Kubernetes Yapılandırması

Ön Koşullar

- Zaten dağıtılmış bir Kubernetes kümesi.
- Kubernetes 1.23 ve üzeri sürümlerini kullanan Amazon EKS dağıtımları için bir Amazon EBS CSI sürücüsü IAM rolü. CSI sürücüsünün düzgün çalışması için bir IAM rolü atamanız gerekir. Amazon EBS CSI sürücüsü IAM rolünü oluşturma talimatlarını bulmak için AWS belgelerini okuyun . Hem yeni hem de eski dağıtımlar için CSI sürücüsünü yüklemeniz gerekir. CSI sürücüsü, temel bir Kubernetes özelliğidir.

Kaynak Gereksinimi

Wazuh'u Kubernetes'e dağıtmak için kümede en azından aşağıdaki kaynakların bulunması gerekir:

- 2 CPU ünitesi
- 3 Gi hafıza
- 2 Gi depolama

Genel Bakış

StatefulSet ve Dağıtım Denetleyicileri

Bir Dağıtım olarak , bir *StatefulSet,* aynı kapsayıcı spesifikasyonuna dayanan Pod'ları yönetir, ancak her bir pod'una bağlı bir kimliği korur. Bu pod'lar aynı spesifikasyondan oluşturulur, ancak birbirlerinin yerine kullanılamazlar: her birinin herhangi bir yeniden planlama boyunca korunan kalıcı bir tanımlayıcısı vardır.

Verileri kalıcı depolamaya kaydeden veritabanları gibi durumlu uygulamalar için kullanışlıdır. Her Wazuh yöneticisinin ve her Wazuh dizinleyicisinin durumları korunmalıdır, bu nedenle her başlatmada durumlarını koruduklarından emin olmak için bunları StatefulSet kullanarak bildiririz.

Dağıtımlar durumsuz kullanım için tasarlanmıştır ve oldukça hafiftir ve durumların bakımının gerekli olmadığı Wazuh panosu için uygun görünmektedir.

Kalıcı birimler (PV), sağlanan kümedeki depolama parçalarıdır. Bir düğümün küme kaynağı olması gibi kümedeki bir kaynaktır. Kalıcı birimler, Birimler gibi birim eklentileridir ancak PV'yi kullanan herhangi bir bireysel pod'dan bağımsız bir yaşam döngüsüne sahiptir. Bu API nesnesi, NFS, iSCSI veya bulut sağlayıcıya özgü bir depolama sistemi olsun, depolamanın uygulanmasının ayrıntılarını yakalar.

Burada, hem Wazuh yöneticisinden hem de Wazuh dizinleyicisinden gelen verileri depolamak için kalıcı birimleri kullanıyoruz.

Daha fazla bilgi için kalıcı birimler sayfasına bakın .

Baklalar

Wazuh docker konteynerlerinin nasıl oluşturulduğunu depolardan inceleyebilirsiniz .

Wazuh master

Bu pod, Wazuh kümesinin ana düğümünü içerir. Ana düğüm, çalışan düğümlerini merkezileştirir ve koordine eder, kritik ve gerekli verilerin tüm düğümler arasında tutarlı olmasını sağlar. Yönetim yalnızca bu düğümde gerçekleştirilir, bu nedenle aracı kayıt hizmeti (authd) buraya yerleştirilir.

Resim	Kontroller
wazuh/wazuh-yöneticisi	Durumsal Küme

Wazuh worker 0 / 1

Bu pod'lar Wazuh kümesinin bir işçi düğümünü içerir. Bunlar ajan olaylarını alacaktır.

Resim	Kontroller
wazuh/wazuh-yöneticisi	Durumsal Küme

Wazuh indexer

Wazuh dizinleyici pod'u Filebeat'ten alınan olayları alır.

Resim	Kontroller
wazuh/wazuh-indeksleyici	Durumsal Küme

Wazuh dashboard

Wazuh kontrol paneli, Wazuh dizinleyici verilerinizi, Wazuh aracı bilgileri ve sunucu yapılandırmasıyla birlikte görselleştirmenize olanak tanır.

Resim	Kontroller
wazuh/wazuh-panosu	Dağıtım

Hizmetler

Wazuh indeksleyici ve gösterge paneli

İsim	Tanım
wazuh-indeksleyici	Wazuh indeksleyici düğümleri için iletişim.
dizinleyici	Bu, Wazuh panosunun uyarıları okumak/yazmak için kullandığı Wazuh dizinleyici API'sidir.
gösterge paneli	Wazuh kontrol paneli hizmeti. https://wazuh.your-domain.com:443

Wazuh

İsim	Tanım
vazuh	Wazuh API'si: wazuh-master.alan-adiniz.com:55000
	Temsilci kayıt hizmeti (authd): wazuh-master.your-domain.com:1515
wazuh-işçiler	Raporlama hizmeti: wazuh-manager.your-domain.com:1514
wazuh-kümesi	Wazuh yönetici düğümleri için iletişim.

Revision #2
Created 23 December 2024 22:27:33 by Ayşegül Sarıkaya
Updated 23 December 2024 22:33:54 by Ayşegül Sarıkaya