



# Host Security Playbook



# Table of Contents

- Agentless scanning via Nessus for Windows, Linux and Unix
  - Prerequisites
  - Results and Remediation Assistance
- Agent based protection for Linux at RealTime
  - Onboarding VM
  - Behavior Modelling
  - Policies
  - Use Cases
    - Block Package Managers Execution
    - File Integrity Monitoring
    - Prevent Cryptominers Execution

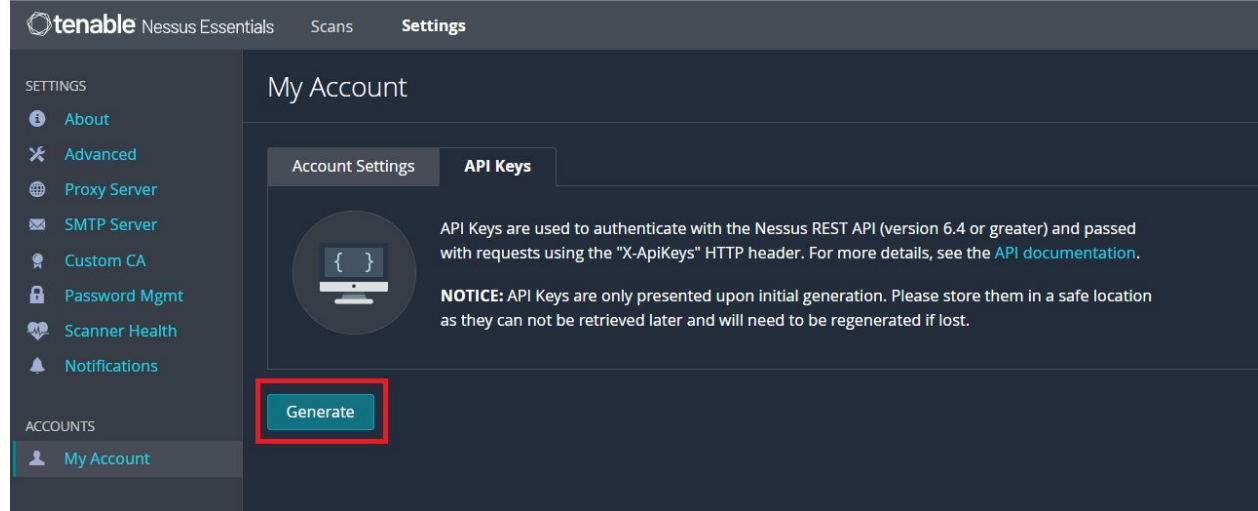
# Nessus Integration Prerequisites

AccuKnox will require the following details to be able to integrate with Nessus and fetch the results:

- **URL of nessus deployment** - The URL that is used to access the Nessus deployment (Eg: `http://nessus.accuknox.com:8834`)
- **Access Key**
- **Secret Key**

The access and secret keys are generated in the Nessus Instance:

- Switch to the **Settings** tab, navigate to **My Account** → **API keys** and click on **Generate**.
- Copy the generated keys.



# Nessus Integration Prerequisites

## ● Folder ID

Fetch the Folder ID from the Nessus Deployment where the scan results are stored:

1. Navigate to the Scans tab and select the folder where the scan results are stored
2. Inspect the page: (ctrl+Shift+J on Windows)

- a. Move to Network tab
- b. Select an entry with the folder\_id variable
- c. Select the Preview tab
- d. Note the id next to the **name** of the folder (In the below screenshot case, the scans are stored in “My Scans” Folder and the id for it is “3”)

The screenshot displays the Nessus Essentials interface. The top navigation bar shows 'Scans' and 'Settings'. The main content area is titled 'My Scans' and contains a table of scan entries:

Name	Schedule	Last Scanned
My Basic Network Scan	On Demand	April 30 at 1:06 PM
Webapp scan test	On Demand	April 30 at 12:59 PM
My Host Discovery Scan	On Demand	April 30 at 12:50 PM

The browser's developer tools are open to the Network tab. The 'Name' column of the network log shows several requests, with the following JSON response highlighted in the preview pane:

```
{
  "folders": [
    {
      "unread_count": 0,
      "custom": 0,
      "default_tag": 0,
      "type": "trash",
      "name": "Trash",
      "id": 2
    },
    {
      "unread_count": 0,
      "custom": 0,
      "default_tag": 0,
      "type": "trash",
      "name": "Trash",
      "id": 2
    },
    {
      "unread_count": 0,
      "custom": 0,
      "default_tag": 1,
      "type": "main",
      "name": "My Scans",
      "id": 3
    }
  ]
}
```

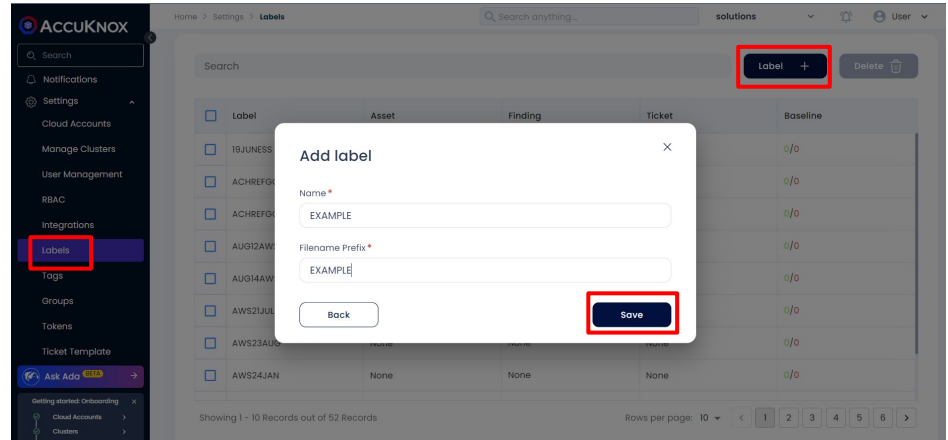
# Nessus Integration

## Method 1: When the Nessus URL is accessible from the AccuKnox SaaS

Forward the gathered prerequisites to AccuKnox team along with the desired scan interval and the integration will be done in the platform from the backend.

## Method 2: When the Nessus URL is not accessible via the AccuKnox SaaS (In case of On Prem Nessus without internet access)

- Create a label from the AccuKnox platform
- CSPM base URL will be:
  - <https://cspm.demo.accuknox.com>  
(In case of demo)
  - <https://cspm.accuknox.com>  
(In case of SaaS subscription)
  - <https://cspm.<your-domain>>  
(In case of On Prem AccuKnox)



# Nessus Integration

- Instead of the AccuKnox platform connecting to Nessus and fetching the results, the results from Nessus can be fetched and forwarded to the AccuKnox platform.
- This will only require outbound connectivity via the Firewall from the Nessus deployment to the AccuKnox SaaS via port 443.
- The data exporter is provided as a docker image [available here](#)
- Replace the \$values in the below command and run on a machine that has docker installed and can reach the nessus deployment.

```
docker run --rm -it \  
-e nessus_url=$nessus_url \  
-e folder_id=$folder_id \  
-e nessus_access_key=$access_key \  
-e nessus_secret_key=$secret_key \  
-e CSPM_BASE_URL=$cspm_url \  
-e label=$label \  
-e internal_tenant_id=$tenant_id \  
-e ARTIFACT_TOKEN=$token \  
accuknox/nessus:v1
```

- After running the command, a message “File Received Successfully” is shown
- After this message is confirmed, wait for a few minutes and the results will be visible on the AccuKnox platform

# Nessus Scan

AccuKnox can integrate with Nessus to provide host scanning capabilities for the Hosts such as Windows, Unix and Linux machines.

To view the results that were aggregated from Nessus, navigate to Issues → Findings and select the Filter as **Host-Endpoint Findings**

The screenshot displays the AccuKnox web interface. On the left is a dark sidebar with a navigation menu. The main content area shows the 'Findings' page, which includes a search bar, a filter dropdown set to 'Host-Endpoint Findings', and a table of scan results. The table has columns for Assetname, Name, Risk factor, Description, and Status. A red box highlights the 'Host-Endpoint Findings' option in the filter dropdown.

	Assetname	Name	Risk factor	Description	Status
	10.0.0.167(agent-name)	Ubuntu 16.04 LTS / 18.04 ...	High	The remote Ubuntu 16.0...	Active
	10.0.0.167(agent-name)	Ubuntu 14.04 LTS / 16.04 ...	Medium	The remote Ubuntu 14.0...	Active
	10.0.0.167(agent-name)	OpenSSL 1.1.0 < 1.1.0j Mult...	Medium	According to its banner,...	Active
<input type="checkbox"/>	10.0.0.167(agent-name)	Ubuntu 20.04 LTS / 22.0...	High	The remote Ubuntu 20.0...	Active
<input type="checkbox"/>	10.0.0.167(agent-name)	Ubuntu 20.04 LTS / 22.0...	Critical	The remote Ubuntu 20.0...	Active
<input type="checkbox"/>	10.0.0.167(agent-name)	Ubuntu 16.04 LTS / 18.04 ...	Medium	The remote Ubuntu 16.0...	Active
<input type="checkbox"/>	10.0.0.167(agent-name)	OpenSSL 1.0.1 < 1.0.1e Info...	Low	According to its banner,...	Active

# Nessus Scan - Thunderbird vulnerability on Linux

Click on the findings to show more information about the vulnerability associated with the Host. There are a set of critical CVEs associated with Thunderbird

The screenshot displays the Accuknox Nessus Scan interface. On the left is a dark sidebar with navigation options: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, and Ask Ada (BETA). The main content area shows a breadcrumb trail: Home > Issues > Findings. Below this is a 'Host-Endpoint Findings' section with a search bar and a table of findings. The table has columns for checkboxes, 'Last seen', and a date. The selected finding is titled 'Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6468-1)' and is marked as 'Critical'. A detailed view of this finding is shown on the right, featuring a 'Description' tab with four bullet points about vulnerabilities in Firefox and Thunderbird, and a 'Details' panel on the right showing asset information, status (Active), ignored status (No), severity (Critical), and tickets (0). A 'Notes' section at the bottom right contains a text input field and a submit button.

Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6468-1)

**Description**    Result    Solution    References    Source Code

- The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6468-1 advisory.
- It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. (CVE-2023-5721)
- An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1. (CVE-2023-5732)
- Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. (CVE-2023-5724)
- A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. (CVE-2023-5725)

**Details**    + Create Ticket

**Asset**  
10.0.0.167(agent-name)

**Asset Type**  
Host\_Scan\_Host

**Status** ✎  
● Active

**Ignored**  
🔌 No

**Severity** ✎  
● Critical

**Tickets**  
0

**Notes** ⓘ  
Add Comments and Press Ctrl + Enter to Submit

Total Records: 298

Accuknox



# Nessus Scan - Result & Solution for Thunderbird vulnerability

Select the **Results** tab for more info regarding the checks done. **Solutions** tab to view the fix for the vulnerability. This shows that Thunderbird needs to be updated.

The screenshot displays the Accuknox interface with a sidebar on the left containing navigation options: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, and Runtime Protection. The main content area shows a list of findings under 'Host-Endpoint Findings' with columns for 'Last seen' and a date '2024-08-07 17:24:51'. Two detailed views of a vulnerability are shown:

- Top View:** Title 'Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6468-1)' with a 'Critical' severity tag. The 'Result' tab is active, showing:
  - Description
  - Result:**
    - Installed package : thunderbird\_1:102.13.0+build1-0ubuntu0.22.04.1
    - Fixed package : thunderbird\_1:115.4.1+build1-0ubuntu0.22.04.1
  - Solution
  - References
  - Source Code
- Details:**
  - Asset: 10.0.0.167(agent-name)
  - Asset Type: Host\_Scan\_Host

- Bottom View:** Same title and severity. The 'Solution' tab is active, showing:
- Description
- Result
- Solution:** Update the affected packages.
- References
- Source Code**
- Details:**
- Asset: 10.0.0.167(agent-name)
- Asset Type: Host\_Scan\_Host
- Status: Active

# Nessus Scan - OpenSSL Vulnerability

An OpenSSL related vulnerability was found that allows an attacker to perform command injection.

The screenshot displays the Nessus Scan interface. On the left is a dark sidebar with navigation options: Dashboard, Inventory, Issues, Findings (selected), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, and Ask Ada (with a 'BETA' badge). Below these are 'Getting started: Onboarding' and links for Cloud Accounts, Clusters, and Registry. The main area shows a table of assets with columns for 'Discovered' and 'Last detected'. A modal window is open for the finding 'OpenSSL 1.1.1 < 1.1.1p Vulnerability', which is marked as 'Critical'. The modal has tabs for Description, Result, Solution, References, and Source Code. The 'Description' tab is active, showing a detailed explanation of the vulnerability and its impact. On the right side of the modal, there are sections for 'Details' (including Asset, Asset Type, Status, Ignored, Severity, and Tickets) and 'Notes'. At the bottom of the modal, there is a search bar for 'Finding in resource' with the value 'Host\_Scan\_Host | 10.21.0.5(PIBSRVNESAP)'. The Accuknox logo is visible in the bottom right corner of the interface.

**OpenSSL 1.1.1 < 1.1.1p Vulnerability** Critical

**Description** | Result | Solution | References | Source Code

**Details** [+ Create Ticket](#)

**Asset**  
10.21.0.5(PIBSRVNESAP)

**Asset Type**  
Host\_Scan\_Host

**Status**   
Active

**Ignored**  
 No

**Severity**   
Critical

**Tickets**  
0

**Notes**   
Add Comments and Press Ctrl + Enter to Submit

**Description**

The version of OpenSSL installed on the remote host is prior to 1.1.1p. It is, therefore, affected by a vulnerability as referenced in the 1.1.1p advisory.

- In addition to the c\_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c\_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c\_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

[Show Less...](#)

Finding in resource

# Nessus Scan - OpenSSL Vulnerability

- The risk of command injection can be eliminated by upgrading the OpenSSL package as the vendor fix is already available..
- A ticket can be created to perform the update and the track progress

**OpenSSL 1.1.1 < 1.1.1p Vulnerability** Critical [🔗](#) ✕

Description **Result** Solution References Source Code **Details** [+ Create Ticket](#)

Path : /snap/core20/2318/usr/bin/openssl  
Reported version : 1.1.1f  
Fixed version : 1.1.1p

**OpenSSL 1.1.1 < 1.1.1p Vulnerability** Critical [🔗](#) ✕

Description Result **Solution** References Source Code **Details** [+ Create Ticket](#)

Upgrade to OpenSSL version 1.1.1p or later.

**Asset**  
10.21.0.5(PIBSRVNESAP)

**Asset Type**  
Host\_Scan\_Host

**Status** [✎](#)  
● Active

# Nessus Scan - Vulnerable Windows Server

The windows server was found to be missing a security update, leading to multiple vulnerabilities

The screenshot displays the AccuKnox interface with a finding titled "KB5032250: Windows Server 2008 R2 Security Update (November 2023)". The finding is marked as "Critical" and "Active". The description states: "The remote Windows host is missing security update 5032250. It is, therefore, affected by multiple vulnerabilities". The vulnerabilities listed are:

- Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36402)
- Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-36397)
- Windows SmartScreen Security Feature Bypass Vulnerability (CVE-2023-36025)

A note mentions that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. The finding is associated with the asset "10.0.0.13(VAGRANT-2008R2)" and is failing since 19/08/2024. The interface also shows a sidebar with navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, and Ask Ada. The main content area shows a table of findings with columns for "Last seen" and "Total Records: 899".

# Nessus Scan - Vulnerable Windows Server

The security update to fix the vulnerabilities can be confirmed and applied.

**KB5032250: Windows Server 2008 R2 Security Update (November 2023)** Critical [🔗](#) ✕

Description   **Result**   Solution   References   Source Code

The remote host is missing one of the following rollup KBs :

- 5032252
- 5032250

- C:\Windows\system32\ntoskrnl.exe has not been patched.  
Remote version : 6.1.7601.18741  
Should be : 6.1.7601.26812

**Details** [+ Create Ticket](#)

**Asset**  
10.0.0.13(VAGRANT-2008R2)

**Asset Type**  
Host\_Scan\_Host

**Status** ✎

---

**KB5032250: Windows Server 2008 R2 Security Update (November 2023)** Critical [🔗](#) ✕

Description   Result   **Solution**   References   Source Code

Apply Security Update 5032250 or Cumulative Update 5032252

**Details** [+ Create Ticket](#)

**Asset**  
10.0.0.13(VAGRANT-2008R2)

**Asset Type**  
Host\_Scan\_Host

**Status** ✎

● Active

# Nessus Scan - RCE Vulnerability in Windows

The windows operating system has a vulnerability that will result in RCE with multiple exploitation methods.

**Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)** Critical

**Description** | Result | Solution | References | Source Code

Two remote code execution vulnerabilities exist in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. There are multiple ways an attacker could exploit the vulnerability, such as convincing a user to open a specially crafted document or viewing it in the Windows Preview pane.

Note that Microsoft does not recommend that IT administrators running Windows 10 implement the workarounds described in ADV200006. Please see the vendor advisory for more information. [Show Less...](#)

Finding for in resource `Host_Scan_Host | 10.0.0.13(VAGRANT-2008R2)`

**Failing since** on 19/08/2024

**Last detected** on 19/08/2024

**Compliance Frameworks**  
Coming Soon...

**Asset Information**

**Details** [+ Create Ticket](#)

**Asset**  
10.0.0.13(VAGRANT-2008R2)

**Asset Type**  
Host\_Scan\_Host

**Status**   
Active

**Ignored**  
 No

**Severity**   
Critical

**Tickets**  
0

**Notes**

Add Comments and Press Ctrl + Enter to Submit

**AccuKnox**

# Nessus Scan - RCE Vulnerability in Windows

The advisory is shown which contains multiple methods for preventing the exploit of this vulnerability. The accepted method can be used as per your model.

## Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006) Critical [🔗](#) ✕

Description   **Result**   Solution   References   Source Code

File checked:  
C:\Windows\System32\atmf.dll: not renamed

Registry value checked:  
Software\Microsoft\Windows NT\CurrentVersion\Windows\DisableATMFD: NULL

**Details** [+ Create Ticket](#)

**Asset**  
10.0.0.13(VAGRANT-2008R2)

**Asset Type**  
Host\_Scan\_Host

## Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006) Critical [🔗](#) ✕

Description   Result   **Solution**   References   Source Code

Microsoft has provided additional details and guidance in the ADV200006 advisory.

**Details** [+ Create Ticket](#)

**Asset**  
10.0.0.13(VAGRANT-2008R2)

**Asset Type**  
Host\_Scan\_Host

# Nessus Scan - Remediation

- Select the findings from the list after grouping/filtering as required and then click on Create Ticket icon.
- In the pop up, select the **Ticket Configuration** and click on **Create Ticket**

The screenshot displays the AccuKnox interface with a 'Create Ticket' modal dialog open. The modal contains the following text and elements:

**Create Ticket**

Please select a ticket configuration. If you do not have a ticket configuration, please go to the [Integrations](#) page.

Ticket Configuration ▾

Close

Create Ticket

The background interface shows a list of findings with the following columns: Description, Status, and a checkbox for selection. The 'Create Ticket' icon in the top right of the findings list is highlighted with a red box.

Description	Status
The remote Ubuntu 16.0...	Active
The remote Ubuntu 14.0...	Active
According to its banner,...	Active
The remote Ubuntu 20.0...	Active
The remote Ubuntu 20.0...	Active
The remote Ubuntu 16.0...	Active
According to its banner,...	Active



# Agent Based VM Security



# VM Onboarding

- Navigate to **Settings** → **Manage Cluster** and click on **Onboard Now**
- Select cluster type as VM, enter Name and Save. Verify prerequisites and install the agents via the commands on screen

Home > Settings > Manage Cluster > Onboard

Search anything...

solutions

Solution

### Cluster Onboarding

- 1 Select cluster type & enter cluster name to create cluster
  - Select Cluster Type: VM
  - Enter Cluster Name: VM-1
- 2 Agents Installation

**Runtime Visibility & Protection**

**Prerequisites:**

- Docker v19.0.3 and Docker Compose v1.27.0+
- Linux Kernel v5.8+ with BPF LSM support
- Make sure RabbitMQ is installed if onboarding in systemd mode. You can find the official instructions to install RabbitMQ [here](#).

**Resource Requirements:**

Docker

- Control Plane Node (Minimum):
  - CPU: 2vCPU
  - Memory: 4 GB
  - Disk: 24 GB
- Worker Node (Minimum):
  - CPU: 2vCPU

Finish

# View onboarded VMs

- Navigate to **Inventory** → **Clusters** and click on the onboarded VM, select **View Nodes**
- In case docker is available, click on **View Workloads** to view the containers

The image is a collage of screenshots from the Accuknox web interface, illustrating the navigation path to view onboarded VMs and their workloads.

- Top Left Screenshot:** Shows the Accuknox sidebar menu with the **Clusters** option highlighted. The breadcrumb path is **Home > Inventory > Clusters**.
- Top Middle Screenshot:** Shows the **Clusters** page with a search bar and a list of clusters. A modal window is open over a cluster, showing options: **+ Add Policies**, **View Workloads**, **View Nodes**, and **View Policies**. Red arrows point from **View Workloads** and **View Nodes** to their respective views in the collage.
- Top Right Screenshot:** Shows the **Workloads** page for a specific VM (VM-1). The breadcrumb path is **Home > Inventory > Clusters > VM-1 > Workloads**. A container named **inspiring\_leakey** is visible within a **container\_namespace**.
- Bottom Left Screenshot:** Shows a sidebar menu with **Clusters** highlighted, and other options like **Issues**, **Compliance**, **Runtime Protection**, **Remediation**, and **Monitors / Alerts**.
- Bottom Right Screenshot:** Shows two nodes: **worker-node01** and **master-node**, each with the Accuknox logo.

# VM Behavior for Containerized Apps

- Navigate to **Runtime Security** → **App Behavior** and select the onboarded VM

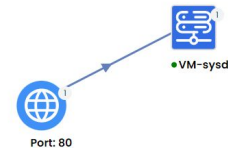
The screenshot displays the AccuKnox 'App Behavior' interface. The left sidebar contains navigation options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, CWP Dashboard, App Behavior (highlighted), Policies, Remediation, Monitors / Alerts, Identity, Reports, and Ask Ada. The main content area shows a table of process activity for the VM 'VM-sysd' in the 'wordpress-mysql' namespace. The table columns include Last Updated Time, Process Accessed, Process, Cluster, Namespace, Workload, Action, and Occurrences. A red box highlights the 'VM-sysd' dropdown and the 'LIST' button. A red arrow points from the text 'Real Time monitoring of file, process and network activity' to the table area.

Last Updated Time	Process Accessed	Process	Cluster	Namespace	Workload	Action	Occu...	Details
07/24/2024 18:41 PM	/bin/sed		VM-sysd	wordpress-mysql	wordpress	Allow	13	Details
07/24/2024 18:41 PM	/bin/sed	/bin/bash	VM-sysd	wordpress-mysql	wordpress	Allow	74	Details
07/24/2024 18:41 PM	/usr/local/bin/php	/bin/bash	VM-sysd	wordpress-mysql	wordpress	Allow	25	Details
07/24/2024 18:41 PM	/usr/bin/shalsum	/bin/bash	VM-sysd	wordpress-mysql	wordpress	Allow	15	Details
07/24/2024 18:41 PM	/usr/bin/cut	/bin/bash	VM-sysd	wordpress-mysql	wordpress	Allow	14	Details

Real Time monitoring of file, process and network activity

Graphical Insights of Network Connections, either to private/public IPs

A partial view of the sidebar showing the 'Remediation', 'Monitors / Alerts', 'Identity', 'Reports', and 'Ask Ada' options.



# VM Hardening

- Navigate to **Runtime Security** → **Policies** and click on **Create Policy**
- Upload policies and click on **Save**. Select **Activate Policies** to save and activate

The image displays two screenshots from the AccuKnox web interface. The top screenshot shows the 'Policies' page with filters for 'VM-1' and 'Workloads'. The 'Create Policy' button is highlighted with a red box. The bottom screenshot shows the 'Create New Policy' form with 'VM-1' selected for the cluster. A 'Confirmation' dialog box is open, asking 'Are you sure you want to save these policies?' with the 'Activate Policies' checkbox checked and highlighted by a red box. The 'Save' button in the background is also highlighted with a red box.

Home > Runtime Security > Policies

Search anything...

solutions

VM-1 x

Namespace

Workloads

Policy Type

Status

Search

Activate

Create Policy +

All (0) Discovered (0) Hardening (0) Custom (0)

Ignore Delete Make Inactive

Home > Runtime Security > Policies > Upload

Search anything...

solutions

Create New Policy

Upload YAML file or create policy through [Policy Editor Tool](#)

Cluster\*

VM-1 x

Uploaded YAML files

1. vm-host.yaml

Remove all

Confirmation

Are you sure you want to save these policies?

Activate Policies

Note : After saving, policies will be saved in an inactive state. Please check the "Activate Policies" option to activate them.

Cancel Save

Cancel Confirm

# Policy alerts for VM

- After a policy violation occurred, navigate to **Monitors/Alerts** → **Alerts**
- Click on any of the alerts to view more information

The screenshot displays the Accuknox Alerts interface. The left sidebar contains navigation options: Home, Monitors Alerts, Alerts, Triggers, Monitors, Identity, Reports, Notifications, and Settings. The main area shows a list of alerts with columns for Timestamps, Message, ClusterName, Action, Severity, Operation, and Pod Name. A red arrow points from the 'Process' operation in the alert list to the 'Raw Logs' section.

**Alerts List:**

Timestamps	Message	ClusterName	Action	Severity	Operation	Pod Name
07-24-24 12:05 IST	you shall not sleep	VM-1	Block	10	Process	
07-24-24 12:04 IST	--	VM-1	Block	--	Syscall	
07-24-24 12:04 IST	--	VM-1	Block	--	Syscall	
07-24-24 12:04 IST	--	VM-1	Block	--	Syscall	

**Alert Details:**

**Informational** July 24, 2024 at 12:05 2 minutes ago

**you shall not sleep**

**ALERT**

Policy Name	Resource	Source	Action	Result	Severity
block-your-sleep	/usr/bin/sleep 1	/usr/bin/bash	Block	Permission denied	10

Operation	Cluster Name	Pod Name	Workload Name	Workload Type
Process	VM-1	--	--	--

**Raw Logs**

```
{
  "Action": "Block"
  "ClusterName": "VM-1"
  "Cwd": "/home/vagrant/"
  "Data": "syscall=SYS_EXECVE"
  "Enforcer": "AppArmor"
  "HostName": "master-node"
  "HostPID": 2936
  "HostPPID": 2927
  "Message": "you shall not sleep"
  "Operation": "Process"
}
```

# VM Security Use Cases



# VM Hardening - Block Execution of package managers

Attackers might try to download additional tools to help with exploiting the environment or downgrade packages to a vulnerable version.

- Replace <vm-hostname> with the target VM's hostname
- Upload and Activate this policy to block the execution of the package managers on the VM

Package managers to be blocked

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorHost
Policymetadata:
  name: block-pkg-mgmt-tools
spec:
  severity: 10
  message: "Alert! Execution of package management process is denied"
  tags:
  - ALERT
  nodeSelector:
    matchLabels:
      kubearmor.io/hostname: <vm-hostname>
  process:
    matchPaths:
      - execname: apt-get
      - execname: apt
      - execname: dnf
      - execname: dpkg
      - execname: gdebi
      - execname: make
      - execname: makepkg
      - execname: pacman
      - execname: rpm
      - execname: yaourt
      - execname: yum
      - execname: zypper
  action:
    Block
  tags:
  - NIST
  - NIST_800-53_CM-7(4)
  - SI-4
  - process
  - NIST_800-53_SI-4
```

The screenshot shows the AccuKnox security console interface. In the foreground, a 'Confirmation' dialog box is open, asking 'Are you sure you want to save these policies?' with a checked 'Activate Policies' option and 'Cancel' and 'Confirm' buttons. The background shows the 'Create New Policy' screen with a 'VM-host' cluster selected and a table of 'Uploaded YAML files' containing '1. harden-pkg-mngt-'. To the right, the 'Policies' page is visible, showing a table with the following data:

Policy Name	Category	Status	Clusters
harden-pkg-mngt-exec (v1)	Custom	Active	VM-host



# VM Hardening - Block Execution of package managers

- Open a new terminal session on the VM
- When a package manager is attempted to be executed, the execution will be blocked and alerts will be visible on the SaaS platform

```
vagrant@master-node:~$ sudo apt update
sudo: unable to execute /usr/bin/apt: Permission denied
vagrant@master-node:~$
```

ACCUKNOX Home > Monitors Alerts > Alerts

Medium August 20, 2024 at 10:19 a few seconds ago

Alert! Execution of package management process inside VM is denied

NIST NIST\_800-53\_CM-7(4) NIST\_800-53\_SI-4 SI-4 process

Policy Name	Resource	Source	Action	Result	Severity
harden-pkg-mngr-...	/usr/bin/apt update	/usr/bin/sudo	Block	Permission denied	5

Operation	Cluster Name	Pod Name	Workload Name	Workload Type
Process	VM-host	--	master-node	Node

Raw Logs

```
{
  "Action": "Block"
  "ClusterName": "VM-host"
  "Cwd": "/home/vagrant/"
  "Data": "syscall=SYS_EXECVE"
  "Enforcer": "AppArmor"
  "HostName": "master-node"
  "HostPID": 3413
  "HostPPID": 3412
  "Message": "Alert! Execution of package management process inside VM is denied"
  "Operation": "Process"
  "Owner": {
    "Name": "master-node"
    "Ref": "Node"
  }
}
```

NOX

# VM Hardening - File Integrity Monitoring

KubeArmor can not only monitor for changes to system binary folders, configuration paths, and credentials paths but also blocks any write attempts

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorHostPolicy
metadata:
  name: hsp-File-Integrity-Monitoring
spec:
  nodeSelector:
    matchLabels:
      kubernetes.io/hostname: vm-name
  severity: 5
  message: Detected and prevented compromise to File integrity
  File:
    matchDirectories:
      - dir: /sbin/
        readOnly: true
        recursive: true
      - dir: /usr/bin/
        readOnly: true
        recursive: true
      - dir: /usr/lib/
        readOnly: true
        recursive: true
      - dir: /usr/sbin/
        readOnly: true
        recursive: true
      - dir: /bin/
        readOnly: true
        recursive: true
      - dir: /boot/
        readOnly: true
        recursive: true
  action: Block
```

- Replace vm-name with the target VM's hostname
- Upload and Activate this policy to block any writes inside the specified directories

Directories with Files to be protected

The screenshot displays the AccuKnox interface. On the left, a 'Create New Policy' dialog is open, showing the upload of a YAML file named 'harden-pkg-mngt-exec'. A 'Confirmation' modal is overlaid on top, asking 'Are you sure you want to save these policies?' with options to 'Activate Policies' and 'Confirm'. On the right, the 'Policies' page is visible, showing a table of policies. The table has columns for Policy Name, Category, Status, and Clusters. One policy is listed: 'harden-pkg-mngt-exec (v1)' with Category 'Custom', Status 'Active', and Clusters 'VM-host'.

Policy Name	Category	Status	Clusters
<input type="checkbox"/> harden-pkg-mngt-exec (v1) KubeArmor Host	Custom Applied a few sec	Active	VM-host

# VM Hardening - File Integrity Monitoring

- Open a new terminal session on the VM
- Try to modify/write to files inside the directories that are specified in the policy
- The write attempt is blocked and an alert is shown on the platform

The image shows a terminal window on the left and an alert notification on the right, both overlaid on the Accuknox web interface.

**Terminal Session:**

```
vagrant@master-node:/$ cd /sbin
vagrant@master-node:/sbin$ sudo touch file
touch: cannot touch 'file': Permission denied
vagrant@master-node:/sbin$
```

**Alert Notification:**

**Critical** August 20, 2024 at 10:32 a few seconds ago

**Detected and prevented compromise to File integrity**

MITRE MITRE\_T1036\_masquerading MITRE\_T1565\_data\_manipulation NIST NIST\_800-53\_AU-2 NIST\_800-53\_SI-4

Policy Name	Resource	Source	Action	Result	Severity
harden-file-integ...	/usr/sbin/file	/usr/bin/touch file	Block	Permission denied	1

**Operation**

Operation	Cluster Name	Pod Name	Workload Name	Workload Type
File	VM-host	--	master-node	Node

**Raw Logs**

```
{
  "Action": "Block"
  "ClusterName": "VM-host"
  "Cwd": "/usr/sbin/"
  "Data": "syscall=SYS_OPENAT fd=-100 flags=O_WRONLY|O_CREAT|O_NOCTTY|O_NONBLOCK"
  "Enforcer": "AppArmor"
  "HostName": "master-node"
  "HostPID": 3555
  "HostPPID": 3554
  "Message": "Detected and prevented compromise to File integrity"
  "Operation": "File"
  "Owner": {
```

# VM Hardening - Prevent cryptominers execution

Deny execution of known cryptominers and prevent execution of binaries from tmp, prevent tampering of sensitive files to protect against Cryptojacking attacks

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorHostPolicy
metadata:
  name: harden-crypto-miners
Spec:
  nodeSelector:
    matchLabels:
      kubearmor.io/hostname: vm-name
  action: Block
  file:
    matchDirectories:
      - dir: /bin/
        readOnly: true
        recursive: true
      - dir: /boot/
        readOnly: true
        recursive: true
      - dir: /sbin/
        readOnly: true
        recursive: true
      - dir: /usr/bin/
        readOnly: true
        recursive: true
      - dir: /usr/local/bin/
        readOnly: true
        recursive: true
      - dir: /var/local/bin/
        readOnly: true
        recursive: true
    message: cryptominer detected and blocked
  process:
    matchDirectories:
      - dir: /tmp/
        recursive: true
    matchPaths:
      - execname: gpk
      - execname: opt
      - execname: dero-sminer-linux-amd64
      - execname: dero-wallet-cli-linux-amd64
      - execname: dero
      - execname: dero-d-linux-amd64
      - execname: masscan
      - execname: nmap
      - execname: ntpdate
      - execname: xmrig
      - execname: zgrab2
  severity: 10
```

- Replace vm-name with the target VM's hostname
- Upload and Activate this policy to protect against cryptojacking

The file directories to be protected against tampering by attacker to mount/hide attack

Prevent execution of binaries from /tmp/ directory to prevent compromise

The binaries to be denied execution

# VM Hardening - Prevent cryptominers execution

- Open a new terminal session on the VM
- Try tampering the files in /bin/ directory or executing a blocked process
- The action is blocked and an alert is shown on the platform

Informational August 20, 2024 at 11:25 16 minutes ago

cryptominer detected and blocked

MITRE MITRE\_T1496\_resource\_hijacking cryptominer

Policy Name	Resource	Source	Action	Result	Severity
harden-crypto-...	/usr/bin/file	/usr/bin/touch file	Block	Permission denied	10

Operation	Cluster Name	Pod Name	Workload Name	Workload Type
File	VM-host	--	master-node	Node

Raw Logs Copy

```
{
  "Action": "Block"
  "ClusterName": "VM-host"
  "Cwd": "/usr/bin/"
  "Data": "syscall=SYS_OPENAT fd=-100 flags=O_WRONLY|O_CREAT|O_NOCTTY|O_NONBLOCK"
  "Enforcer": "AppArmor"
  "HostName": "master-node"
  "HostPID": 4298
  "HostPPID": 4297
  "Message": "cryptominer detected and blocked"
  "Operation": "File"
  "Owner": {
```

Informational August 20, 2024 at 11:36 3 minutes ago

cryptominer detected and blocked

MITRE MITRE\_T1496\_resource\_hijacking cryptominer

Policy Name	Resource	Source	Action	Result	Severity
harden-crypto-...	/usr/bin/file.swp	/usr/bin/vim.basi...	Block	Permission denied	10

Operation	Cluster Name	Pod Name	Workload Name	Workload Type
File	VM-host	--	master-node	Node

Raw Logs Copy

```
{
  "Action": "Block"
  "ClusterName": "VM-host"
  "Cwd": "/usr/bin/"
  "Data": "syscall=SYS_OPENAT fd=-100 flags=O_RDWR|O_CREAT|O_EXCL"
  "Enforcer": "AppArmor"
  "HostName": "master-node"
  "HostPID": 4380
  "HostPPID": 4379
  "Message": "cryptominer detected and blocked"
  "Operation": "File"
  "Owner": {
```