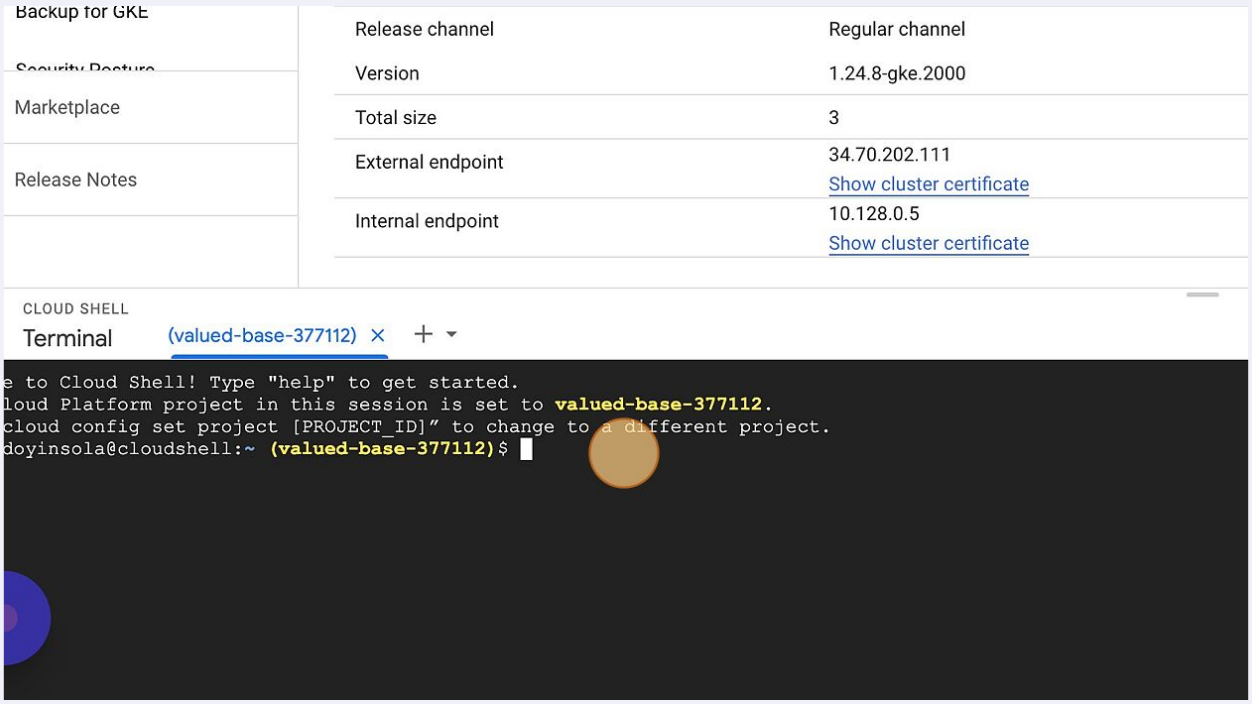
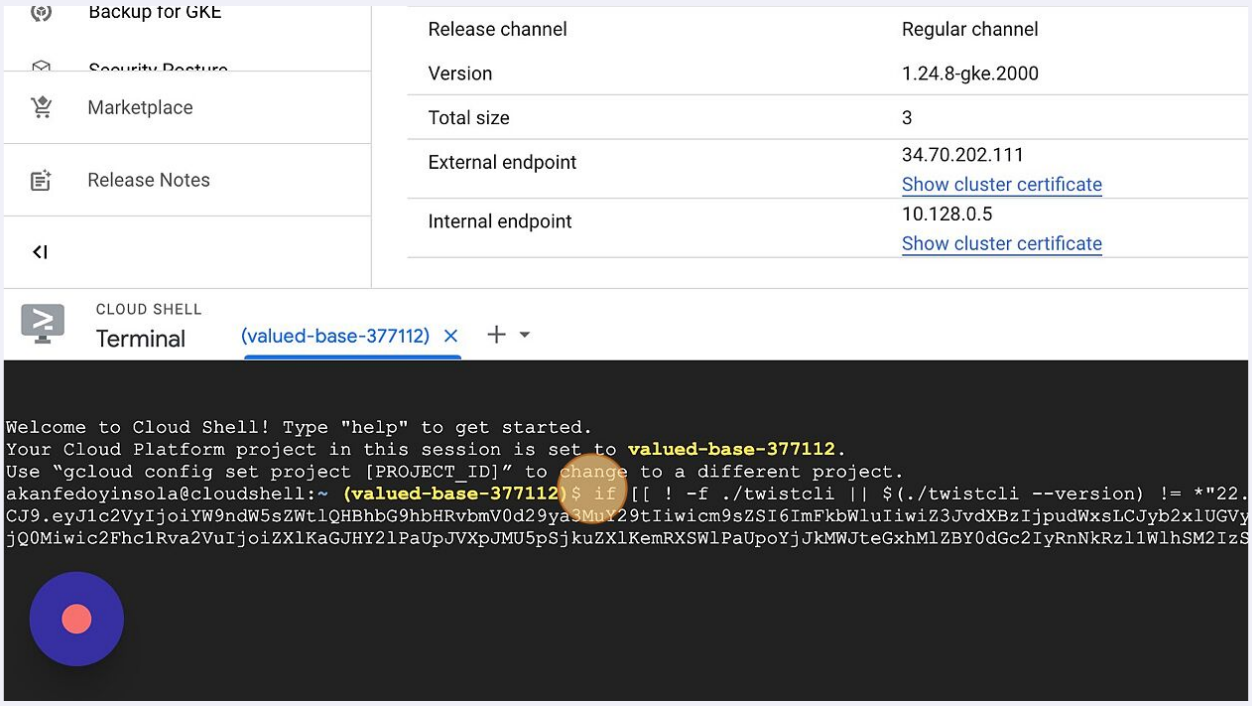
Prismacloud Workflow

1 Navigate to [console.cloud.google.com/kubernetes/clusters/de...]

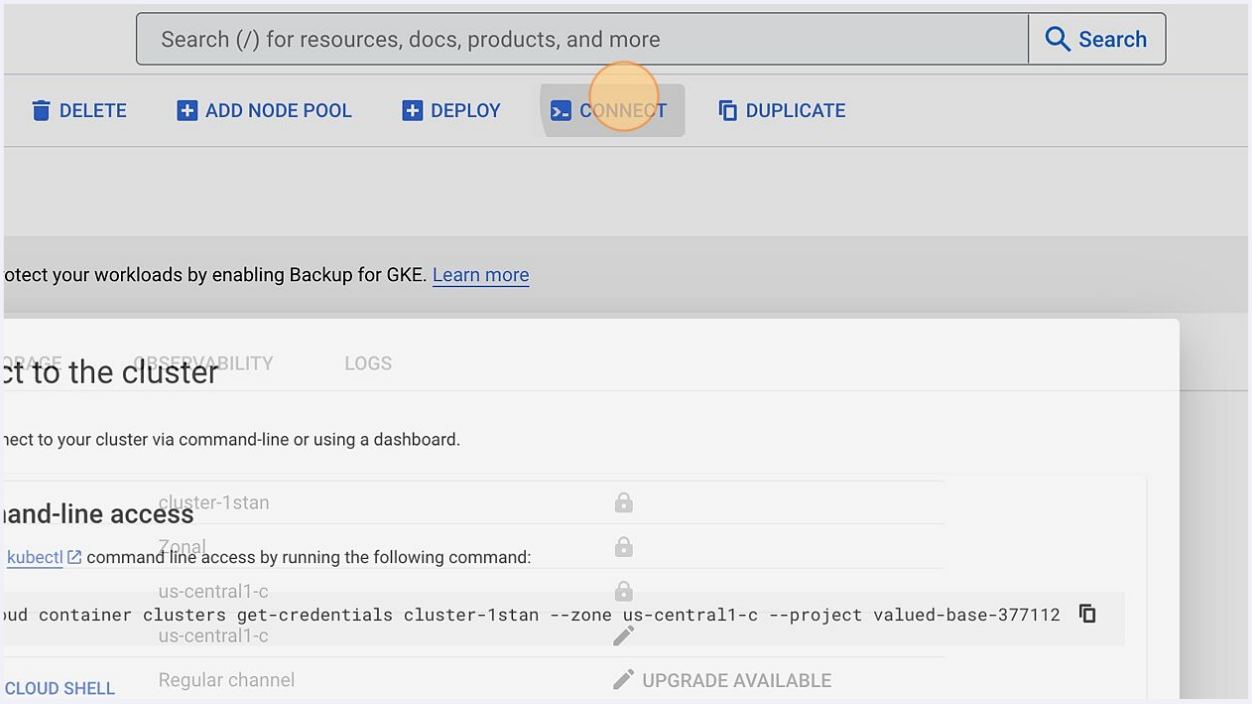
2 Click here.



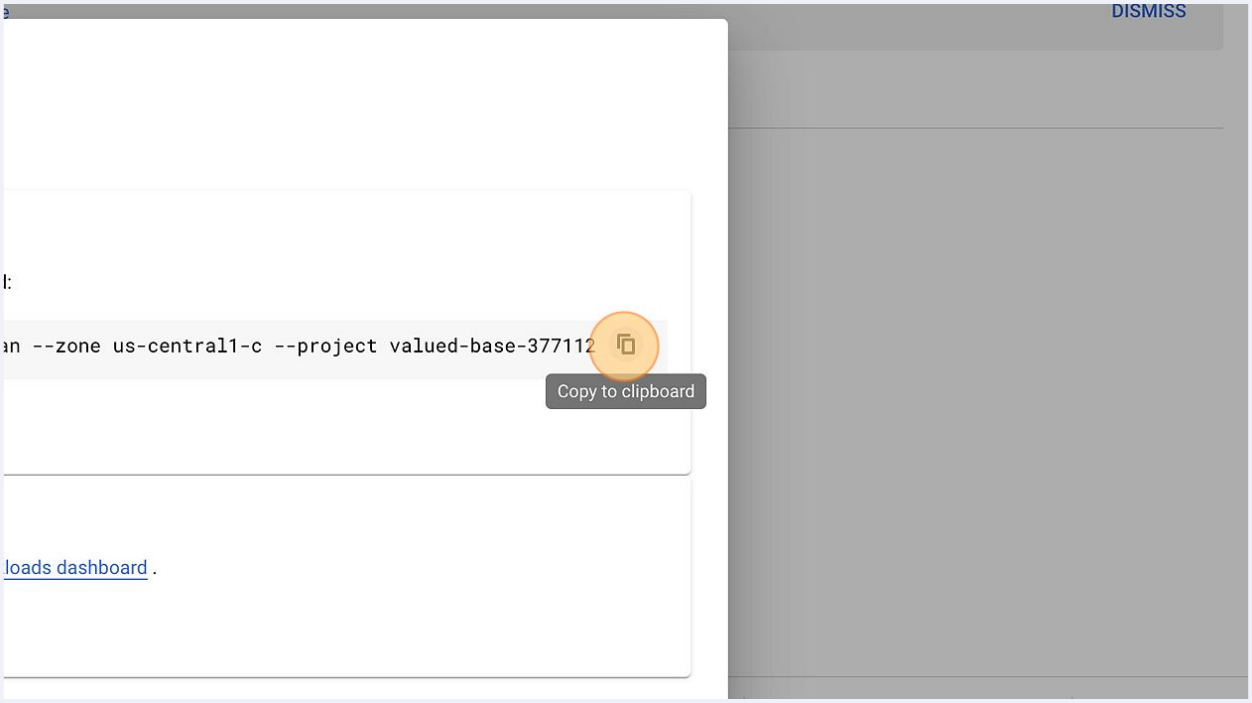
3 Click "akanfedoyinsola@cloudshell:~ (valued-base-377112)$ if [[! -f ./twistcli || $(./twistcli --version) != *"22.12.427"*]]; then curl --progress-ba..."



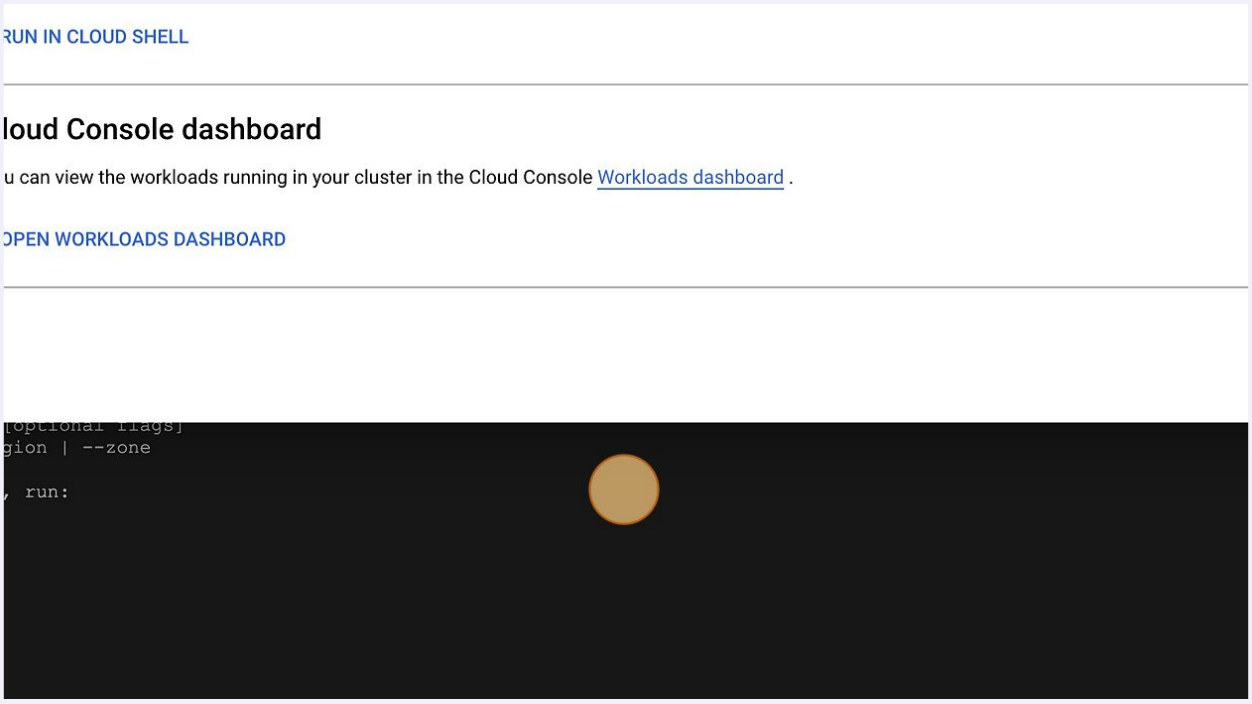
4 Click "CONNECT"



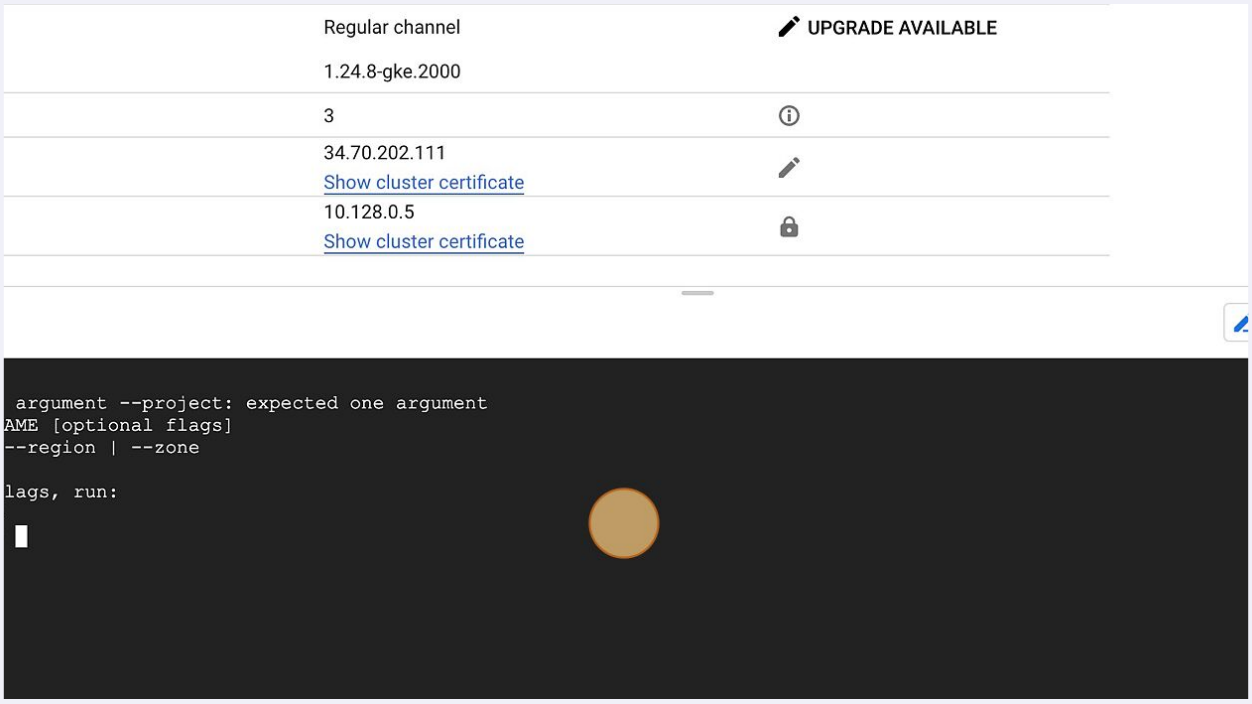
5 Click here.



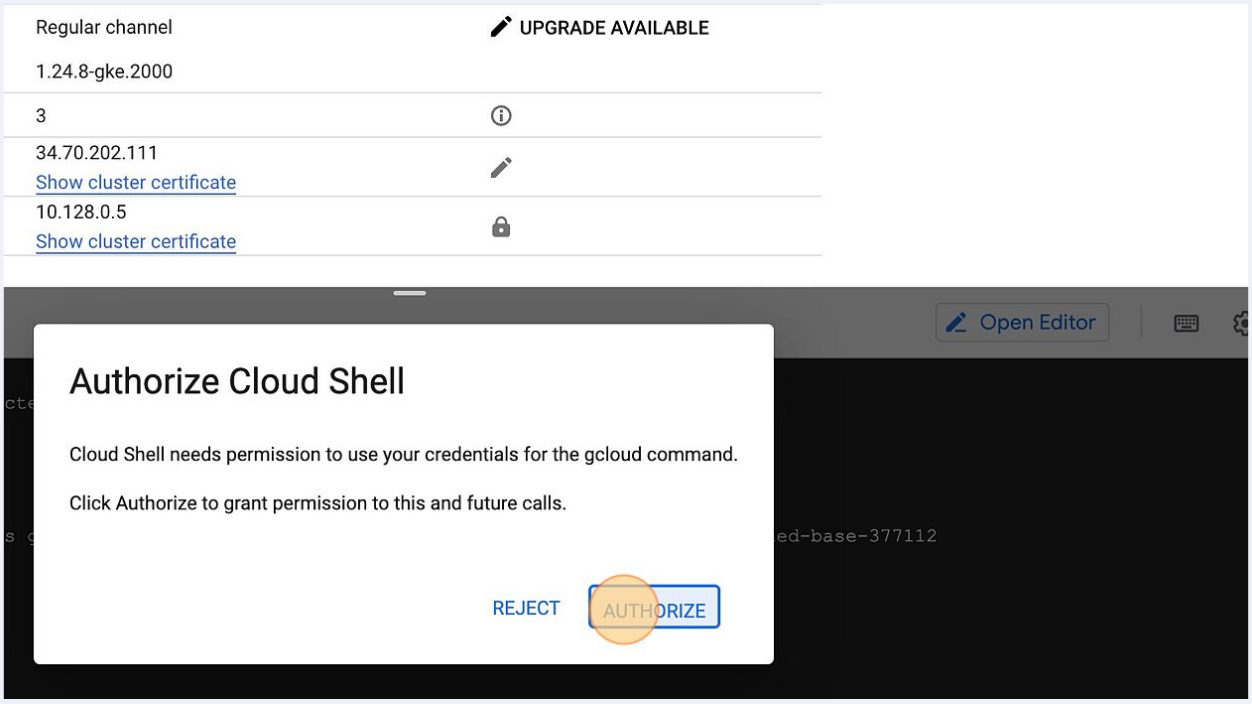
6 Click here.



7 Click "akanfedoyinsola@cloudshell:~ (valued-base-377112)$"

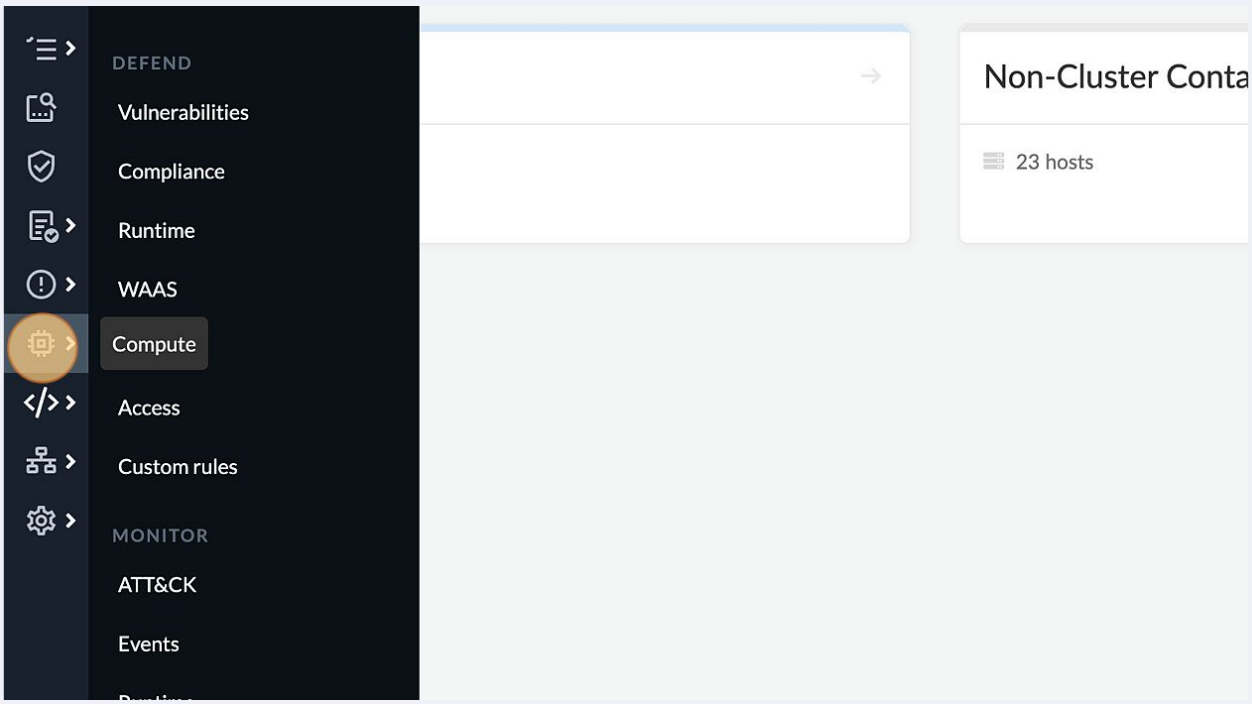


8 Click "AUTHORIZE"

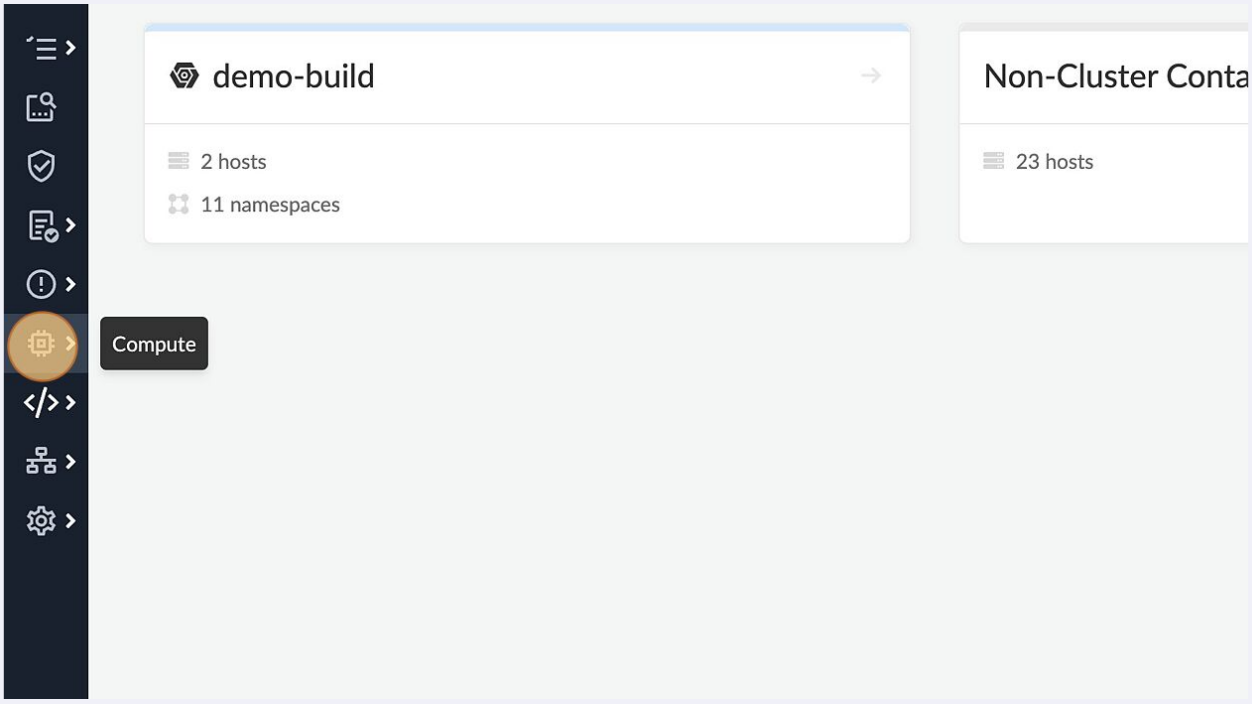


9 Switch to tab "Prisma Cloud | Compute"

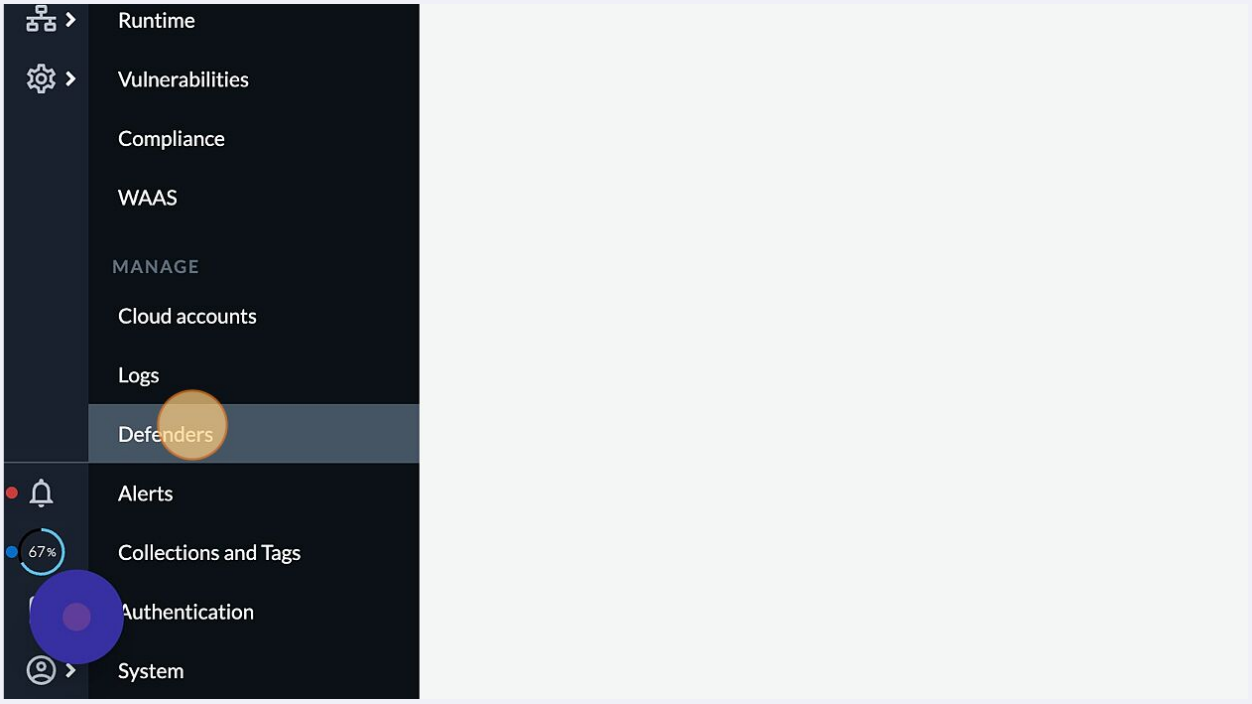
10 Click this icon.



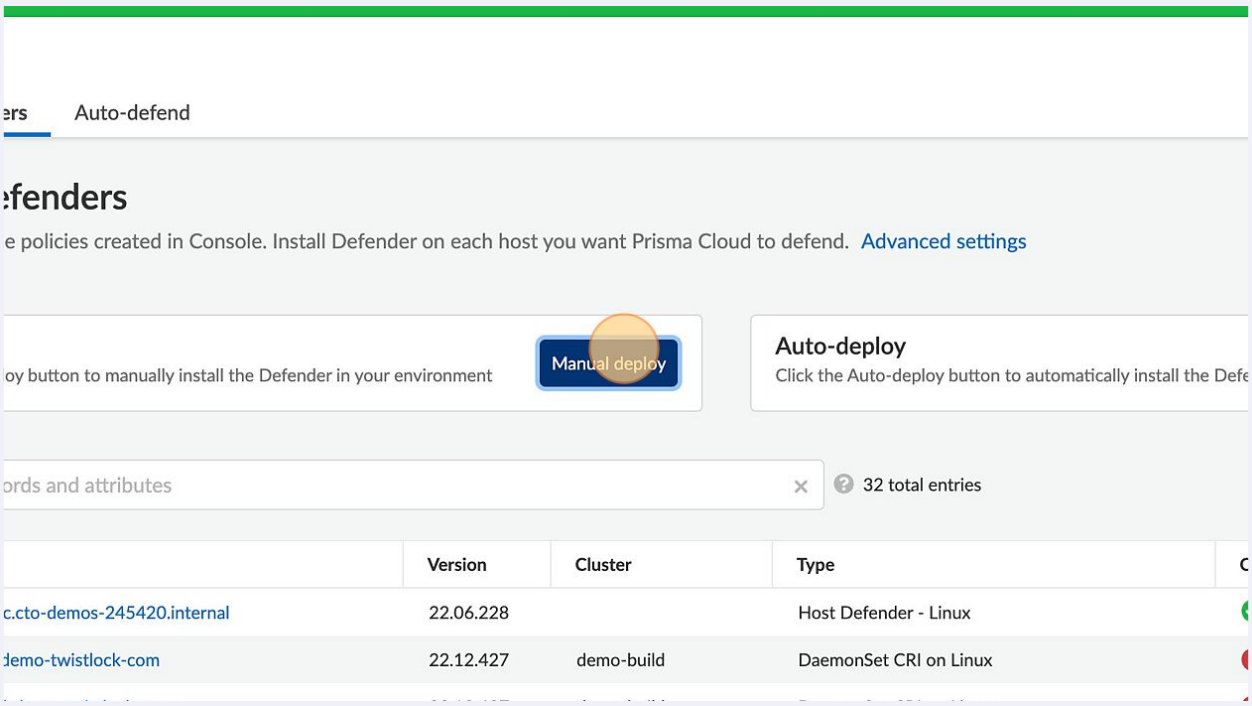
11 Click this icon.



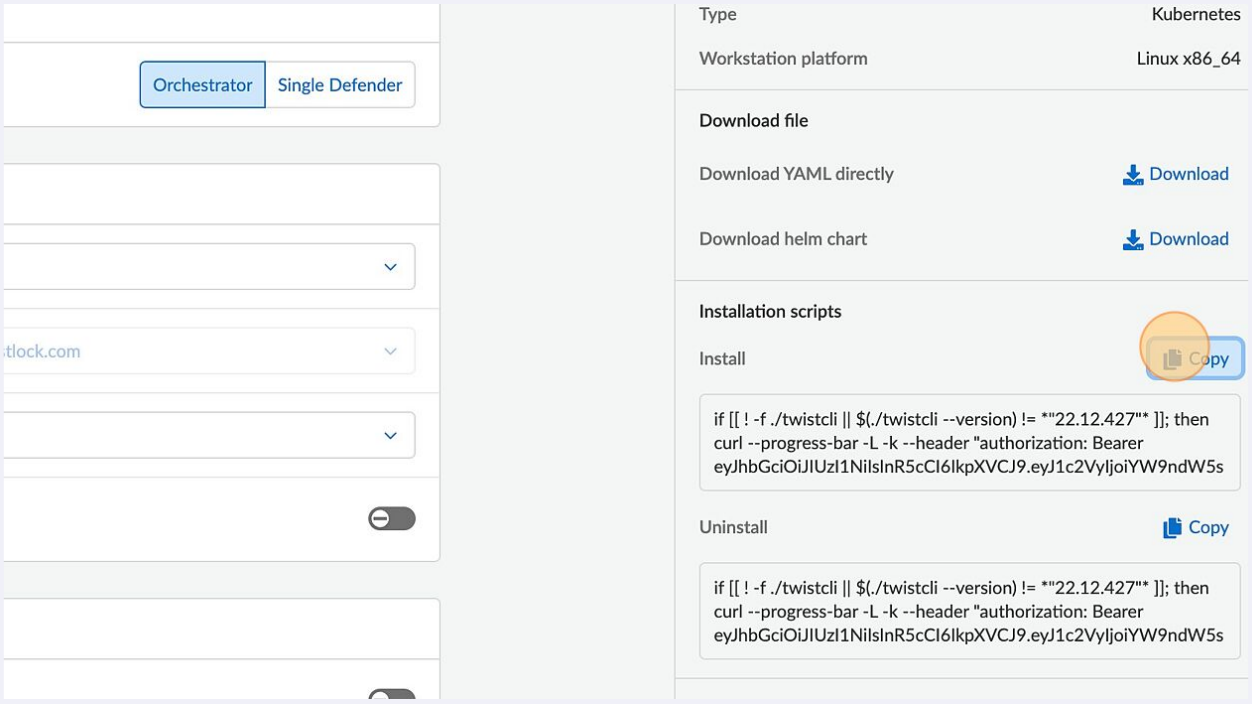
12 Click "Defenders"



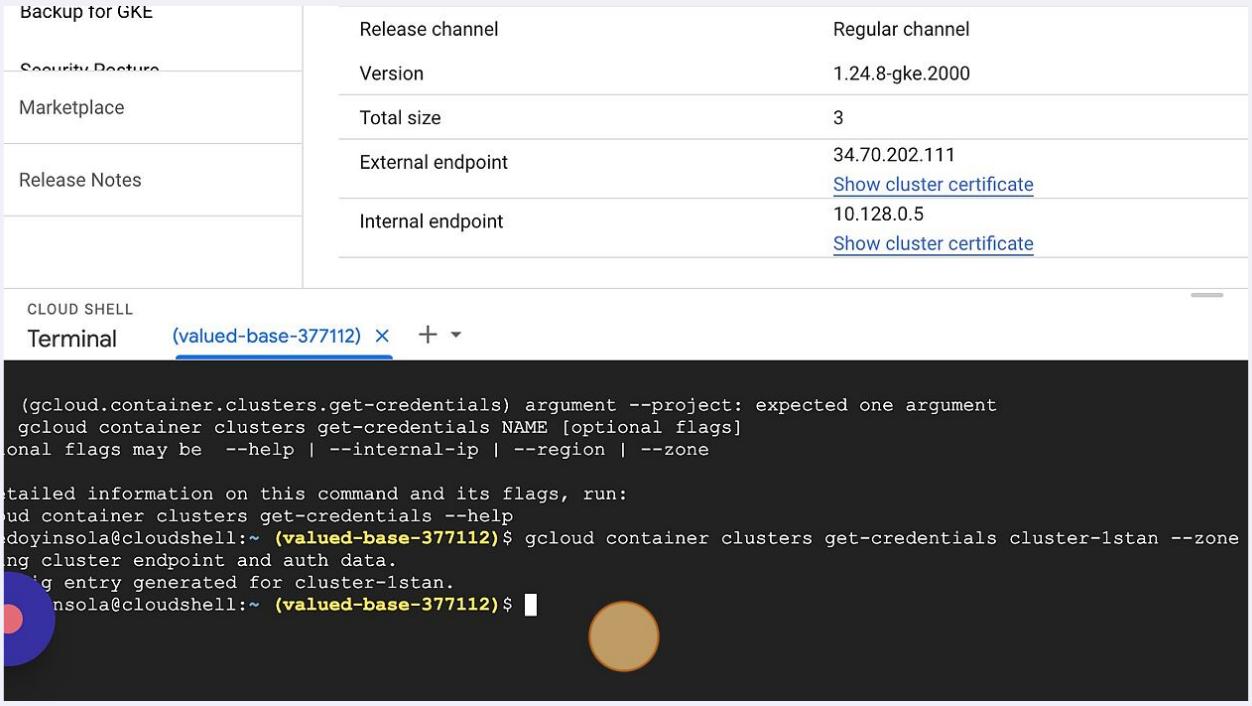
13 Click "Manual deploy"



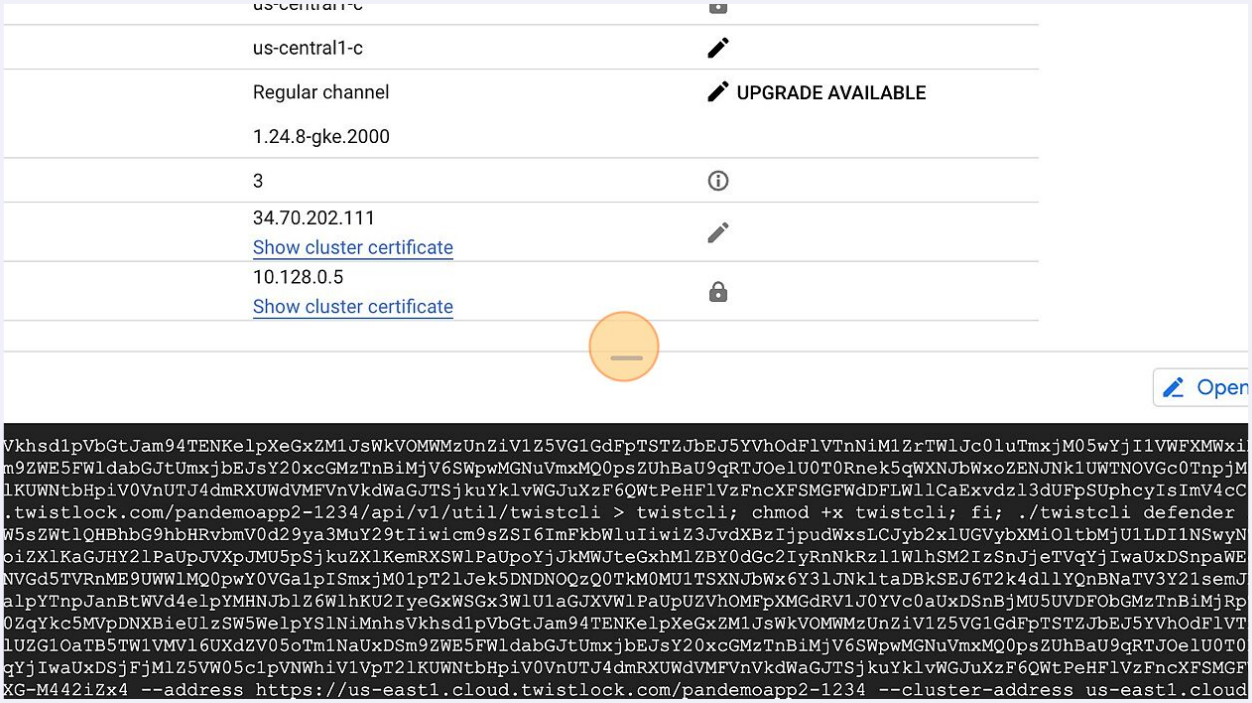
14 Click this icon.



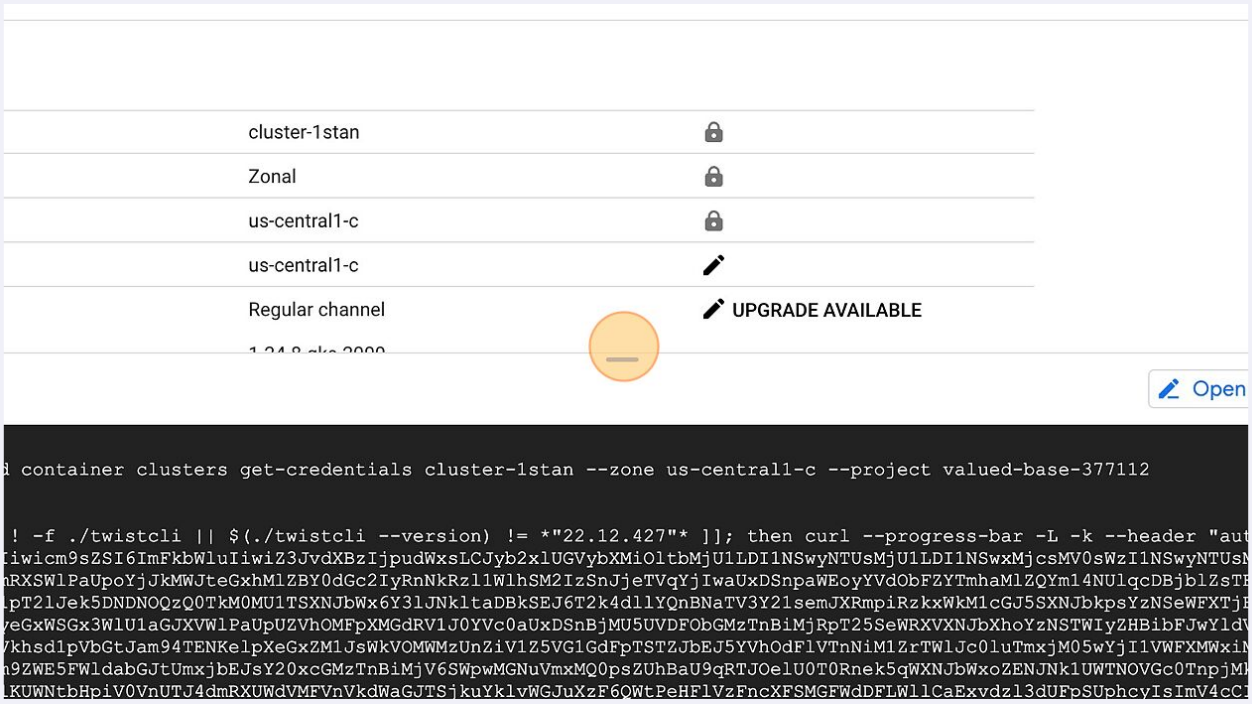
15 Click here.



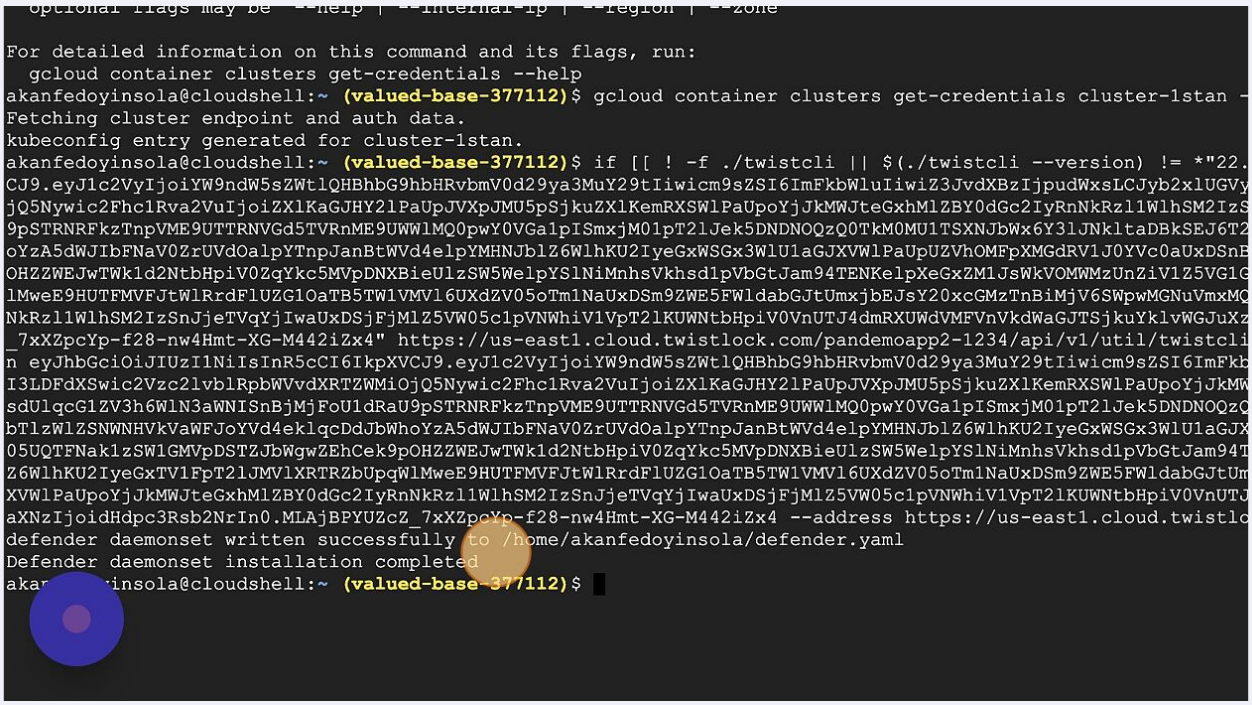
16 Click here.



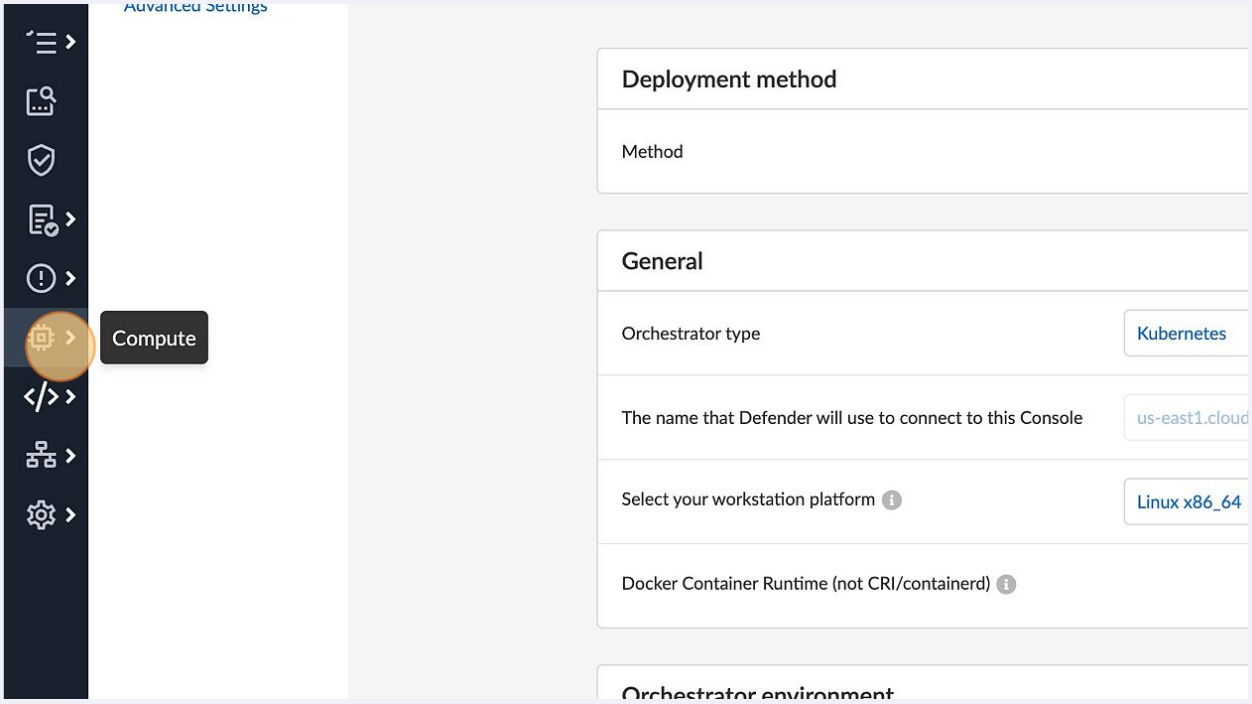
17 Click here.



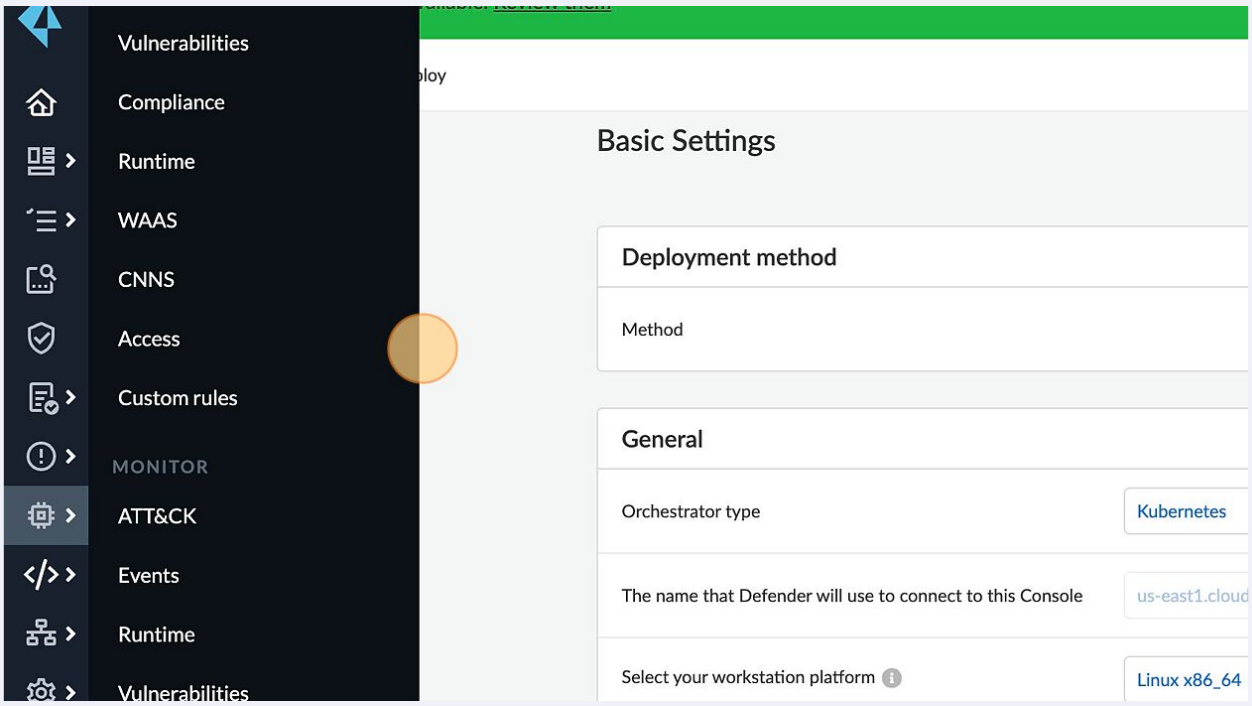
18 Click "Defender daemonset installation completed"



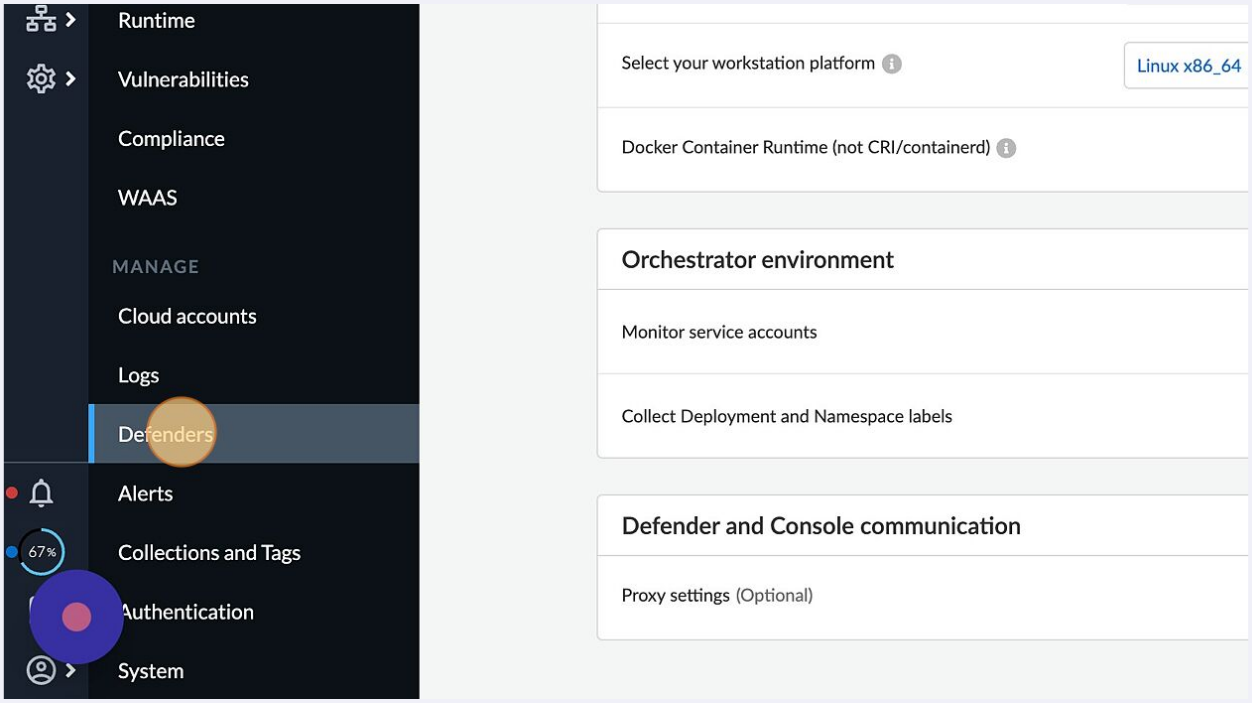
19 Click this link.



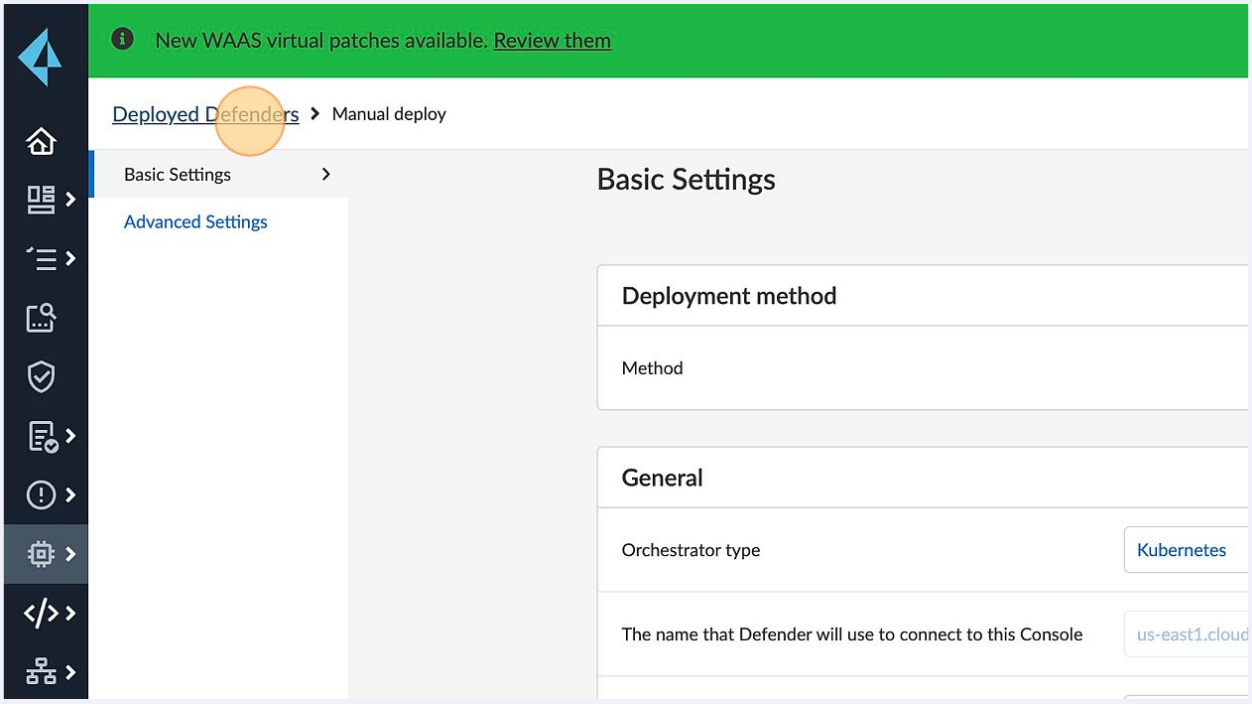
20 Click here.



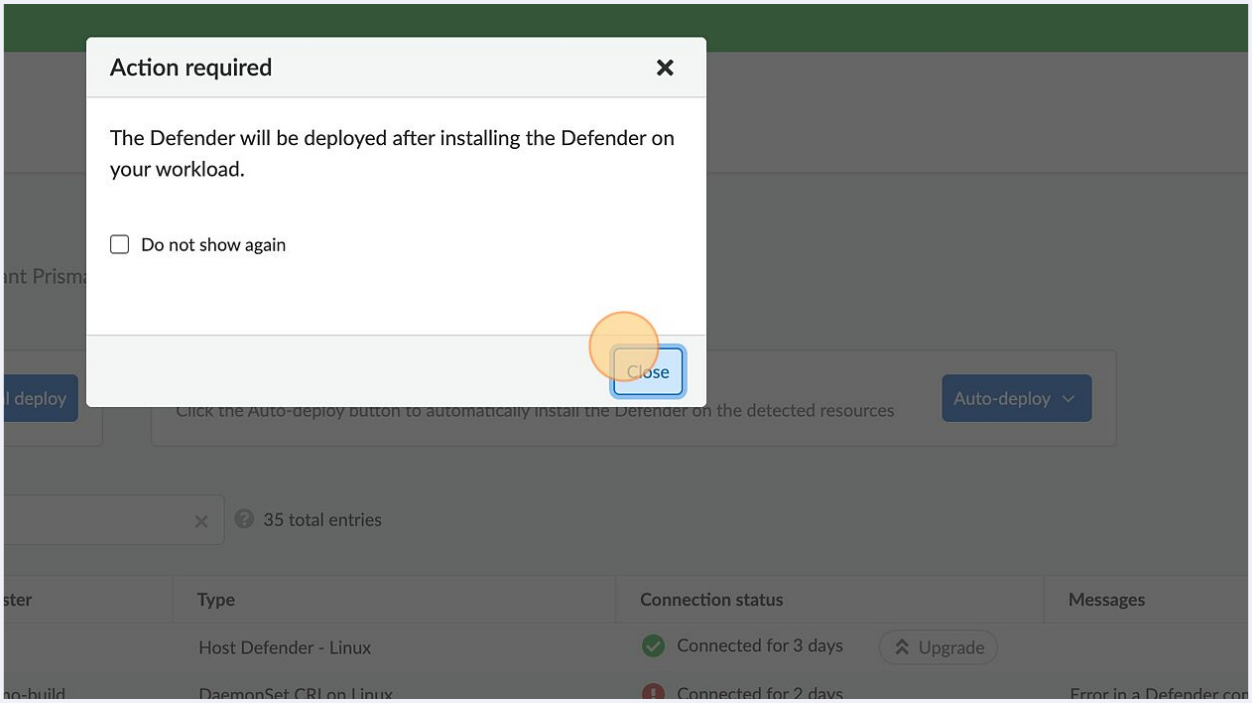
21 Click "Defenders"



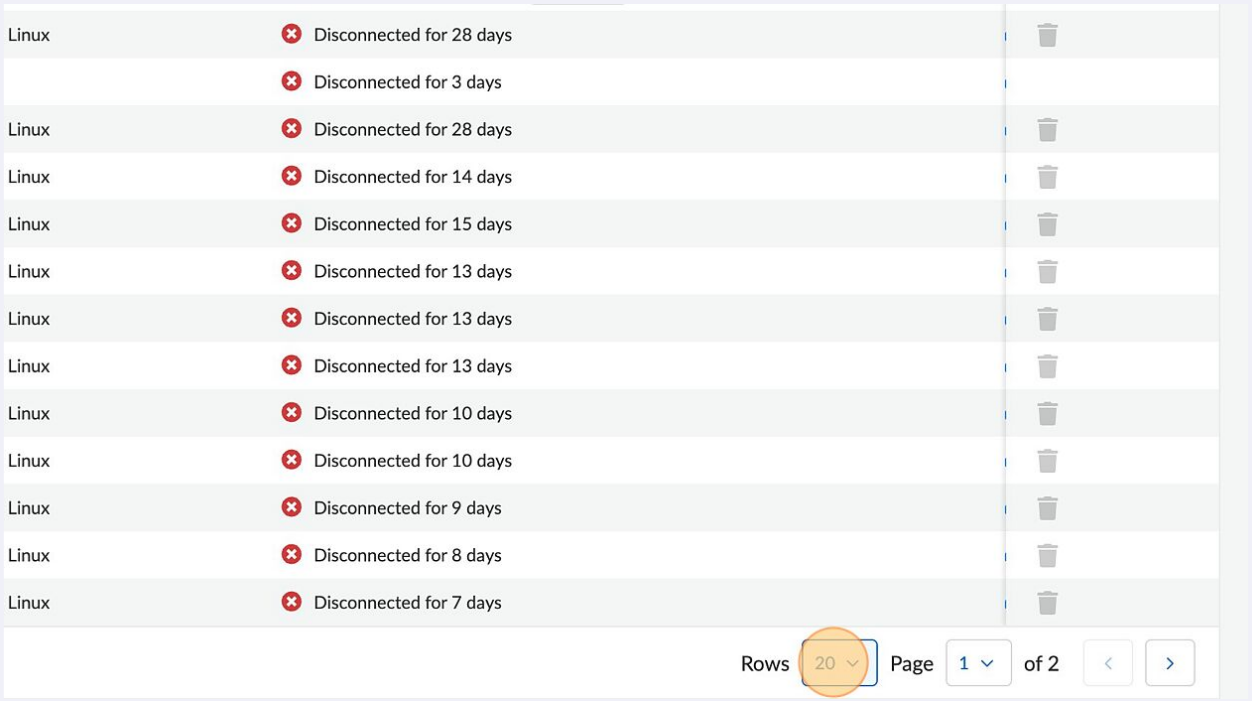
22 Click "Deployed Defenders"



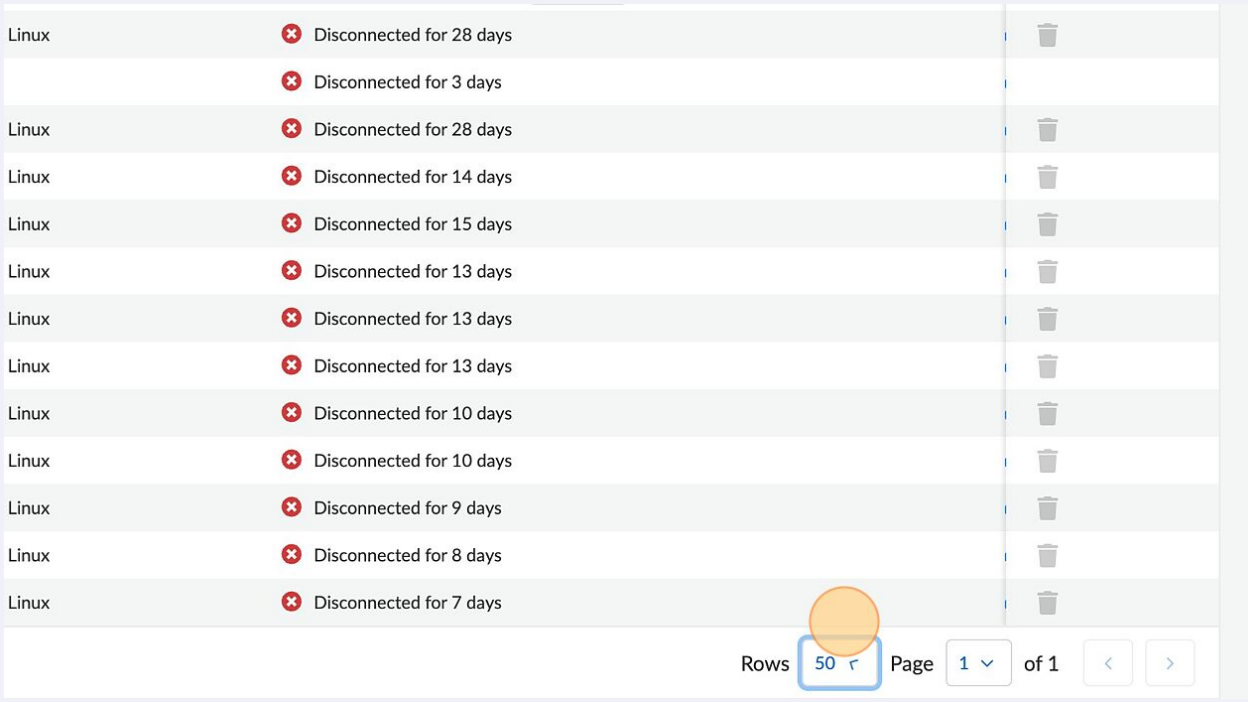
23 Click "Close"



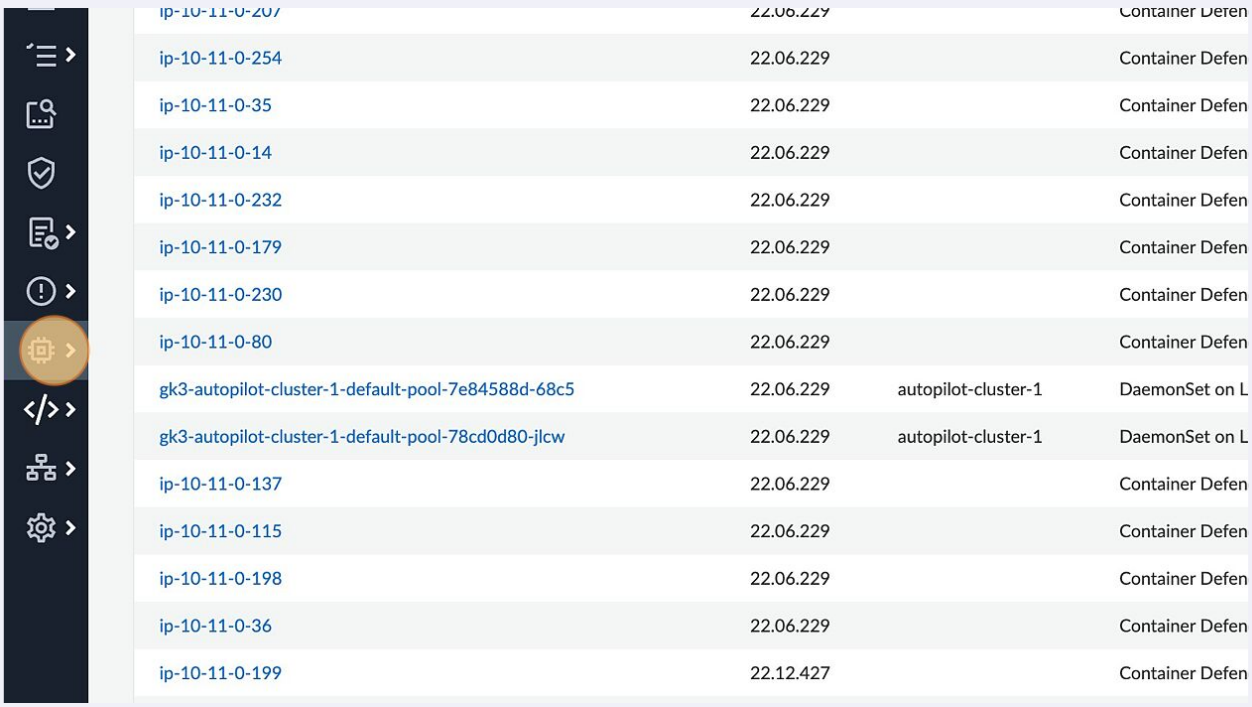
24 Click "20"



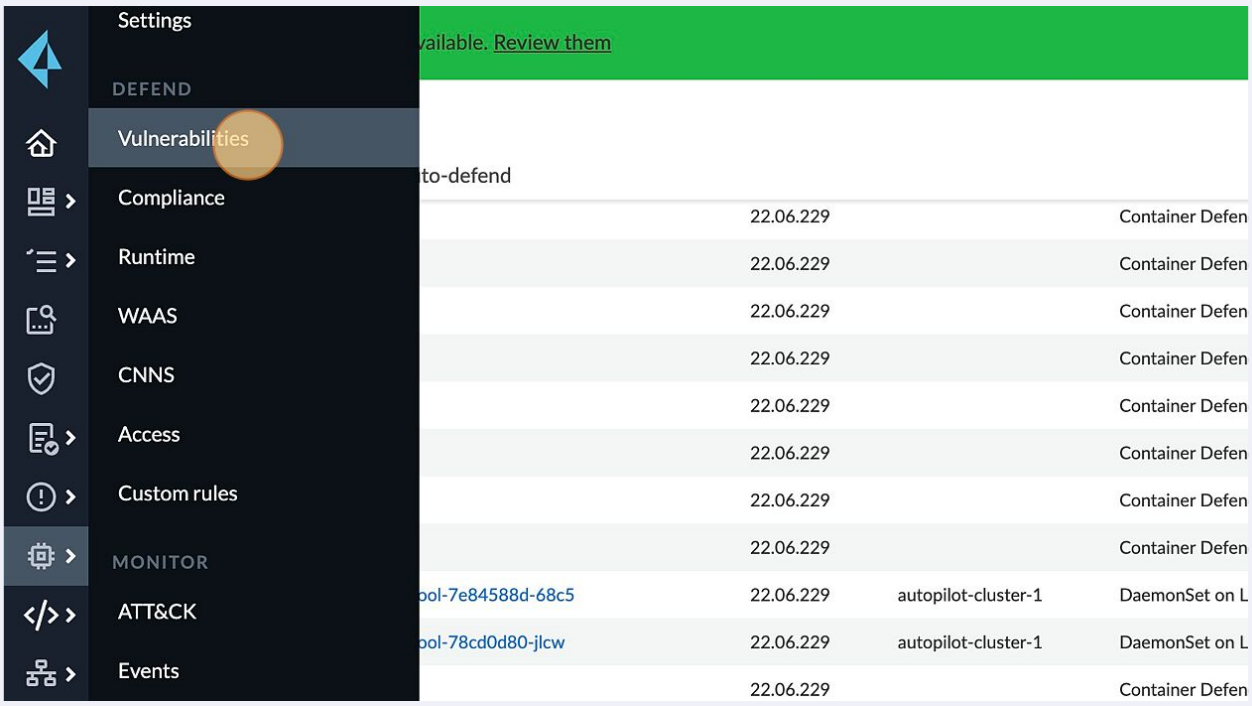
25 Click "50"



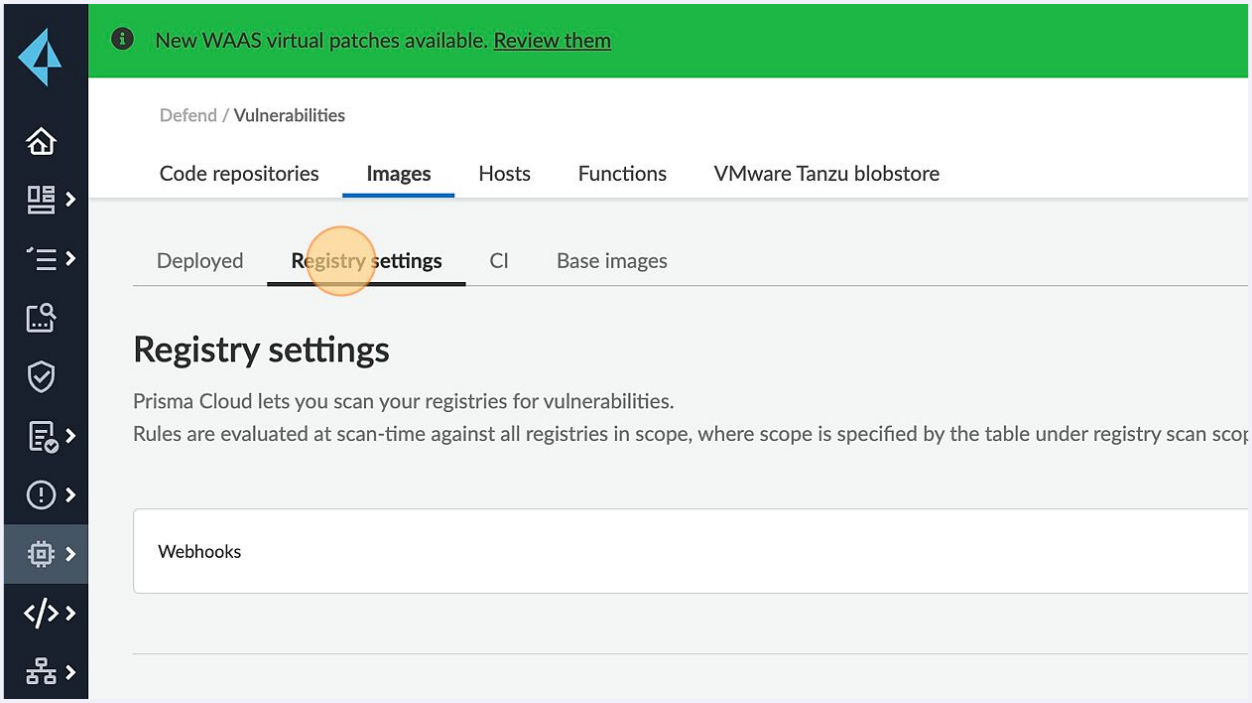
26 Click this icon.



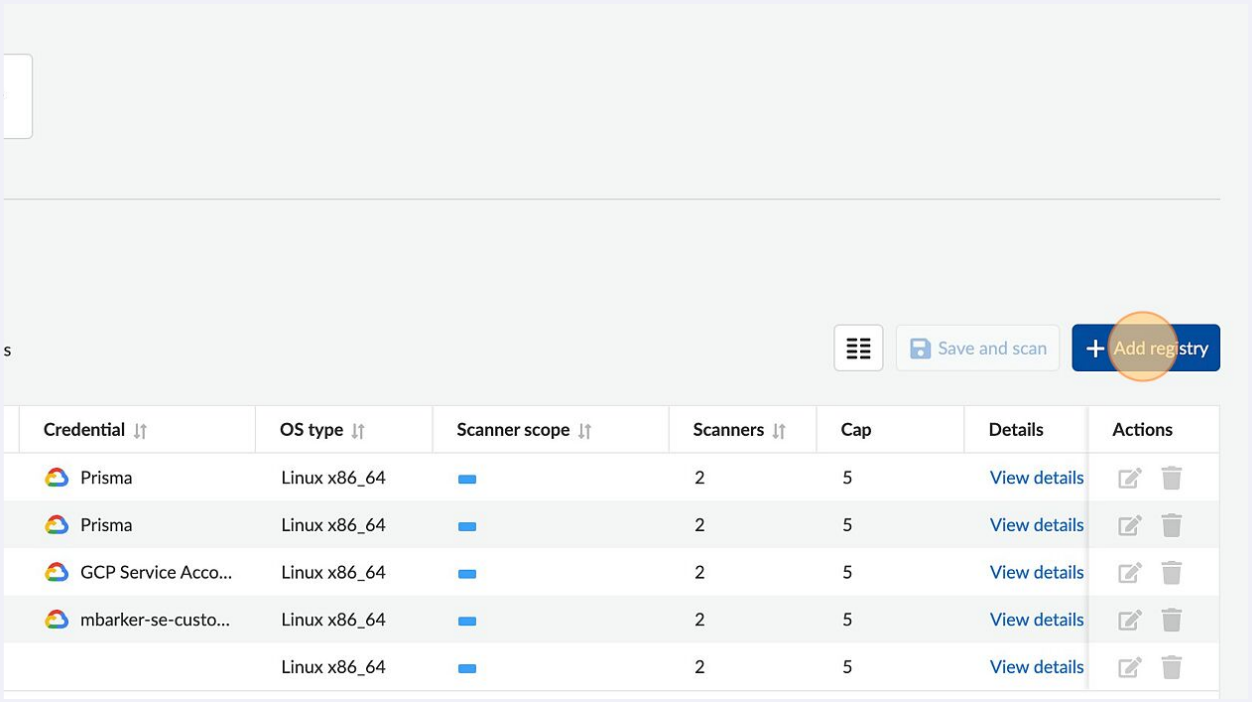
27 Click "Vulnerabilities"



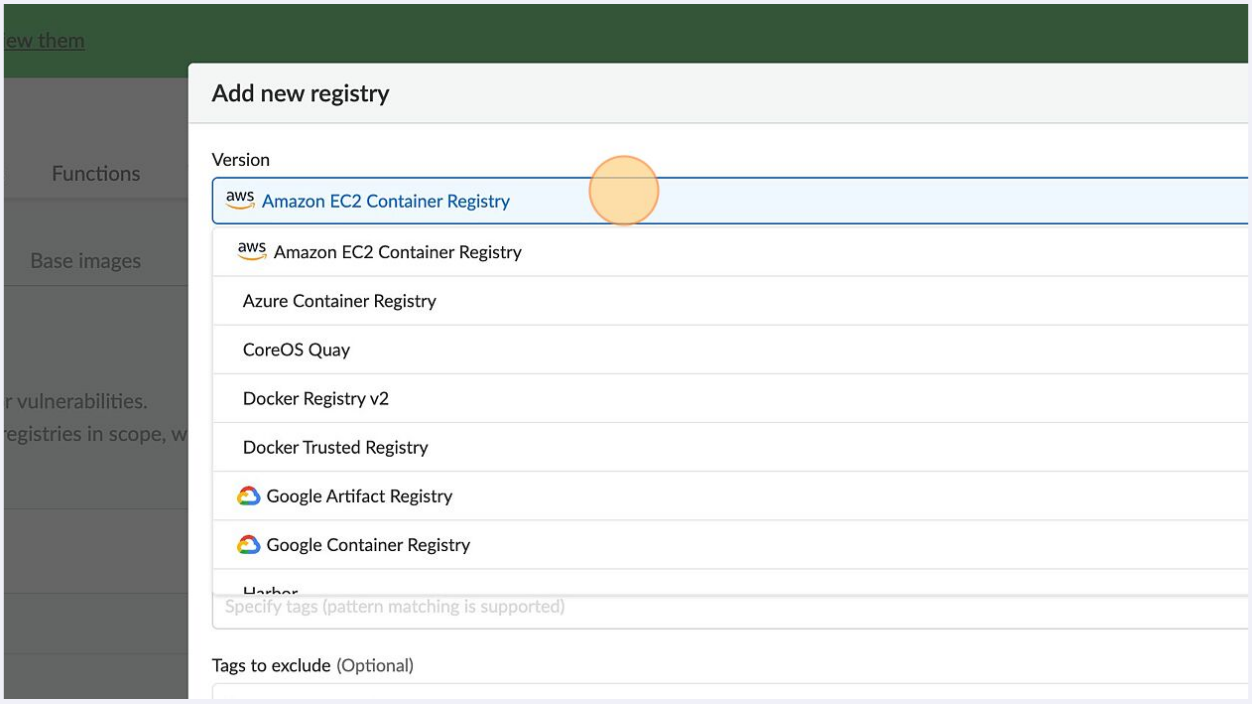
28 Click "Registry settings"



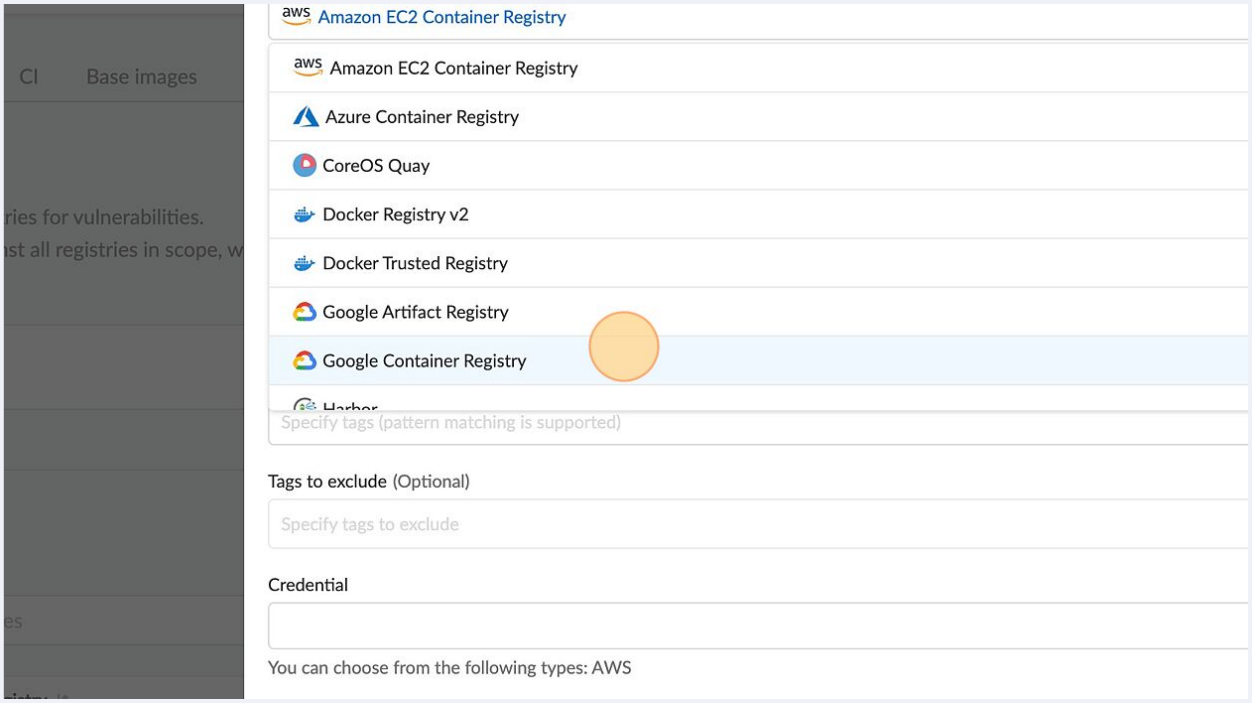
29 Click "Add registry"



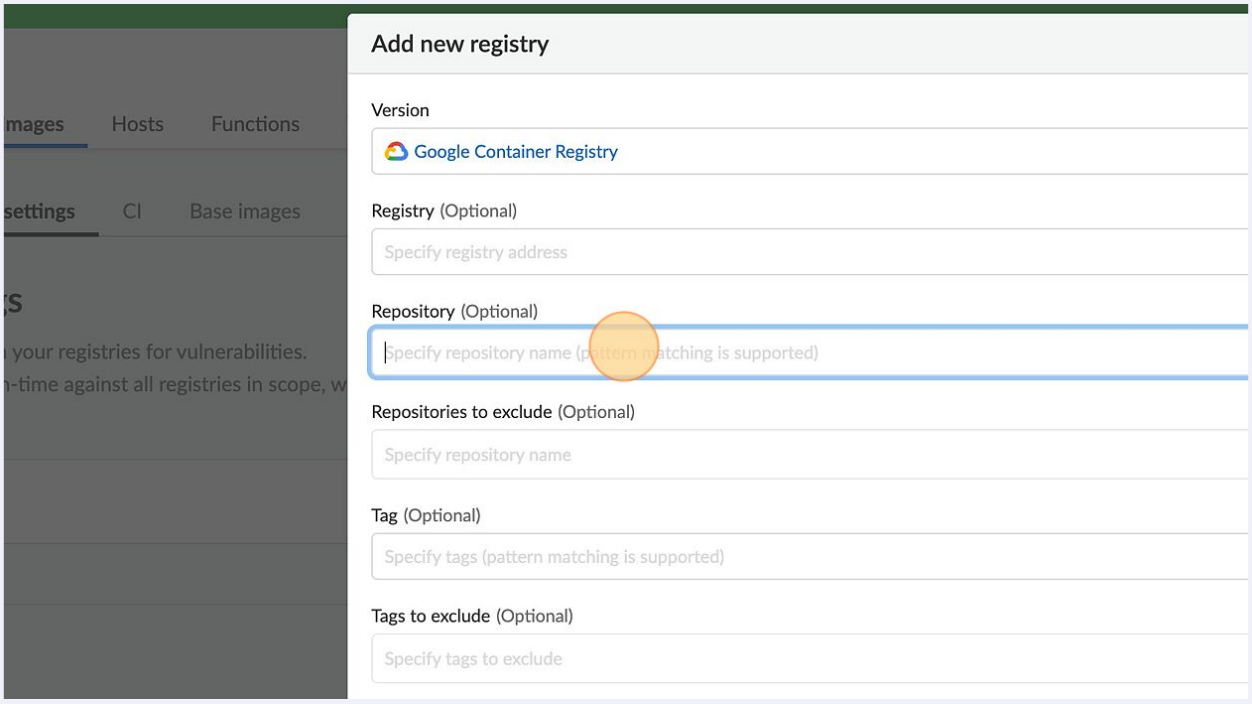
30 Click "Amazon EC2 Container Registry"



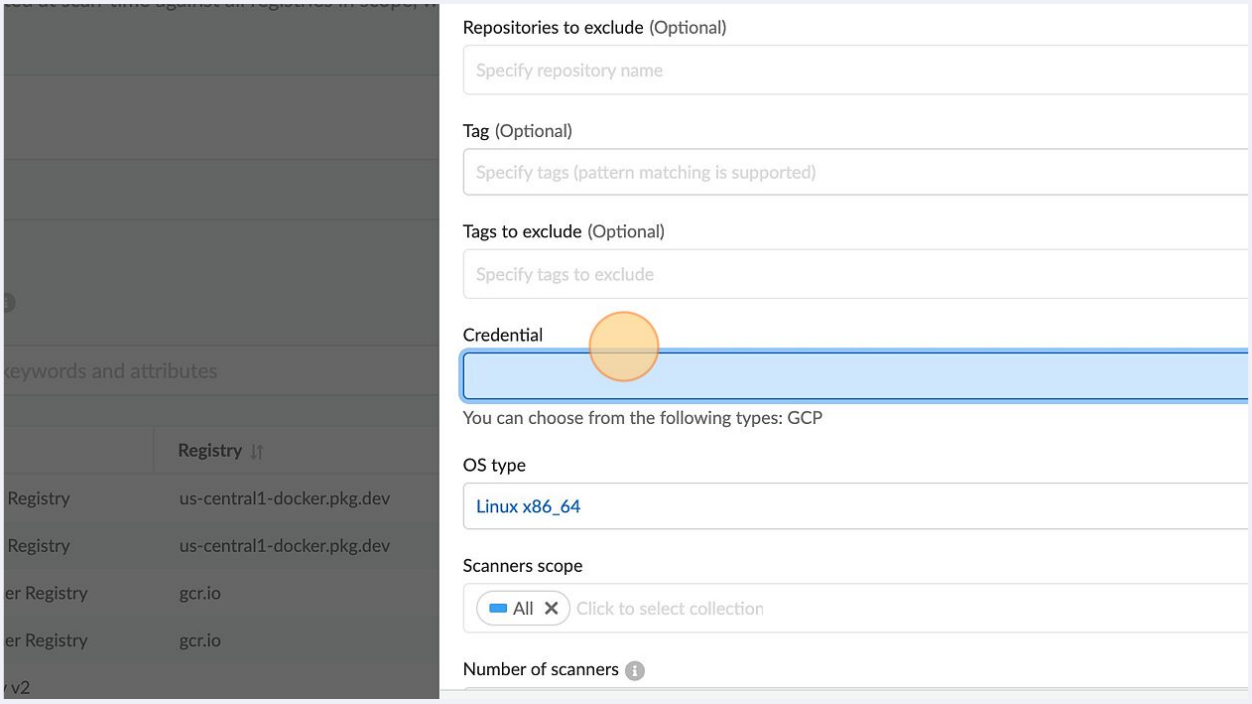
31 Click "Google Container Registry"



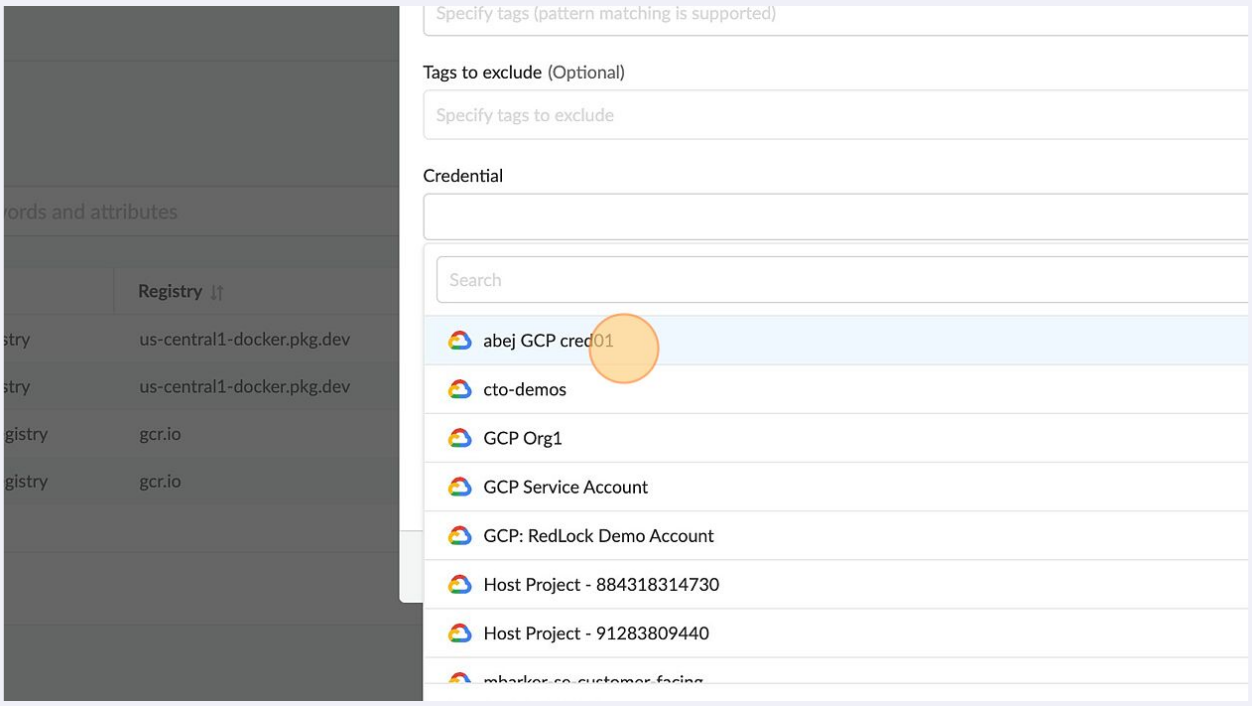
32 Click the "Repository(Optional)" field.



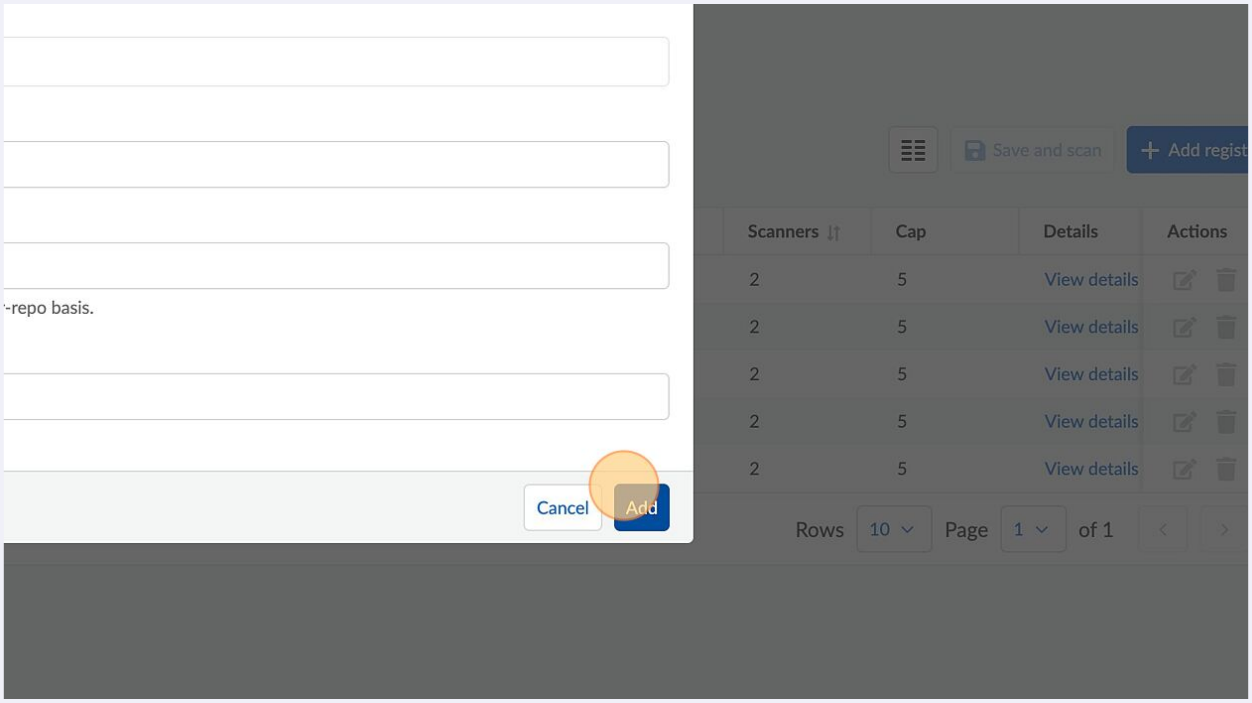
33 Click this button.



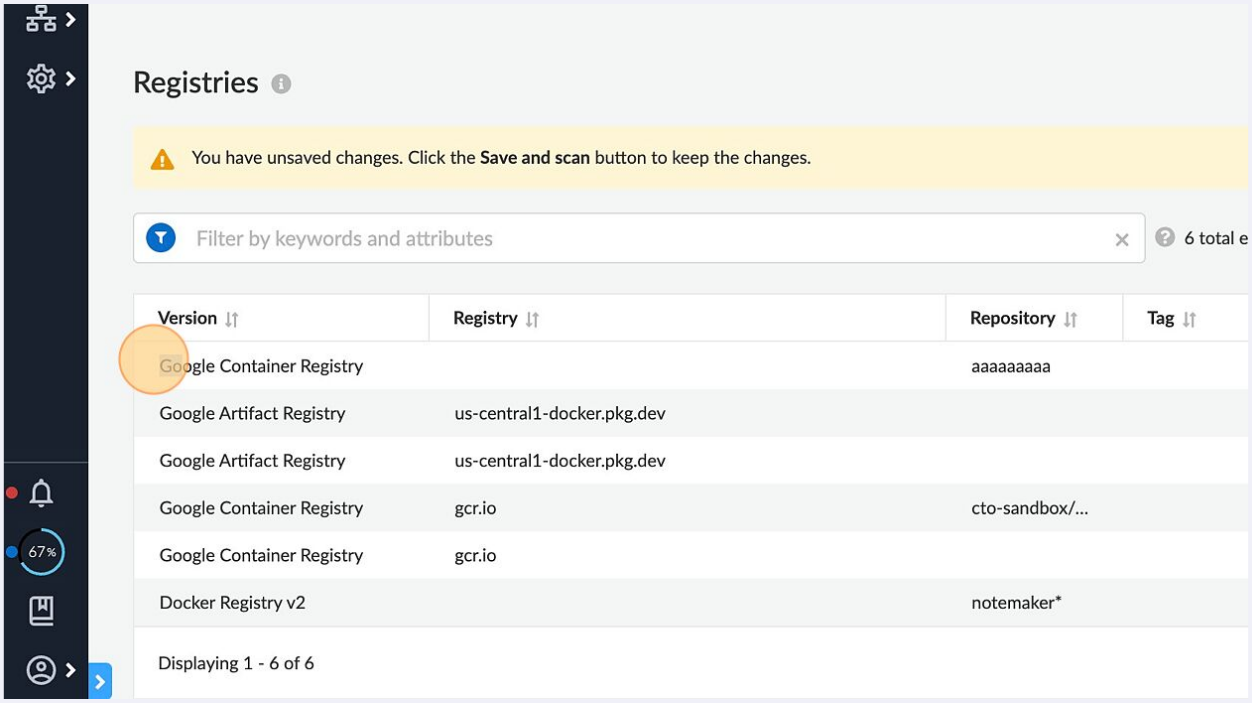
34 Click "abej GCP cred01"



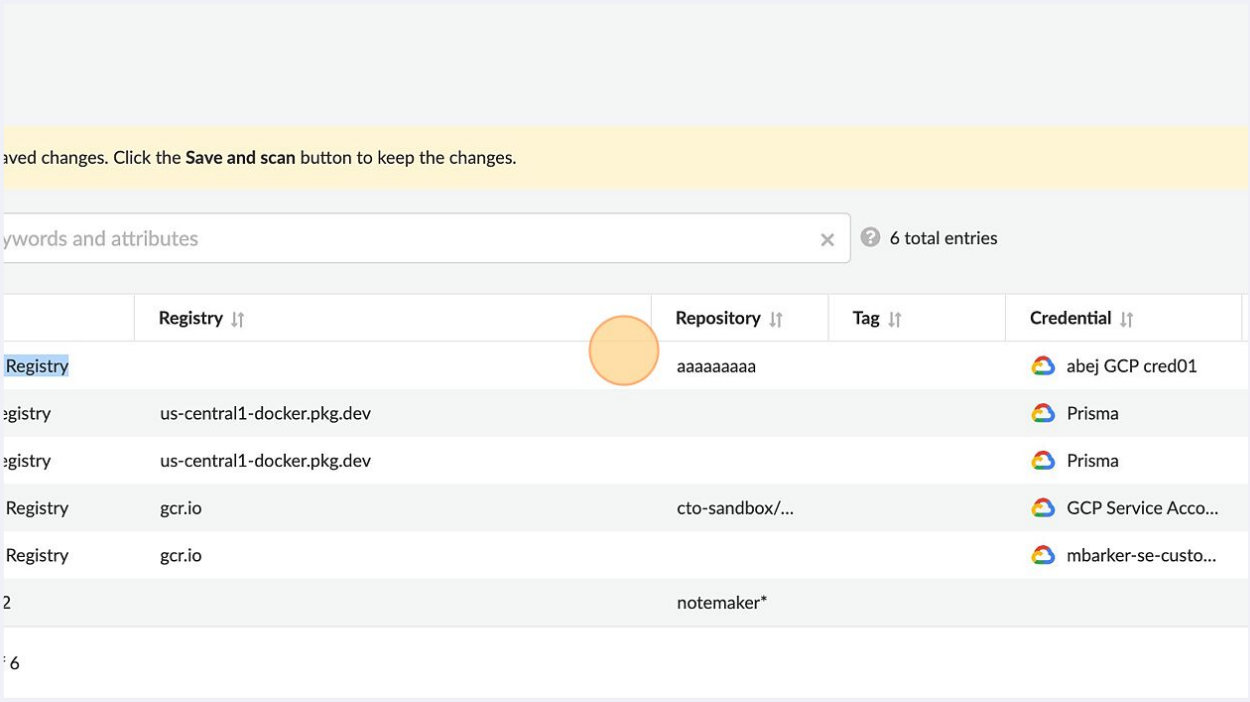
35 Click "Add"



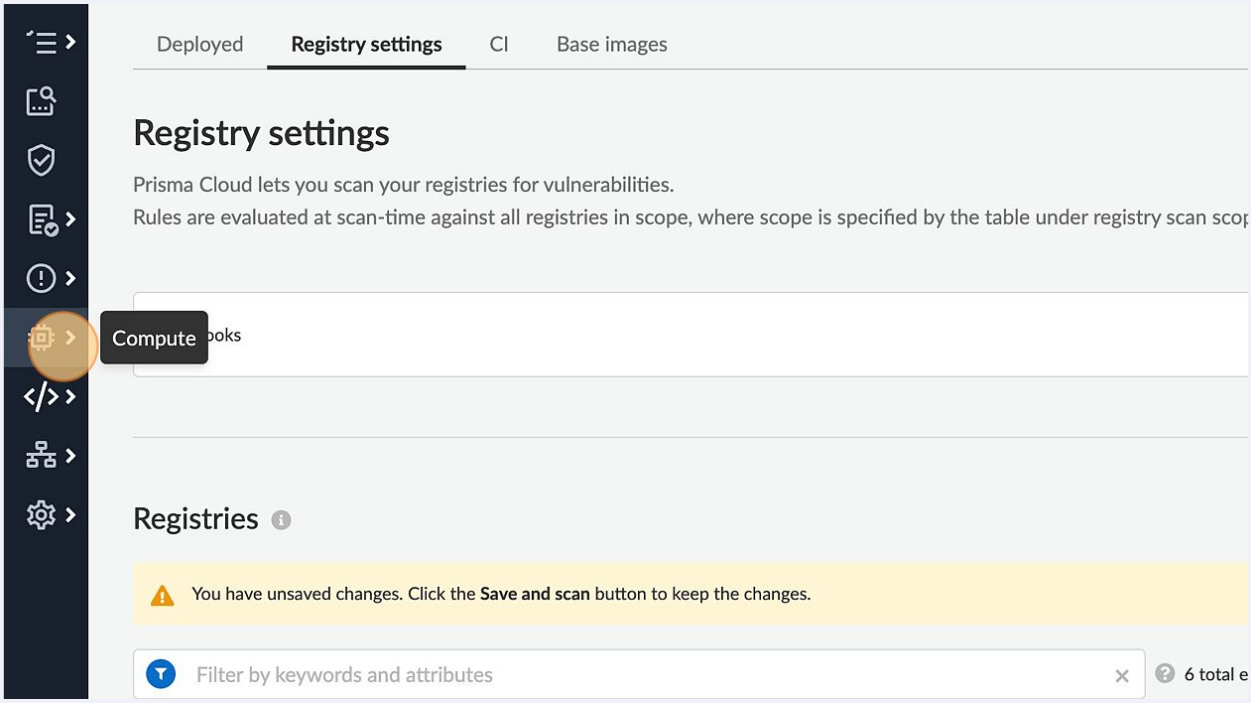
36 Click "Google Container Registry"



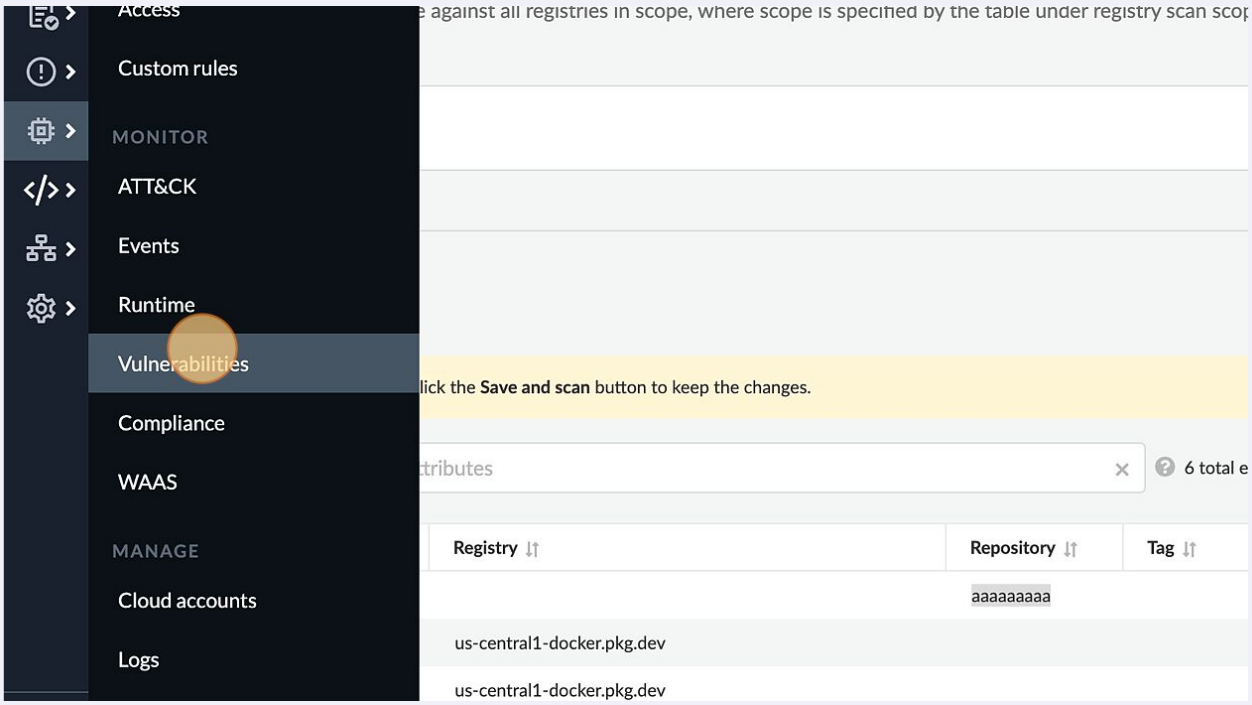
37 Click here.



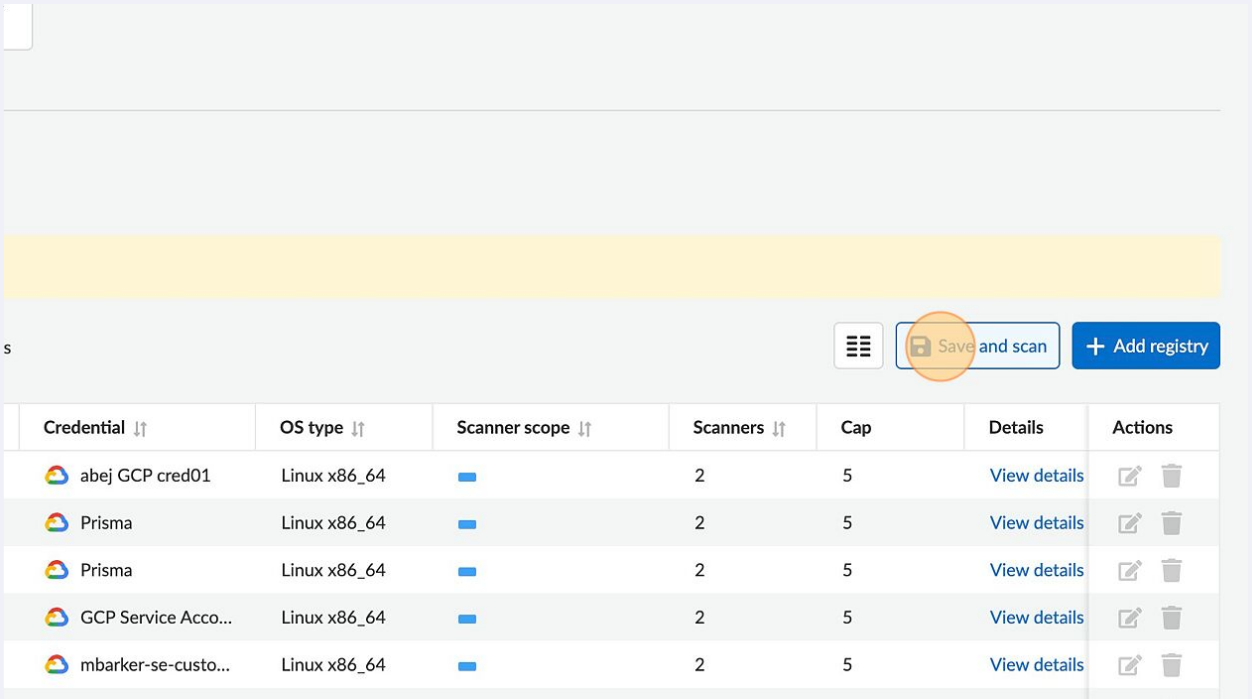
38 Click this link.



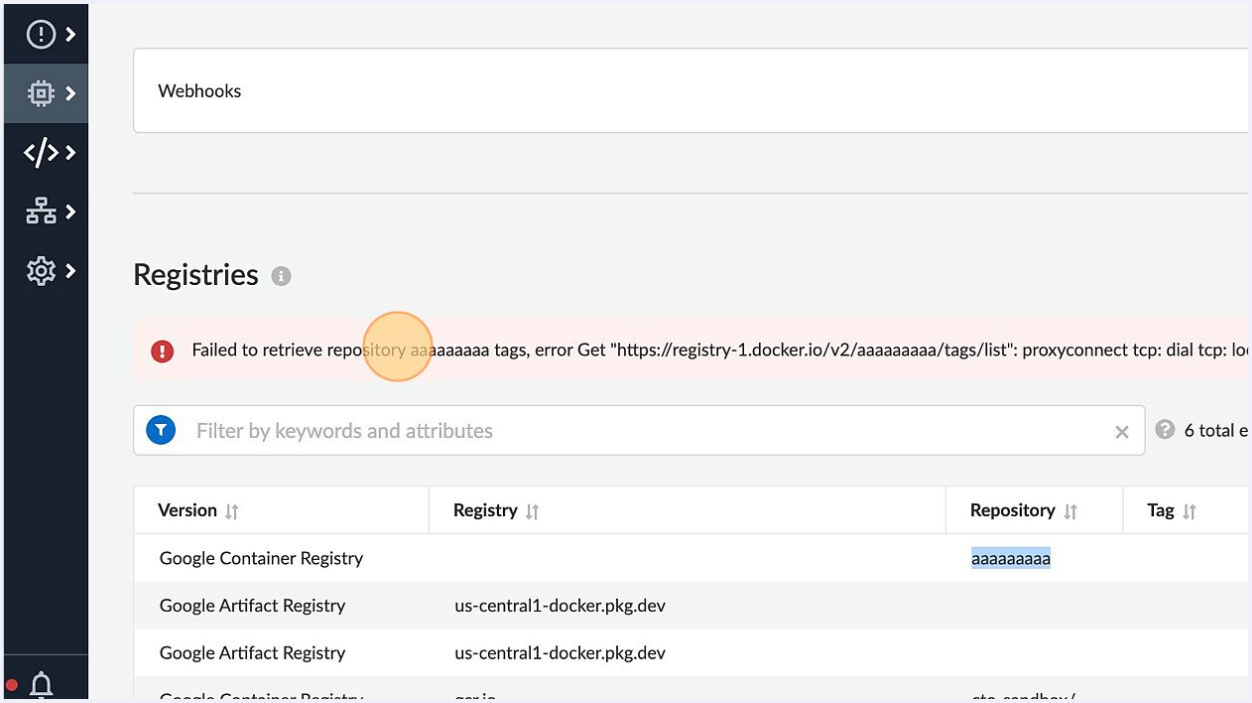
39 Click "Vulnerabilities"



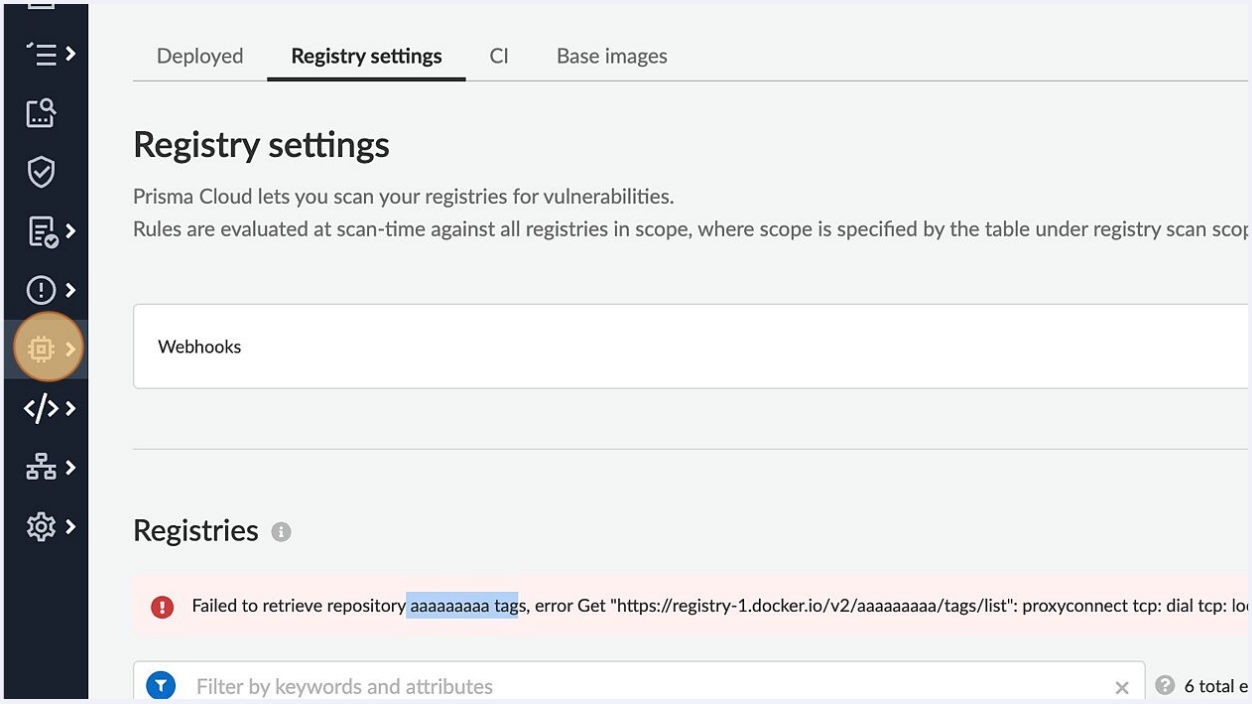
40 Click "Save and scan"



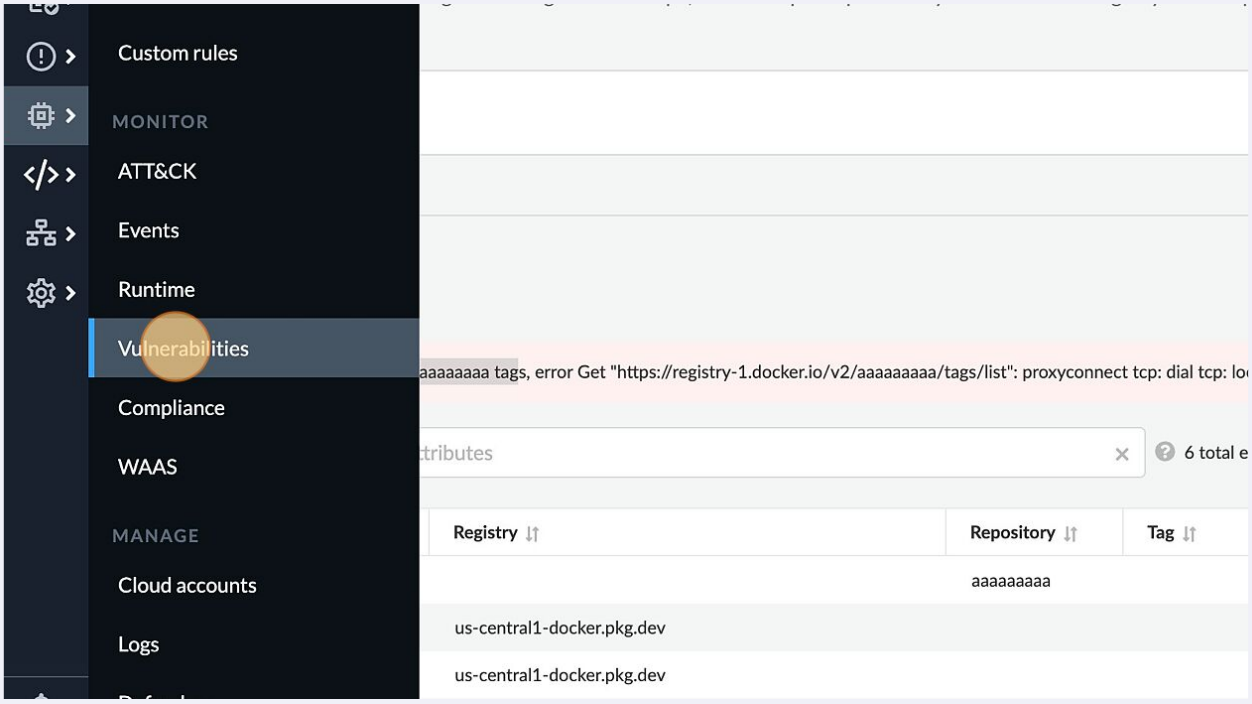
41 Click "Failed to retrieve repository aaaaaaaaa tags, error Get "https://registry-1.docker.io/v2/aaaaaaaaa/tags/list": proxyconnect tcp: dial tcp: looku..."



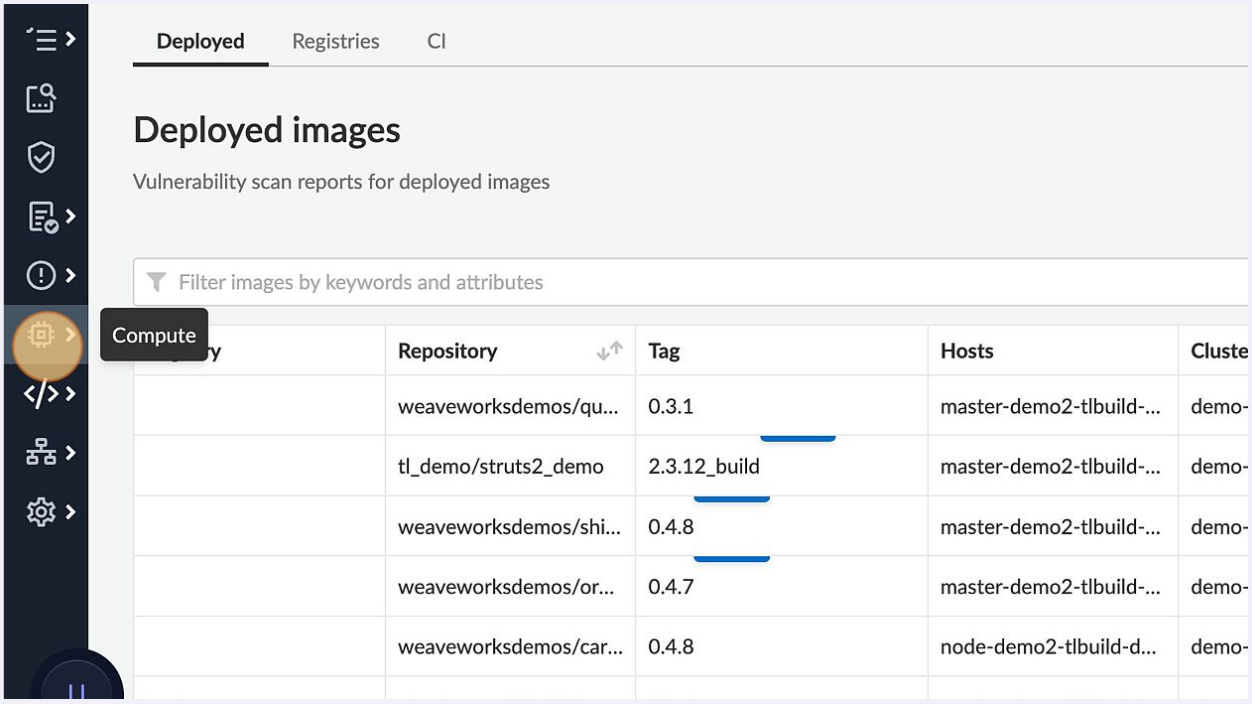
42 Click here.



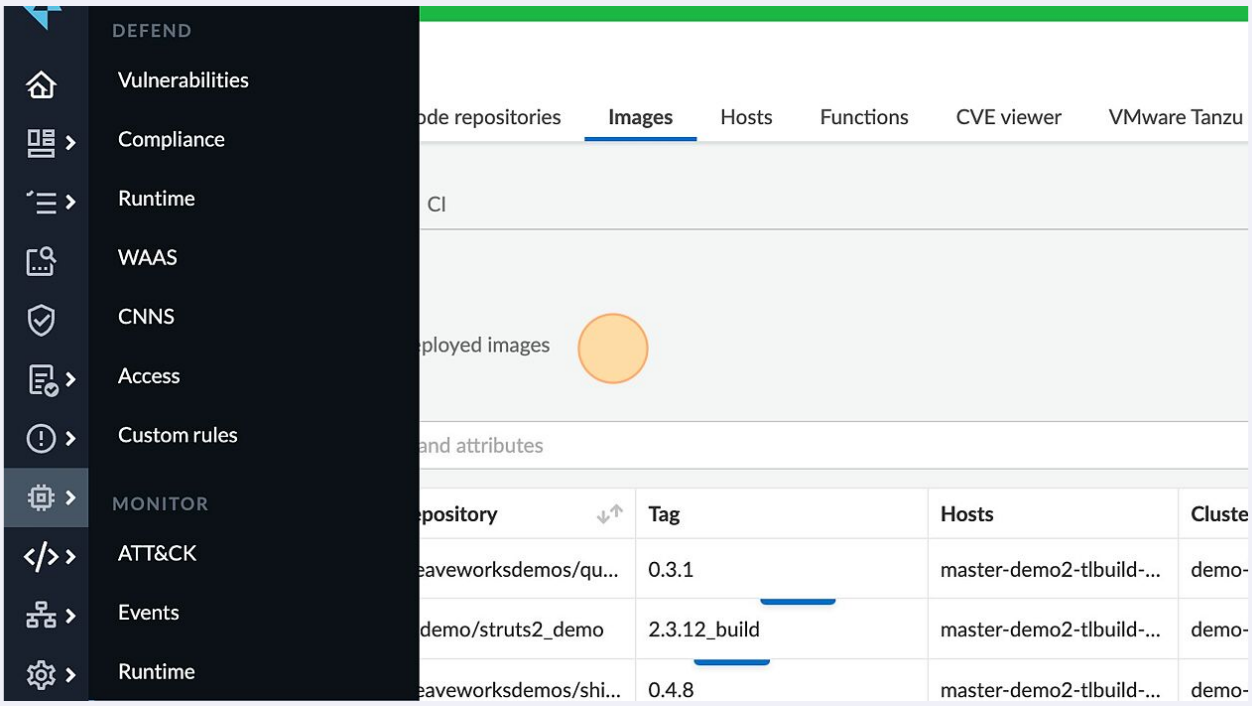
43 Click "Vulnerabilities"



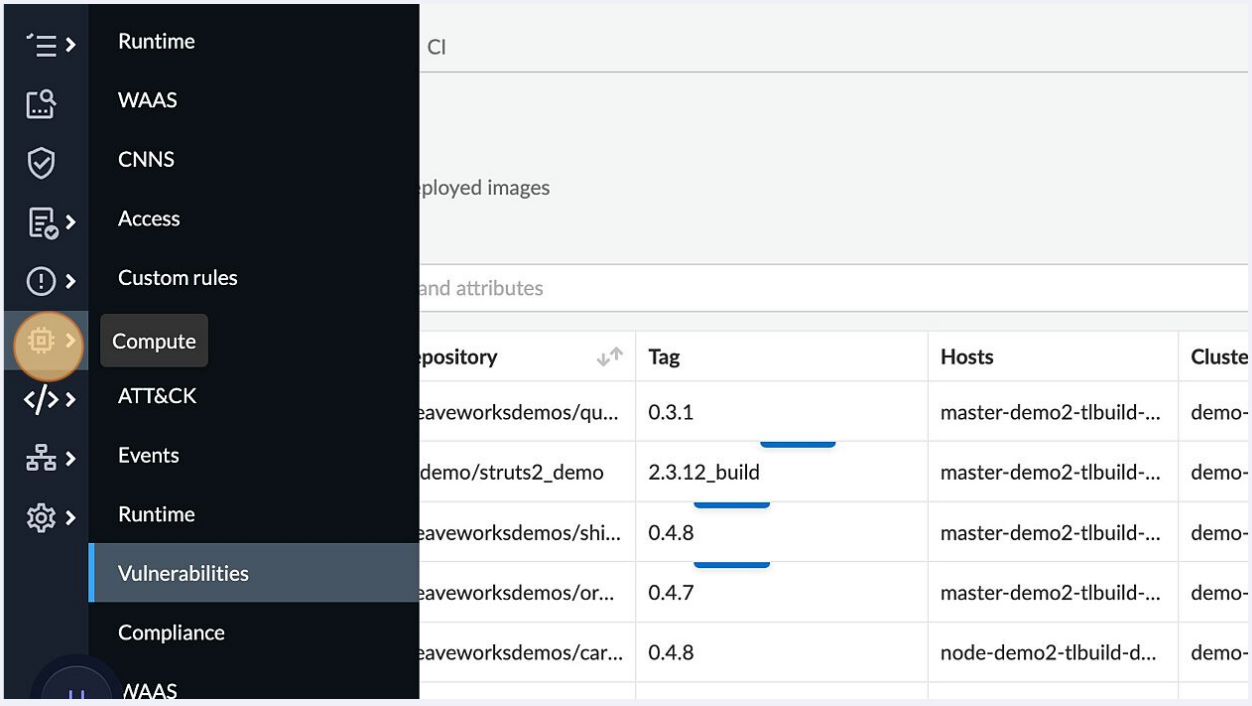
44 Click this link.



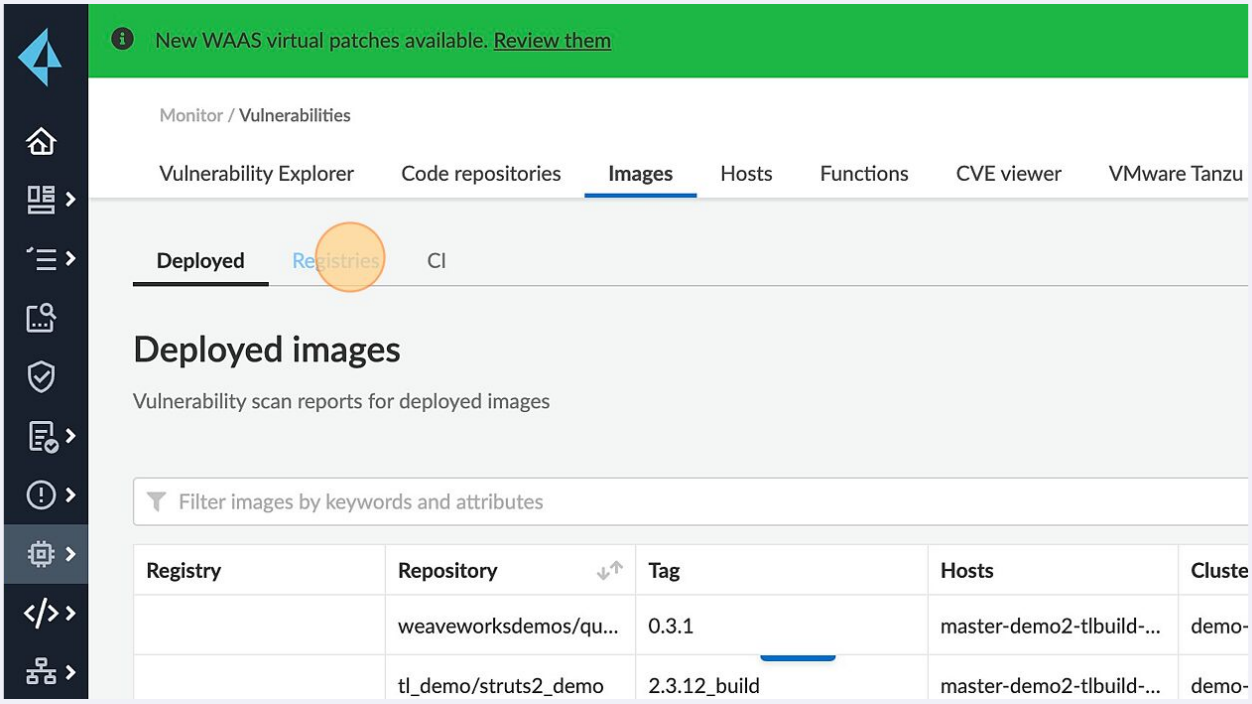
45 Click "Vulnerability scan reports for deployed images"



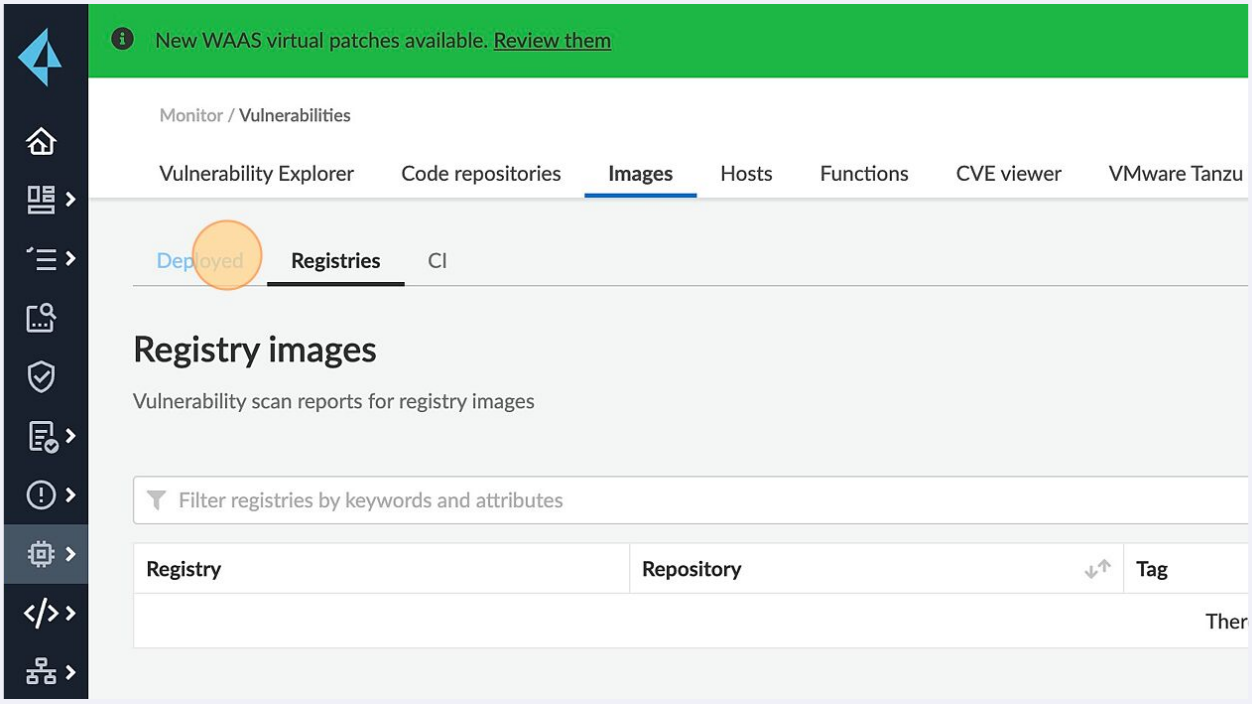
46 Click this image.



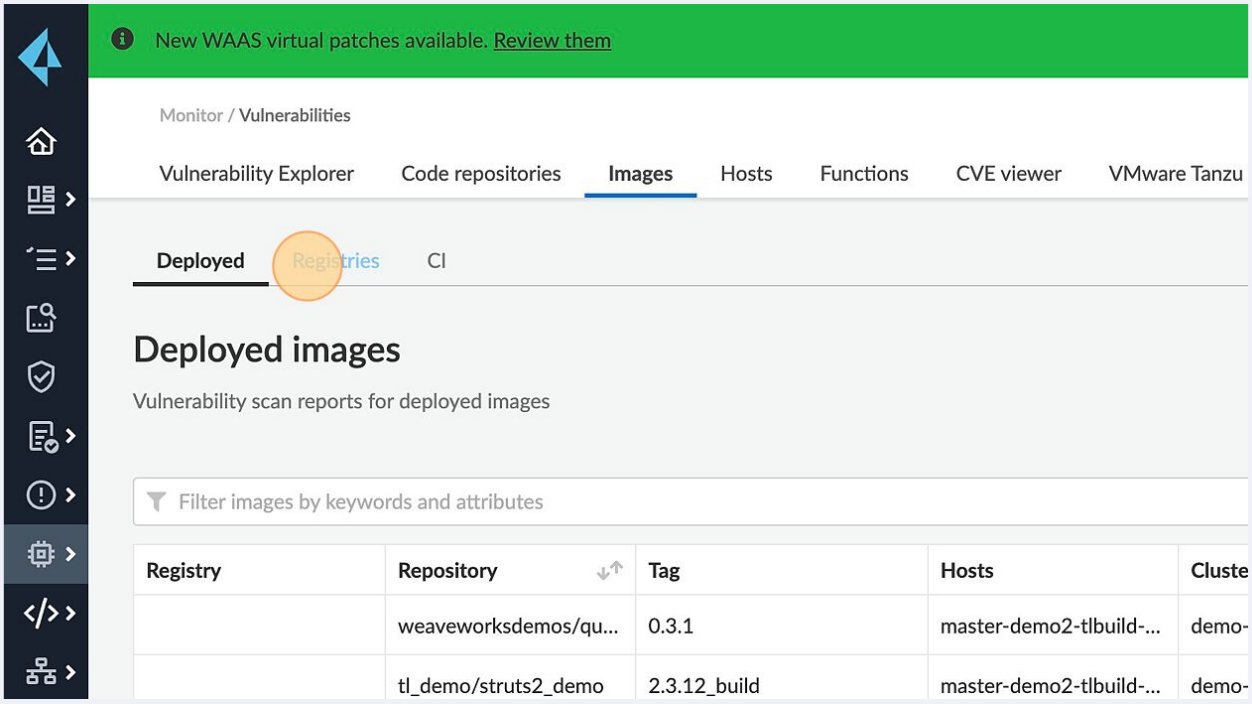
47 Click "Registries"



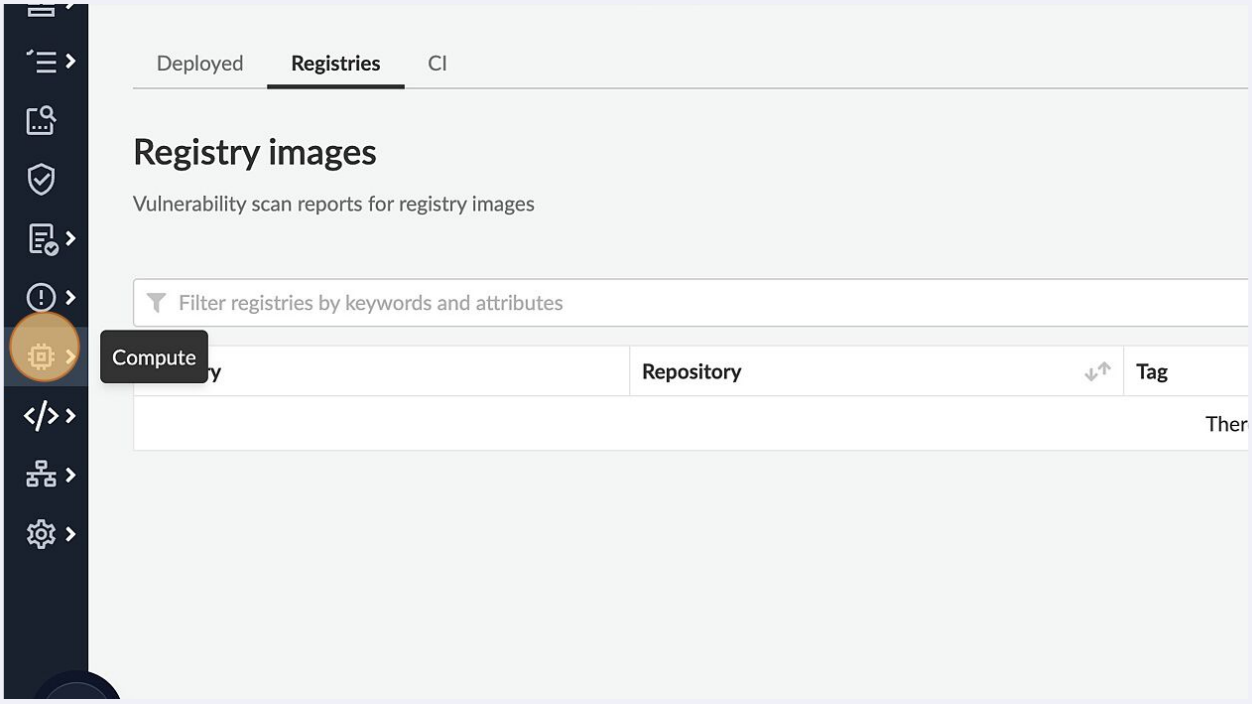
48 Click "Deployed"



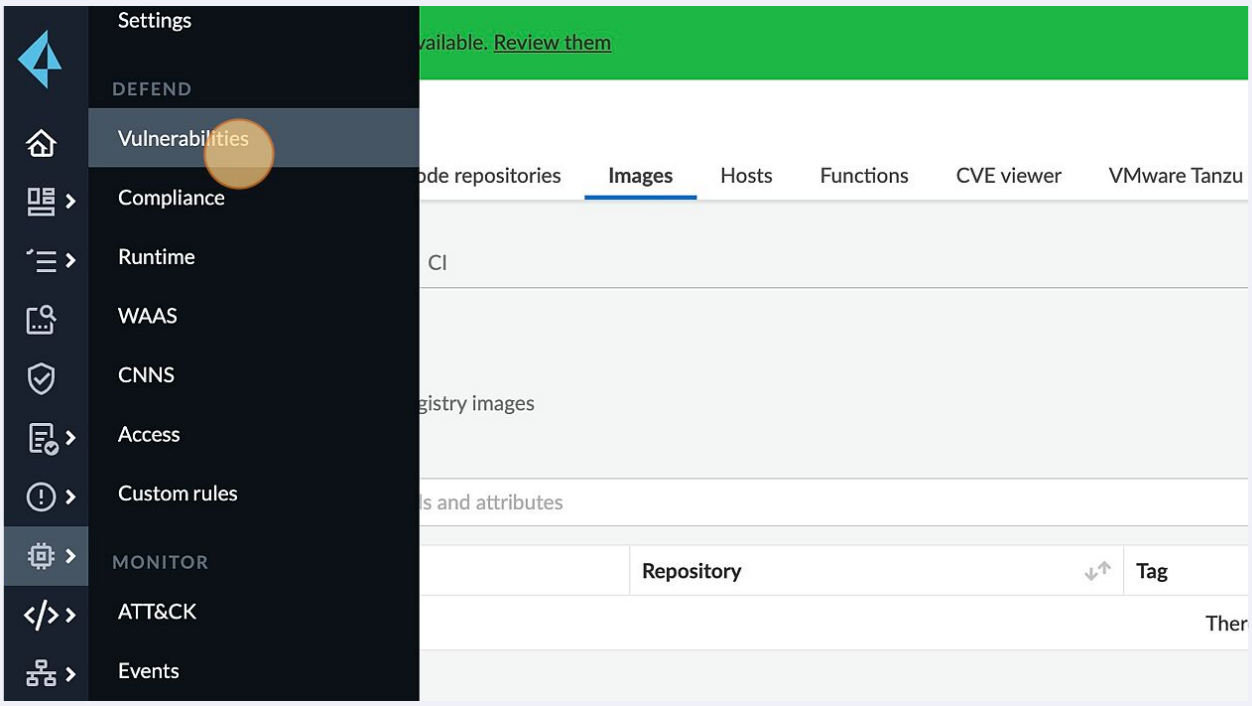
49 Click "Registries"



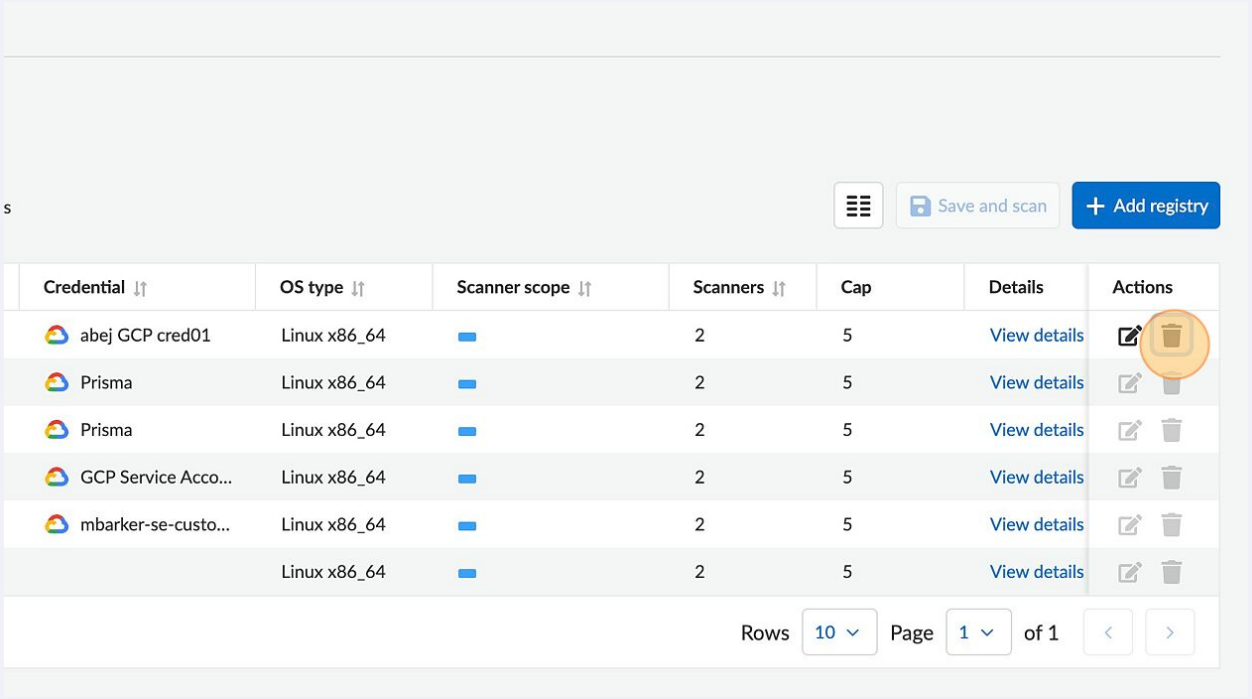
50 Click here.



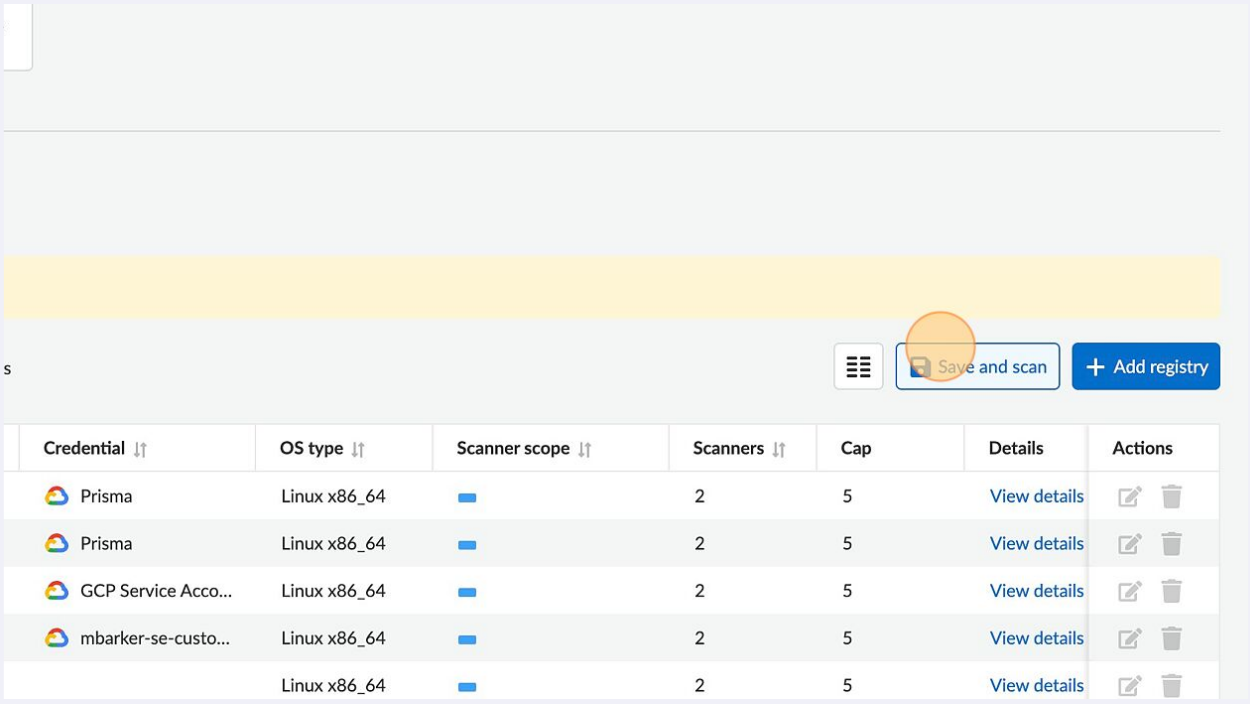
51 Click "Vulnerabilities"



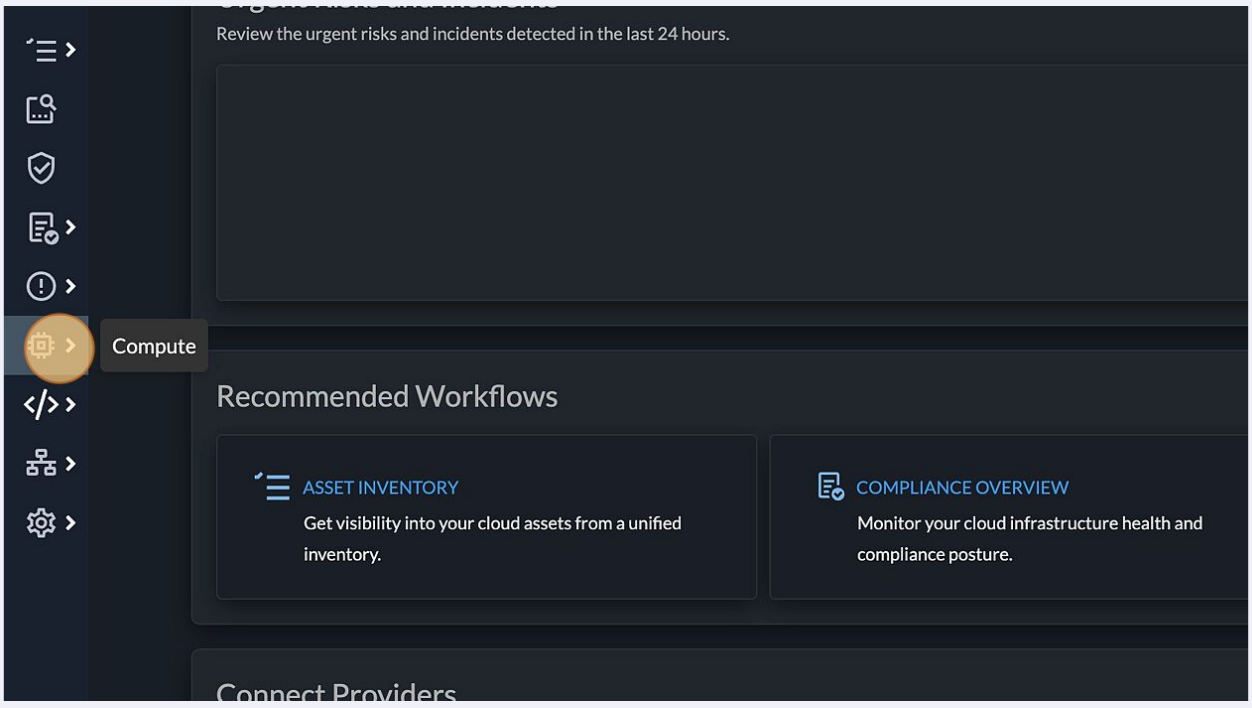
52 Click this button.



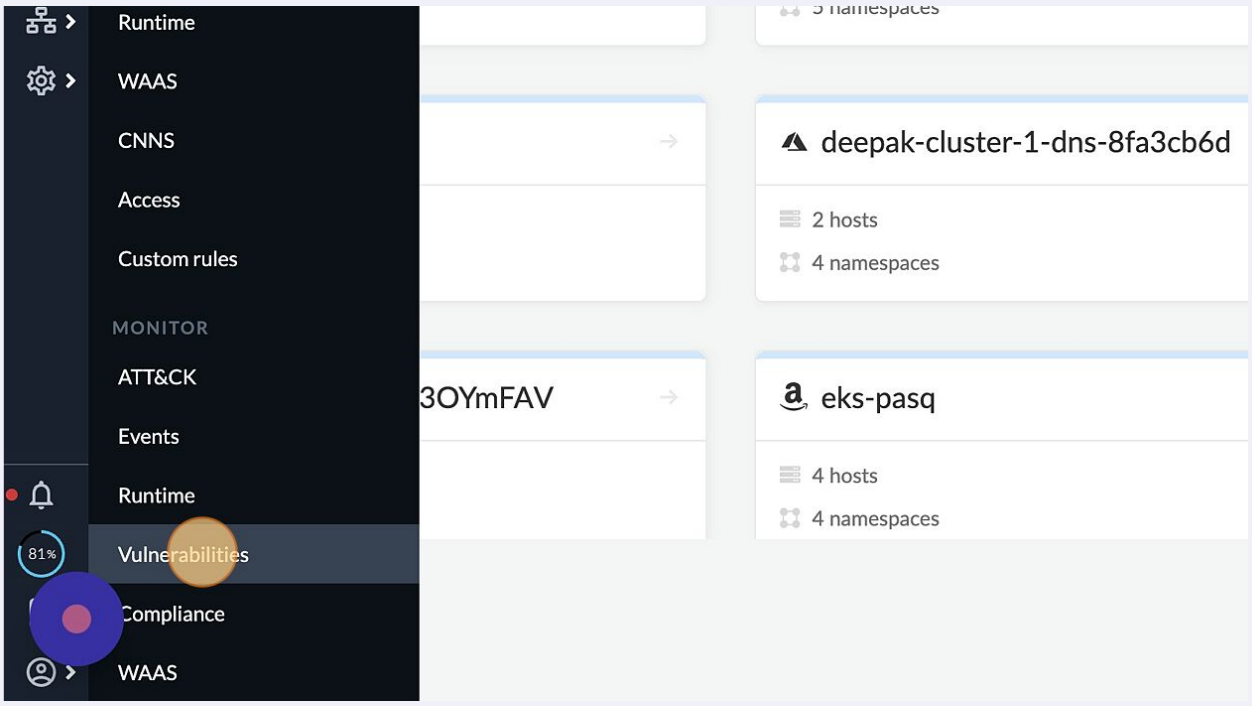
53 Click "Save and scan"



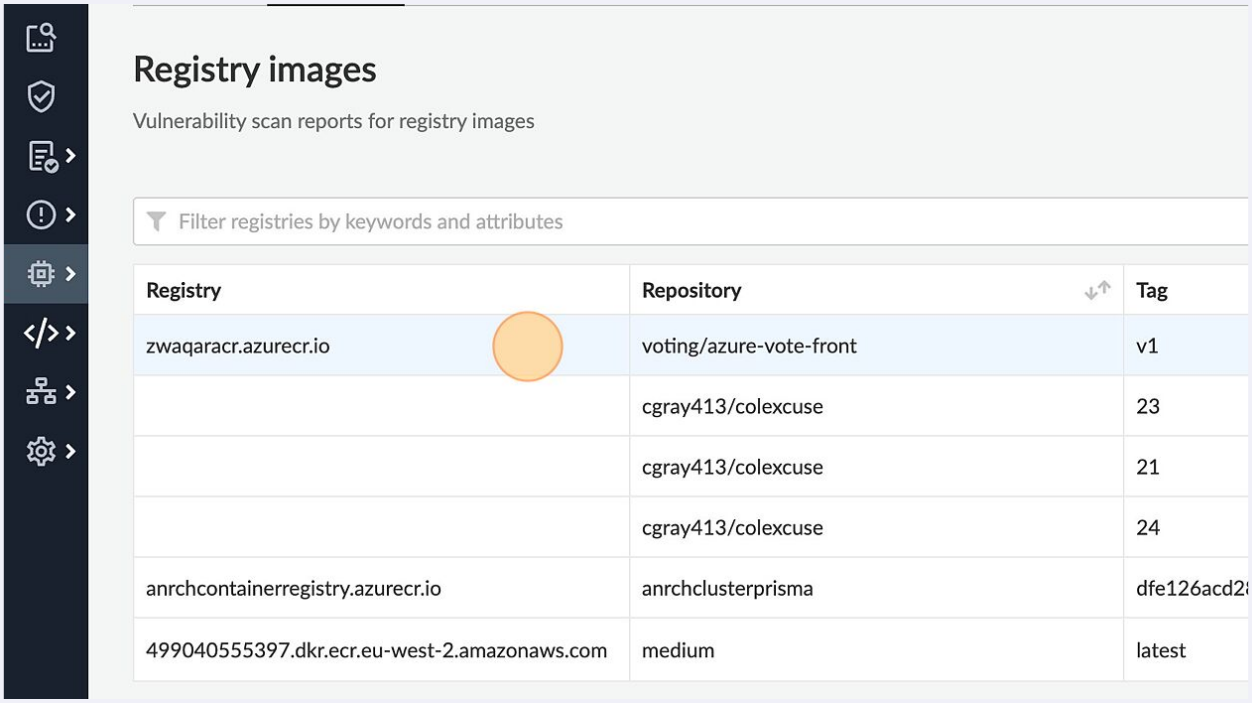
54 Click this icon.



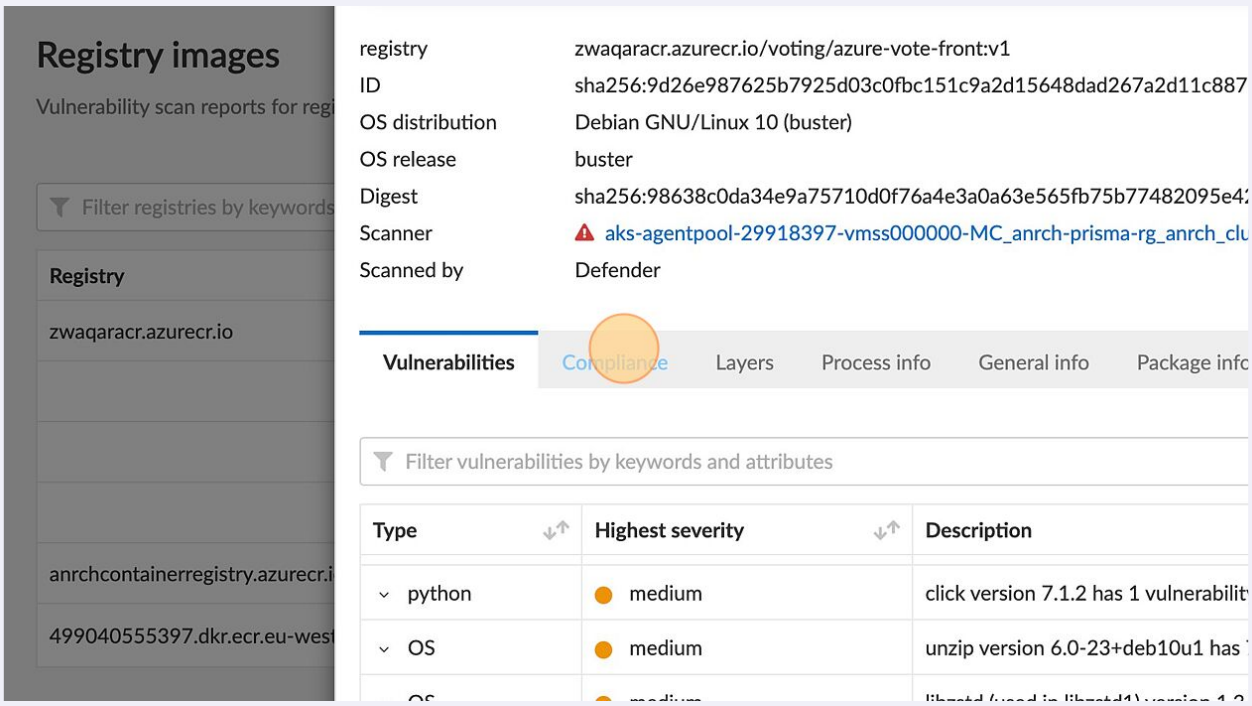
55 Click "Vulnerabilities"



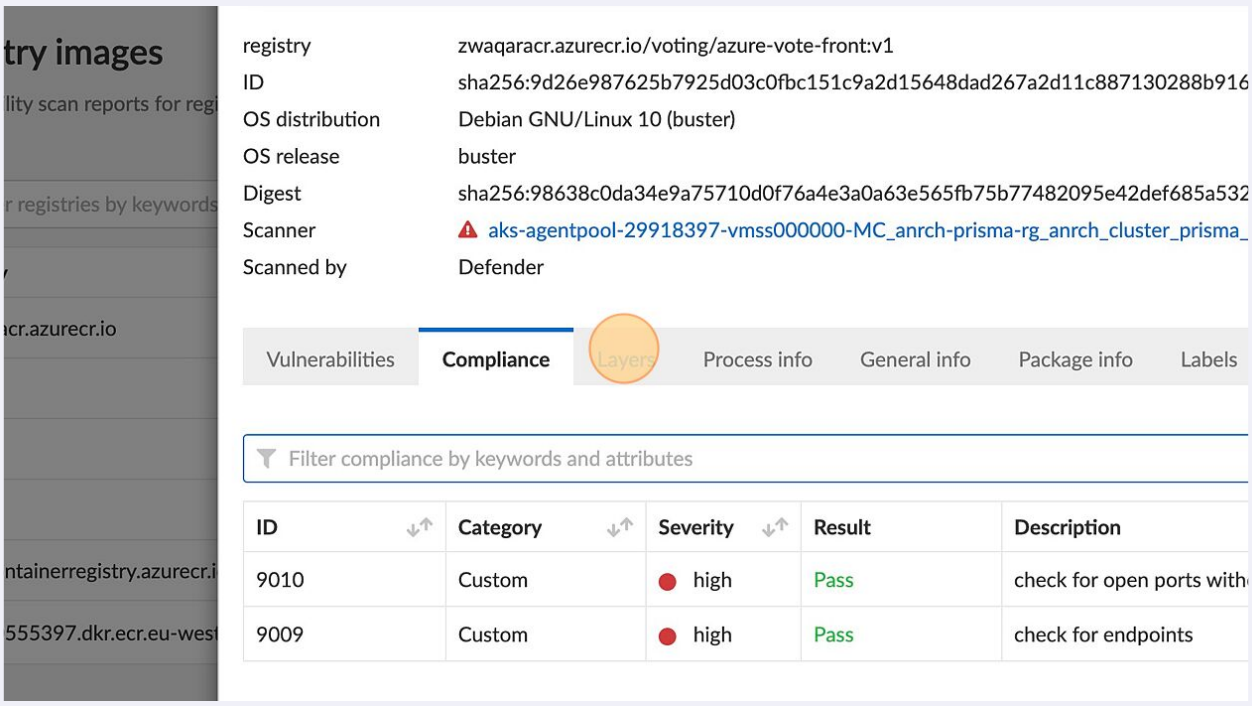
56 Click "zwaqaracr.azurecr.io"



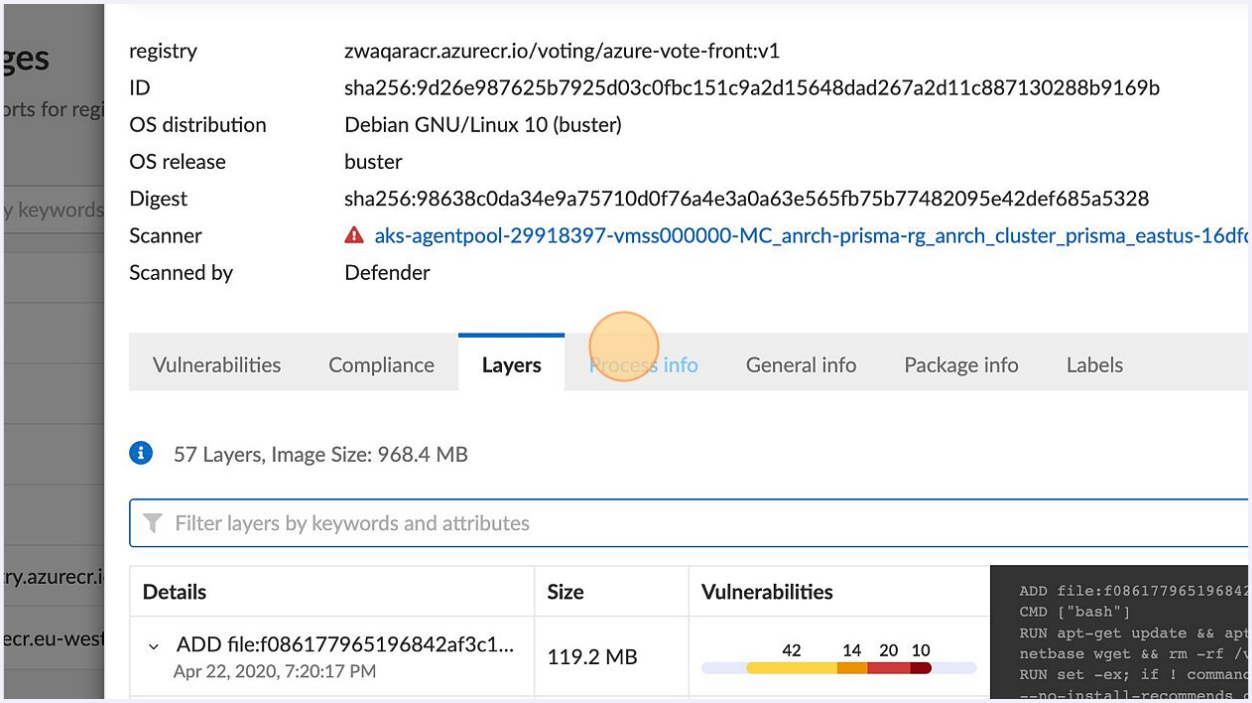
57 Click "Compliance"



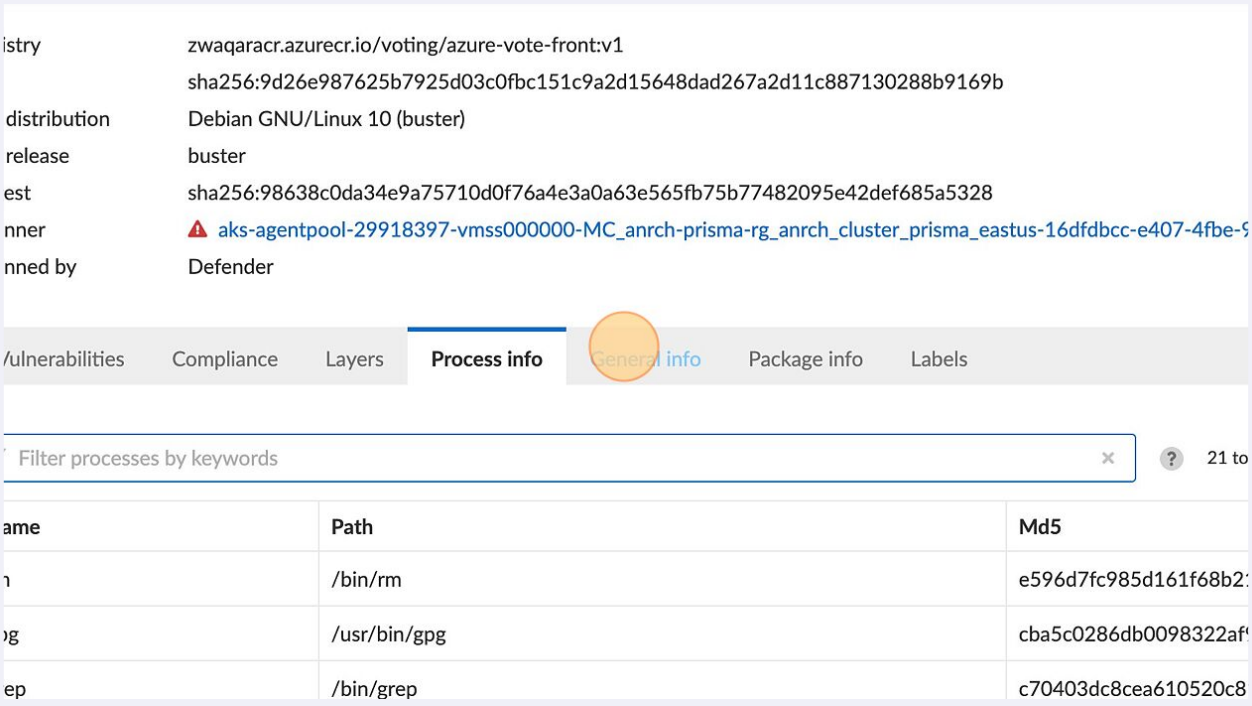
58 Click "Layers"



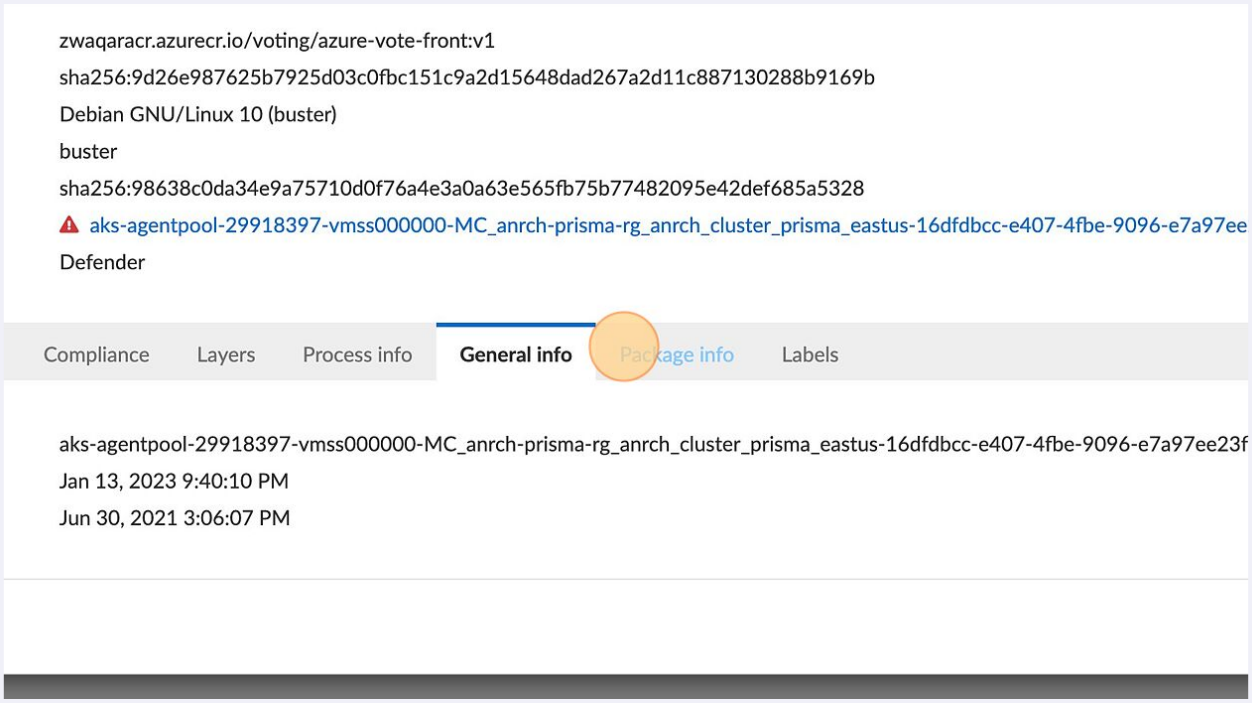
59 Click "Process info"



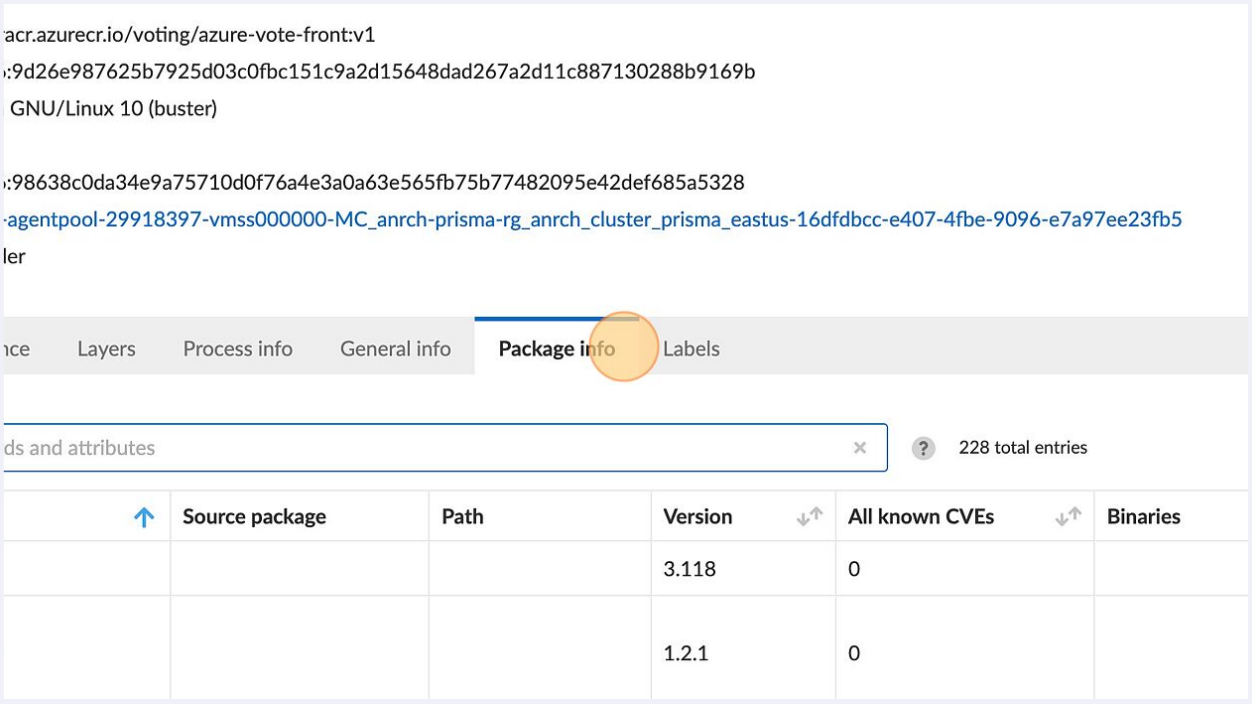
60 Click "General info"



61 Click "Package info"



62 Click "Package info"



63 Click "Defender"