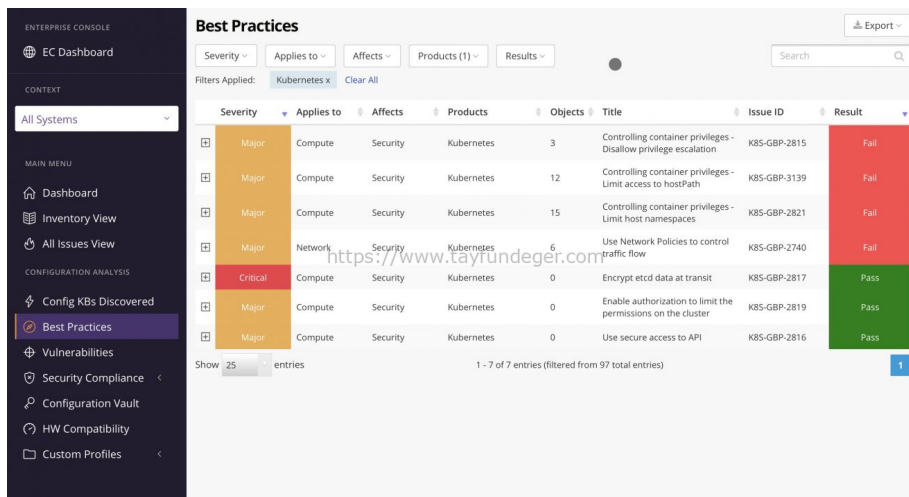


Runecast Kubernetes Ortamınızı Nasıl Analiz Eder?

Kubernetes'i en basit hali ile anlatacak olursak, container üzerinde çalışan **mikroservis** tabanlı uygulamaların orkestrasyon işlemini gerçekleştiriyor. Yani sizin arka tarafta kullandığınız angular js'de uygulamanız olabilir ve arka tarafta mysql database'iniz olabilir. Kubernetes sayesinde database instance sayısını arttırabilir ve bunları orkestrasyon işlemini sağlayabilirsiniz. **Kubernetes**, **container** ortamındaki otomasyonu, orkestrasyonu sağlarken sunucunun dolaylı olarak network trafiğininde optimize edebiliyor. Yani şöyle düşünün, kubernetes otomasyon ve orkestrasyon işlemlerini yaparken burada load balancing, storage yönetimi, kaynak yönetimi gibi işleride yönetiyor. Bir container'in nasıl ve nerede devreye girmesi gerektiğini yönetiyor.

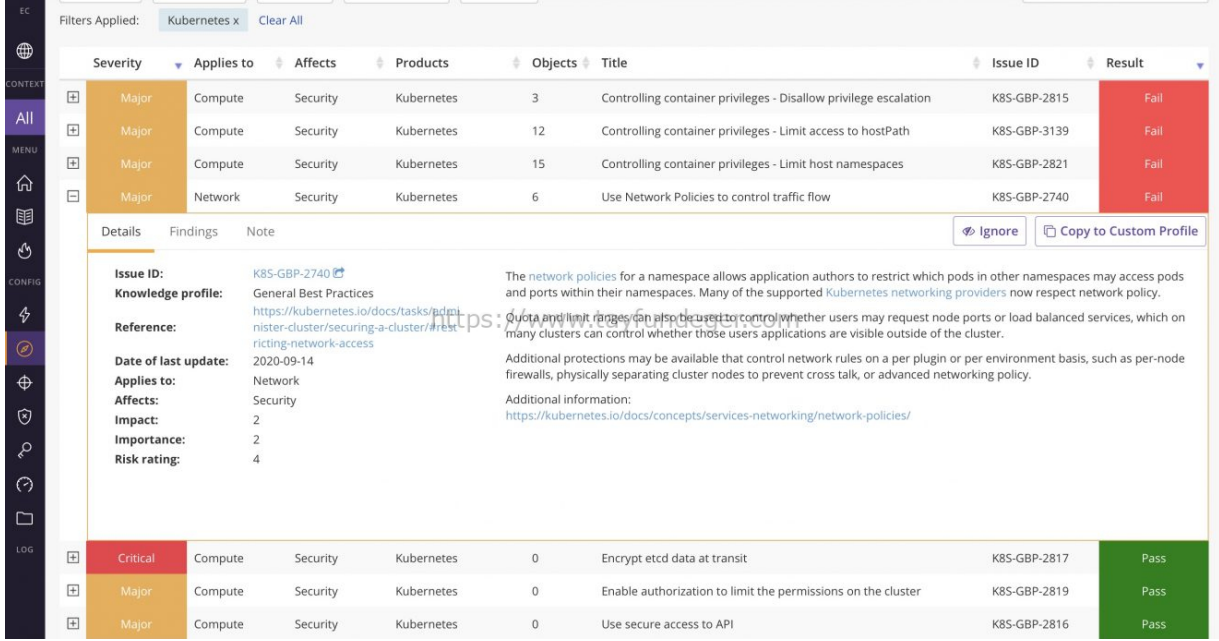
Runecast ile birlikte Kubernetes'i ilk olarak 4.5 sürümünde duymaya başladık. Kubernetes altyapılarını tasarlarken cluster ve workload'ları güvence altına almak gerekir. Burada bir orkestrasyon işlemi yapıldığı için çok fazla değişken olacaktır. Bu süreç oldukça dikkat gerektiren süreçler olduğu için eğer 3 party bir üründen faydalanmıyorsanız bazı standartları gözden kaçırmayı oldukça olasıdır. Runecast sayesinde Kubernetes uygulamaları ve Center for Internet Security (CIS) uyumluluk standartları otomatik olarak kontrol edilir ve olumsuz bir durum var ise bu size raporlanır.

Runecast sayesinde sanallaştırma ortamlarını proaktif olarak izlerken aynı zamanda Kubernetes altyapılarınıda proaktif olarak izleyebiliyoruz. Kubernetes Best Practices 'lerine göre kritik sorunların ve düzeltilmesi gereken adımlarını Runecast üzerinde kolayca görebiliriz. Ayrıca mimarinizde oluşan güvenlik açıklarınıda basit bir şekilde görebilirsiniz.



Severity	Applies to	Affects	Products	Objects	Title	Issue ID	Result
Major	Compute	Security	Kubernetes	3	Controlling container privileges - Disallow privilege escalation	KBS-GBP-2815	Fail
Major	Compute	Security	Kubernetes	12	Controlling container privileges - Limit access to hostPath	KBS-GBP-3139	Fail
Major	Compute	Security	Kubernetes	15	Controlling container privileges - Limit host namespaces	KBS-GBP-2821	Fail
Major	Network	Security	Kubernetes	6	Use Network Policies to control traffic flow	KBS-GBP-2740	Fail
Critical	Compute	Security	Kubernetes	0	Encrypt etcd data at transit	KBS-GBP-2817	Pass
Major	Compute	Security	Kubernetes	0	Enable authorization to limit the permissions on the cluster	KBS-GBP-2819	Pass
Major	Compute	Security	Kubernetes	0	Use secure access to API	KBS-GBP-2816	Pass

Runecast kullanıyorsanız Kubernetes altyapınızı basit bir şekilde kontrol edebileceğinizi söylemiştim. Runecast'a login olduktan sonra Best Practices bölümüne giriş yapıyoruz. Burada Products bölümünde yer alan Kubernetes seçeneğini seçerek Kubernetes ile ilgili Best Practices'lere aykırı olan bulguları karşımıza getiriyoruz.



Severity	Applies to	Affects	Products	Objects	Title	Issue ID	Result
Major	Compute	Security	Kubernetes	3	Controlling container privileges - Disallow privilege escalation	K8S-GBP-2815	Fail
Major	Compute	Security	Kubernetes	12	Controlling container privileges - Limit access to hostPath	K8S-GBP-3139	Fail
Major	Compute	Security	Kubernetes	15	Controlling container privileges - Limit host namespaces	K8S-GBP-2821	Fail
Major	Network	Security	Kubernetes	6	Use Network Policies to control traffic flow	K8S-GBP-2740	Fail

Details

Findings

Note

Issue ID:

Knowledge profile:

Reference:

Date of last update:

Applies to:

Affects:

Impact:

Importance:

Risk rating:

K8S-GBP-2740

General Best Practices

<https://kubernetes.io/docs/tasks/pod-manage-cluster/securing-a-cluster/#restricting-network-access>

2020-09-14

Network

Security

2

2

4

The [network policies](#) for a namespace allows application authors to restrict which pods in other namespaces may access pods and ports within their namespaces. Many of the supported [Kubernetes networking providers](#) now respect network policy.

[Quota and limit ranges](#) can also be used to control whether users may request node ports or load balanced services, which on many clusters can control whether those users applications are visible outside of the cluster.

Additional protections may be available that control network rules on a per plugin or per environment basis, such as per-node firewalls, physically separating cluster nodes to prevent cross talk, or advanced networking policy.

Additional information:
<https://kubernetes.io/docs/concepts/services-networking/network-policies/>

Critical

Compute

Security

Kubernetes

0

Encrypt etcd data at transit

K8S-GBP-2817

Pass

Major

Compute

Security

Kubernetes

0

Enable authorization to limit the permissions on the cluster

K8S-GBP-2819

Pass

Major

Compute

Security

Kubernetes

0

Use secure access to API

K8S-GBP-2816

Pass

Runecast Kubernetes Ortamınızı Nasıl Analiz Eder? Kubernetes kullanıyorsanız network tarafında yapacağınız izolasyonlara dikkat etmeniz gerekmektedir. Yukarıdaki örnekte Kubernetes objelerinde bir network policy'nin kullanılmadığı belirtiliyor. Ancak Kubernetes Best Practices'lerinde bunun kullanılması gerektiği belirtiliyor. Trafik akışını IP adresi veya port düzeyinde (OSI katmanı 3 veya 4) kontrol etmek istiyorsanız cluster'ınızda belirli uygulamalar için Kubernetes NetworkPolicies kullanmayı düşünebilirsiniz. Container mimarilerinde bu genellikle atlanan veya gözardı edilen bir konudur. Ancak bir saldırı veya atak durumunda bunların ne kadar önemli olduğunun farkına varırız.

Best Practices

Severity Applies to Affects Products (1) Results

Filters Applied: Kubernetes x Clear All

Severity	Applies to	Affects	Products	Objects	Title	Issue ID	Result
Major	Compute	Security	Kubernetes	3	Controlling container privileges - Disallow privilege escalation	K8S-GBP-2815	Fail
Major	Compute	Security	Kubernetes	12	Controlling container privileges - Limit access to hostPath	K8S-GBP-3139	Fail
Major	Compute	Security	Kubernetes	15	Controlling container privileges - Limit host namespaces	K8S-GBP-2821	Fail
Major	Network	Security	Kubernetes	6	Use Network Policies to control traffic flow	K8S-GBP-2740	Fail

Details Findings Note

Affected objects

- k8s-demo.outer.space
 - default
 - ingress-nginx
 - kube-node-lease
 - kube-public
 - kubernetes-dashboard
 - kube-system

Automatic checks

Object	Finding description	Finding value
default	Network policy status	Not assigned

Ignore Copy to Custom Profile

Critical	Compute	Security	Kubernetes	0	Encrypt etcd data at transit	K8S-GBP-2817	Pass
Major	Compute	Security	Kubernetes	0	Enable authorization to limit the permissions on the cluster	K8S-GBP-2819	Pass

Ayrıca Best Practices'e aykırı olan bu durumun cluster'da mı yoksa node'lar arasında mı olduğunu ayrıca Findings bölümünden görebilirsiniz. Yani bunun güzel yanı aslında komple node ve cluster'lara kadar taramalar yapıp bunların özelinde uyumsuzlukları çıkartıyor.

Vulnerabilities

Severity Applies to Products (1) CVEs Results

Filters Applied: Kubernetes x Clear All

Severity	Title	Issue ID	Applies to	Products	Objects	CVEs	Result
Major	CVE-2020-8554: Man in the middle using LoadBalancer or ExternalIPs	K8S-VUL-3248	Compute	Kubernetes	0	CVE-2020-8554	Pass

Details Note

Ignore Copy to Custom Profile

Issue ID: K8S-VUL-3248

Knowledge profile: Vulnerabilities

Reference: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8554>

Applies to: Compute

CVEs: CVE-2020-8554

If a potential attacker can already create or edit services and pods, then they may be able to intercept traffic to other pods (or nodes) in the cluster.

An attacker that is able to create a ClusterIP service and set the `spec.externalIPs` field can intercept traffic to that IP.

An attacker that is able to patch the status (which is considered a privileged operation and should not typically be granted to users) of a LoadBalancer service can set the `status.loadBalancer.ingress.ip` to similar effect.

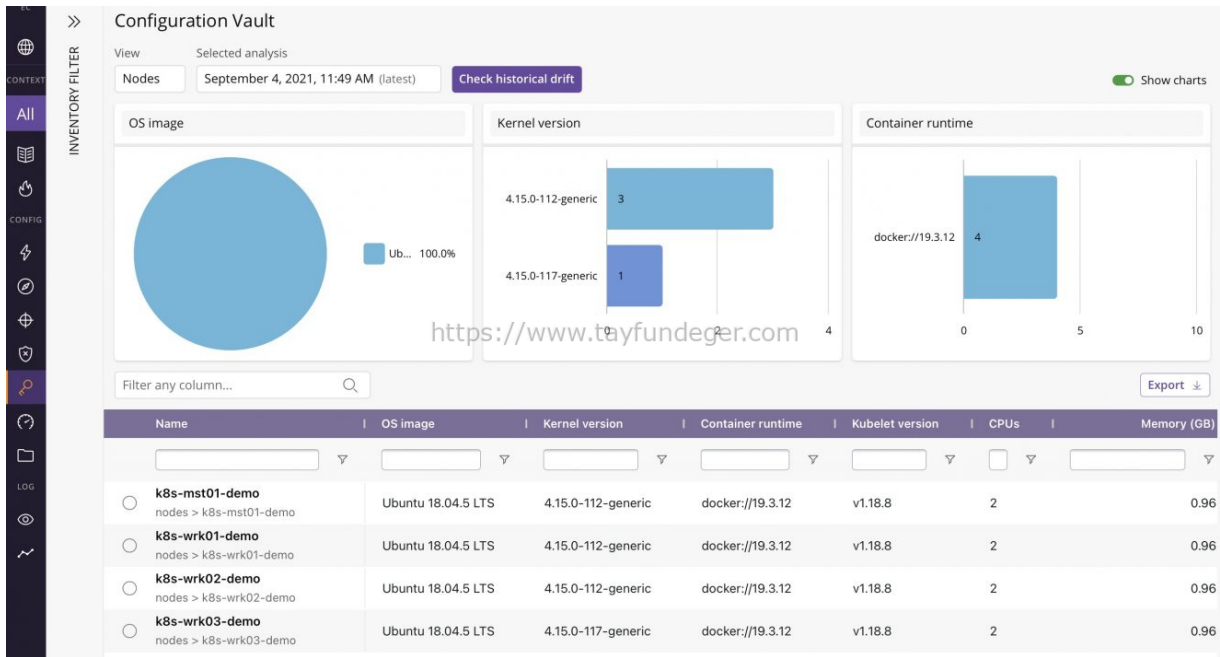
This issue is a design flaw that cannot be mitigated without user-facing changes.

More information: <https://github.com/kubernetes/kubernetes/issues/97076>

Show 25 entries 1 - 1 of 1 entries (filtered from 60 total entries)

Vulnerabilities bölümünde güvenlik açıklarını görebilirsiniz. Runecast birden fazla ürünü kontrol ettiği için yukarıda yer alan Products bölümünden Kubernetes'i seçmeniz gerekiyor. Kubernetes'i seçtiğimizde, Kubernetes ortamındaki güvenlik zaafiyetlerini görebilirsiniz. Yukarıdaki örnekte, CVE-2020-8554'un güvenlik zaafiyetini görebilirsiniz. Kubernetes kullanan kişiler bilir bu güvenlik zaafiyeti ilk çıktığında çok konuşulmuştu. Çünkü bu açık sayesinde cluster'da yeni pod'lar oluşturabilir ve gelen trafiği izleyebilirsiniz.

Gördüğünüz gibi oldukça ciddi bir güvenlik zaafiyeti ancak Runecast kullanıyorsanız Kubernetes altyapınızda bulunan güvenlik zaafiyetlerini ayrıca düşünmenize gerek kalmıyor. Çünkü Runecast, Kubernetes'in güvenliği için CIS Benchmark'ı kapsayarak node düzeyinde ve cluster düzeyinde otomatik Kubernetes analizleri sunar. Runecast Analyzer , CIS 1.6.0'a karşı kontrollerin kapsamı ile CIS Benchmarks ile güvenlik uyumluluğunuzu proaktif olarak denetler . Ayrıca güvenlik açığı eşlemesi sağlar.



Kubernetes bulunan ortamlarda Configuration Vault özelliğini kullanabilirsiniz. Bu özellik sayesinde konfigürasyon farklılıklarını görebilir ve buna göre müdahalelerde bulunabilirsiniz. Yukarıdaki örnekte node'lar arasında bulunan kernel version farklılığını görebilirsiniz. Ayrıca burada CPU, Memory, Kubelet version, Pod sayısı, OS Image gibi değerleride görebilirsiniz. İlerleyen versiyonlarda muhtemelen Configuration Vault bölümünde daha fazla veri ile karşılaşırız diye düşünüyorum.

Kendi altyapınızda güvenli bir şekilde çalışan Runecast Analyzer, hem bulutta hem de şirket içinde neler olup bittiğine ilişkin öngörülerle Kubernetes altyapınız için güvenlik uyumluluğu kontrollerini otomatikleştirir. Bu durum altyapıya proaktif yaklaşmanızı ve her zaman kontrol altında tutmanıza olanak sağlar.

Runecast Vmware Analyzer – Türkiye Distribütör firması “OTD Bilişim” satış ekibi

otd.salesgrp@onlineteknikdestek.com ile iletişime geçebilirsiniz.