls to the various resources operating in the Azure environment. In addition, security teams must identify and monitor new cloud infrastructure and applications that are deployed to ensure they conform with regulatory and internal compliance requirements.

Managing security and visibility on Azure cloud an containers with Sysdig

With unified security, compliance, and monitoring, enterprises can confidently run cloud-native workloads on Azure container services in private, hybrid, and multi-cloud environments. By automating these critical capabilities for a secure DevOps workflow, teams can maximize performance, increase agility, manage security risk, and ship cloud applications faster.

Azure container services provide baseline coverage for security and monitoring across the container platform. As you scale out the number of applications, clusters, locations, and cloud providers, Sysdig extends Azure container services, providing additional security and monitoring capabilities to:

Secure the build

- Automate scanning within CI/CD pipelines and registries.
- Consolidate container and host scanning.
- Efficiently flag vulnerabilities and identify owners.
- Block vulnerable images from being deployed.

Detect and respond to runtime threats

- See all threats with Falco, the open standard for detection, and implement zero-day threat detection.
- Enforce compliance and governance via policy as code based on Open Policy Agent (OPA).
- Prevent lateral movement with Kubernetes network policies.
- Conduct incident response using detailed records.
- Get deep runtime visibility into cloud and Azure container services.

Continuously validate cloud posture and compliance

- Identify misconfigurations and compliance violations at build and runtime.
- Monitor account and access security at the individual and group levels.
- Measure progress with detailed reports.
- Save time with out-of-the-box policies for PCI, NIST, and SOC 2.

Monitor containers, Kubernetes, and cloud services

- Prevent issues by monitoring performance and capacity.
- Accelerate troubleshooting using granular data.
- Scale Prometheus monitoring across clusters and clouds.
- Audit container activity and accelerate incident response.

Sysdig provides the only comprehensive, unified platform that features cloud and container security and monitoring. By incorporating the capabilities of a Cloud Workload Protection Platform (CWPP) with Cloud Security Posture Management (CSPM), as well as health and performance observability, we equip DevOps and Security teams with a single source of truth across cloud workloads, accounts, containers, and Kubernetes.

These tools operate as a unified security and visibility layer over Azure environments to eliminate silos of information that exist across operations, development, DevOps, and security teams. At Sysdig, we enable security and DevOps teams to accurately identify and triage incidents, quickly determine cause, and perform forensics even for container workloads that are no longer running.

Using the Sysdig platform, security and DevOps teams can identify and report on security issues across the entire Azure environment, including suspicious user behavior, threats to data, and vulnerabilities affecting running images in specific namespaces and clusters. For example, if a new vulnerability is reported, Sysdig will help your DevOps teams quickly identify the affected images in a particular region, namespace, or cluster. With this approach, you can resolve issues quickly by analyzing vulnerabilities and granular system data automatically correlated with cloud and Kubernetes context.

Sysdig is a SaaS-first platform. We provide reliable and secure cloud applications with centralized visibility and security for operating Azure container and cloud services at scale. With a single agent deployed per Azure virtual machine instance, the Sysdig platform can scale to 10,000+ nodes to secure and monitor containers and applications running on Azure.

You can get started quickly with guided onboarding, out-of-the-box dashboards, and curated workflows. Because Sysdig plugs into your cloud environment and existing DevOps workflow using automation and out-of-the-box integrations, visibility and security controls won’t slow you down.

Sysdig provides container and orchestration insights for Azure using the following:

- **ImageVision™** identifies vulnerabilities and misconfigurations in CI/CD tools and at runtime.
- **ContainerVision™** provides granular visibility into container, network, application, and system activity.
- **ServiceVision™** enriches data with metadata from Azure, hosts, AKS/Kubernetes, and containers.
- **CloudVision™** enables a consolidated view of cloud configurations and activity.

Securing Azure container services

Let's look at the various security controls provided by Azure and how Sysdig extends security, compliance, and monitoring for Azure solutions across the cloud-native stack and container lifecycle.

Azure provides security capabilities, including:

- Secure hosting infrastructure with Microsoft Azure Virtual Machines (AVM).
- Access Control with Azure Active Directory and Azure RBAC.
- Image scanning with Azure Defender for container registries.
- Compliance visibility and enforcement with Azure Security Center and Azure Policy.

Host security

Cloud security is the highest priority for Azure. Customers benefit from a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations. As a managed service, Microsoft AVM is protected by Azure global network security procedures.

Microsoft Azure provides...

To securely operate containers on Azure, Microsoft supports secure, stable, and high-performance operating systems to run cloud-native applications. This includes Red Hat Enterprise Linux (RHEL) and Flatcar Container Linux by Kinvolk.

Sysdig adds...

Sysdig provides host scanning to help you detect package vulnerabilities on virtual and physical server or cloud-native host instances. Detailed reports will help your operational teams understand what needs to be patched to avoid incidents like breaches or zero-day vulnerabilities.

Sysdig Secure provides detection for host OS and non-OS packages and reduces time-to-fix by assessing impact and ownership using rich cloud and Kubernetes context. A single vulnerability management solution for hosts and containers will help you reduce risk, keep pace with regulatory requirements and compliance, and save time by consolidating workflows.

Authentication and authorization

User access to Azure container services is provided through standard interfaces, including the Web UI, CLI, and APIs. Additionally, services interact with Azure container services so they can gain awareness of their orchestration state and execute actions against these platforms. Imagine a CI/CD pipeline pushing a new deployment into production. How do you control and measure who can do what?

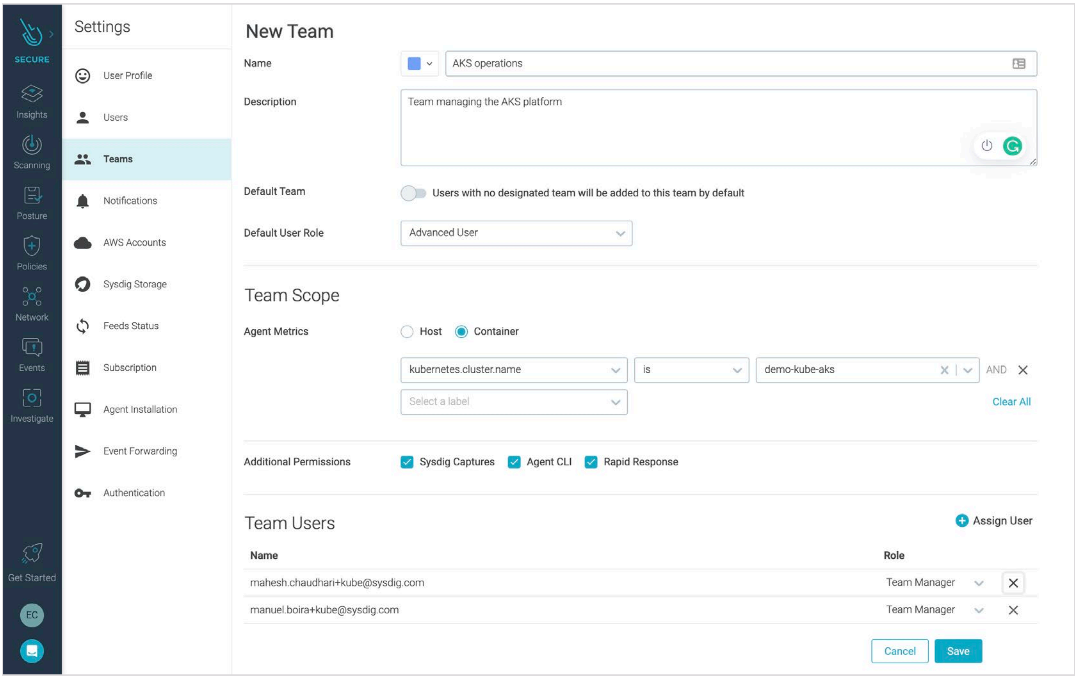
Microsoft Azure provides...

Azure Active Directory (Azure AD) and Azure role-based access control (Azure RBAC) enable you to manage access to Azure services and resources securely. Using Azure AD and/or RBAC, you can create and manage Azure users and groups, and use permissions to allow or deny access to Azure resources. Azure AD/RBAC administrators control who can be authenticated (signed in) and authorized (have permissions) to use Microsoft AKS resources.

Sysdig adds...

With Sysdig, you can define who can access any of the visibility, metrics, notifications, and security policies for your Azure container services. This feature, known as Teams, introduces the concept of service and metadata-based access control to complement the existing Azure AD mechanisms.

With Sysdig Teams, administrators can define groups of users that have access to a limited service or set of services deployed on Azure. For example, an application owner might only see vulnerability scan results of images in a specific namespace. Limiting the exposure with access controls and providing a default configuration for each specific team helps streamline security information for users and teams.



New Team

Name: AKS operations

Description: Team managing the AKS platform

Default Team: Users with no designated team will be added to this team by default

Default User Role: Advanced User

Team Scope

Agent Metrics: ○ Host ● Container

kubernetes.cluster.name | is | demo-kube-aks | AND

Select a label

Additional Permissions: ☑ Sysdig Captures ☑ Agent CLI ☑ Rapid Response

Team Users

Name	Role
mahesh.chaudhari+kube@sysdig.com	Team Manager
manuel.boira+kube@sysdig.com	Team Manager

Sysdig supports role-based access controls (RBAC) to define user privileges and provides federated access control across different teams in an organization. In addition to the admin role, a variety of access roles are available, including View Only, Standard User, Advanced User, and Team Manager.

Image scanning

Applications and infrastructure components are built on top of readily available packages, many of which are open-source software that might contain old library versions. It's important to know where these packages originally came from, who built them, and whether there are any known vulnerabilities inside them.

Microsoft Azure provides...

Microsoft Azure Container Registry (ACR) is a fully-managed Open Container Initiative (OCI) compatible container registry that makes it easy for developers to store, manage, and deploy container images. Microsoft ACR is integrated with Azure container services like Azure Container Instances (ACI) and AKS, simplifying your development to production workflow.

As container adoption in Azure takes off, ACR scanning is the first step towards delivering continuous security and compliance. Azure Defender, integrated with Azure Security Center, includes a vulnerability scanner to scan the images in your Azure Resource Manager-based ACR image repositories. This capability can help you ensure your ACR-based images are scanned for both vulnerabilities and misconfigurations so that you don't run exploitable applications on Azure.

Sysdig adds...

Sysdig Secure provides container scanning capabilities that extend beyond ACR default image scanning. WIth Sysdig Secure, development and DevOps teams can check for vulnerabilities, compliance, and misconfigurations in base images, OS packages, and third-party libraries, like Python packages from PIP or Java JAR files that developers might use in their application images.

Using what Sysdig calls ImageVision, development teams can automate detection of vulnerabilities and misconfigurations for a range of image aspects. Pre-configured policies detect general security threats and bad practices, as well as map to security and compliance standards, like PCI DSS or NIST 800-190.

There are two image scanning approaches supported by Sysdig Secure for Azure:

- Backend scanning: Container images are retrieved, and copies are stored local to the Sysdig backend where the scanning takes place. Post-scan, you can view the results within the Sysdig Secure UI.
- Inline scanning: Container image scan takes place local to where the container image is already stored, for example, within ACR. With a local, inline scanning approach, you don't need to share registry credentials or image contents outside of your Azure environment.

Only metadata about the scan results are sent back to Sysdig. This protects privacy and can help prevent credential leaking.

Sysdig Secure incorporates Kubernetes metadata to add context into vulnerability reporting to help cloud teams map vulnerabilities back to specific applications and services, quickly identifying the team responsible for implementing a fix.

To help users more easily understand the security and compliance posture of their container images, Sysdig image scanning reports allow DevOps and security teams to smoothly access information about their catalog of images, packages, and Common Vulnerabilities and Exposures (CVEs) to support making decisions about where to focus efforts.

You can, for instance, filter image scanning results along with parameters, such as CVE age, software versions, and whether a fix is available. Scanning reports are accessible via the user interface, and can be downloaded and shared across teams to improve communication about risk and take action to improve security.

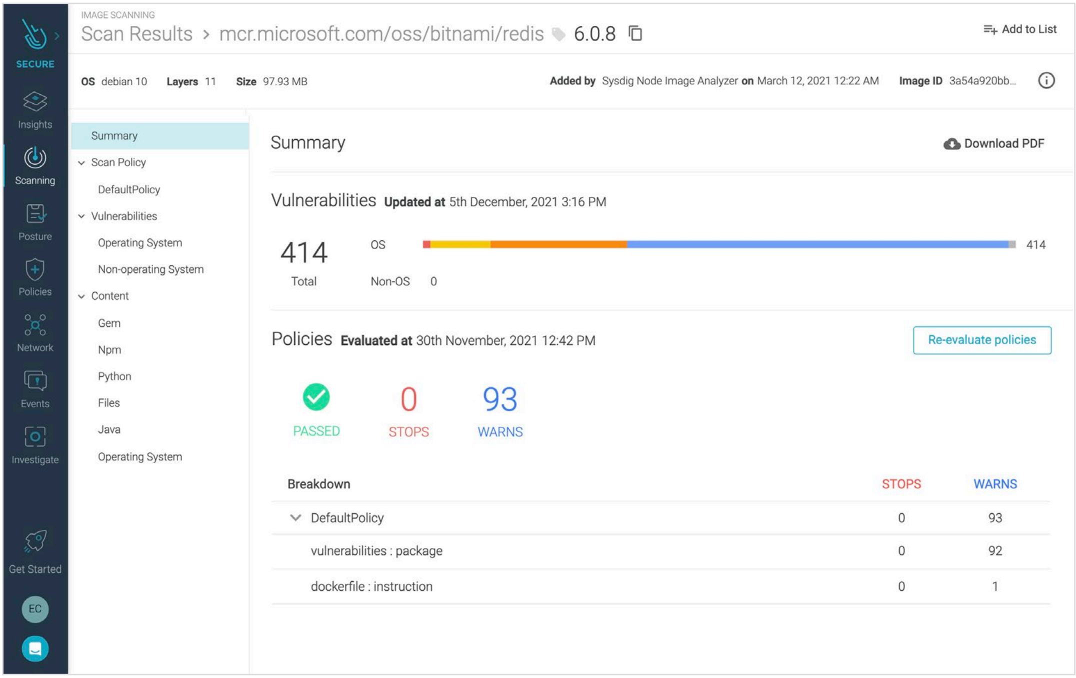


IMAGE SCANNING

Scan Results > mcr.microsoft.com/oss/bitnami/redis 6.0.8

OS debian 10 **Layers** 11 **Size** 97.93 MB **Added by** Sysdig Node Image Analyzer **on** March 12, 2021 12:22 AM **Image ID** 3a54a920bb...

Summary

Vulnerabilities **Updated at** 5th December, 2021 3:16 PM

414 Total

OS 414

Non-OS 0

Policies **Evaluated at** 30th November, 2021 12:42 PM

PASSED

0 STOPS

93 WARNS

Breakdown	STOPS	WARNS
DefaultPolicy	0	93
vulnerabilities : package	0	92
dockerfile : instruction	0	1

Sysdig will also perform a continuous scan of your running containers and alert you when new high/critical CVEs are published that impact your workloads. This enables you to assess your exposure immediately. Affected services and accountable teams can be quickly identified using Kubernetes or cloud metadata, like service, deployment, or application.

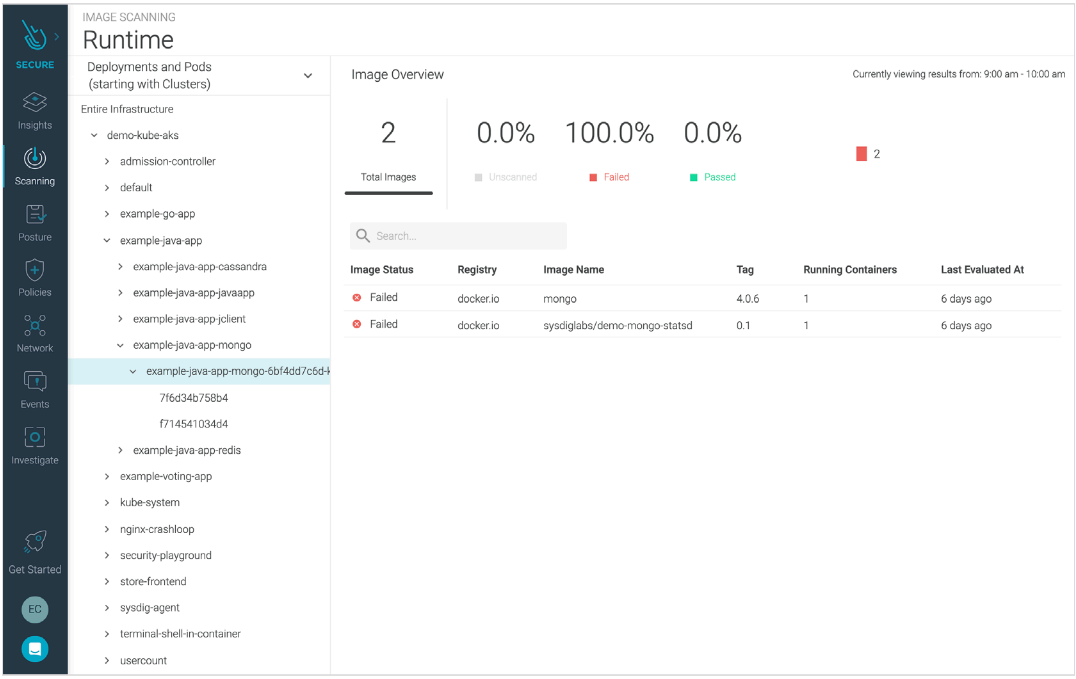


Image Status	Registry	Image Name	Tag	Running Containers	Last Evaluated At
Failed	docker.io	mongo	4.0.6	1	6 days ago
Failed	docker.io	sysdiglabs/demo-mongo-statsd	0.1	1	6 days ago

CI/CD pipeline security

CI/CD pipelines automate steps in your software delivery process, such as build and test, to help your teams deliver updates to customers faster and more frequently. Embedding security into your delivery pipeline as you build applications helps you identify and address vulnerabilities faster, and keeps your developers productive.

Microsoft Azure provides...

Azure allows you to set up a CI/CD pipeline to automate your software delivery process.

Azure provides several tools for DevOps teams to automate the software delivery process such as Azure Repos for version control and Azure Pipelines for automatically building, testing, and deploying code. In addition, Azure Pipeline allows developers to visualize and automate these different stages.

Azure Pipelines is a fully managed, continuous integration service that automates the build, test, and deploy phases of the release process every time there is a code change, based on the defined release model.

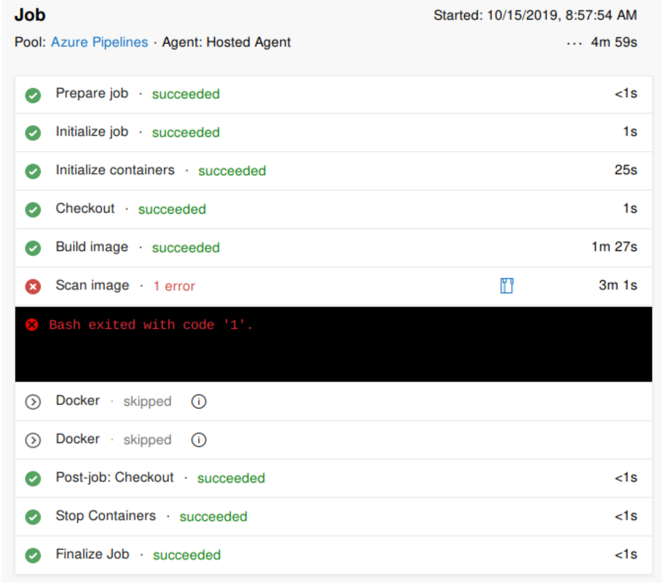
Additionally, Microsoft is embracing the community driven GitHub Actions CI/CD to help developers automate common tasks across the build, test, and deploy lifecycle with GitHub.

Sysdig adds...

Image Scanning for Azure Pipelines and GitHub Actions raises the confidence that DevOps teams have in the security of their deployments, detecting known vulnerabilities and validating container build configuration early in their pipelines. By detecting these issues before the images are published into a container registry or deployed in production, you can apply fixes faster and improving delivery to production time.

Sysdig Secure image scanning integrates directly into your CI/CD pipeline of choice, including Azure Pipelines, GitHub Actions, Jenkins, Bamboo, GitLab, CircleCI, and more. You can catch vulnerabilities and misconfigurations in third-party libraries, official/unofficial OS and packages, configuration checks, credential exposures, and metadata. Using inline scanning, you can detect issues before the images are pushed to a registry.

Leveraging scanning integration with CI/CD pipelines, developers can understand that an image failed to pass the scan, why a failure occurred, and what needs to be fixed. For non-critical policy violations, warnings will suggest what needs to be changed to improve the security of the container image without aborting the pipeline.



Job Started: 10/15/2019, 8:57:54 AM

Pool: Azure Pipelines · Agent: Hosted Agent ··· 4m 59s

```
✓ Prepare job · succeeded                     <1s
✓ Initialize job · succeeded                   1s
✓ Initialize containers · succeeded           25s
✓ Checkout · succeeded                         1s
✓ Build image · succeeded                  1m 27s
✗ Scan image · 1 error                      3m 1s
✗ Bash exited with code '1'.
○ Docker · skipped
○ Docker · skipped
✓ Post-job: Checkout · succeeded              <1s
✓ Stop Containers · succeeded                 <1s
✓ Finalize Job · succeeded                    <1s
```

Using Sysdig, images built in Azure Pipelines or using GitHub Actions can be scanned inline without having images leave the infrastructure and without needing a staging registry. Multiple scans can be run in parallel, thereby improving throughput.

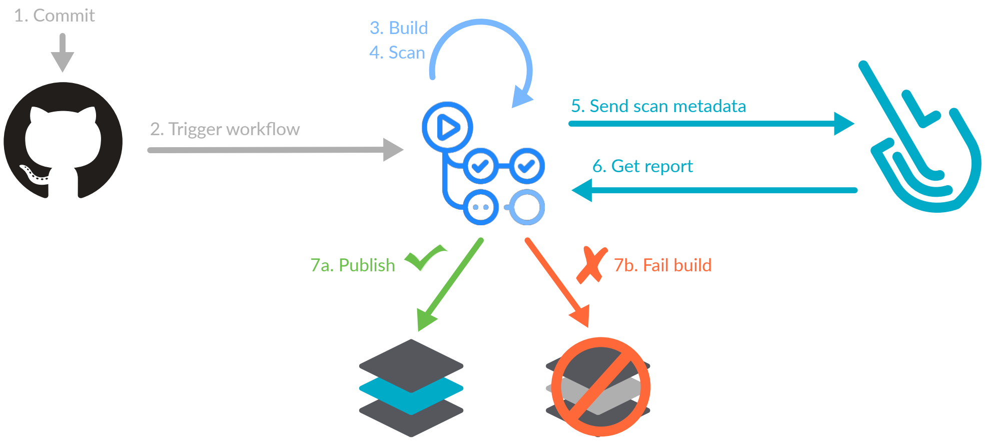


Image assurance

Image assurance focuses on preventing unapproved images from being deployed in your container environment. This helps you reduce issues and errors by evaluating and verifying images based on your defined policies prior to running in production. It's an important element of container security because it addresses security issues, based on defined thresholds set by you, before a container is allowed to run.

As "prevention is worth a pound of cure," by implementing image scanning and assurance on admission controllers, you can be confident that anything deployed conforms to your security policies.

Microsoft Azure provides...

Kubernetes admission controllers can be used with AKS to prevent unapproved images from being deployed in your orchestrated container cluster. Using this Kubernetes capability, AKS supports the evaluation of requests to the Kubernetes API to deny requests that fail to meet defined security requirements.

Sysdig adds...

AKS can check against Sysdig Secure to evaluate whether an image is compliant with the configured security policies. When using the admission controller, this security validation decision will be propagated back to the API, which will reply to the original requester and only persist the object in the etcd database if the image passes the checks.

Additionally, Sysdig provides an Admission Controller that builds upon Kubernetes and elevates scan policies from detection to actual prevention. Container images that do not fulfill the configured admission policies will be rejected from your cluster before being assigned to a node and allowed to run.

The Sysdig Admission Controller provides granular admission policies, allowing you to define a global policy per cluster, but also at the level of particular namespaces or image paths (i.e., registries). Using this capability, you can set policies such as:

- Only allow images that pass the scanning evaluation criteria.
- Only allow images that have been evaluated recently.
- Only allow images that have been scanned before creation is requested to Kubernetes.
- Scan unscanned requested images immediately.

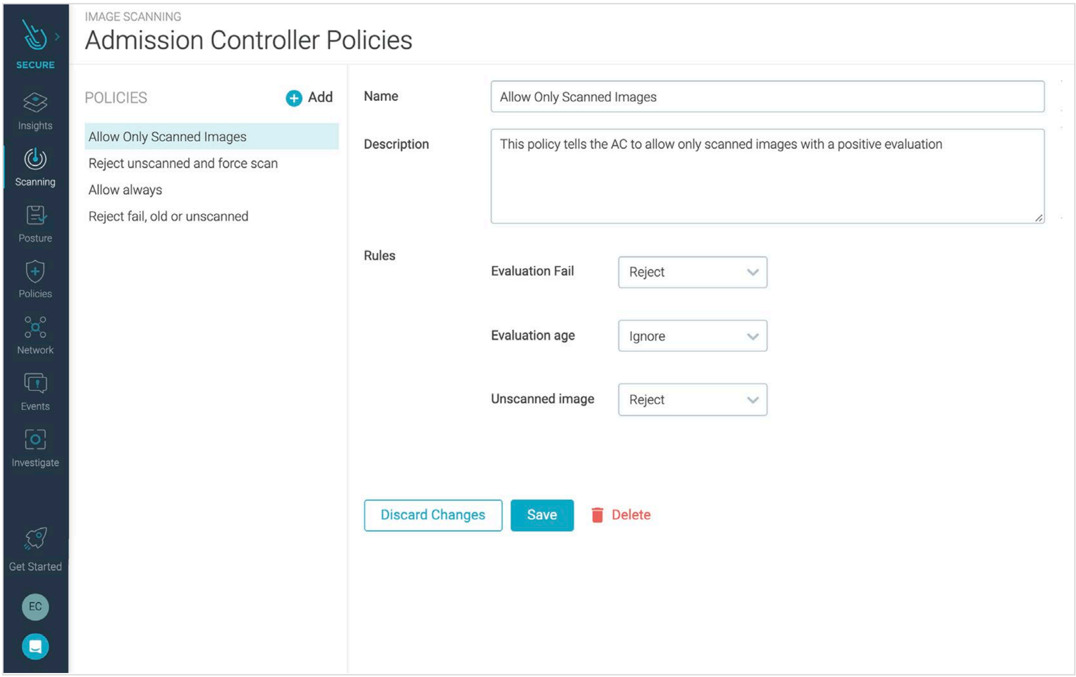


IMAGE SCANNING

Admission Controller Policies

POLICIES

- Allow Only Scanned Images
- Reject unscanned and force scan
- Allow always
- Reject fail, old or unscanned

Name: Allow Only Scanned Images

Description: This policy tells the AC to allow only scanned images with a positive evaluation

Rules

Evaluation Fail: Reject

Evaluation age: Ignore

Unscanned image: Reject

Registry security

In addition to securing your container images, the security of your registry itself is another key step to reduce risk for your organization. Using RBAC with Azure AD to manage who can pull and push container images, as well as using a private registry, are some of the steps you can take to protect your organization.

Microsoft Azure provides...

The Microsoft ACR managed container image registry service is secure, scalable, and reliable. ACR supports private image repositories with resource-based permissions using Azure AD and RBAC so that specific users, or Microsoft AVM instances, can access repositories and images. Developers can use the Docker CLI, the Azure CLI, or the Azure portal to push, pull, and manage images.

Sysdig adds...

Sysdig Secure container image scanning supports all Docker v2 compatible registries, including Microsoft ACR, Red Hat Quay, Amazon ECR, DockerHub Private Registries, Google Container Registry, Artifact Registry, JFrog Artifactory, SuSE Portus, and VMware Harbor.

To configure image scanning, you will enter your private registry credentials into Sysdig Secure. To ensure security, these credentials are encrypted when stored.

Continuous Compliance

Validating compliance in a dynamic cloud environment can be challenging. New layers of abstraction can obscure the visibility you need to prove compliance with standards such as NIST, HIPAA, PCI, and SOC 2. Enterprise computing environments running microservices in Azure can consist of hundreds or thousands of interconnected applications and services, as well as a large and diverse set of users. To maintain control over the security of this vast environment, a standard way to implement controls, scan systems, and capture data for compliance is needed.

Microsoft Azure provides...

Microsoft has achieved more than 90 compliance certifications, including over 50 specific to global regions and countries, such as the US, the European Union, Germany, Japan, the United Kingdom, India, and China. In addition, Azure features more than 35 compliance offerings specific to the needs of key industries, including health, government, finance, education, manufacturing, and media.

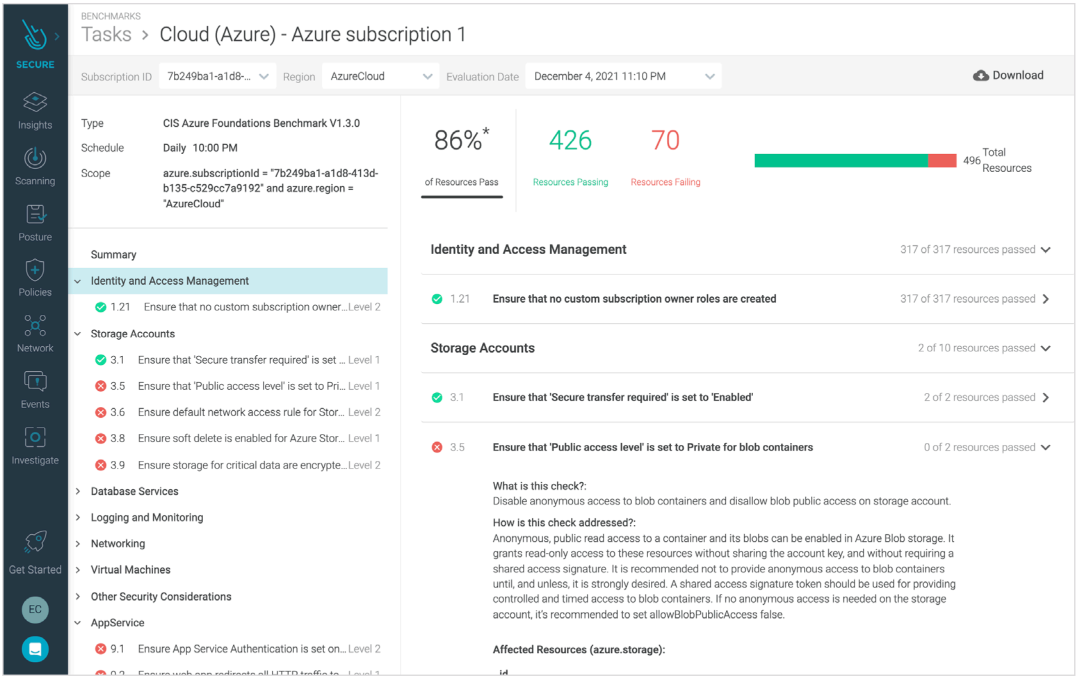
For example, Azure Policy is a service that enables you to assess, audit, and evaluate the configurations of your Azure resources. It monitors and records your Azure resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Sysdig adds....

Sysdig extends compliance for cloud and containers to help you adhere to the requirements for standards like NIST and PCI. Being able to validate that a deployment is compliant with desired configurations is one of the first compliance steps. But compliance requirements don’t end there. Compliance for containers introduces unique requirements and should be implemented at various points:

- Checking against cloud, container, and infrastructure security best practices using Center for Internet Security (CIS) benchmarks for Docker and Kubernetes.
- During build, mapping container image scanning policies to standards like NIST 800-190, PCI, and HIPAA.
- During runtime, using policies to continuously detect attack frameworks like MITRE ATT&CK or check compliance after deployment.
- Auditing any changes in your container environments, which is part of SOC 2, PCI, ISO, and HIPAA requirements.

Sysdig helps you track progress using compliance dashboards. Starting with the infrastructure layer, Sysdig performs specific host, platform, and container compliance checks, like Kubernetes benchmarks and Docker CIS benchmarks. Sysdig also provides remediation guidance for correcting policy violations. This makes resolving configuration issues faster when they come up.



BENCHMARKS

Tasks > Cloud (Azure) - Azure subscription 1

Subscription ID 7b249ba1-a1d8-... Region AzureCloud Evaluation Date December 4, 2021 11:10 PM Download

Type	CIS Azure Foundations Benchmark V1.3.0
Schedule	Daily 10:00 PM
Scope	azure.subscriptionId = "7b249ba1-a1d8-413d-b135-c529cc7a9192" and azure.region = "AzureCloud"

86%* of Resources Pass

426 Resources Passing

70 Resources Failing

496 Total Resources

Summary

- Identity and Access Management
  - ✓ 1.21 Ensure that no custom subscription owner... Level 2
- Storage Accounts
  - ✓ 3.1 Ensure that 'Secure transfer required' is set ... Level 1
  - ✗ 3.5 Ensure that 'Public access level' is set to Pri... Level 1
  - ✗ 3.6 Ensure default network access rule for Stor... Level 2
  - ✗ 3.8 Ensure soft delete is enabled for Azure Stor... Level 1
  - ✗ 3.9 Ensure storage for critical data are encrypte... Level 2
- Database Services
- Logging and Monitoring
- Networking
- Virtual Machines
- Other Security Considerations
- AppService
  - ✗ 9.1 Ensure App Service Authentication is set on... Level 2
  - ✗ 9.2 Ensure web app redirects all HTTP traffic to... Level 1

Identity and Access Management 317 of 317 resources passed

✓ 1.21 **Ensure that no custom subscription owner roles are created** 317 of 317 resources passed

Storage Accounts 2 of 10 resources passed

✓ 3.1 **Ensure that 'Secure transfer required' is set to 'Enabled'** 2 of 2 resources passed

✗ 3.5 **Ensure that 'Public access level' is set to Private for blob containers** 0 of 2 resources passed

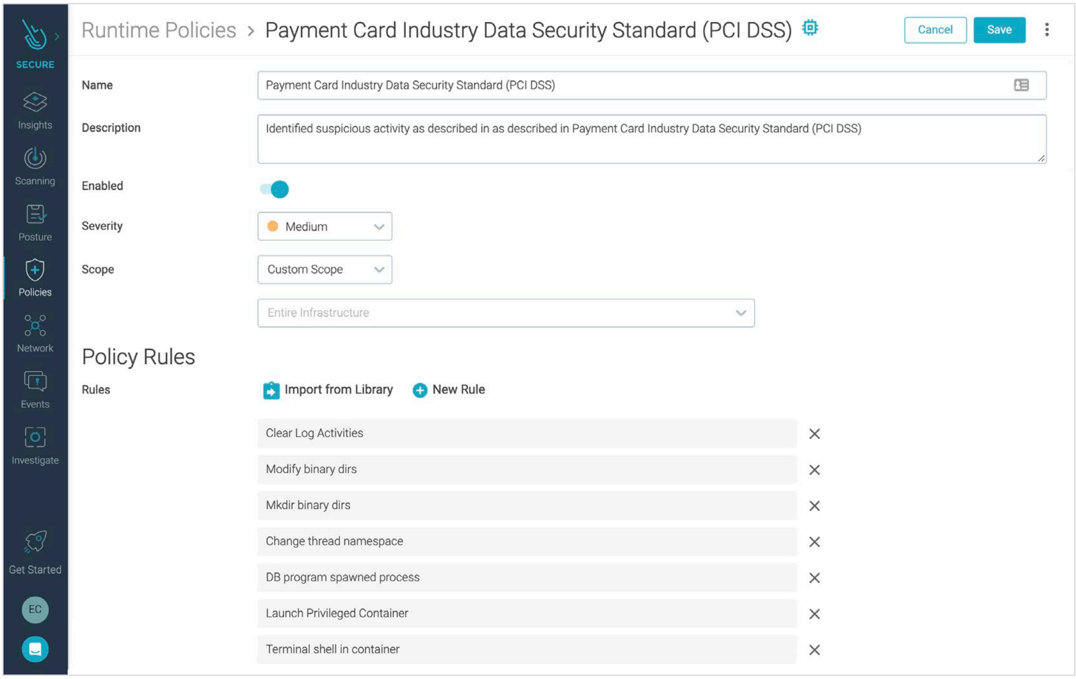
What is this check?:
Disable anonymous access to blob containers and disallow blob public access on storage account.

How is this check addressed?:
Anonymous, public read access to a container and its blobs can be enabled in Azure Blob storage. It grants read-only access to these resources without sharing the account key, and without requiring a shared access signature. It is recommended not to provide anonymous access to blob containers until, and unless, it is strongly desired. A shared access signature token should be used for providing controlled and timed access to blob containers. If no anonymous access is needed on the storage account, it's recommended to set allowBlobPublicAccess false.

Affected Resources (azure.storage):

id

Sysdig also provides runtime compliance assurance, translating leading security standards into a set of security detection policies. This enables analysis of container behavior aligned with compliance standards after deployment.



Runtime Policies > Payment Card Industry Data Security Standard (PCI DSS)

Name	Payment Card Industry Data Security Standard (PCI DSS)
Description	Identified suspicious activity as described in as described in Payment Card Industry Data Security Standard (PCI DSS)
Enabled	●
Severity	Medium
Scope	Custom Scope Entire Infrastructure

Policy Rules

Rules

- Clear Log Activities
- Modify binary dirs
- Mkdir binary dirs
- Change thread namespace
- DB program spawned process
- Launch Privileged Container
- Terminal shell in container

Network security

The shift of applications to containers and the cloud is a catalyst for rethinking your security model. Many cloud teams are taking a Zero Trust approach, requiring authentication and authorization even for networks internal to their organization.

The ability to segment, isolate, and control networks is a critical point of control for Zero Trust and is increasingly critical to achieving more effective security in container and Kubernetes environments.

Without the right tools, DevOps teams will struggle to see how their containerized apps are communicating, and may miss malicious attempts that take advantage of open network policies. Applying a Zero Trust network security model is challenging in Kubernetes, without knowing how applications are being used.

Microsoft Azure provides...

Containerized applications on Azure typically require access to other services running within the Kubernetes cluster, as well as external Azure cloud services. Azure addresses network security for Kubernetes with several mechanisms.

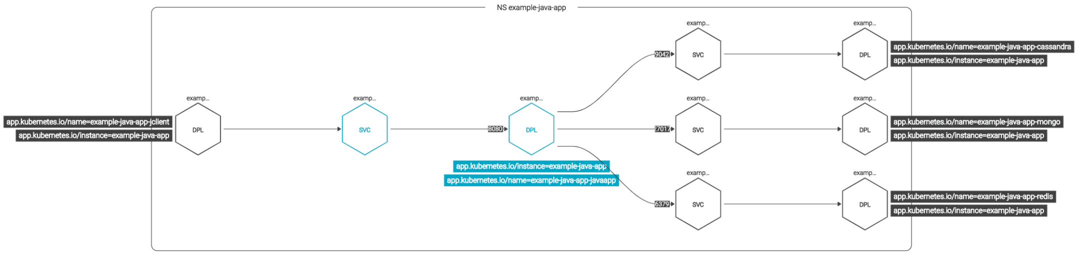
For securing connections to on-premises networks, you can deploy your AKS cluster into Azure virtual network subnets. Kubernetes ingress controllers can then be defined with private, internal IP addresses, so services are only accessible over this internal network connection. Azure uses network security group rules to filter the flow of traffic in virtual networks. These rules define the source and destination IP ranges, ports, and protocols that are allowed or denied access to resources.

In addition, AKS supports limiting network traffic between pods in your cluster by using Kubernetes network policies. . Kubernetes network policies allow or deny specific network paths within the cluster based on namespaces and label selectors.

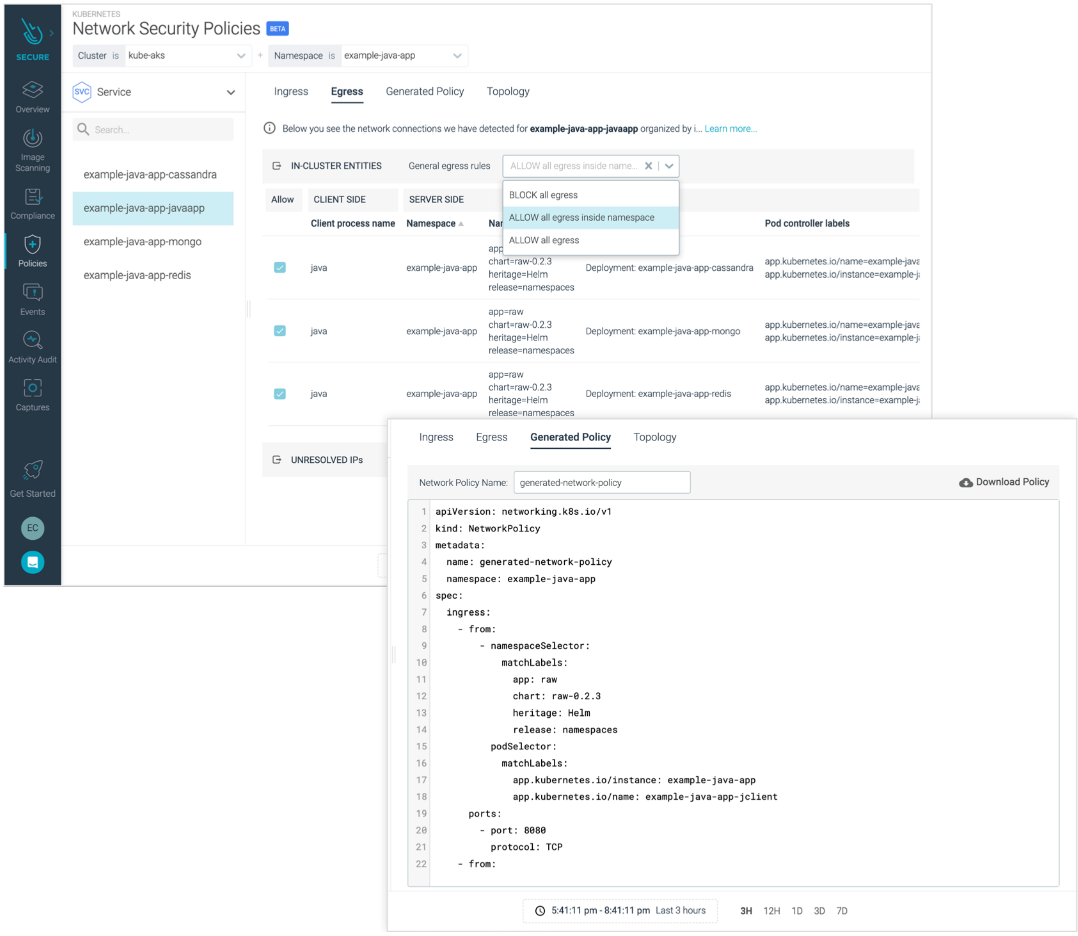
Sysdig adds...

With native network control in Kubernetes, supported by AKS as noted above, you get better performance, reliability, and security because Kubernetes itself enforces network microsegmentation. The challenge, however, is that Kubernetes network policies can be hard to implement without the right application knowledge and Kubernetes expertise. Sysdig helps remove these barriers to simplify implementing Zero Trust network security with the Kubernetes controls available with AKS.

Sysdig Secure automatically discovers all network traffic for AKS pods, services, and applications through visibility into system calls. The data is auto-tagged with Kubernetes context and labels, and used to simplify your experience when implementing Kubernetes network policies.


NS example-java-app
examp...
DPL
SVC
SVC
DPL
8080
9042
27017
6379
app.kubernetes.io/name=example-java-app-jclient
app.kubernetes.io/instance=example-java-app
app.kubernetes.io/instance=example-java-app
app.kubernetes.io/name=example-java-app-javaapp
app.kubernetes.io/name=example-java-app-cassandra
app.kubernetes.io/instance=example-java-app
app.kubernetes.io/name=example-java-app-mongo
app.kubernetes.io/instance=example-java-app
app.kubernetes.io/name=example-java-app-redis
app.kubernetes.io/instance=example-java-app

Dynamic topology maps let you visualize all network communication between apps and services, and drill down into the traffic flow over a particular time frame. Using this information in a simple UI, you can apply segmentation and refine network policies to allow or block connections. Sysdig will automatically generate a YAML file that you can use to apply the policy to your Kubernetes cluster.



Cluster is kube-aks + Namespace is example-java-app

example-java-app-cassandra
example-java-app-javaapp
example-java-app-mongo
example-java-app-redis

Below you see the network connections we have detected for **example-java-app-javaapp** organized by i...

IN-CLUSTER ENTITIES — General egress rules: ALLOW all egress inside name...

Allow	CLIENT SIDE		SERVER SIDE		
	Client process name	Namespace ▲	Nar		Pod controller labels
☑	java	example-java-app	app chart=raw-0.2.3 heritage=Helm release=namespaces	Deployment: example-java-app-cassandra	app.kubernetes.io/name=example-java app.kubernetes.io/instance=example-j
☑	java	example-java-app	app=raw chart=raw-0.2.3 heritage=Helm release=namespaces	Deployment: example-java-app-mongo	app.kubernetes.io/name=example-java app.kubernetes.io/instance=example-j
☑	java	example-java-app	app=raw chart=raw-0.2.3 heritage=Helm release=namespaces	Deployment: example-java-app-redis	app.kubernetes.io/name=example-java app.kubernetes.io/instance=example-j

Network Policy Name: generated-network-policy

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: generated-network-policy
  namespace: example-java-app
spec:
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              app: raw
              chart: raw-0.2.3
              heritage: Helm
              release: namespaces
          podSelector:
            matchLabels:
              app.kubernetes.io/instance: example-java-app
              app.kubernetes.io/name: example-java-app-jclient
      ports:
        - port: 8080
          protocol: TCP
    - from:
```

5:41:11 pm - 8:41:11 pm Last 3 hours

In addition, Sysdig Secure can fingerprint every connection, as well as the processes that are establishing connections. This Audit Tap capability helps cloud teams investigate network activity at a fine-grained level with full visibility into context, including labels. Enterprises subject to regulations, such as NIST and PCI, can leverage this capability along with network segmentation to meet compliance requirements.

Using Sysdig to enable Zero Trust network security based on an open, standards-based approach vetted by the community delivers better performance, reliability, and security because Kubernetes itself provides enforcement. This eliminates the need for man-in-the-middle enforcement mechanisms. By providing an easy-to-use interface and automating guardrails for teams who may lack Kubernetes expertise, Sysdig helps Azure users save time and reduce network security risk.

File Integrity Monitoring

File integrity monitoring (FIM) gives you visibility into file related activity across your container clusters running on Azure. It's used to detect tampering with critical system files and directories, as well as unauthorized changes, regardless of whether the activity is a malicious attack or an unplanned operational activity.

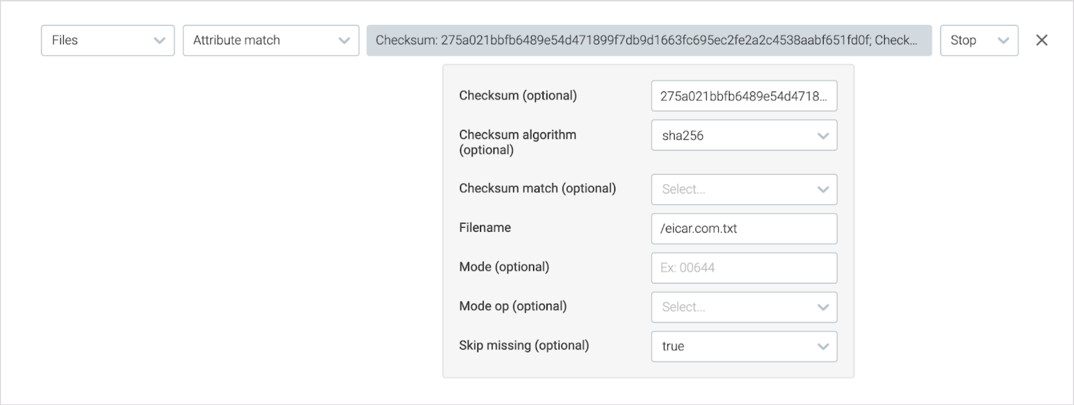
Microsoft Azure provides...

Azure Security Center with Azure Defender can examine your operating system files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack. By comparing the current state of these items with the state during the previous scan, Azure file integrity monitoring can identify if any suspicious modifications have been made and send you an alert.

Sysdig adds....

Sysdig enables file integrity monitoring at both the image scanning steps and as a part of runtime security. During image scanning, by policy, you can also check for specific file attributes within your registries and CI/CD pipelines. This allows you to fail builds early if FIM policies aren't met. File integrity monitoring policies allows you to:

- Check if a file exists or is missing, and trigger alerts based on the condition.
- Validate a specific file against its SHA256 hash to check for suspicious and potentially dangerous conditions like modifications to executable files.
- Validate file permissions to check, for example, if a file has an executable bit where it's not expected.
- Check for file names based on regex.
- Inspect image contents for exposed passwords, credential leaks, etc.

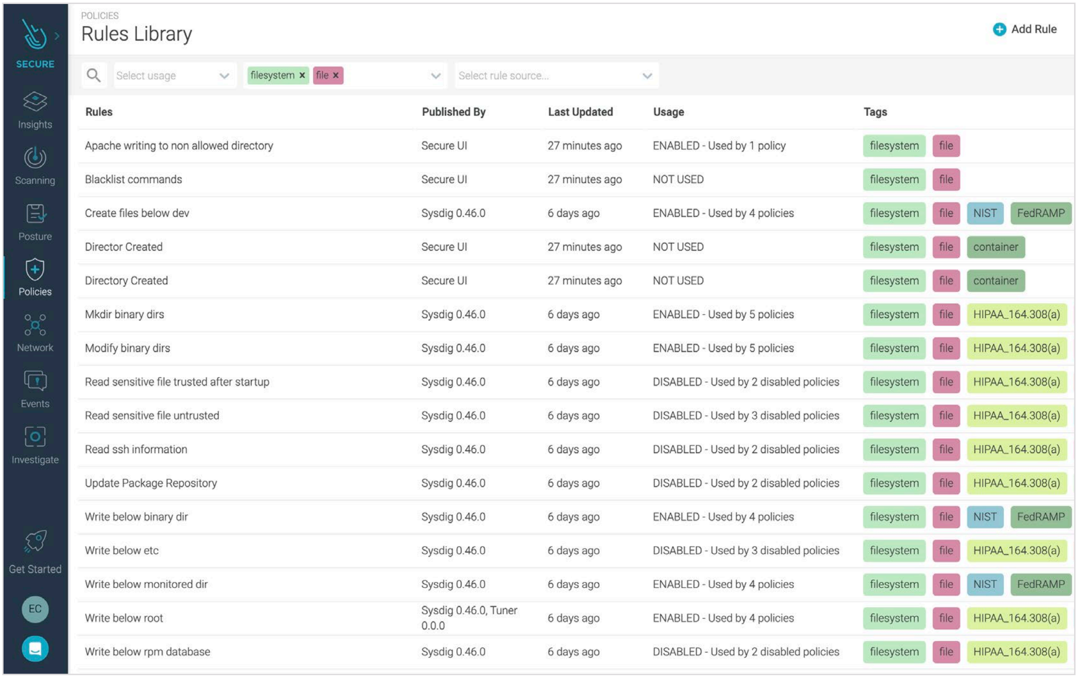


Checksum: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f; Check...

Checksum (optional)	275a021bbfb6489e54d4718...
Checksum algorithm (optional)	sha256
Checksum match (optional)	Select...
Filename	/eicar.com.txt
Mode (optional)	Ex: 00644
Mode op (optional)	Select...
Skip missing (optional)	true

For runtime, you can implement FIM policies to detect and alert on any suspicious filesystem changes. Below are common checks that Sysdig rules can help you enforce to ensure file integrity and a strong security posture:

- Creation or removal of files or directories.
- Renaming of files or directories.
- Changes to file or directory security settings such as permissions, ownership, and inheritance.
- Changes to the files of a container.
- Modification of files below the container's path.
- Deletion of bash history.



Rules Library

Rules	Published By	Last Updated	Usage	Tags
Apache writing to non allowed directory	Secure UI	27 minutes ago	ENABLED - Used by 1 policy	filesystem file
Blacklist commands	Secure UI	27 minutes ago	NOT USED	filesystem file
Create files below dev	Sysdig 0.46.0	6 days ago	ENABLED - Used by 4 policies	filesystem file NIST FedRAMP
Director Created	Secure UI	27 minutes ago	NOT USED	filesystem file container
Directory Created	Secure UI	27 minutes ago	NOT USED	filesystem file container
Mkdir binary dirs	Sysdig 0.46.0	6 days ago	ENABLED - Used by 5 policies	filesystem file HIPAA_164.308(a)
Modify binary dirs	Sysdig 0.46.0	6 days ago	ENABLED - Used by 5 policies	filesystem file HIPAA_164.308(a)
Read sensitive file trusted after startup	Sysdig 0.46.0	6 days ago	DISABLED - Used by 2 disabled policies	filesystem file HIPAA_164.308(a)
Read sensitive file untrusted	Sysdig 0.46.0	6 days ago	DISABLED - Used by 3 disabled policies	filesystem file HIPAA_164.308(a)
Read ssh information	Sysdig 0.46.0	6 days ago	DISABLED - Used by 2 disabled policies	filesystem file HIPAA_164.308(a)
Update Package Repository	Sysdig 0.46.0	6 days ago	DISABLED - Used by 2 disabled policies	filesystem file HIPAA_164.308(a)
Write below binary dir	Sysdig 0.46.0	6 days ago	ENABLED - Used by 4 policies	filesystem file NIST FedRAMP
Write below etc	Sysdig 0.46.0	6 days ago	DISABLED - Used by 3 disabled policies	filesystem file HIPAA_164.308(a)
Write below monitored dir	Sysdig 0.46.0	6 days ago	ENABLED - Used by 4 policies	filesystem file NIST FedRAMP
Write below root	Sysdig 0.46.0, Tuner 0.0.0	6 days ago	ENABLED - Used by 4 policies	filesystem file HIPAA_164.308(a)
Write below rpm database	Sysdig 0.46.0	6 days ago	DISABLED - Used by 2 disabled policies	filesystem file HIPAA_164.308(a)

Runtime security

Protecting running containers and your production environment is critical to reducing risk to your applications on Azure. As a start, it's important to configure applications with the minimum privilege and access permissions. In addition, you need to be able to create and maintain policies that observe workload behaviors to detect and respond to runtime threats that cannot be protected against by CI/CD or registry scanning alone.

Several security threats, by their very nature, only manifest during runtime, including:

- Zero-day vulnerabilities and non-public vulnerabilities specific to your own software.
- Software bugs causing erratic behavior or resource leaking.
- Internal privilege escalation attempts or hidden/embedded malware.

Real-time visibility into the activity of running containers is key to not only preventing unauthorized access, but is also a necessary control that enables you to meet compliance mandates.

Microsoft Azure provides...

To protect running containers, Microsoft recommends that you configure containers to operate with the lowest privileges and access required to get the job done. Azure Security Center will identify unmanaged containers and assess the configurations of these containers against the best practices ruleset documented in the CIS Docker Benchmark. If your containers don't satisfy any of the CIS controls, Security Center will alert you.

Using Security Center with Azure Defender, you can deploy a Log Analytics agent to monitor your Linux AKS nodes for suspicious activities. such as web shell detection and connection with known suspicious IP addresses. In addition, the Azure solution monitors for container-specific issues, such as privileged container creation, suspicious access to API servers, and Secure Shell (SSH) servers running inside a Docker container.

At the cluster level, Security Center and Azure Defender provide AKS threat protection by monitoring Kubernetes audit logs. You can, for instance, monitor for exposed Kubernetes dashboards, creation of high privileged roles, and the creation of sensitive mounts.

Sysdig adds....

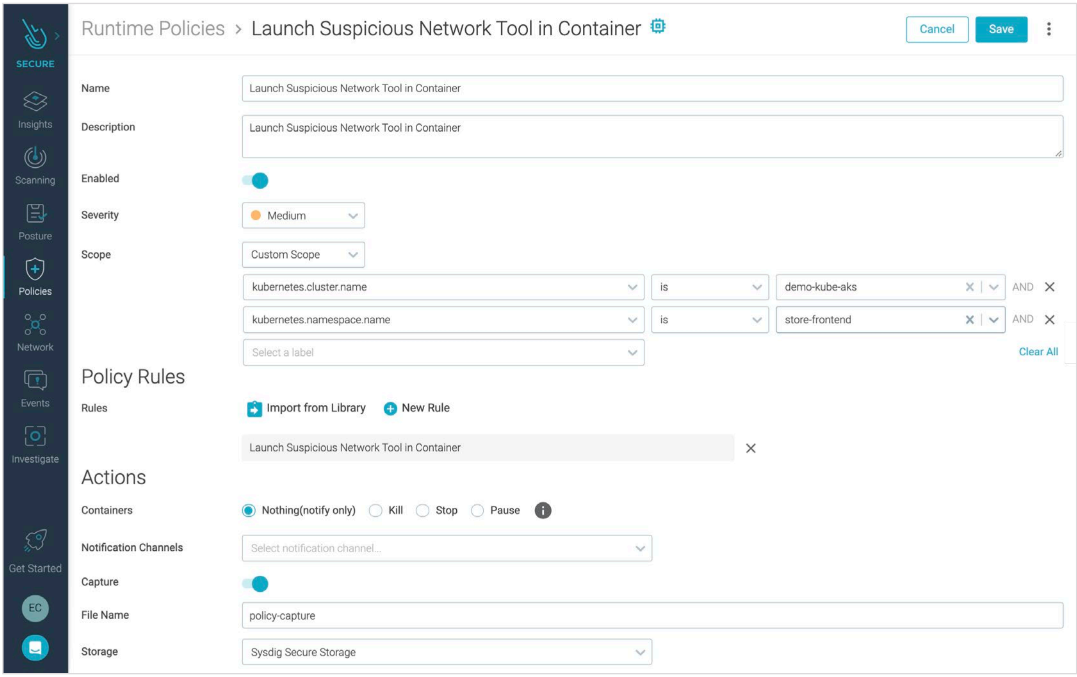
Security Monitoring

Visibility into cloud and container behaviors is one of the most important aspects of operating a secure cloud environment. Cloud teams need monitoring across Azure in order to identify threats like crypto-mining or denial of service (DoS) attacks. By automating identification of activity as abnormal deviations in a particular performance metric, organizations are able to stay ahead of potential attacks.

It is also important to reduce risk by configuring applications with the minimum privilege and access permissions. At the same time, you need to be able to create and maintain a runtime policy that observes workload behavior and looks for anomalous activity, blocking any threats and attacks not caught in your CI/CD or registry scanning.

Threat detection

Sysdig uses the CNCF Falco project open-source detection engine to monitor anomalous activity on hosts and containers at runtime. It ingests and monitors activity from Azure Activity Logs, as well as your orchestration layer, when using Kubernetes and GKE. Sysdig runtime security helps Azure users answer questions like, “who did what, where, and when?” within their containers, Kubernetes, and Azure cloud resources.



Runtime Policies > Launch Suspicious Network Tool in Container

Name: Launch Suspicious Network Tool in Container

Description: Launch Suspicious Network Tool in Container

Enabled: ●

Severity: Medium

Scope: Custom Scope

kubernetes.cluster.name is demo-kube-aks AND

kubernetes.namespace.name is store-frontend AND

Select a label

Policy Rules

Rules: Launch Suspicious Network Tool in Container

Actions

Containers: ● Nothing(notify only) ○ Kill ○ Stop ○ Pause

Notification Channels: Select notification channel...

Capture: ●

File Name: policy-capture

Storage: Sysdig Secure Storage

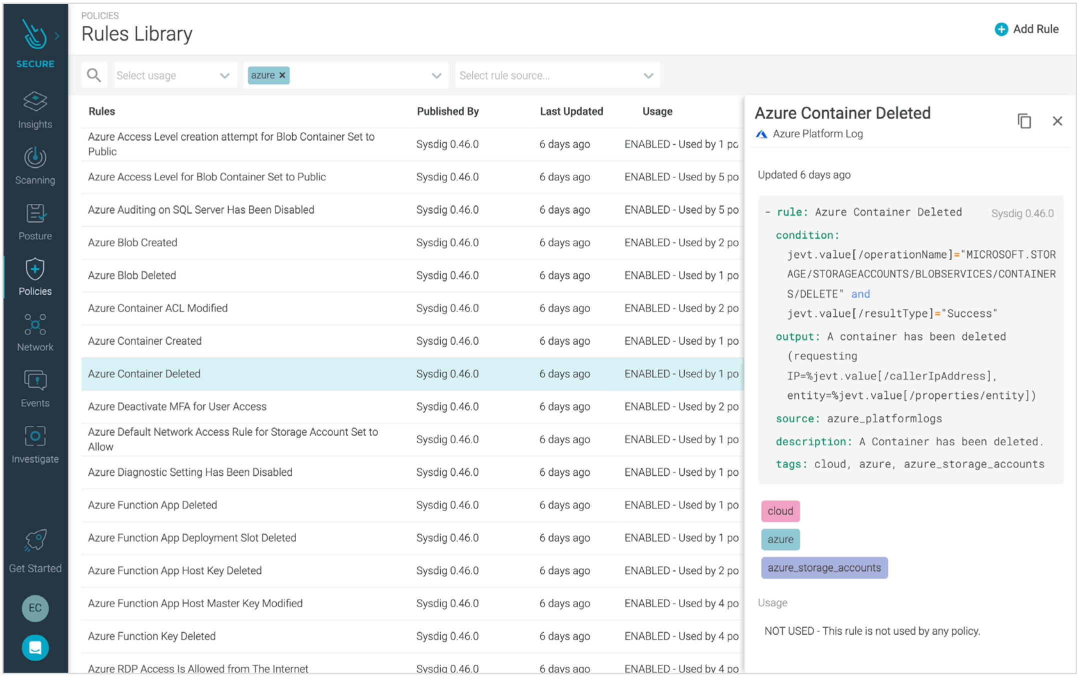
To reduce risk, threat detection must be continuous. Scanning your containers once during the CI/CD process or from your registry is simply not enough. Detecting software vulnerabilities is extremely valuable, however, some security threats only manifest during runtime. These include:

- Zero-day vulnerabilities and non-public vulnerabilities specific to your own software.
- Software bugs causing erratic behavior or resource leaks.
- Internal privilege escalation attempts or hidden/embedded malware.

Sysdig provides default policies out-of-the-box, along with more than 200 rules that simplify the job of customizing security to meet your requirements. Using Sysdig Secure policies, you can easily implement runtime security to detect threats to your Azure cloud and container services. This includes:

- Container runtime security policies for regulatory container compliance standards: NIST, PCI, ISO, HIPAA, and SOC2.
- Runtime detection of the most pervasive container attacks: Cryptomining, secrets exfiltration, container isolation breaches, and lateral movements.
- Security monitoring for unexpected process activity, outbound connections, and terminal shell sessions.
- Azure Activity Log detection rules to identify suspicious activity across your Azure services.

Using an extensible policy engine powered by open-source Falco, operations and security teams can customize their own rules through a visual interface to build fine-tuned policies that match unique business requirements. In addition, Falco rules that are community-sourced and curated are available on the Cloud Native Security Hub.



Rules Library

Rules	Published By	Last Updated	Usage
Azure Access Level creation attempt for Blob Container Set to Public	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Access Level for Blob Container Set to Public	Sysdig 0.46.0	6 days ago	ENABLED - Used by 5 po
Azure Auditing on SQL Server Has Been Disabled	Sysdig 0.46.0	6 days ago	ENABLED - Used by 5 po
Azure Blob Created	Sysdig 0.46.0	6 days ago	ENABLED - Used by 2 po
Azure Blob Deleted	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Container ACL Modified	Sysdig 0.46.0	6 days ago	ENABLED - Used by 2 po
Azure Container Created	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Container Deleted	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Deactivate MFA for User Access	Sysdig 0.46.0	6 days ago	ENABLED - Used by 2 po
Azure Default Network Access Rule for Storage Account Set to Allow	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Diagnostic Setting Has Been Disabled	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Function App Deleted	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Function App Deployment Slot Deleted	Sysdig 0.46.0	6 days ago	ENABLED - Used by 1 po
Azure Function App Host Key Deleted	Sysdig 0.46.0	6 days ago	ENABLED - Used by 2 po
Azure Function App Host Master Key Modified	Sysdig 0.46.0	6 days ago	ENABLED - Used by 4 po
Azure Function Key Deleted	Sysdig 0.46.0	6 days ago	ENABLED - Used by 4 po
Azure RDP Access Is Allowed from The Internet	Sysdig 0.46.0	6 days ago	ENABLED - Used by 4 po

Azure Container Deleted

Azure Platform Log

Updated 6 days ago

```
- rule: Azure Container Deleted        Sysdig 0.46.0
  condition:
    jevt.value[/operationName]="MICROSOFT.STOR
    AGE/STORAGEACCOUNTS/BLOBSERVICES/CONTAINER
    S/DELETE" and
    jevt.value[/resultType]="Success"
  output: A container has been deleted
    (requesting
    IP=%jevt.value[/callerIpAddress],
    entity=%jevt.value[/properties/entity])
  source: azure_platformlogs
  description: A Container has been deleted.
  tags: cloud, azure, azure_storage_accounts
```

cloud

azure

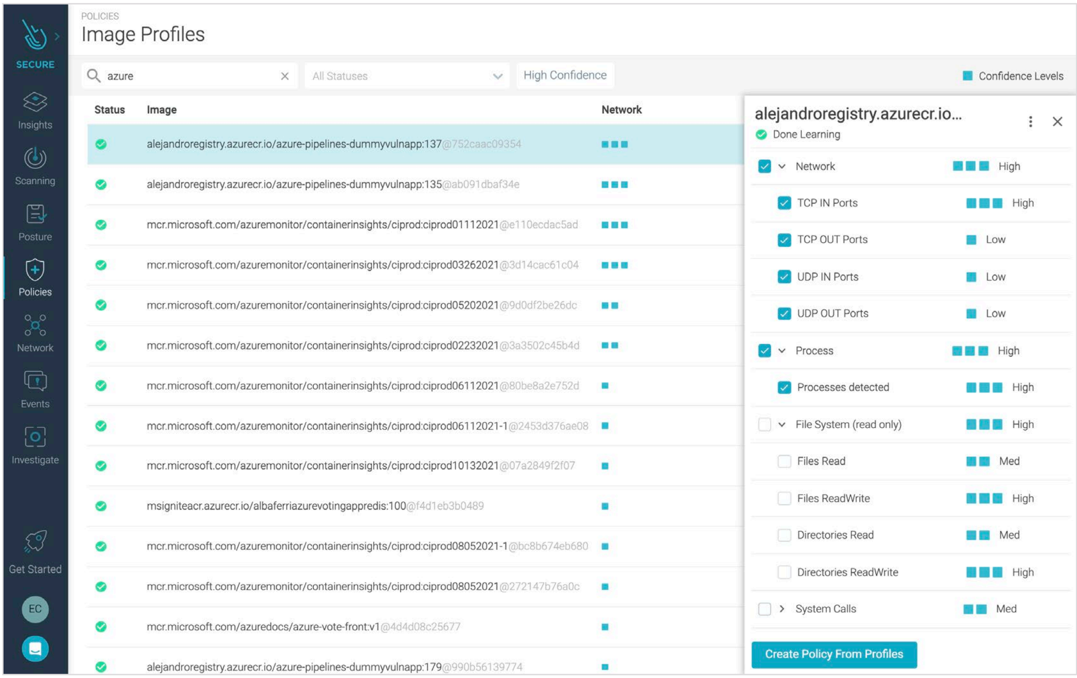
azure_storage_accounts

Usage

NOT USED - This rule is not used by any policy.

Runtime image profiling

To ease the burden of creating and maintaining runtime security in large-scale environments, Sysdig Secure features runtime image profiling. Image profiling automatically models, analyzes, and learns container runtime behavior to create a comprehensive container runtime profile and automatically build policies for you. This includes analyzing kube-apiserver activity and syscalls while enriching them with various metadata, including AKS, and cloud labels. This approach enhances anomaly detection through machine learning and helps you block threats before they propagate.



POLICIES

Image Profiles

azure ✕ | All Statuses | High Confidence | 🟦 Confidence Levels

Status	Image	Network
✓	alejandroregistry.azurecr.io/azure-pipelines-dummyvulnapp:137@752caac09354	■■■
✓	alejandroregistry.azurecr.io/azure-pipelines-dummyvulnapp:135@ab091dbaf34e	■■■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod01112021@e110ecdac5ad	■■■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod03262021@3d14cac61c04	■■■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod05202021@9d0df2be26dc	■■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod02232021@3a3502c45b4d	■■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod06112021@80be8a2e752d	■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod06112021-1@2453d376ae08	■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod10132021@07a2849f2f07	■
✓	msigniteacr.azurecr.io/albaferriazurevotingappredis:100@f4d1eb3b0489	■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod08052021-1@bc8b674eb680	■
✓	mcr.microsoft.com/azuremonitor/containerinsights/ciprod:ciprod08052021@272147b76a0c	■
✓	mcr.microsoft.com/azuredocs/azure-vote-front:v1@4d4d08c25677	■
✓	alejandroregistry.azurecr.io/azure-pipelines-dummyvulnapp:179@990b56139774	■

alejandroregistry.azurecr.io...

✓ Done Learning

☑ ⌄ Network	■■■	High
☑ TCP IN Ports	■■■	High
☑ TCP OUT Ports	■	Low
☑ UDP IN Ports	■	Low
☑ UDP OUT Ports	■	Low
☑ ⌄ Process	■■■	High
☑ Processes detected	■■■	High
□ ⌄ File System (read only)	■■■	High
□ Files Read	■■	Med
□ Files ReadWrite	■■■	High
□ Directories Read	■■	Med
□ Directories ReadWrite	■■■	High
□ › System Calls	■■	Med

Create Policy From Profiles

Microsoft Azure Cloud Security

Threat research conducted by Sysdig shows that having a single view across cloud, workloads, and containers speeds the time to both detect and respond to lateral movement attacks, a common technique used in the majority of security breaches.

However, using multiple cloud and container security tools complicates security operations because it requires manual correlation of different data sources to fully understand a breach and identify the impacted systems. Gaps are created and rather than comprehensive security, organizations end up with blind spots. Sysdig pairs Cloud Security Posture Management (CSPM) and cloud threat detection with cloud workload protection, including container and Kubernetes security features in a single platform.

Sysdig reduces the time required to identify threats in your Azure cloud services and containers from weeks to hours. Cloud development teams can see exactly where an attacker started and each step they took as they moved through the environment.

Threat Detection with Azure Activity Logs

Cloud activity logs help security teams view and maintain audit trails for activity that takes place with cloud-based services. Cloud logs record administrative and other service activity and are essential for helping your organization monitor unexpected or unwanted behavior. They are intended to provide you with a level of transparency that helps meet security and compliance mandates in the cloud.

Microsoft Azure provides...

Azure Activity Logs provide insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started. For some events, you can view the change history to see what changes happened during a particular event time. Activity logs can be exported and stored for security analysis and auditing of the activity recorded within your Azure subscription.

Sysdig adds....

Growth of your infrastructure, through usage, assets, workloads, and number of events and operational logs available can increase to a size that demands a more automated approach to analysis and response.

Sysdig automates Azure Activity Log evaluation in real-time by using a flexible set of security rules based on open-source Falco threat detection – the same engine that detects threats across containers and Kubernetes deployments.

Once configured, Sysdig Secure continuously detects and reports suspicious cloud activity and events for a wide range of Azure services, such as IAM, virtual machines, and storage. Here are just a few use case examples:

- Look for suspicious IAM activity and abnormal permission changes.
- Detect process execution patterns for unexpected behavior or remote code executions.
- Look for credential theft, especially for longer-lived or high-privilege credentials.
- Identify changes in the configuration of cloud resources (e.g., cloud storage).

Continuously validate cloud configurations

Wrongly configured hosts, container runtimes, clusters, or cloud resources can leave a door open to an attack, or create an easy way to escalate privileges and perform lateral movement.

Benchmarks, best practices, and hardening guides, such as those provided by the Center for Internet Security (CIS), provide you with information about how to spot those misconfigurations, why they are a problem, and how to remediate them.

Microsoft Azure provides...

Microsoft has collaborated with the Center for Internet Security to create the, CIS Microsoft Azure Foundations Security Benchmark. This CIS Benchmark standard provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure.

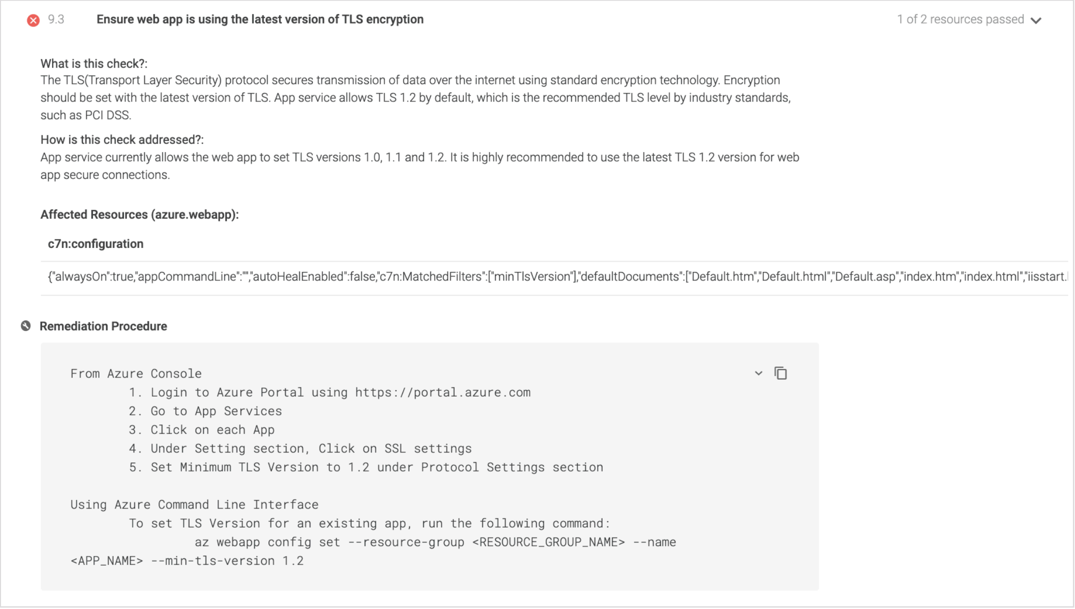
The CIS Microsoft Azure Foundations Security Benchmark provides recommendations across a wide range of cloud areas including:

- Identity and access management
- Storage accounts
- Database services
- Logging and monitoring
- Networking
- Virtual machines

Sysdig adds....

Sysdig Secure automates environment checks based on the CIS Microsoft Azure Foundations Security Benchmark as well as other compliance standards to detect and flag cloud misconfigurations.

Sysdig Secure leverages open source Cloud Custodian to provide curated, out-of-the-box policies to quickly assess configurations and the security posture of your Azure cloud. You can schedule Azure assessments and provide real-time insight with interactive dashboards. Within the Sysdig Secure UI, recommendations are provided to help users make the necessary changes to remediate misconfigurations.



9.3 **Ensure web app is using the latest version of TLS encryption**

What is this check?:
The TLS(Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology. Encryption should be set with the latest version of TLS. App service allows TLS 1.2 by default, which is the recommended TLS level by industry standards, such as PCI DSS.

How is this check addressed?:
App service currently allows the web app to set TLS versions 1.0, 1.1 and 1.2. It is highly recommended to use the latest TLS 1.2 version for web app secure connections.

Affected Resources (azure.webapp):

c7n:configuration

{"alwaysOn":true,"appCommandLine":"","autoHealEnabled":false,"c7n:MatchedFilters":["minTlsVersion"],"defaultDocuments":["Default.htm","Default.html","Default.asp","index.htm","index.html","iisstart.

Remediation Procedure

```
From Azure Console
        1. Login to Azure Portal using https://portal.azure.com
        2. Go to App Services
        3. Click on each App
        4. Under Setting section, Click on SSL settings
        5. Set Minimum TLS Version to 1.2 under Protocol Settings section

Using Azure Command Line Interface
        To set TLS Version for an existing app, run the following command:
                az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --min-tls-version 1.2
```

Monitoring Azure container services

Monitoring the dynamic nature of container-based applications is critical for high availability and performance of cloud services. Microservice architectures running on containers and cloud have made applications easier to scale and faster to develop, allowing faster innovation and accelerated time-to-market for new features. As the number of microservices grows within an application, it can become difficult to ensure visibility inside these environments. Microservices-based applications can be distributed across multiple instances, and containers can move across multi-cloud infrastructure as needed. Monitoring the Kubernetes orchestration state is key to understanding if Kubernetes is keeping all of the service instances up and running.

Microsoft Azure provides...

Microsoft offers Azure Monitor, a service that monitors and observes the operational health of Azure resources and applications through logs, metrics, and events.

Azure Monitor provides data and insights into applications and system-wide performance changes, and can help you optimize resource utilization. It collects monitoring and operational data in the form of logs, metrics, and events to give you visibility into Azure resources and services that run on Azure. With Azure Monitor, you can detect anomalous behavior, set alarms, visualize logs and metrics, take automated actions, and troubleshoot issues to help you keep your applications running smoothly.

The Container Monitoring solution in Azure Monitor shows which containers are running, what container image they're running, and where containers are running. You can troubleshoot containers by viewing and searching centralized logs that show container CPU, memory, storage, and network usage and performance information.

Sysdig Adds....

Sysdig Monitor allows you to maximize the performance and availability of your cloud infrastructure, services, and applications. Built on open source, it provides immediate, deep visibility into rapidly changing container environments. You can resolve issues faster by using granular data derived from actual system calls enriched with cloud and Kubernetes context along with Prometheus metrics. Sysdig Monitor helps you remove silos by unifying data across teams for hybrid and multi-cloud monitoring..

With Sysdig Monitor, we offer a scalable managed Prometheus service that frees cloud teams from the burden of setting up and managing their own monitoring system without sacrificing the benefits of the Prometheus open standard. Sysdig Monitor provides automatic discovery and assisted deployment of Prometheus monitoring integrations along with preconfigured dashboards and alerts.

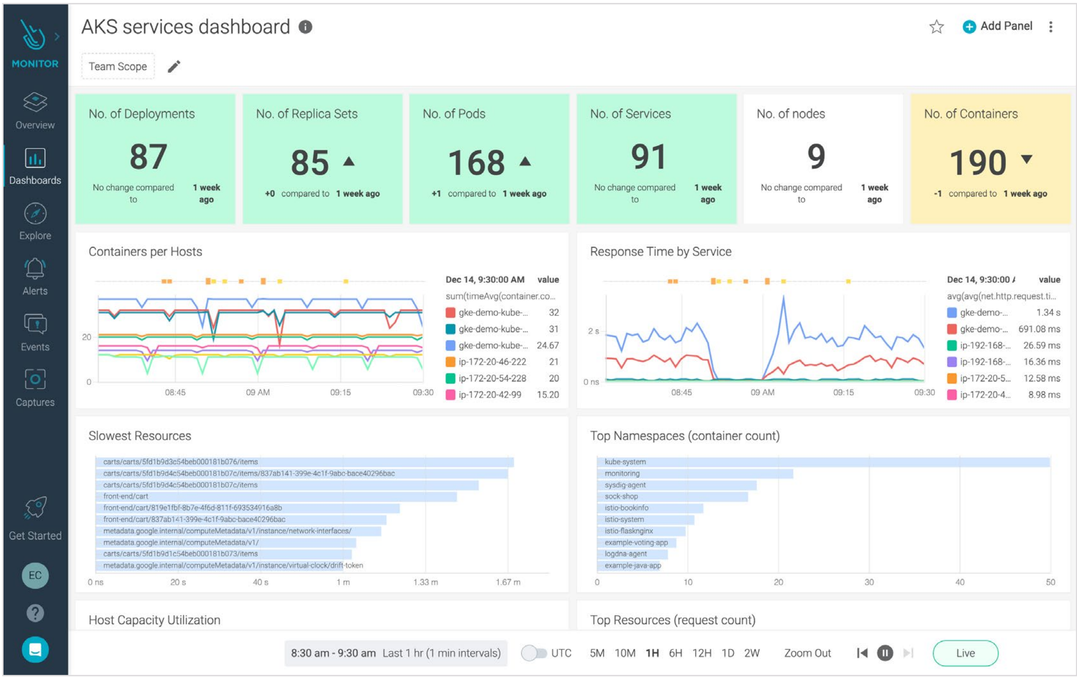
Support for the Prometheus Query Language (PromQL) and a PromQL Explorer Sysdig simplifies your interaction with metrics to speed mean time to discover (MTTD) using queries. In addition, a PromQL Library helps you discover popular queries from the monitoring community to learn new ways to get to the information that really matters.

Sysdig provides a single source of truth that helps you resolve issues faster by using granular data derived from kernel-level system calls enriched with cloud and Kubernetes context. Using Sysdig Monitor with Sysdig Secure enables you to remove silos by unifying data across teams to ensure the performance and security of your public and hybrid cloud deployments.

Kubernetes and container monitoring

With Sysdig, cloud teams receive automatic alerts and detailed health and performance information, including golden signals for clusters, deployments, namespaces, and workloads. Deep visibility into container activity enriched with cloud and Kubernetes context allows teams to manage the complexity of container deployments. This allows you to:

- Monitor health and performance with deep visibility into infrastructure, services, and applications. Get the operational status of the cluster with Kubernetes orchestration monitoring.
- Immediately identify owners for issue resolution using container and cloud context.
- Identify pods consuming excessive resources and monitor capacity limits.
- Control unexpected billing and application rollouts and rollbacks of deployment by monitoring auto-scaling behavior.
- Reduce cost by optimizing capacity across clusters and clouds.



Dec 14, 9:30:00 AM	value
sum(timeAvg(container.co...	
🟥 gke-demo-kube-...	32
🟦 gke-demo-kube-...	31
🟦 gke-demo-kube-...	24.67
🟧 ip-172-20-46-222	21
🟩 ip-172-20-54-228	20
🟪 ip-172-20-42-99	15.20

Dec 14, 9:30:00 /	value
avg(avg(net.http.request.ti...	
🟦 gke-demo-...	1.34 s
🟥 gke-demo-...	691.08 ms
🟩 ip-192-168-...	26.59 ms
🟪 ip-192-168-...	16.36 ms
🟧 ip-172-20-5...	12.58 ms
🟪 ip-172-20-4...	8.98 ms

carts/carts/5fd1b9d3c54beb000181b076/items
carts/carts/5fd1b9d4c54beb000181b07c/items/837ab141-399e-4c1f-9abc-bace40296bac
carts/carts/5fd1b9d4c54beb000181b07c/items
front-end/cart
front-end/cart/819e1fbf-8b7e-4f6d-811f-693534916a8b
front-end/cart/837ab141-399e-4c1f-9abc-bace40296bac
metadata.google.internal/computeMetadata/v1/instance/network-interfaces/
metadata.google.internal/computeMetadata/v1/
carts/carts/5fd1b9d1c54beb000181b073/items
metadata.google.internal/computeMetadata/v1/instance/virtual-clock/drift-token

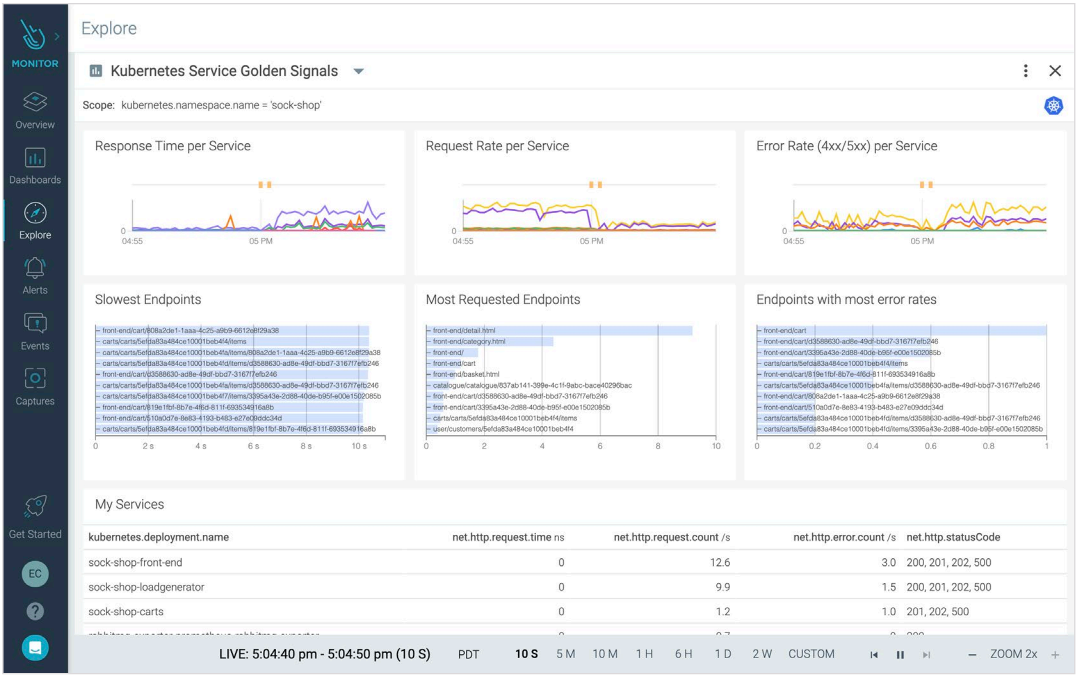
kube-system
monitoring
sysdig-agent
sock-shop
istio-bookinfo
istio-system
istio-flasknginx
example-voting-app
logdna-agent
example-java-app

Application & services monitoring

Latency, error, traffic, and saturation metrics are known as the golden signals for monitoring service health. These metrics indicate the real health and performance of your application as seen by users interacting with that service. You can save time by looking at what really matters, avoiding traps that could mask the real problems with applications.

Sysdig Monitor allows you to:

- Improve application performance and rapidly solve issues with deep container visibility and granular metrics, enriched with Kubernetes and cloud context.
- Monitor the impact of a given security incident on the availability of a service to your users.
- Reduce risk by utilizing enterprise-grade access controls for your monitoring system, including teams, SSO, and RBAC.
- Leverage your existing developer investment with full Prometheus and PromQL compatibility. DevOps teams can use the industry-standard their developers prefer without running into scaling challenges.
- Get productive faster by using PromCat.io, a resource catalog of Prometheus integrations with curated, documented, and supported monitoring integrations for Kubernetes platforms and cloud-native services.
- Extend monitoring to hundreds of applications and services using Prometheus-compatible exporters, dashboards, and alerts. Out-of-the-box dashboards (including PromQL and Grafana dashboards) display metrics from cloud services, databases, and other key components in your application environment.
- Accelerate time to insight with a single source of truth for application availability and security, so teams can resolve issues faster.


MONITOR
Overview
Dashboards
Explore
Alerts
Events
Captures
Get Started
EC
Explore
Kubernetes Service Golden Signals
Scope: kubernetes.namespace.name = 'sock-shop'
Response Time per Service
0
04:55
05 PM
Request Rate per Service
0
04:55
05 PM
Error Rate (4xx/5xx) per Service
0
04:55
05 PM
Slowest Endpoints
front-end/cart/808a2de1-1aaa-4c25-a9b9-6612e8f29a38
carts/carts/5efda83a484ce10001beb4f4/items
carts/carts/5efda83a484ce10001beb4fa/items/808a2de1-1aaa-4c25-a9b9-6612e8f29a38
carts/carts/5efda83a484ce10001beb4fd/items/d3588630-ad8e-49df-bbd7-3167f7efb246
front-end/cart/d3588630-ad8e-49df-bbd7-3167f7efb246
carts/carts/5efda83a484ce10001beb4fa/items/d3588630-ad8e-49df-bbd7-3167f7efb246
carts/carts/5efda83a484ce10001beb4f7/items/3395a43e-2d88-40de-b95f-e00e1502085b
front-end/cart/819e1fbf-8b7e-4f6d-811f-693534916a8b
front-end/cart/510a0d7e-8e83-4193-b483-e27e09ddc34d
carts/carts/5efda83a484ce10001beb4fd/items/819e1fbf-8b7e-4f6d-811f-693534916a8b
0
2 s
4 s
6 s
8 s
10 s
Most Requested Endpoints
front-end/detail.html
front-end/category.html
front-end/
front-end/cart
front-end/basket.html
catalogue/catalogue/837ab141-399e-4c1f-9abc-bace40296bac
front-end/cart/d3588630-ad8e-49df-bbd7-3167f7efb246
front-end/cart/3395a43e-2d88-40de-b95f-e00e1502085b
carts/carts/5efda83a484ce10001beb4f4/items
user/customers/5efda83a484ce10001beb4f4
0
2
4
6
8
10
Endpoints with most error rates
front-end/cart
front-end/cart/d3588630-ad8e-49df-bbd7-3167f7efb246
front-end/cart/3395a43e-2d88-40de-b95f-e00e1502085b
carts/carts/5efda83a484ce10001beb4f4/items
front-end/cart/819e1fbf-8b7e-4f6d-811f-693534916a8b
carts/carts/5efda83a484ce10001beb4fa/items/d3588630-ad8e-49df-bbd7-3167f7efb246
front-end/cart/808a2de1-1aaa-4c25-a9b9-6612e8f29a38
front-end/cart/510a0d7e-8e83-4193-b483-e27e09ddc34d
carts/carts/5efda83a484ce10001beb4fd/items/d3588630-ad8e-49df-bbd7-3167f7efb246
carts/carts/5efda83a484ce10001beb4fd/items/3395a43e-2d88-40de-b95f-e00e1502085b
0
0.2
0.4
0.6
0.8
1
LIVE: 5:04:40 pm - 5:04:50 pm (10 S)
PDT
10 S
5 M
10 M
1 H
6 H
1 D
2 W
CUSTOM
ZOOM 2x

My Services

kubernetes.deployment.name	net.http.request.time ns	net.http.request.count /s	net.http.error.count /s	net.http.statusCode
sock-shop-front-end	0	12.6	3.0	200, 201, 202, 500
sock-shop-loadgenerator	0	9.9	1.5	200, 201, 202, 500
sock-shop-carts	0	1.2	1.0	201, 202, 500

Container forensics and incident response

When troubleshooting an issue or performing a post-mortem analysis of a security incident, one of the typical challenges is that when a container stops, the information within it is also gone. This happens frequently with container solutions. Containers are frequently scaled up and down with a cluster or across nodes to meet the ebb and flow of demand.

Sysdig's 2021 Container Security and Usage Report found that 49 percent of Sysdig customer containers live less than five minutes. Real-time visibility into short-lived containers, as well as the ability to capture a snapshot of what happened surrounding any incident, is critical to identifying the root cause of problems.

Microsoft Azure provides...

Azure Monitor provides Azure insights using logs, metrics, and events., This information helps you understand how your applications are performing and proactively identify issues affecting your apps and the resources they depend on.

Azure Monitorlit was, however, was not built for troubleshooting dynamic containers. The ephemeral nature of containers makes it difficult to analyze what happened with a security incident after the container is gone. How can you reproduce the steps taken by the intruder? How did they gain access? What was the impact? Did they install any malware? Was any data leaked? How far did the attack extend?

Sysdig adds...

Sysdig forensics and aActivity aAudit speeds incident response and enables audit for Kubernetes. Sysdig captures and correlates executed commands, network, and Kubernetes activity so SOC teams can spot what happened. With Sysdig captures, you can also record all container activity at a detailed level, including spawned processes, network connections, file system activity, etc., so you can understand events in detail and conduct Kubernetes investigationsforensics after the container is long gone.

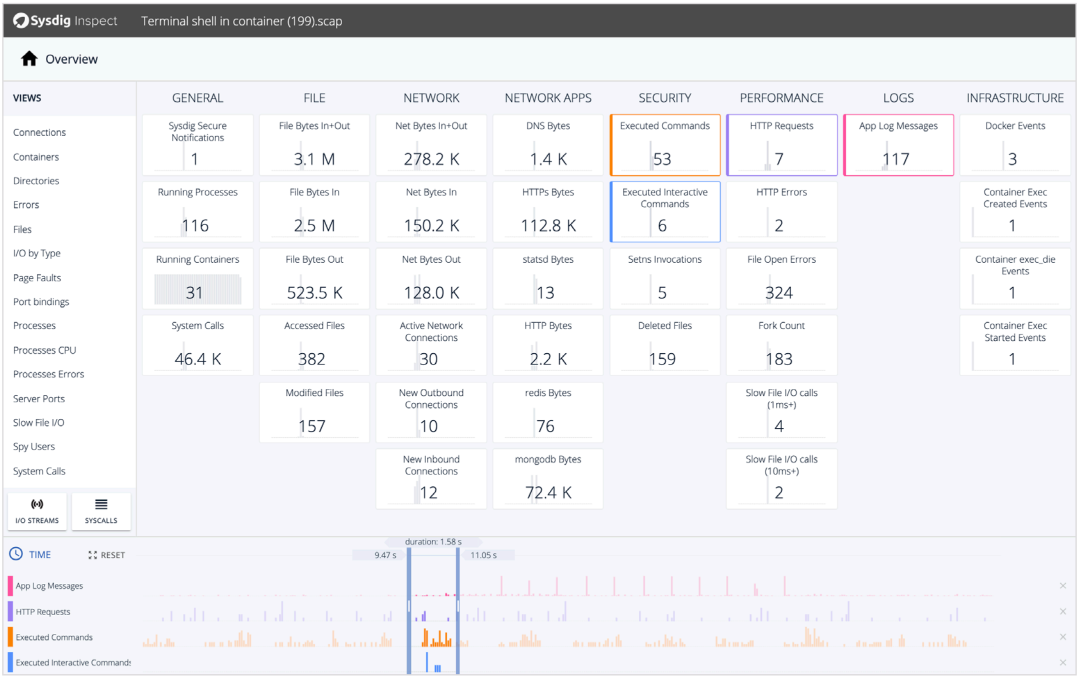
Read more about this in the blog Incident response in Kubernetes with Sysdig's Activity Audit.

Sysdig will deliver notifications to your alerting channels or SIEM. This allows you to consolidate security findings across your container environments so you can view and manage security alerts, and automate compliance checks across your Azure account.

With Sysdig, security teams can resolve issues inside pods and conduct forensics by reconstructing system activities correlated with AKS application context.

Sysdig provides:

- Streamlined incident response to quickly determine what happened with a detailed activity record, so you can investigate incidents such as data exfiltration, lateral movement, etc.
- Sysdig captures that support forensics to help you quickly understand and contain the impact of any security breach. Easily recreate the steps taken on intrusion, including file activity, network traffic, application protocols, commands, logs, and events.
- Insights into what took place in your Azure environment even if the containers that were running are long gone.



GENERAL	FILE	NETWORK	NETWORK APPS	SECURITY	PERFORMANCE	LOGS	INFRASTRUCTURE
Sysdig Secure Notifications 1	File Bytes In+Out 3.1 M	Net Bytes In+Out 278.2 K	DNS Bytes 1.4 K	Executed Commands 53	HTTP Requests 7	App Log Messages 117	Docker Events 3
Running Processes 116	File Bytes In 2.5 M	Net Bytes In 150.2 K	HTTPs Bytes 112.8 K	Executed Interactive Commands 6	HTTP Errors 2		Container Exec Created Events 1
Running Containers 31	File Bytes Out 523.5 K	Net Bytes Out 128.0 K	statsd Bytes 13	Setns Invocations 5	File Open Errors 324		Container exec_die Events 1
System Calls 46.4 K	Accessed Files 382	Active Network Connections 30	HTTP Bytes 2.2 K	Deleted Files 159	Fork Count 183		Container Exec Started Events 1
	Modified Files 157	New Outbound Connections 10	redis Bytes 76		Slow File I/O calls (1ms+) 4		
		New Inbound Connections 12	mongodb Bytes 72.4 K		Slow File I/O calls (10ms+) 2		

Better together with Azure + Sysdig Secure DevOps Platform

Implementing a secure DevOps workflow for Azure container services will help you simplify the transition to applications built on top of AKS. The following table summarizes the security and monitoring layers outlined above, highlighting Microsoft Azure solutions as well as the joint benefits of leveraging the Sysdig Secure DevOps Platform to further enhance security, compliance, and monitoring for containers and Kubernetes.

Container platforms

	Azure	Benefits of Sysdig + Azure
Kubernetes	Reduce platform operational overhead and simplify container application deployment. • Azure Kubernetes Service (AKS) • Azure Red Hat OpenShift (ARO)	Automate container application security, compliance, monitoring, and troubleshooting to confidently run containers, Kubernetes, and cloud services.

Security

	Azure	Benefits of Sysdig + Azure
Host OS	Microsoft Azure Virtual Machines – protected by Azure global network security procedures. Secure operating systems including Red Hat Enterprise Linux (RHEL) and Flatcar Container Linux.	Implement host scanning to identify vulnerabilities. Analyze AVM configurations to ensure hosts meet CIS benchmark best practices.
Access Control	Azure Active Directory and RBAC – secure authentication and access control.	Implement service-based access control to streamline security and monitoring information to individual users and teams.

	Azure	Benefits of Sysdig + Azure
Image Scanning & Vulnerability Management	Security Center with Azure Defender – scan images pushed to ACR.	Scan images pre-deployment within CI/CD pipelines (Azure Pipelines, GitHub Actions, etc.) and supported registries (ACR, Quay, DockerHub, etc.), and report on the impact of new CVEs to containers running in production.
Compliance	Azure Policy – evaluate the configuration settings of your Azure resources.	Enforce continuous compliance with out-of-the box configuration checks for PCI, GDPR, NIST, HIPAA, etc. and report with custom assessments and dashboards.
File Integrity Monitoring	Security center with Azure Defender – examine OS files, Windows registries, application software, and Linux system files for changes.	Sysdig Secure filesystem policies enable you to quickly implement file integrity monitoring (FIM) for containers and alert on suspicious changes to files and directories.
Runtime Security	Security Center with Azure Defender – monitor Linux AKS nodes for suspicious activities.	Detect anomalous behavior and attacks using deep system call visibility and AKS event auditing. Scope runtime policies based on AKS labels and metadata. Powered by the open-source CNCF runtime security project Falco.
Cloud Workload Protection Runtime Detection & Threat Prevention	Azure Activity Logs	Scope runtime security policies for containers and infrastructure with cloud and Azure context to detect and prevent anomalous behavior. Detect and block attacks, combining deep visibility through system calls, Azure Activity Logs, and audit events with Azure metadata. Powered by open-source CNCF runtime security project Falco.

	Azure	Benefits of Sysdig + Azure
Network Security	Leverage Azure virtual network subnets to secure connections together with Kubernetes ingress controllers. Limit network traffic between AKS pods using Kubernetes network policies.	Simplify Zero Trust network security with Kubernetes controls. Automatically discover all network traffic for AKS pods, services, and applications through visibility into system calls. Auto-tag data with Kubernetes context and labels, simplifying your experience when implementing Kubernetes network policies.
Container Forensics	N/A	Conduct forensics and post-mortem analysis even after AKS terminates containers/pods.

Compliance

	Azure	Benefits of Sysdig + Azure
Compliance to meet standards like NIST, PCI, SOC 2, etc.	Azure Policy – assess, audit, and evaluate the configurations of your Azure resources against desired configurations.	Continuously validate compliance using out-of-the-box image scanning policies, automated CIS benchmark checks for Docker and Kubernetes, and container runtime policies.

Monitoring / Visibility

Monitoring	Azure	Benefits of Sysdig + Azure
Container, Kubernetes, and Cloud service metrics and events	Azure Monitor with Container Monitoring – Observe the operational health of Azure resources and applications through logs, metrics, and events. View logs to see CPU, memory, storage, and network usage and performance information.	Get deep visibility into container infrastructure, services, and applications. Visualize and correlate container, Kubernetes, and infrastructure metrics and events across clusters and clouds. This helps to identify and resolve issues faster. Extend monitoring to hundreds of applications and services using Prometheus-compatible exporters, out-of-the-box dashboards, and alerts.

Conclusion

Visibility into security, compliance, and performance is necessary for a successful cloud transformation journey. Microsoft provides baseline coverage for security and monitoring with Azure container services. As you scale out the number of applications, clusters, and locations, Sysdig complements Azure offerings to enable developers, cloud teams, and security teams to extend capabilities to further reduce risk and ensure availability of your applications.

With Sysdig for Azure, you can secure the build pipeline, detect and respond to runtime threats, continuously validate compliance, and monitor and troubleshoot containers, Kubernetes, and cloud services. The Sysdig Secure DevOps Platform provides a SaaS-first option that enables you to scale simply with DevOps integrations that help you ensure the success of your cloud-native initiatives.

Start your free trial today to experience what Sysdig can do for your Azure container services deployments: https://sysdig.com/company/free-trial/

Find out how the Sysdig Secure DevOps Platform can help you and your teams confidently run cloud-native apps in production. Contact us for additional details about the platform, or to arrange a personalized demo.

www.sysdig.com

sysdig