# Wazuh Endekslerinin Taşınması

Bu bölümde, anlık görüntüleri kullanarak Wazuh dizinlerini taşımaya odaklanıyoruz. Bu, orijinal zaman damgasını kaybetmeden uyarıları bir Wazuh dizinleyici kümesinden diğerine geri yüklemeye yardımcı olur.

## Paylaşımlı Dosya Sistemini Kurun

Anlık görüntü deposu için paylaşımlı bir dosya sistemi oluşturmak amacıyla bir Ağ Dosya Sistemi (NFS) kullanılmasını öneririz.

### NFS Sunucusu

Adanmış bir sunucuda NFS'yi kurmak için aşağıdaki adımları uygulayın:

1. Anlık görüntü deposu için şu dizinde bir hedef `/mnt` dizinİ oluşturun :

   ```
   mkdir /mnt/snapshots
   ```

2. Aşağıdaki komutları çalıştırarak NFS'yi yükleyin:

   **Yum**

   ```
   yum update
   yum install -y nfs-utils
   yum install exportfs
   systemctl enable nfs-server
   systemctl start nfs-server
   ```

   **APT**

   ```
   apt -y install nfs-kernel-server
   systemctl start nfs-kernel-server.service
   ```

3. Aşağıdaki komutu kullanarak `/mnt/snapshots` dizinini `/etc/exports` dosyasına ekleyin. `<NETWORK_ADDRESS/CIDR>` değişkenini ağ adresinizle değiştirin.

```
echo "/mnt/snapshots     <NETWORK_ADDRESS/CIDR>(rw,sync,no_root_squash,no_subtree_check)" |
sudo tee -a /etc/exports
```

   Nerede:
   - `rw`- Paylaşılan dizine hem okuma hem de yazma erişimi sağlar.
   - `sync`- NFS sunucusunun değişiklikleri hemen diske yazmasını zorlar ve dosya sistemini senkron hale getirir.
   - `no_root_squash`- NFS istemci sistemindeki "root" kullanıcısının NFS sunucusundaki dosyalara tam ve kısıtlanmamış erişime sahip olmasını sağlar.
   - `no_subtree_check`- Büyük dizin ağaçları için performansı artırabilen alt ağaç denetimini devre dışı bırakır.

4. NFS yapılandırmasını uygulayın:

```
exportfs -a
```

# Wazuh Indexer

Paylaşımlı dosya sistemi kurulumunu tamamlamak için Wazuh dizinleyici düğümünde (düğümlerinde) aşağıdaki adımları gerçekleştirin.

1. Anlık görüntü deposu için şu dizinde bir hedef `/mnt` dizin oluşturun :

```
mkdir /mnt/snapshots
```

2. NFS istemcisini yükleyin:

   **Yum**

```
yum -y install nfs-utils
```

   **APT**

```
apt -y install nfs-common
```

3. Paylaşılan dizini `/mnt/snapshots`Wazuh dizinleyici düğümüne(düğümlerine) bağlayın. `<NFS_SERVER_IP>`

Değişkeni NFS sunucusunun IP adresiyle değiştirin:

```
mount -t nfs <NFS_SERVER_IP>:/mnt/snapshots /mnt/snapshots
```

4. `wazuh-indexer`Kullanıcıya dizinin sahipliğini verin `/mnt/snapshots`:

```
chown wazuh-indexer:wazuh-indexer /mnt/snapshots
```

5. Yapılandırmayı ekleyin: `path.repo:/mnt/snapshots` depo yolunu belirtmek için `/etc/wazuh-indexer/opensearch.yml` dosyasına:

```
network.host: "127.0.0.1"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
cluster.name: "wazuh-cluster"

node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer
path.repo: /mnt/snapshots

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/wazuh-indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/wazuh-indexer-key.>plugins.security
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false
plugins.security.ssl.http.enabled_ciphers:
  - "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
  - "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384"
plugins.security.ssl.http.enabled_protocols:
  - "TLSv1.2"
plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=indexer,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"
```

```
plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".opendistro-alerting-config", ".opendistro-alert>
### Option to allow Filebeat-oss 7.10.2 to work ###
compatibility.override_main_response_version: true
```

6. Yapılandırma değişikliklerini uygulamak için Wazuh dizinleyicisini yeniden başlatın:

```
systemctl restart wazuh-indexer
```

Uyarı: `ll` yardımcı programını kullanarak `/mnt/snapshots` dizininin Wazuh dizinleyici düğümlerinde `wazuh-indexer:wazuh-indexer` sahipliğine sahip olduğunu doğruladığınızdan emin olun.

NFS paylaşım dizini `/mnt/snapshots`'ı anlık görüntü deposu olarak kullanmak için hedef Wazuh dizinleyici(ler)de Paylaşılan dosya sistemini kur > Wazuh dizinleyici adımlarını tekrarlayın.

# Anlık Görüntü Deposunu Kurun

Wazuh kontrol panelinde aşağıdaki adımları uygulayın:

1. **Sol üst menüye** ☰ tıklayın , **Indexer yönetimi** > **Anlık Görüntü Yönetimi** > **Depolar'a** gidin ve yeni bir anlık görüntü deposu oluşturmak için **Depo oluştur'u seçin.**
2. Bir depo adı girin, depo türünü **Paylaşılan dosya sistemi** olarak seçin , depo konumunu girin `/mnt/snapshots`ve yeni deponun kaydını yapmak için **Ekle'yi seçin.**

Anlık görüntü deposu oluştur

Benzer bir anlık görüntü deposu kurmak için yukarıdaki adımları hedef Wazuh kümesinde tekrarlayın.

# Anlık Görüntüler Alın

1. **Sol üst menüye** ☰ tıklayın ve **Indexer yönetimi** > **Anlık Görüntü Yönetimi** > **Anlık Görüntüler** bölümüne gidin .
2. **Anlık görüntü al'ı** seçin ve bir Anlık Görüntü adı girin.
3. Kaynak dizin desenlerini seçin veya girin.
4. Anlık görüntüleri depolamak için daha önce oluşturulan depoları seçin.
5. **Gelişmiş seçenekleri** seçin ve **Anlık görüntülere küme durumunu dahil et** seçeneğini işaretleyin.

Anlık görüntülere küme durumunu dahil et seçeneği

6. Yeni bir anlık görüntü oluşturmak için **Ekle'yi** seçin .

Anlık görüntü dosyaları `/mnt/snapshots` depolama konumuna kaydedilir .

Anlık görüntü dosyası kaydedildi

# Anlık Görüntüleri Geri Yükle

Wazuh dizin geçiş adımlarını tamamlamak için eski Wazuh dizinleyicilerinden alınan anlık görüntüleri hedef Wazuh dizinleyicilerine geri yükleyin. Hedef Wazuh dizinleyicisinde aşağıdaki adımları gerçekleştirin.

Not

**Anlık görüntüleri geri yükleme** işlemine geçmeden önce hedef Wazuh kümesinde Paylaşımlı dosya sistemini kur ve Anlık görüntü deposunu kur bölümlerindeki adımların gerçekleştirilmesi gerekir .

1. Anlık görüntü dosyalarını yüklemek için hedef Wazuh kümesindeki Wazuh dizinleyici düğümlerini şu komutu kullanarak yeniden başlatın:

   ```
   systemctl restart wazuh-indexer
   ```

2. **Sol üst menüye** ☰ tıklayın , **Indexer yönetimi** > **Anlık Görüntü Yönetimi** > **Anlık Görüntüler'e** gidin ve Anlık Görüntüler sayfasını yenileyin. Depo konumundaki anlık görüntüler `/mnt/snapshots`hedef Wazuh kümesinin panosunda gösterilecektir.
3. Anlık görüntüyü seçin ve **Geri Yükle'ye**`restored_` tıklayın. Dizinleri orijinal adlarına geri yüklemek için öneki silin . `restored_`Önek, çakışan dizin adlarını önlemek için vardır.
4. **Gelişmiş seçenekleri** seçin ve tüm seçeneklerin işaretli olmadığından emin olun.

   Anlık görüntü gelişmiş seçeneklerini geri yükle

   

5. Göç sürecini tamamlamak için **Anlık görüntüyü geri yükle'yi** seçin.

   Anlık görüntüyü geri yükle

   

---

Revision #3
Created 31 December 2024 18:03:46 by Ayşegül Sarıkaya
Updated 31 December 2024 21:32:00 by Ayşegül Sarıkaya