



Inovação com dados em nuvem

TRILHA

#TheDevConf
Oracle

Como fazer uma jornada para nuvem
(quase) sem turbulência?

Tales Casagrande

23.03.21 10h00



Inovação com dados em nuvem

TRILHA

#TheDevConf
Oracle



Este trabalho está licenciado sob uma Licença Creative Commons Atribuição-Compartilhagual 4.0 Internacional.
Para ver uma cópia desta licença, visite <http://creativecommons.org/licenses/by-sa/4.0/>.



Inovação com dados em nuvem

**COMO FAZER UMA JORNADA
PARA NUVEM (QUASE)
SEM TURBULÊNCIA**



Índice

1. Considerações iniciais e pré-requisitos	4
Recursos usados	4
Tópicos não cobertos	4
2. Considerações iniciais e pré-requisitos	4
2.1. Oracle Cloud	4
2.2. Trend Micro Cloud One	4
3. Provisionando os recursos	5
3.1. Criação de uma instancia VM	5
4. Protegendo o Servidor	8
5. Protegendo uma aplicação vulnerável em Python	11
5.1. Preparando o ambiente	12
5.2. Realizando um ataque	13
5.3. Visualizando os eventos	14
6. Concluindo	15

1. Considerações iniciais e pré-requisitos

Recursos usados

OCI (all free tier)

- Compute VM 2.1 Shape

Trend Micro Cloud One

- Cloud One Workload Security
- Cloud One Application Security

Local

- Gerador de chaves SSH – usado: PuttyGen
- SSH Terminal Client – usado: Putty / MobaXterm

Tópicos não cobertos

Instalação dos softwares na máquina host

- Gerador de chaves SSH – usado: PuttyGen
- SSH Terminal Client – Putty / MobaXterm
- Instalação do Git
- Instalação do Docker

2. Considerações iniciais e pré-requisitos

2.1. Oracle Cloud

Para esse workshop será necessário criar uma conta na Oracle Cloud é gratuito será a onde iremos prover toda a infraestrutura para o workshop.

Link <https://cloud.oracle.com>

2.2. Trend Micro Cloud One

O Trend Micro Cloud One é uma plataforma para times de infraestrutura, segurança e desenvolvimento que com 6 módulos ajuda os times a moverem seu workloads para nuvem ou proteger aplicações que já nasceram em nuvem ou até mesmo ajudar na excelência operacional da nuvem.

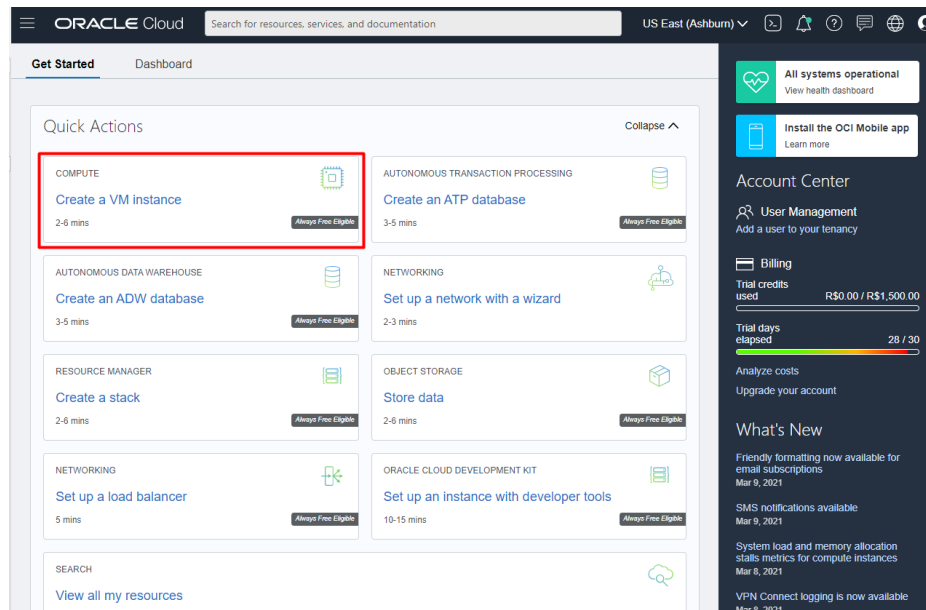
Para esse workshop será necessário criar uma conta no Cloud One, a criação da conta é gratuita e iremos utilizar para realizar a proteção dos workloads e aplicações.

Link <https://cloudone.trendmicro.com/>

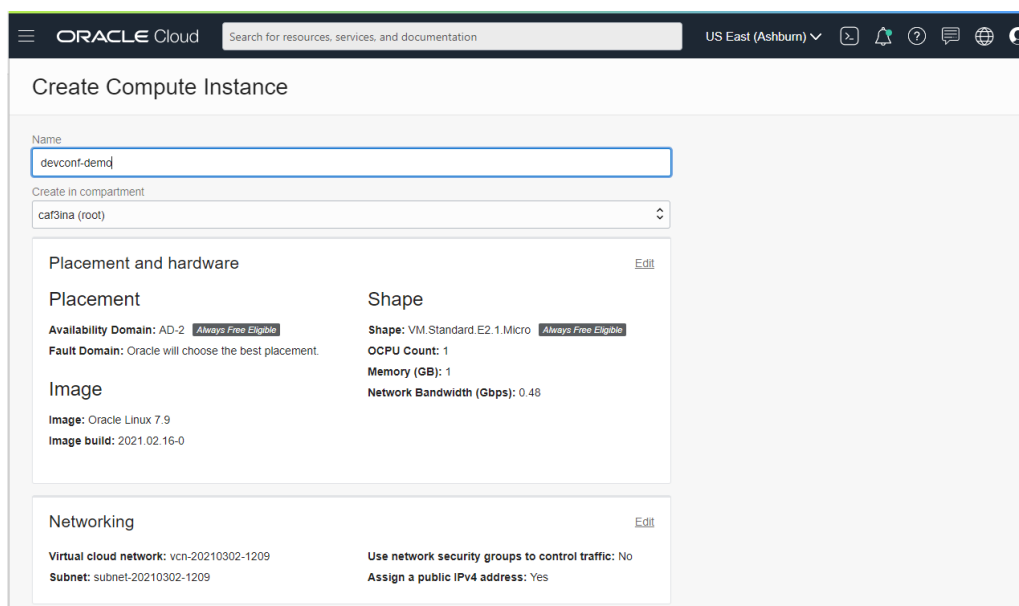
3. Provisionando os recursos

3.1. Criação de uma instancia VM

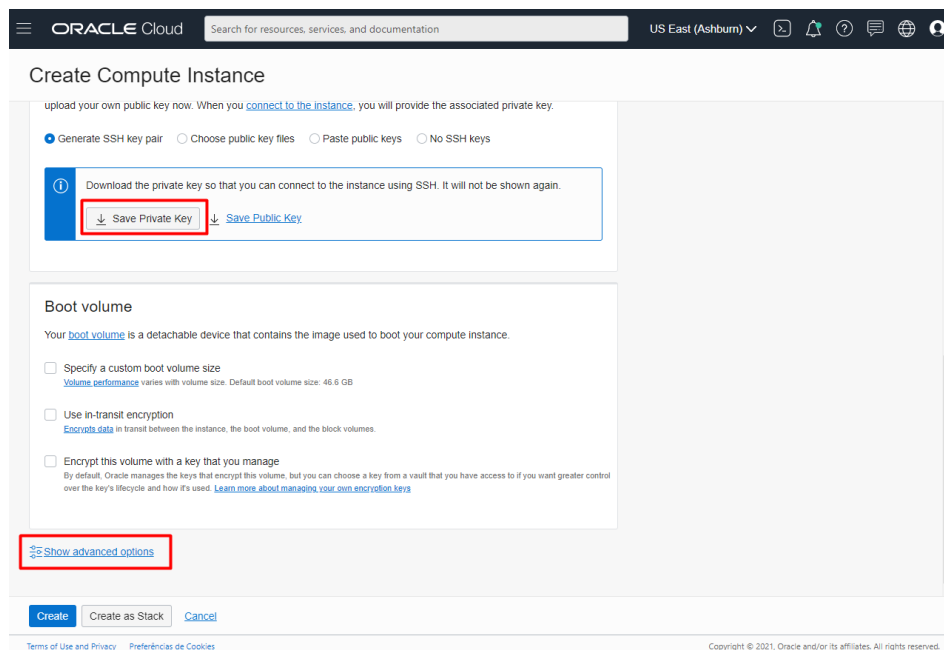
Navegue no menu direito até Compute > Instances também é possível usar a visualização no meu principal como o exemplo abaixo:



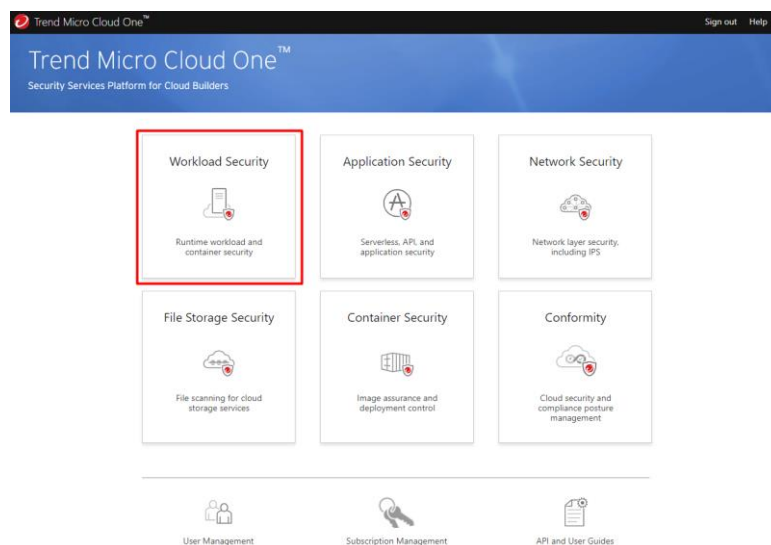
Defina um nome para seu workload, faça o download das chaves privadas para uma conexão futura via ssh.



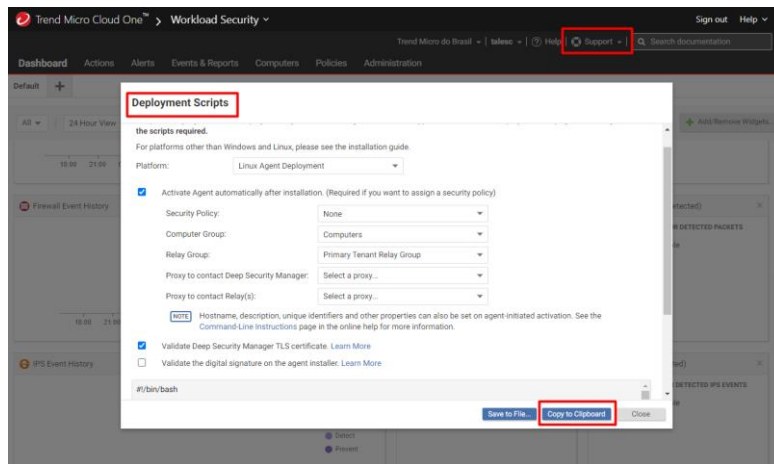
Clique em show advanced options, iremos colocar um script na inicialização do servidor dessa forma realizando a instalação do agente do Cloud One Workload Security.



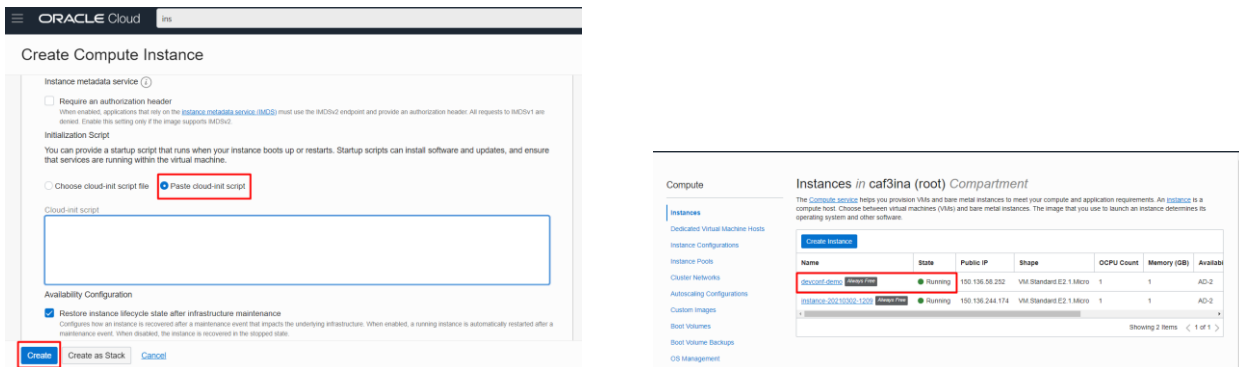
Acessar a plataforma Cloud One (a conta deve ser criada previamente) e escolher a opção Workload Security.



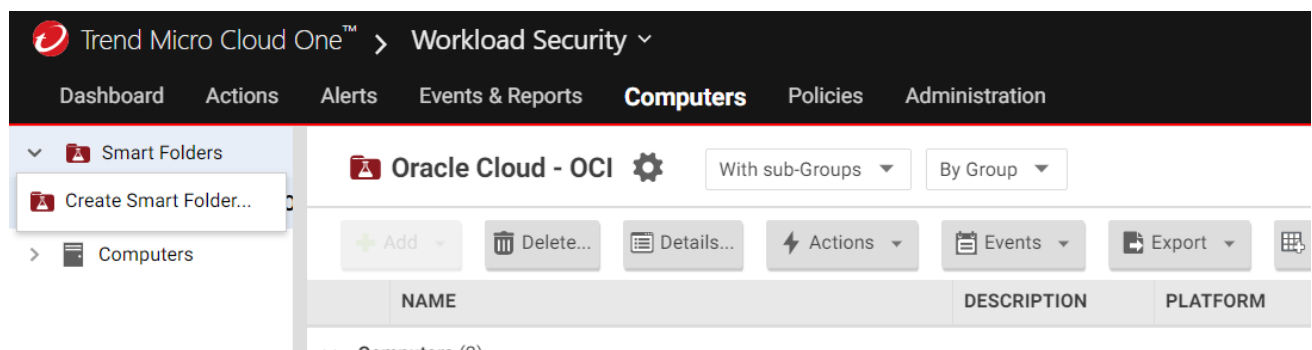
No meu Support selecione a opção Deployment Scripts, selecione a Plataforma Linux Agent Deployment e clique em Copy to Clipboard, iremos copiar o script de instalação e colocar na inicialização do Servidor.



Novamente na console do OCI, selecione a opção Paste cloud-init script e cole o script gerado a partir da console do Cloud One. Após isso selecione create e aguarde alguns minutos até a inicialização do Servidor.



Enquanto o Servidor é inicializado iremos criar uma Smart Folder para Organizarmos nosso ambiente. Acesse novamente a console do Cloud One e navegue no meu conforme abaixo no menu Computers > Smart Folde > Create Smart Folder.



Define um nome para a Smart Folder no Search Criteria utilize o exemplo da imagem abaixo

Smart Folder Editor

General Information

Folder Display Name: Oracle Cloud - OCI

Search Criteria

Use this query builder to define the filtering rule(s) Deep Security will use to dynamically populate your Smart Folder. Create a rule by selecting a computer property and then specifying the condition that property must meet. For example, you can create a rule which will select all computers whose hostname contains the string "gold". You can use multiple rules to specify multiple conditions that must be met for a computer to be display in the folder.

AND OR

Operating System CONTAINS Oracle Linux

Organize by Tag or Label Key Values

Within your Smart Folder, Deep Security can automatically create and maintain a set of sub-folders based on the values of a specific tag or label key. If you provide the tag or label key, Deep Security will create a sub-folder for each value of that key and populate that folder with the matching computers.

☐ Automatically create sub-folders for each value of a specific tag or label key.

Preview Save Cancel

Com o Servidor já inicializado é possível visualizarmos no Cloud One, nesse exemplo tenho dois Servidores um on-premise e outro criado anteriormente.

Trend Micro Cloud One™ > Workload Security

Dashboard Actions Alerts Events & Reports **Computers** Policies Administration

Smart Folders

Oracle Cloud - OCI

With sub-Groups By Group

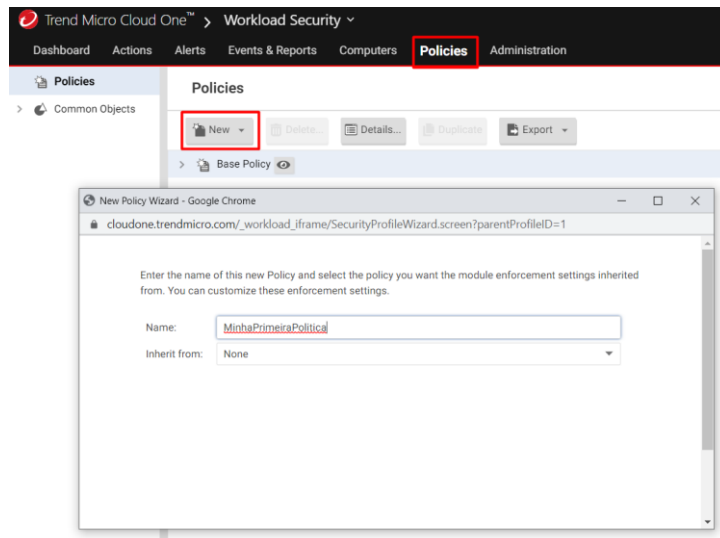
Search this page

NAME	DESCRIPTION	PLATFORM	POLICY	STATUS
devconf-demo.subnet03021213.vcn03021213.oraclevcn.com		Oracle Linux Release 7 (64 bit)	None	Managed (Offline)
oracle-dev.wayneenterprises.com		Oracle Linux Release 8 (64 bit)	None	Managed (Online)

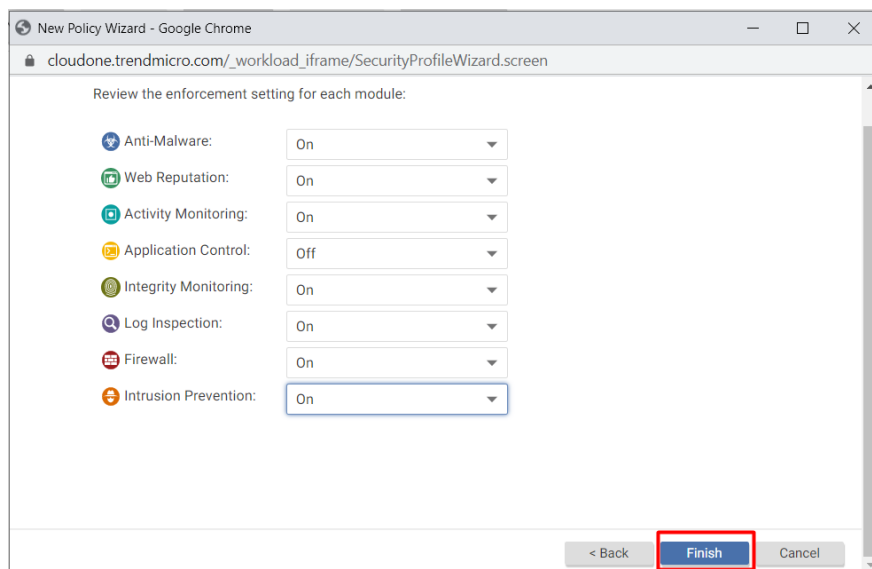
4. Protegendo o Servidor

É possível automatizar o processo para que sempre que um novo servidor for adicionado na console do Cloud One ele já inicie com proteção, basta selecionarmos a política no Deployment Scripts.

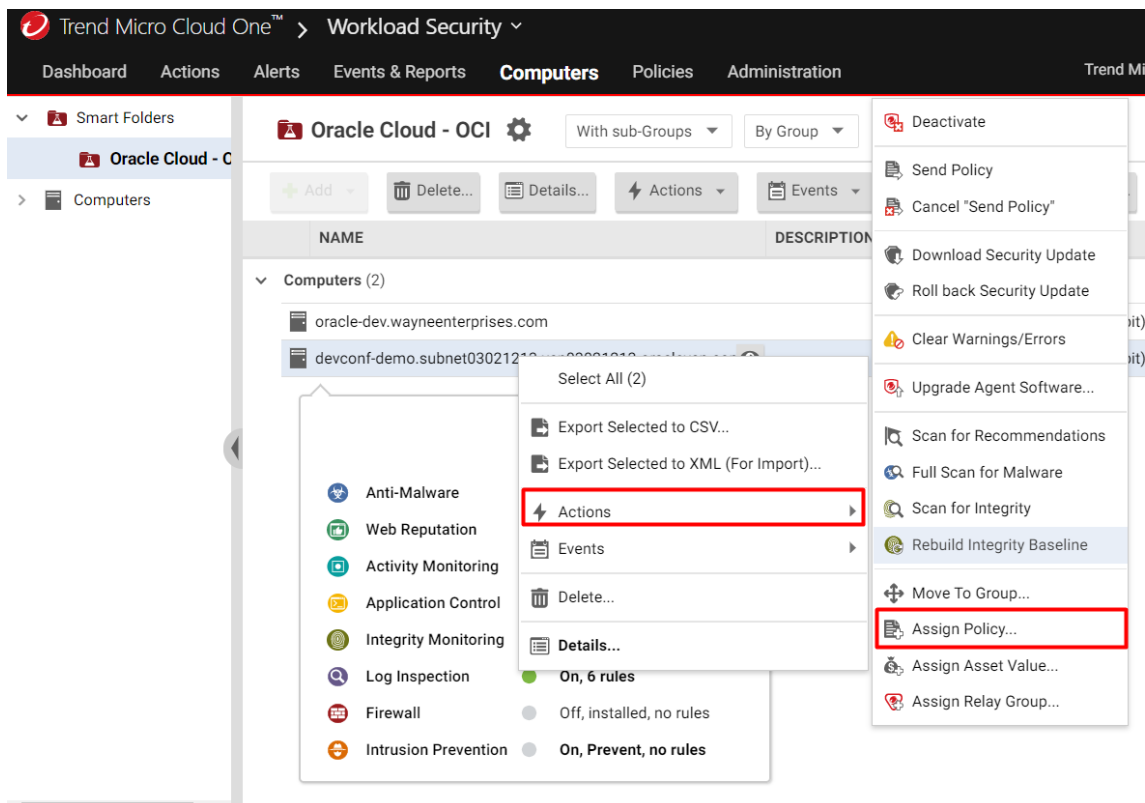
No meu Policies, basta clicar em new, definir um nome e clicar em next.



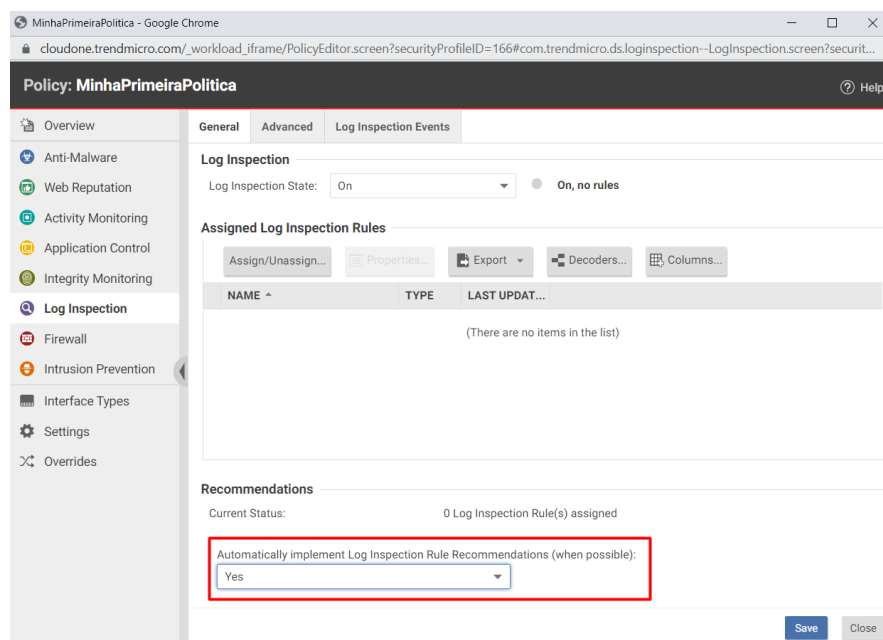
Na opção “Do you want to base this policy on an existing Computer's current configuration? Podes escolher a opção No, não iremos utilizar nenhuma herança.



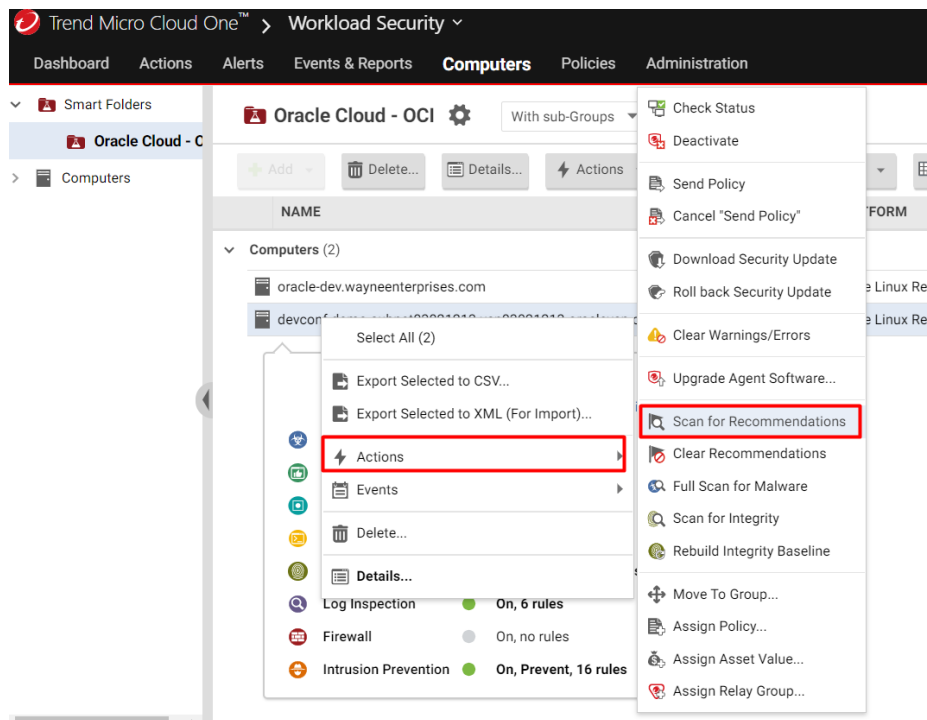
Cada módulo do Workload Security oferece uma camada de proteção, que agora serão habilitados na política.



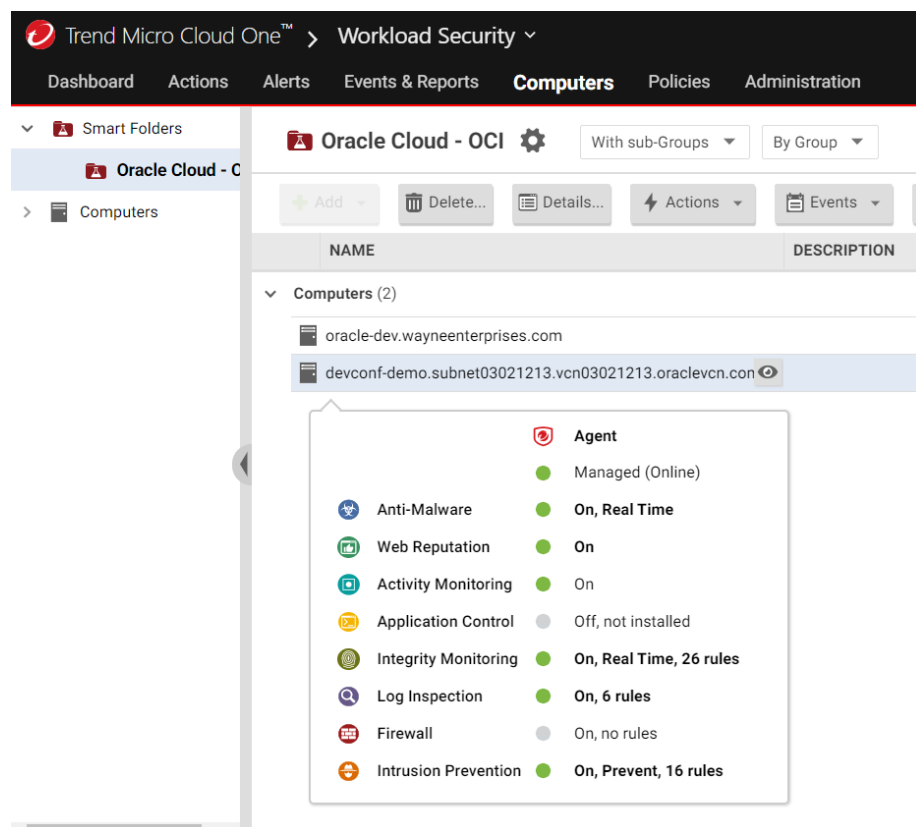
Em Assign Policy selecione a política que acabamos de criar. Para os módulos Log Inspection, Integrity Monitoring e Intrusion Prevention mude o status do Recommendations para yes dessa forma a ferramenta irá identificar falhas de segurança e aplicações para iniciar o monitoramento.



Após mudar para Yes, iremos executar o Scan for Recommendations para o Workload Security aplique as regras.

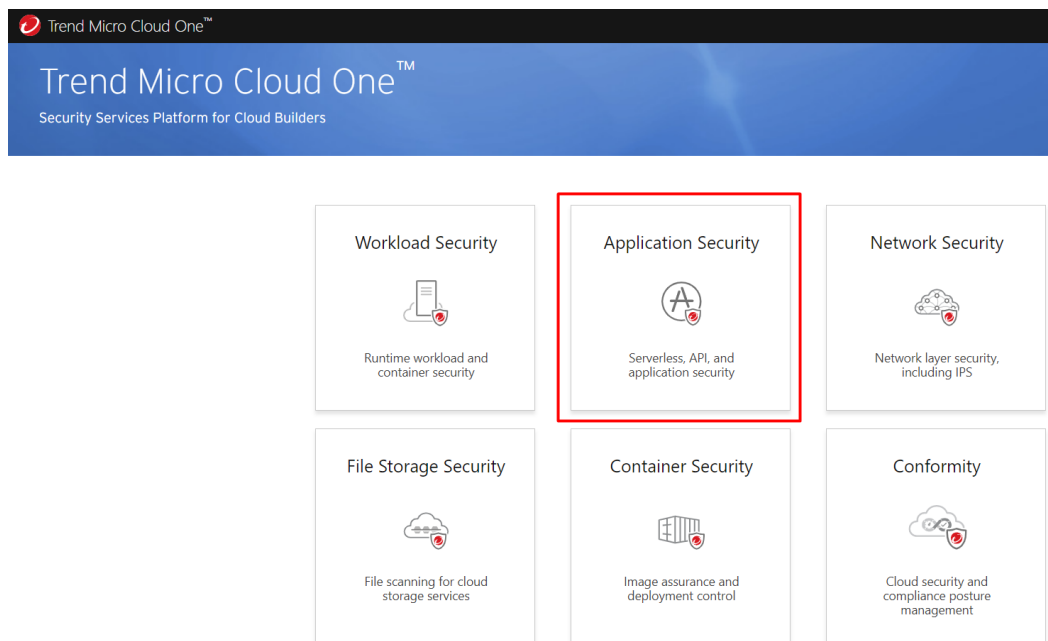


Após a execução podemos ver que já existem regras aplicadas no Servidor.



5. Protegendo uma aplicação vulnerável em Python

Não podemos instalar um agente quando falamos de código, o Application Security ajuda nesses desafios protegendo aplicações com apenas duas linhas de código.



5.1. Preparando o ambiente

Iremos utilizar um aplicativo da web django simples e vulnerável para testar e aprender como se proteger usando o Trend Micro Application Security.



Acesse o Servidor que criamos a cima via ssh e eleve o privilegio caso necessário.

```
$ yum install git -y
$ git clone https://github.com/caf3ina/HeadPage.git
$ cd HeadPage/
```

Edite a seguinte linha em `src /headpage /settings.py` para servidor do HeadPage ouvir em todas as interfaces. Isso pode ser perigoso, se possível, executado dentro de uma VM na interface somente de host.

```
ALLOWED_HOSTS = ['*']
```

Crie um arquivo com o nome `trend_app_protect.ini` e coloque as informações abaixo. Informações abaixo:

```
[trend_app_protect]
key = my-key
secret = my-secret
```

Obtenha a chave e o segredo do console do Cloud One Application Security

<https://cloudone.trendmicro.com/docs/application-security/python/#install-the-agent>

```
$ docker build --tag=headpage:latest .
$ docker run -d --rm -p 8000:8000 --name headpage headpage:latest
```

Acesse a página <http://meu-ip:8000/social/>

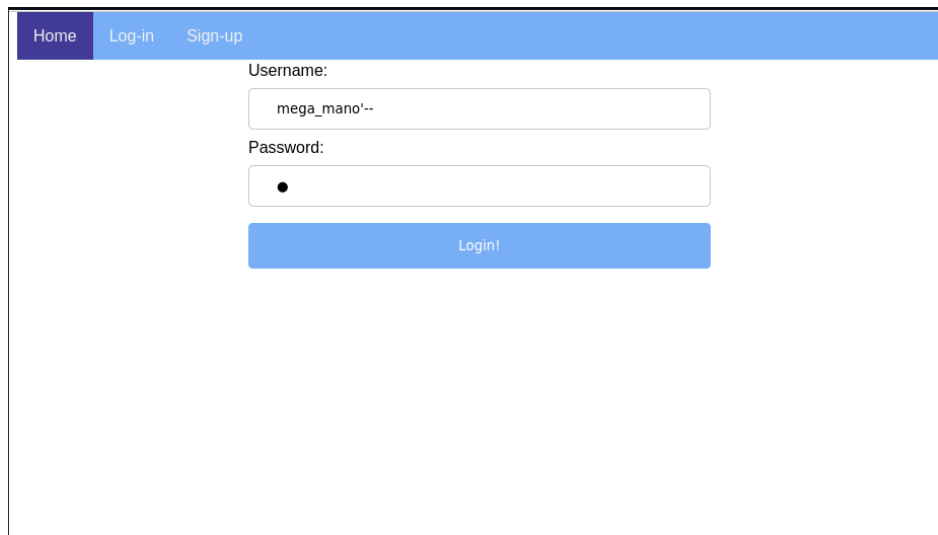
5.2 Realizando um ataque

Iremos explorar uma falha de **SQL Injection** que é uma falha bem comum em aplicações Web.

Na página Home da HeadPage, utilize as credenciais abaixo e depois clique em login:

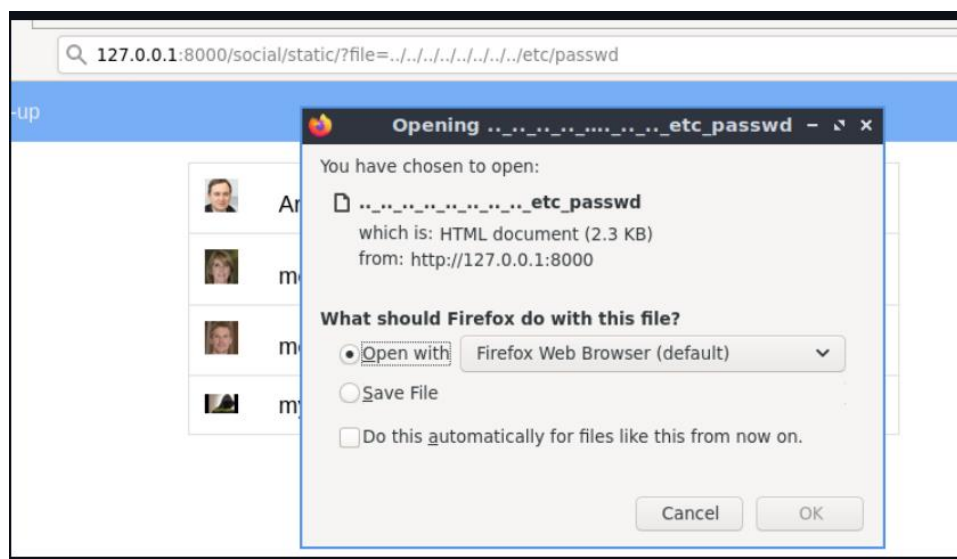
```
Username: mega_mano'–
Senha: qualquer_uma
```

```
$ docker run -d --rm -p 8000:8000 --name headpage headpage:latest
```



Um segundo ataque que podemos realizar é o **Path Traversal**, alguns arquivos estáticos são retornados após solicitações GET.

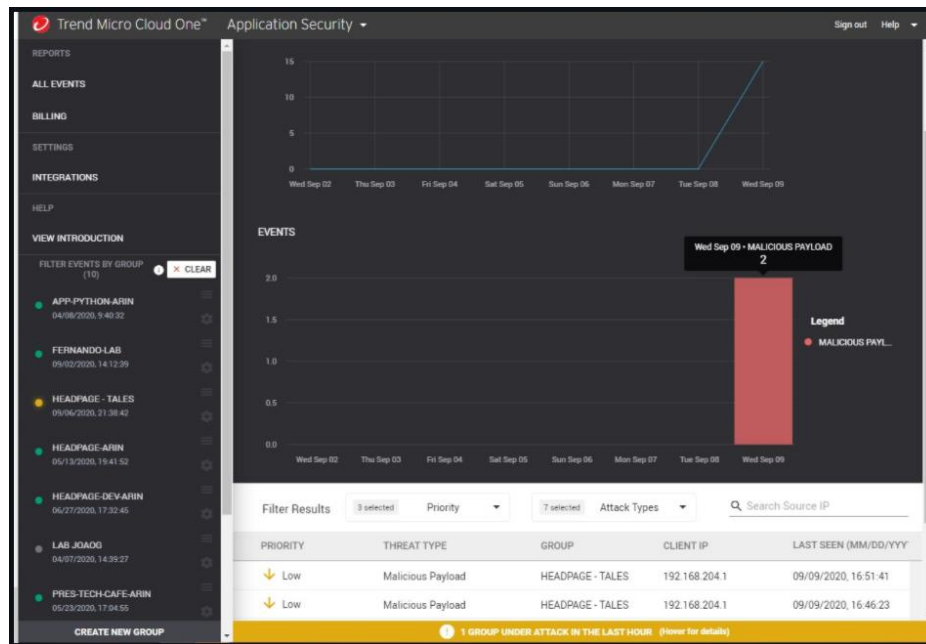
Acesse a url: `http://meuip: 8000/social/static/?file=privacy.txt`



5.3 Visualizando os eventos

Na console do Cloud One dentro do Application Security podemos ver os eventos conforme abaixo, é possível criar políticas para apenas gerar log ou bloquear.

Os eventos podem ser enviados para o Slack, Pagerduty, New Relic Insights ou até mesmo um Tópico SNS.



6. Concluindo

É importante adicionarmos camadas de proteção em todas as fases da criação de uma aplicação, dessa forma teremos visibilidade do que acontece no host, no código e teremos uma aplicação estável e segura.

