

# **Professional Portfolio**

**Tevin Agtarap**

Cybersecurity & Information Assurance

Splunk Engineer | Cloud Security Specialist | SIEM & Compliance Expert

# **Table of Contents**

1. Resume .....	1
2.Splunk Security Portfolio .....	8
3.AWS Cloud Security & Vulnerability Portfolio .....	46
4. Azure Security Portfolio.....	75

# TEVIN AGTARAP

Mobile: 406.202.8047 | Email: [agtaraptevin@gmail.com](mailto:agtaraptevin@gmail.com) | LinkedIn: <https://www.linkedin.com/in/tevinagtarap/>  
| Clearance: Top Secret/SCI

## PERFORMANCE SUMMARY

---

**Incident Response & SIEM Management** – Develop, customize, and maintain SIEM solutions such as Splunk and ePO (Trellix/McAfee) to support organizational security posture and conduct log analysis, threat detection, and response coordination.

**Compliance & Security knowledge** – Leverage knowledge of frameworks such as NIST, implement and manage security controls that meet compliance requirements. Adept at collaborating within teams or working independently to address dynamic security challenges effectively.

**Vulnerability Assessment & Management** – Conduct vulnerability assessments of DoD information systems and suggest remediation actions for identified vulnerabilities.

- Security Information & Event Management (SIEM) ■ ePO DLP Management ■ Team Leadership
- Cybersecurity & Risk Management ■ Project Management ■ ACAS Configuration
- IT Infrastructure & Operations ■ Cloud Vulnerability & Solutions ■ eMASS Administration
- SOC & Incident Response ■ Regulatory Compliance ■ Stakeholder Engagement

---

**Bachelor of Science, Cybersecurity & Information Assurance 2021**, Western Governors University, Salt Lake City, UT

**Master of Science, Cybersecurity & Information Assurance 2024**, Western Governors University, Salt Lake City, UT

## CERTIFICATIONS

---

**Splunk – Splunk Core Certified Power User, Splunk Enterprise Certified Admin**

**CompTIA - A+, Project+, Network+, Security+, CySA+, Pentest+, CASP+**

**AWS – Certified Cloud Practitioner**

**ISC2 – Certified in Cybersecurity**

**CIW Web Security Associate**

**ITIL**

## PROFESSIONAL EXPERIENCE

---

**Applied Research Laboratories, The University of Texas at Austin (ARL: UT)** – Austin, TX

*Splunk Engineer - 03/2025 - Present (FULL TIME – 40HRS A WEEK)*

- Design and deploy Splunk Enterprise on Linux/Windows across single and distributed environments.
- Install/configure search heads, indexers, UF/HF, deployment server, cluster manager

- Own data onboarding: inputs.conf, props.conf, transforms.conf
- Develop dashboards for ISSOs/ISSMs and business leaders, visualizing system health, alerts, and compliance posture.
- Train users on SPL, onboarding, dashboards, and best practices
- Evaluate and pilot new Splunk features, apps, and TAs; integrate and operationalize when they add value.

**Army Future Command – Austin, TX**

*Information Assurance Engineer III 10/2/2023 – 03/02/2025 (FULL TIME – 40HRS A WEEK)*

- Assist stakeholders in identifying and evaluating technical and operational security risks, threats, weaknesses, and vulnerabilities associated with information systems.
- Monitor DISA STIGs for updates and communicate any changes to stakeholders.
- Conduct research and investigations of cyber events to include those that potentially violate regulatory requirements.
- Assist with ACAS scans on NIPR and SIPR machines. Direct remediation teams to open vulnerabilities that need to be remediated.
- Develop and maintain cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
- Incident response and protection using ePO and Microsoft defender. Physical incident response in identifying asset and securing asset for further investigation and forensics.
- Monitor controls in eMASS to help push assess only and assess and authorize packages through the RMF process.

**BAE SYSTEMS – HILL AFB, UT**

*CYBER ANALYST II (ISSO/ISSM) 03/13/2023 – 9/23/2023 (FULL TIME – 40HRS A WEEK)*

- Serve as cybersecurity technical advisor, consultant, and primary point of contact to the Program Manager, Information System Owner, and other stakeholders
- Assessment and analysis of threats, vulnerabilities, and risk for assigned system(s)
- Ensure continuous monitoring (e.g., weekly, monthly, etc.) in accordance with cognizant security authority requirements are being implemented and met.
- Ensure all DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals

- Work with NIST 800-53 and JSIG to insure DoD Risk Management framework best practices
- Interfacing with information assurance managers, including reviewing documentation, such as systems security plans (SSPs), risk assessment reports, accreditation packages, and Plan of Actions and Milestones (POA&Ms)
- Perform or review Security Impact Assessments for configuration changes and facilitate approval or disapproval of changes with the appropriate stakeholders
- Provide mentoring to other team members

**DEPARTMENT OF DEFENSE, AIR FORCE – HILL AFB, UT (NH-2210-3) INFORMATION SYSTEM SECURITY OFFICER, 08/29/2022 – 03/10/2023 (FULL TIME – 40HRS A WEEK)**

- Support for Special Access Program (SAP) Information Assurance activates
- Review, prepare and update Automated Information System (AIS) authorization packages, perform selfinspections, identify AIS vulnerabilities, and implement countermeasures, prepare reports on the status of security safeguards applied to the computer systems
- Analyze complexities of existing technology, review/revise/develop policy, initiate plans for enhancements, and provide management sufficient technical and cost analysis information, through written documentation and oral briefings
- Work with the ISSM in designing and implementing government regulatory compliance requirements
- Communicate with ISSM and incident response team on any security incidents
- Work with NIST 800-53 and JSIG to insure DoD Risk Management framework best practices
- Coordinate any changes or modifications to hardware, software, or firmware of a system with the ISSM and AO/DAO prior to the change
- Identify cyber security vulnerabilities and assist with the implementation of the countermeasures for them

**D.A. DAVIDSON COMPANIES, IT RISK MANAGEMENT TEAM, REMOTE – HELENA, MT IT SECURITY OPERATIONS SPECIALIST II, 04/12/2021 – 05/27/2022 (FULL TIME – 40HRS A WEEK)**

- Administer the provisioning, de-provisioning, and review of access controls on systems to ensure the principle of least privilege, separation of duties and need to know is being followed in adherence to Davidson policies
- Handling events such as identifying security issues, extensive troubleshooting, and coordinating resolution with various IT groups
- Troubleshoot and resolve hardware/software failures as well as security breaches, threats, and availability issues

- Regularly provide proactive support including security configurations, security policy modification recommendation and diagnostics of remote network security issues
- SME on Vulnerability Management/analysis using enterprise vulnerability scanners. Create, run, analysis and remediate vulnerabilities found on Davidson infrastructure based on critically of vulnerability
- Ensure Davidson is implanting best practice security policies that address business needs while protecting corporate assets
- Whitelisting Host/URL'S in enterprise proxy. Trace I.P addresses using proxy to analyse traffic
- Tools and Programs used: Enterprise proxy, Splunk, Enterprise Vulnerability Scanners, Enterprise SIEM, Ivanti Ticketing system, Project tracking via Jira, Phantom, 0365 – Security and Compliance, SolarWinds, SailPoint, Polarity

**STATE OF MONTANA, DEPARTMENT OF ADMINISTRATION SITSD/NTSB, Helena, MT IT**

**System Administrator, 07/01/2017 – 04/09/2021 (Full Time – 40hrs a week)**

- Implement customer service to non-technical clients, management, and stakeholders
- Manage 10-20 daily support tickets through Service Now, responding to Tier 1, 2, 3 and escalating tickets when necessary
- Partner with State of Montana NOC and SOC to troubleshoot network issues, oversee installation of applications and software for state employees, and ensure proper authentication of state network devices using Active Directory
- Leverage Python, C#, Java, and CLI interface with Cisco and Juniper network devices to assist with programming switches, routers, and scripts
- Configure and install voice software, hardware, and network equipment, using AVAYA Manager for voice configurations and Putty/SSH for media gateways, switches, routers, and audio codes
- Partner with CenturyLink now Lumen to implement, troubleshoot and add or disconnect telecommunication services
- Achieved Governor's and Department of Administration's Awards for Excellence in Performance for implementation of state-wide VoIP infrastructure
- Help update and configure Voice Ops servers to work with Carbon Black
- Implement project management skills when deploying and working with State of Montana stake holders to implement Avaya VoIP phones

**COMPU SOURCE, INC., Bozeman, MT**

**Information Technology Specialist, 05/21/2014 – 04/13/2016 (Full Time – 40hrs a week)**

- Managed team of 2-5 employees, including training and project management
- Ensured industry standards and compliance of cabling layouts by utilizing blueprints, spliced fiber optic cable, installed cameras and security systems, and tested cables using Fluke
- Installed Cisco switches into Panduit data racks and patched in Computers, IP Phones, Printers, and Fax Machines, troubleshooting all devices when necessary for hospital staffing 500+
- Designed rack and row layouts to optimize air circulation and functionality, and built out data centers by leveraging proper equipment to pull in fiber and copper cable and ensured achievement of product warranties and standards

**STATE OF MONTANA**, Helena, MT

**Web Developer**, 07/01/2013 – 05/01/2014 (*Part Time – 30hrs a week*)

- Created, designed, and updated Department of Justice web pages by leveraging Dreamweaver and WordPress CMS to edit HTML/PHP and build and manage site
- Collaborated and effectively communicated with state employees to ensure satisfaction and executed administrative office duties
- Partnered with Lead Web Developer and Department of Justice Security team to ensure safety requirements of website, including multi-factor authentication, Web Application firewalls, proper port usage, and more
- Assisted Lead Web Developer with patching and renewing software and certificates needed for WordPress and server

**PROFESSIONAL ORGANIZATIONS**

---

**(ISC)2 – International Information Systems Security Certification Consortium**, Member **COMMUNITY**

**INVOLVEMENT**

---

**Vapor Detailing**, Owner, Helena Summer Jobs Program Coordinator, & Charity Partner (2016- Present) **AWARDS**

---

**Governor's Award for Excellence in Performance 2018**, State of Montana

**Governor's Award for Excellence in Performance 2020**, State of Montana

**Department of Administration Award for Excellence in Performance 2018**, State of Montana

# Splunk Security Portfolio

Dashboards, SOAR Automation, and Enterprise Deployment

Prepared by Tevin

September 18, 2025

## Executive Summary

Hands-on Splunk engineer focused on practical, auditor-friendly security analytics across SIEM dashboards (AU-2), on-prem Splunk SOAR 6.4.x, and Splunk Enterprise deployments.

## Skills Matrix

Area	Technologies / Skills	Proficiency	Highlights
Splunk Platform	Splunk Enterprise 9.x-10.x; SH/IDX/CM/HF/UF	Expert	Air-gapped builds; role-based access
Splunk SOAR	SOAR 6.4.x; Apps; Assets; Playbooks	Advanced	On-prem deployment; vault usage
SPL & Dashboards	SPL; Dashboard Studio; tokens; drilldowns	Expert	AU-2 views; exec summaries
Security Analytics	NIST 800-53; MITRE ATT&CK	Advanced	Auditor-friendly searches
Data Onboarding	CIM; TAs; props/transforms; WinEventLog; auditd	Advanced	Normalization & hygiene
Automation	Python; PowerShell; Bash	Advanced	Automation scripts & APIs

# SIEM Dashboard Portfolio

## NIST AU-2 Linux and Windows Compliance Monitoring Dashboard's Splunk - Security Information & Event Management (SIEM) Dashboard Portfolio

### Linux

#### NIST AU-2 Authentication Events Details Summary:

This detailed view displays authentication events from the last 3 days, showing login attempts, failures, and sessions across the system. The log captures various security events including successful user sessions (marked as LOGIN/LOGOUT), failed authentication attempts (marked as FAILED), and their associated risk levels (LOW/HIGH). Each entry provides timestamp, host system, username, event type, status, risk assessment, and source information, enabling granular tracking of user authentication activities and potential security incidents for compliance monitoring.

NIST AU-2 Linux Compliance Monitoring ▾

Comprehensive compliance monitoring for all AU-2 requirements

Global Time Range

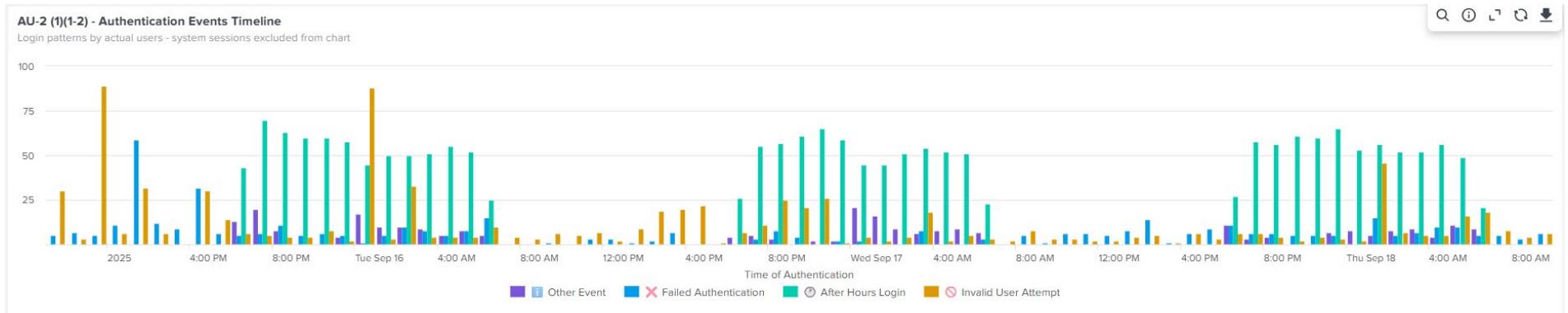
Last 3 days

AU-2 (1)(1-2) - Authentication Events Details

All login attempts, failures, and sessions - system sessions marked

Time	host	User	EventType	Status	Risk	Source
2025-09-18 09:46:53	sgl-lap019	jsong	User Session Started	LOGIN	LOW	/var/log/auth.log
2025-09-18 09:46:37	khanson-idd	khanon	User Session Started	LOGIN	LOW	/var/log/secure
2025-09-18 09:46:08	gsdb3	jyudichakj	Failed Authentication	FAILED	HIGH	/var/log/auth.log
2025-09-18 09:44:35	mistestapp	choej	User Session Ended	LOGOUT	LOW	/var/log/secure
2025-09-18 09:43:14	sgl-lap107	jsong	User Session Ended	LOGOUT	LOW	/var/log/auth.log
2025-09-18 09:43:05	gsdb3	jyudichakj	Failed Authentication	FAILED	HIGH	/var/log/auth.log
2025-09-18 09:41:37	sgl-lap107	jsong	User Session Ended	LOGOUT	LOW	/var/log/auth.log
2025-09-18 09:38:15	gsdb3	jyudichakj	Failed Authentication	FAILED	HIGH	/var/log/auth.log
2025-09-18 09:37:50	gsdb3	anandha	Failed Authentication	FAILED	HIGH	/var/log/auth.log

< Prev 1 2 3 4 5 ... Next >



## AU-2 Privileged Rights Usage Details Summary:

This report tracks sudo, su, and elevated privilege usage across systems. The detailed log shows privileged actions including root role changes, authentication attempts, audit commands, and sudo command executions on various hosts. Each entry displays timestamp, host, action type, command executed, result (SUCCESS/FAILED), and risk level (HIGH for root access/failed auth, LOW for normal operations). The timeline graph below visualizes the trend of privileged command usage over time, categorizing events by type (sudo commands, scripts, authentication, etc.) to identify patterns and potential security concerns.

**AU-2 (6)(1-2), (7-13) - Use of Privileged Rights Details**

All sudo, su, and elevated privilege usage

Time	host	Action	Command	Result	Risk
2025-09-18 09:51:08	sgl-git	Root Role Change	/usr/sbin/sshd	✓ SUCCESS	HIGH - Root Access
2025-09-18 09:51:08	sgl-git	Authentication	/usr/sbin/sshd	✓ SUCCESS	HIGH - Root Access
2025-09-18 09:51:07	bhopkins-pc2	Audit Command	-	✓ SUCCESS	LOW - Normal
2025-09-18 09:51:07	bhopkins-pc2	Sudo Command	-	Unknown	HIGH - Root Access
2025-09-18 09:51:07	bhopkins-pc2	Audit Command	/usr/local/ncpa/plugins/check_luks	✓ SUCCESS	LOW - Normal
2025-09-18 09:51:07	esl-git	Root Login	/usr/sbin/sshd	X FAILED	HIGH - Failed Auth
2025-09-18 09:51:07	twtcn51	Root Login	/usr/sbin/sshd	X FAILED	HIGH - Failed Auth

◀ Prev 1 2 3 4 5 ... Next ▶

**AU-2 (6)(1-2), (7-13) - Privileged Rights Timeline**

Trend of privileged command usage

Time of Privileged Event

Legend:

- bash
- /etc/arl\_compliance/report.sh
- Script/Binary
- Sudo Command
- date
- ls
- nvidia-detect
- su
- su command
- sudo authentication
- OTHER

## AU-2 User and Group Management Events Summary:

This report monitors user account and group management activities across the system. The log shows user modification events tracking changes to administrative accounts with risk levels ranging from MEDIUM to HIGH. All entries indicate "Admin access modified" in the details, suggesting privilege-level changes. The timeline graph below visualizes the frequency and distribution of user management activities (User Modified, User Deleted, Group Created, User Created, Password Changed) over time, helping identify patterns in account administration and potential unauthorized changes to user privileges.

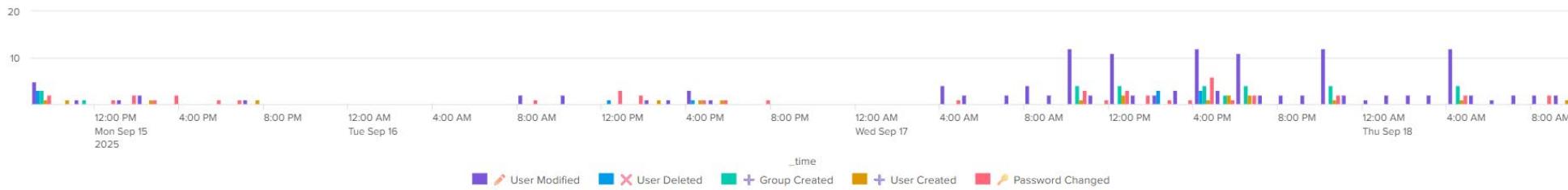
AU-2 (5)(1-2) - User and Group Management Events

Time	host	Action	Target	Risk	Details
2025-09-18 09:05:51	titan2	>User Modified	admmike	HIGH	Admin access modified
2025-09-18 09:05:51	titan2	>User Modified	desimone	MEDIUM	
2025-09-18 08:05:52	titan2	>User Modified	admmike	HIGH	Admin access modified
2025-09-18 08:05:52	titan2	>User Modified	desimone	MEDIUM	
2025-09-18 07:05:53	titan2	>User Modified	admmike	HIGH	Admin access modified

< Prev 1 2 3 Next >

AU-2 (5)(1-2) - User Management Timeline

User/Group Creation, Modification, and Deletion Events\*



## AU-2 Security Relevant File and Object Activity Summary:

This report monitors access to critical system files, with all access shown having system flag enabled. The log tracks activities including audit log monitoring events for log collection systems and file activity monitoring for other system files. All recorded actions are performed by root user, with most events marked as automated system processes. Risk levels are classified as LOW for both log collection and other file activities. The timeline graph below visualizes file access patterns and actions performed (accessed, deleted, security events, cron jobs, etc.) to identify potential unauthorized access or unusual file system behavior across the monitoring period.

### AU-2 (2)(1-6), (3-4) - Security Relevant File and Object Activity

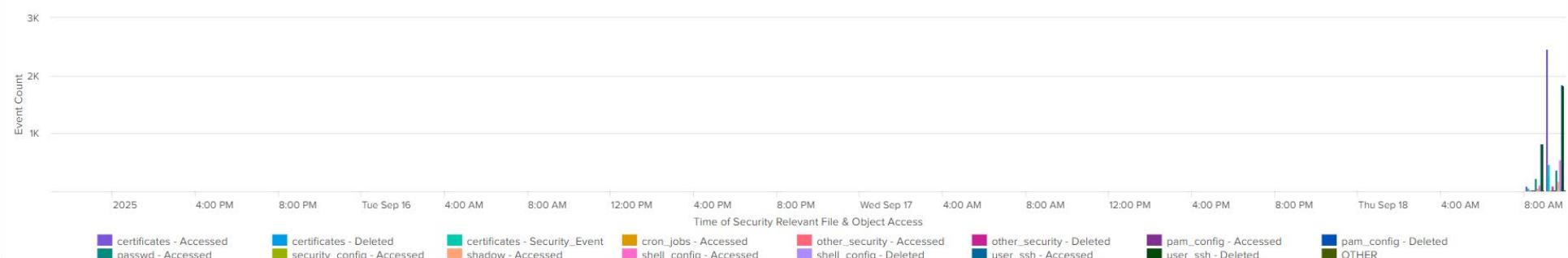
Monitor access to critical system files - all access shown with system flag

Time	Host	File Name	Full Path	What Happened	Risk Level	User	System/Automated
2025-09-18 09:51:30	ndlbwrk4	audit.log	/var/log/audit/audit.log	<span>🔍 Audit Log Monitoring (mode: 100600)</span>	<span>LOW - Log Collection System</span>	root	Yes
2025-09-18 09:51:30	ndlrbkrb1	audit.log	/var/log/audit/audit.log	<span>🔍 Audit Log Monitoring (mode: 100600)</span>	<span>LOW - Log Collection System</span>	root	Yes
2025-09-18 09:51:30	sgl-lap002	wtmp	/var/log/wtmp	<span>💻 File Activity (mode: 100664)</span>	<span>LOW - Other File</span>	root	No
2025-09-18 09:51:30	ndlbkik1	audit.log	/var/log/audit/audit.log	<span>🔍 Audit Log Monitoring (mode: 100600)</span>	<span>LOW - Log Collection System</span>	root	Yes

< Prev 1 2 3 4 5 ... Next >

### AU-2 (2)(1-6), (3-4) - File Activity Timeline

Shows which files were accessed and what actions were performed



## Print Logs Summary:

This report tracks print job activities across network printers. The log shows successfully completed print jobs from various hosts, with all events marked as PRINTED status and MEDIUM risk level. Print jobs are distributed across different printers in the organization, with file sizes ranging from small documents (34.3 KB) to larger files (4935.4 KB). The total pages printed vary from single pages to multi-page documents (up to 16 pages). All print activities are monitored to ensure compliance with document handling policies and to detect potential data exfiltration attempts through physical printing.

Print Logs								
Time	Host	EventType	Status	Risk	Printer	TotalPages	Size_KB	
2025-09-18 09:55:51	bpre034	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_BW_Mailroom	16	4935.4	
2025-09-18 09:08:15	pre039	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_Color_Penrod3rd	1	34.3	
2025-09-18 08:43:45	bpre037	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_Color_T500	1	83.3	
2025-09-18 08:43:24	bpre037	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_Color_T500	4	433.5	
2025-09-18 08:27:30	pre055	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_BW_Mailroom	1	63.1	
2025-09-18 08:23:23	bpre037	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_BW_Mailroom	1	83.1	
2025-09-18 08:23:14	bpre037	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_BW_Mailroom	4	433.3	
2025-09-18 08:16:36	bpre037	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_Color_Mailroom	4	433.2	
2025-09-18 08:16:26	pre055	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_BW_Mailroom	1	93.0	
2025-09-18 08:16:25	bpre037	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_Color_Mailroom	1	83.2	
2025-09-18 08:14:43	pre055	🖨️ Print Job	✅ PRINTED	🟡 MEDIUM	SGL_BW_Mailroom	3	288.4	

## USB Logs Summary:

This report monitors USB device connections and disconnections across the network. The log tracks both standard USB devices and USB storage devices, with events showing CONNECTED and DISCONNECTED statuses. Most USB activities are classified as MEDIUM risk, with USB storage disconnection events marked as HIGH risk due to potential data exfiltration concerns. Multiple disconnection events from the same host suggest repeated USB device removal or potential security policy violations. The monitoring helps detect unauthorized USB usage and potential data transfer attempts through removable media.

USB Logs				
Time	Host	EventType	Status	Risk
2025-09-15 23:44:02	bpre015	🔌 USB USB	✅ CONNECTED	🟡 MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	🔌 USB USB	✗ DISCONNECTED	🟡 MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	🔌 USB USB	✗ DISCONNECTED	🟡 MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	🔌 USB USB	✗ DISCONNECTED	🟡 MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	🔌 USB USB	✗ DISCONNECTED	🟡 MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	🔌 USB USB	✗ DISCONNECTED	🟡 MEDIUM
2025-09-15 21:02:02	swrx242	🔌 USB USB	✅ CONNECTED	🟡 MEDIUM
2025-09-15 21:01:18	fid-commandpost	💾 USB Storage	✗ DISCONNECTED	🔴 HIGH
2025-09-15 20:49:25	sgl-lap-zc02	🔌 USB USB	✅ CONNECTED	🟡 MEDIUM

## USB/CD/Burn Activity Summary:

This report monitors removable media and optical disc activities across the network. The log tracks multiple event types including unknown audio devices (USB headsets), CD/DVD burning operations, and CD/DVD device detections. All events are system-initiated with varied risk levels - HIGH risk for unknown audio devices and active CD/DVD burning operations (potential data exfiltration), and MEDIUM risk for standard CD/DVD device detection. Notable activities include mounted CD/DVD burning sessions with specific file references and multiple audio device connections via USB. The monitoring helps identify unauthorized media usage and potential data transfer attempts through optical media or unauthorized peripheral connections.

**USB/CD/Burn Activity**

Time	Host	User	EventType	Status	Risk	DeviceDetails
2025-09-17 13:59:37	sgl-lap053	[System]	🎤 AUDIO DEVICE	⚠️ DETECTED	🔴 HIGH - UNKNOWN AUDIO	🎧 Audio Device ()
2025-09-17 13:59:37	sgl-lap053	[System]	🎤 AUDIO DEVICE	⚠️ DETECTED	🔴 HIGH - UNKNOWN AUDIO	🎧 Audio Device (Logi USB Headset)
2025-09-17 11:02:56	pre038	[System]	🔥 CD/DVD BURNING	⚠️ DETECTED	🔴 HIGH - CD/DVD BURNING	brasero
2025-09-17 11:02:56	pre038	[System]	🔥 CD/DVD BURNING	⚠️ DETECTED	🔴 HIGH - CD/DVD BURNING	brasero
2025-09-17 11:02:52	pre038	[System]	🔥 CD/DVD BURNING	⚠️ DETECTED	🔴 HIGH - CD/DVD BURNING	brasero
2025-09-17 10:30:43	pre024	[System]	🎤 AUDIO DEVICE	⚠️ DETECTED	🔴 HIGH - UNKNOWN AUDIO	🎧 Audio Device ()
2025-09-17 10:30:43	pre024	[System]	🎤 AUDIO DEVICE	✅ CONNECTED	🔴 HIGH - UNKNOWN AUDIO	🎧 Audio Device ()
2025-09-17 10:30:43	pre024	[System]	🎤 AUDIO DEVICE	⚠️ DETECTED	🔴 HIGH - UNKNOWN AUDIO	🎧 Audio Device (Logitech USB Headset)
2025-09-17 09:53:46	filo-pc	filo	🔥 CD/DVD BURNING	✅ MOUNTED	🔴 HIGH - CD/DVD BURNING	👤 User: filo, Disc: K3b (UID: 14015)
2025-09-17 08:30:28	filo-pc	[System]	💿 CD/DVD DEVICE	⚠️ DETECTED	🟡 MEDIUM - CD/DVD ACTIVITY	💿 CD/DVD Activity
2025-09-17 07:40:06	pre038	[System]	🔥 CD/DVD BURNING	⚠️ DETECTED	🔴 HIGH - CD/DVD BURNING	brasero

## Windows

### NIST AU-2 Windows Compliance Monitoring ▾

Comprehensive NIST AU-2 compliance monitoring

Display ▾ Actions ▾ Edit

Global Time Range

Last 3 days ▾

#### AU-2 (1)(1-2) - Authentication Events Details

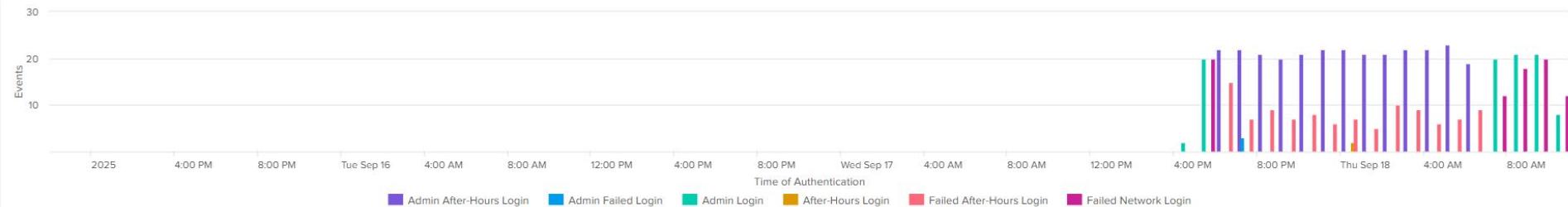
All login attempts by users

Time	computer	User	Source	EventType	Status	Risk
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	ahazarian	local	User Logoff	LOGOUT	LOW
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	-rzoch	10.14.106.94	Local Network Login	LOGIN	LOW-MEDIUM
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	rzoch	ARLUT	Admin Privileges Assigned	LOGIN	MEDIUM
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	bishop	local	User Logoff	LOGOUT	LOW
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	-alvarez	10.14.105.53	Local Network Login	LOGIN	LOW-MEDIUM
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	dew2254	local	User Logoff	LOGOUT	LOW
2025-09-18 10:23:12	atlprint.arlut.utexas.edu	logan	local	User Logoff	LOGOUT	LOW

< Prev 1 2 3 4 5 ... Next >

#### AU-2 (1)(1-2) - Authentication Events Timeline

Login patterns by users



## AU-2 (6)(1-2), (7-13) - Use of Privileged Rights Details

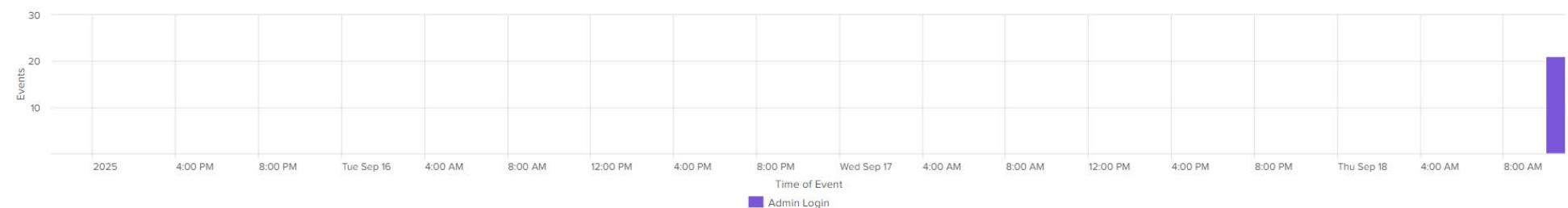
User privileged actions

Time	computer	Action	User	What Happened	Risk
2025-09-18 10:20:31	gtorres-wl.arlut.utexas.edu	👑 Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:20:23	prod-wd.arlut.utexas.edu	👑 Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:20:06	mcleod-wl2.arlut.utexas.edu	👑 Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:19:59	gtorres-wl.arlut.utexas.edu	👑 Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:19:57	SPTEST.arlut.utexas.edu	🔑 Admin Login	- ectectedadmin	Admin account logged in	HIGH

< Prev 1 2 3 4 5 Next >

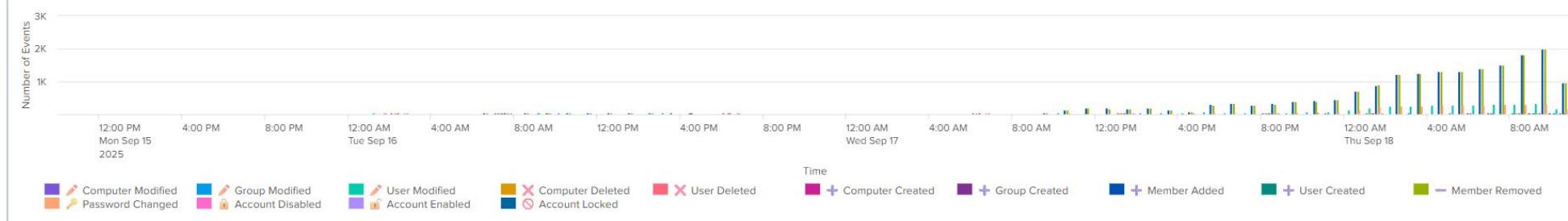
## AU-2 (6)(1-2), (7-13) - Privileged Rights Timeline

User privileged actions



## AU-2 (5)(1-2) - User Management Timeline

Trend of user management activities

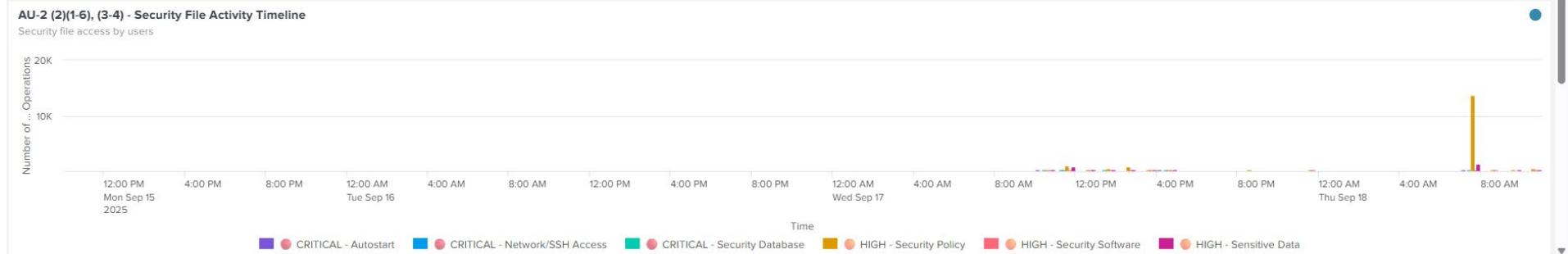


AU-2 (2)(1-6), (3-4) - Security File and Object Activity

Security file access by users

Time	Computer	User	File Name	What Happened	Risk Level	Process
2025-09-18 10:23:05	sccmits.arlut.utexas.edu	SQLServerReportingservices	rsreportserver.config	File Read	MEDIUM - Configuration	I:\Program Files\Microsoft SQL Server Reporting Services\SSRS\RSHosting Service\RSHostingService.exe
2025-09-18 10:23:05	sccmits.arlut.utexas.edu	SQLServerReportingservices	config.json	File Read	MEDIUM - Configuration	I:\Program Files\Microsoft SQL Server Reporting Services\SSRS\RSHosting Service\RSHostingService.exe
2025-09-18 10:23:05	sccmits.arlut.utexas.edu	SQLServerReportingservices	Microsoft.BI.Server.Management.WebApi.dll	File Read	MEDIUM - Executable	I:\Program Files\Microsoft

< Prev 1 2 3 4 5 Next >



USB/CD/BURN

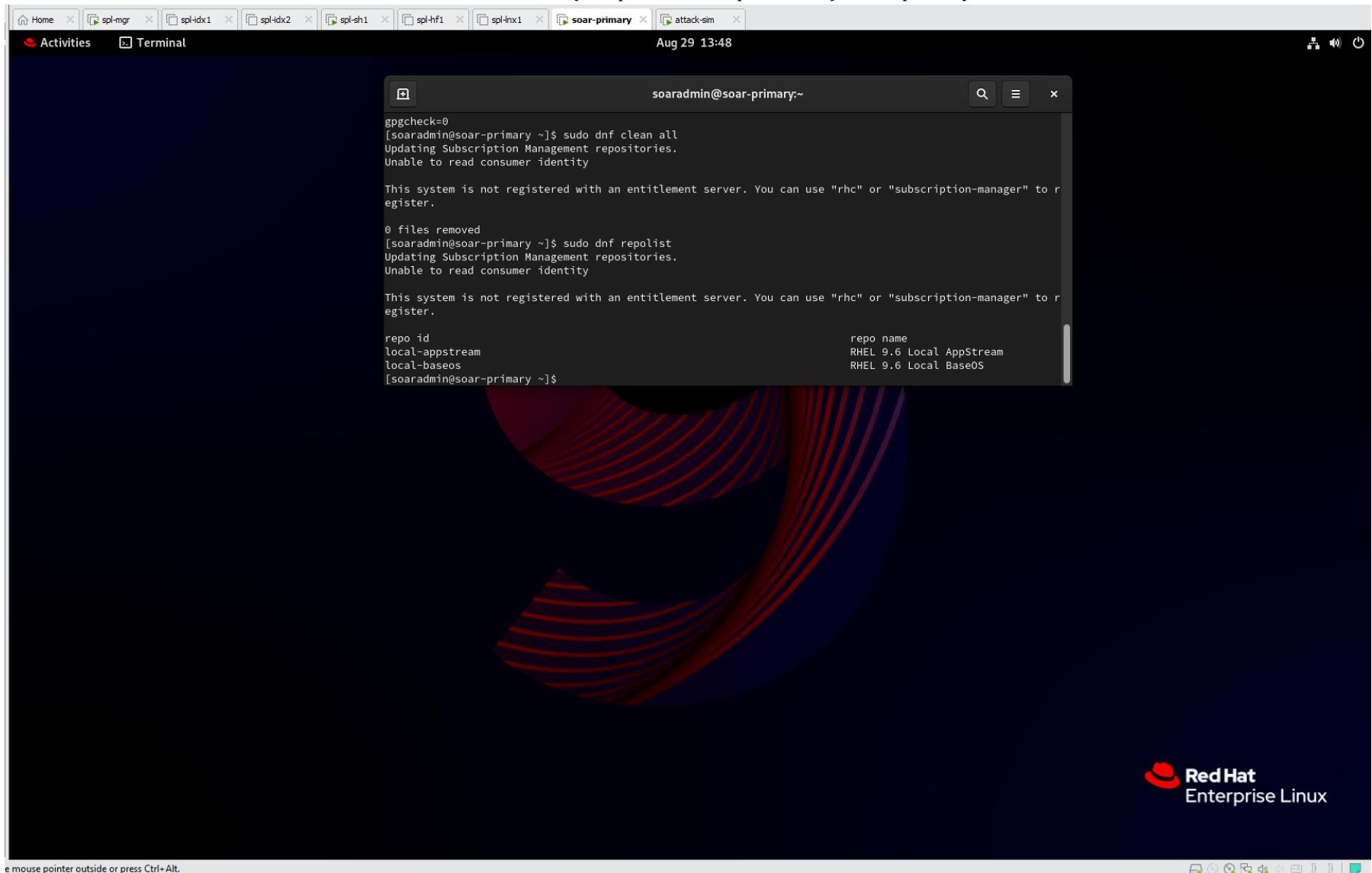
Time	Host	User	EventType	Status	Risk	DeviceDetails	FileDirection	FileName
2025-09-18 10:22:19	cliffhanger.arlut.utexas.edu	dclifton	FILE TRANSFER	BULK TRANSFER (5 files)	HIGH - FILE TRANSFER	File: 8748459.SLDDRW	FROM REMOVABLE (Bulk 5 files)	8748370.SLDDRW, 8748378.SLDDRW, 8748417.SLDDRW, 8748418.SLDDRW, 8748459.SLDDRW
2025-09-18 10:11:38	atl-docs-wv.arlut.utexas.edu	cperez	FILE TRANSFER	BULK TRANSFER (3 files)	HIGH - FILE TRANSFER	File: WAS 2025-SEPTEMBER.xls	FROM REMOVABLE (Bulk 3 files)	WAS 2025-SEPTEMBER.xls, control-flow-ex-2.png, control-flow-ex.png
2025-09-18 10:10:40	atl-docs-wv.arlut.utexas.edu	cperez	FILE TRANSFER	BULK TRANSFER (3 files)	HIGH - FILE TRANSFER	File: WAS 2025-SEPTEMBER.xls	FROM REMOVABLE (Bulk 3 files)	WAS 2025-SEPTEMBER.xls, control-flow-ex-2.png, control-flow-ex.png
2025-09-18 10:08:31	aspd-wind-wv.arlut.utexas.edu	sndsc-prod	FILE TRANSFER	FILE ACCESSED	HIGH - FILE TRANSFER	File: bin	FROM REMOVABLE (Inbound)	bin

Created by Tevin Agtarap on 9/18/2025

## Splunk SOAR Deployment & Demonstration

### Splunk SOAR Deployment and Demonstration

Install REHL Linux 9.6 (Compatible with Splunk Soar) – soar-primary VM



A screenshot of a Red Hat Enterprise Linux 9.6 desktop environment. The terminal window shows the following command output:

```
gpgcheck=0
[soaradmin@soar-primary ~]$ sudo dnf clean all
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

0 files removed
[soaradmin@soar-primary ~]$ sudo dnf repolist
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

repo id                                repo name
local-appstream                           RHEL 9.6 Local AppStream
local-baseos                             RHEL 9.6 Local BaseOS
[soaradmin@soar-primary ~]$
```

The desktop interface includes a dock with various application icons and a Red Hat logo in the bottom right corner.

### Install Splunk SOAR

```
C:\windows\System32\OpenSSH\scp.exe: stat local "splunk-soar-6.3.0.718-4c6c4889-el8-x86_64.tgz": No such file or directory
PS C:\Users\agtarap\Documents\SplunkLabFiles> scp splunk_soar-unpriv-6.4.1.361-bea76553-el8-x86_64.tgz soaradmin@192.168.221.60:/tmp/
>>
soaradmin@192.168.221.60's password:
splunk_soar-unpriv-6.4.1.361-bea76553-el8-x86_64.tgz                                         33%  546MB 102.3MB/s   00:10 ETA
```

```
[soaradmin@soar-primary ~]$ ls -la /tmp/*.tgz
-rw-rw-r--. 1 soaradmin soaradmin 1698174673 Aug 28 07:51 /tmp/splunk_soar-unpriv-6.4.1.361-bea76553-el8-x86_64.tgz
[soaradmin@soar-primary ~]$
```

### Install Splunk Soar on soar-primary VM

```
[soaradmin@soar-primary ~]$ sudo -u phantom /opt/phantom/bin/start_phantom.sh
Starting all Splunk SOAR services
Starting Connection pooler (PgBouncer): [ OK ]
Checking database connectivity: [ OK ]
Checking external database version: [ OK ]
Checking component versions: [ OK ]
Starting Supervisord: [ OK ]
Starting Splunk SOAR daemons: [ OK ]
Checking Supervisord processes: [ OK ]
Starting Web application server (uwsgi): [ OK ]
Starting Web server (nginx): [ OK ]
Starting Embedded Universal Forwarder: [ OK ]
Starting Watchdog daemon: [ OK ]
Splunk SOAR startup successful
```

### Splunk SOAR

The image shows a screenshot of a web browser displaying the Splunk SOAR login page. The page has a dark background with white text. At the top, it says "Splunk SOAR". Below that is a form with two input fields: "Username" and "Password", separated by a vertical line. To the right of the "Password" field is a blue rectangular button with the white text "Sign in". Below the form, there is a small link in a smaller font that reads "Forgot Password?".

splunk>

## Create soare\_service account in Splunk

The screenshot shows the Splunk Enterprise interface with the 'Users' page selected. At the top, there's a search bar and navigation links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. A green 'New User' button is located in the top right corner. The main content area displays a table titled 'Showing 1-2 of 2 Users'. The table has columns for Name, Authentication system, Full name, Email address, Time zone, Default app, Default app inherited from, Roles, Last login, Status, and an edit icon. Two users are listed: 'admin' and 'soar\_service'. Both users have 'Splunk' as their authentication system and 'Administrator' as their full name. Their email addresses are 'changeme@example.com' and 'SOAR Service Account' respectively. The time zone is 'America/Chicago' for the service account. Both users have 'launcher' as their default app and 'system' as their default app inherited from. They both have the 'admin' role. The last login date is '9/3/2025, 9:05:55 AM'. Both users are marked as 'Active'.

Name	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last login	Status	⋮
admin	Splunk	Administrator	changeme@example.com		launcher	system	admin	9/3/2025, 9:05:55 AM	● Active	<span>edit</span>
soar_service	Splunk	SOAR Service Account		America/Chicago	launcher	system	admin can_delete power user		● Active	<span>edit</span>

Showing 1-2 of 2 Users

## Finishing configuring Splunk SOAR

The screenshot shows the Splunk SOAR interface at the URL <https://localhost:8443>. The browser status bar indicates 'Not secure'. The SOAR logo is in the top left, and a search bar is in the top right. The top navigation bar includes links for 'SS UPDATES', 'Information System...', 'Meeting Room Boo...', 'Service Now - Login...', 'Commons Cafe | Co...', 'Login | Splunk', 'Employee Time and...', 'Dashboards | Splun...', 'Staff Home Page', and 'Other f...'. On the far right, there are icons for a profile, notifications (0), and configuration. The main dashboard features a large central box titled 'Automation ROI Summary' with the date range '2025-09-10 - 2025-09-16'. Inside this box, it says 'Welcome to Splunk SOAR' and 'The following tour will introduce you to the basic concepts you need to know to get started'. It includes two large numerical values: '0' for Resolved events and '0m' for Mean dwell time. To the right, it shows '0m' for Time saved and '\$0' for Dollars saved. Below this, there's a section titled 'Events by Status' with a note 'No Data'. On the left side of the main box, there's a 'Resolved events' card with '0' and 'Mean dwell time' sections, and an 'Open' card with '0' and 'SLA SEVERE' sections. The bottom of the main box has 'Get Started' and 'Exit Tour' buttons. The overall interface is dark-themed.

**Install Connector**

splunkbase.splunk.com/app/5848

About upgrading to... How to upgrade Spl... Online Courses - Le... Updates for SS Splunk.conf

Welcome to the new Splunkbase! To return to the old Splunkbase, click here.

**splunkbase** Collections Apps Find an app Submit an app TA

Main Page / Apps / Splunk

## splunk> Splunk

This app integrates with Splunk to update data on the device, in addition to investigate and ingestion actions  
Built by Splunk LLC

 Download ⌂ ⌂

Latest Version 2.20.2 September 8, 2025 Release notes Compatibility SOAR On-Prem Platform Version: 7.0, 6.4, 6.3 Rating 5 ★★★★★ (2) Rate this app Support Splunk Supported Connector Learn more Ranking #2 in SIEM

**Summary** Details Installation Troubleshooting Contact Version History

This app integrates with Splunk to update data on the device, in addition to investigate and ingestion actions

**Supported Actions**

- test connectivity: Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials
- get host events: Get events pertaining to a host that have occurred in the last 'N' days on poll; ingest logs from the Splunk instance

Categories SIEM  
Created By Splunk LLC

SS UPDATES Information System... Meeting Room Boo... Service Now - Login... Commons Cafe | Co... Login | Splunk Employee Time and... Dashboards | Splunk... Staff Home Page ARL Staff Directory MAP ARL Other favorites

brown-pluto-coconut version 6.4.1.361 soar\_local\_admin

Apps Search... Search app names Install App App Updates New Apps App Wizard

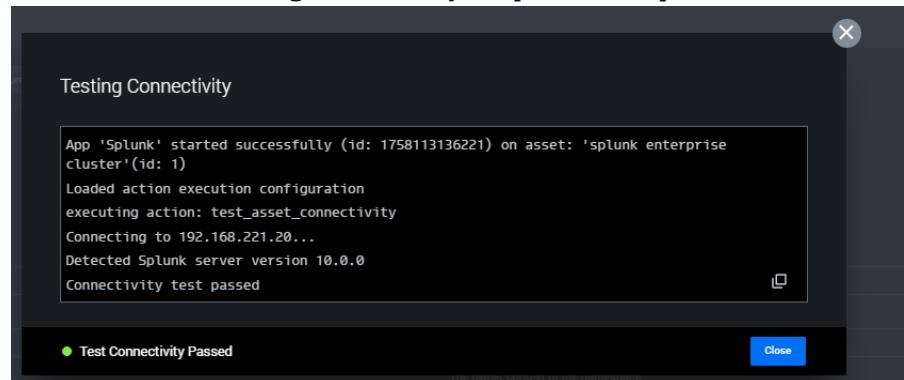
Configured Apps Unconfigured Apps (1) Draft Apps Orphaned Assets Python update required All categories

**splunk>** Splunk Publisher: Splunk Version: 2.20.2 Python version: 3.9 Documentation

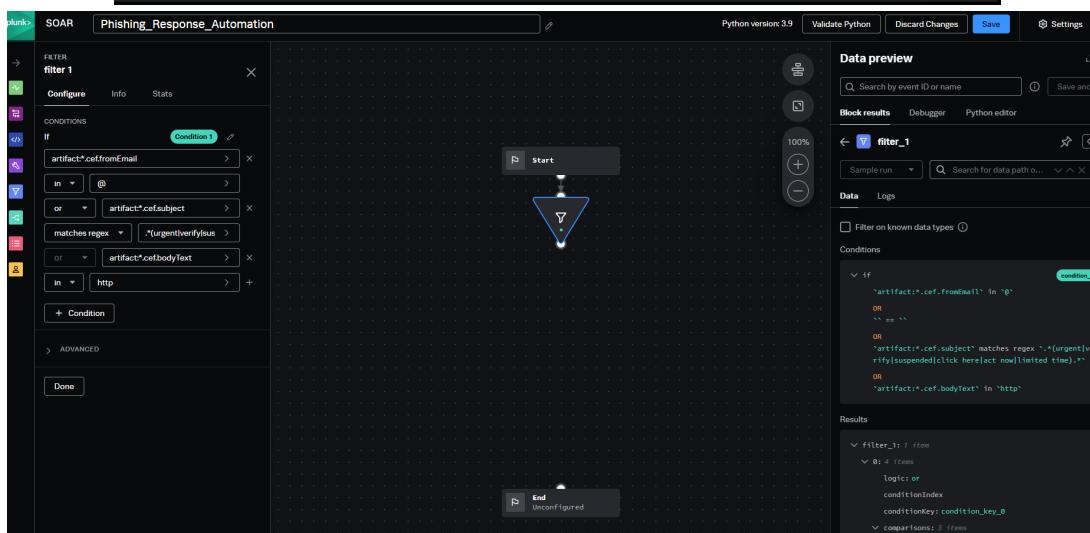
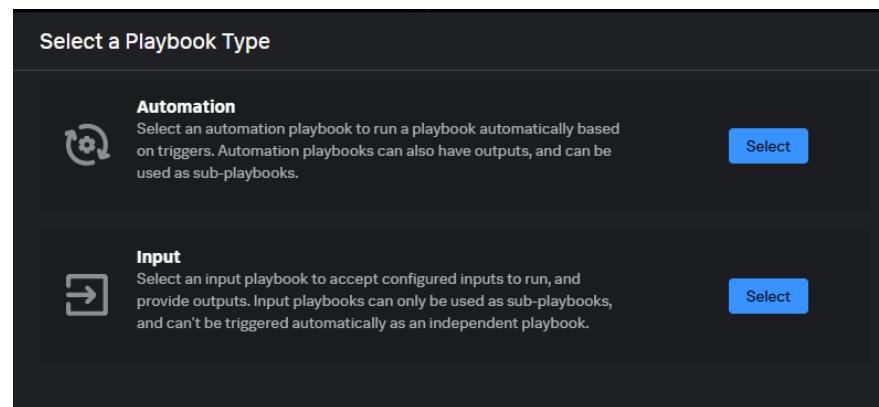
This app integrates with Splunk to update data on the device, in addition to investigate and ingestion actions  
6 supported actions

Show 20

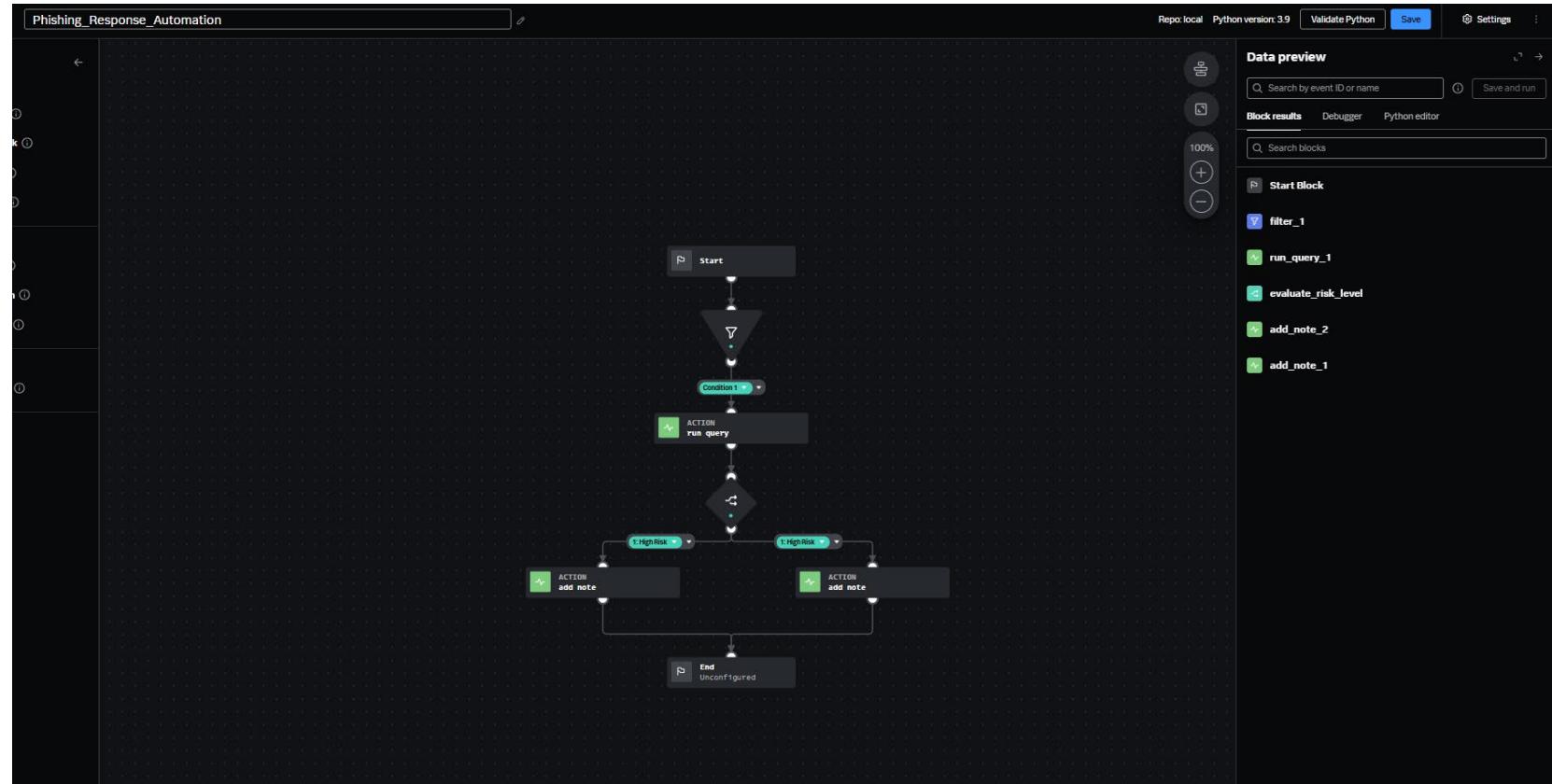
## Testing Connectivity to Splunk Enterprise



## Creating SOAR Playbooks!



## Full playbook built out



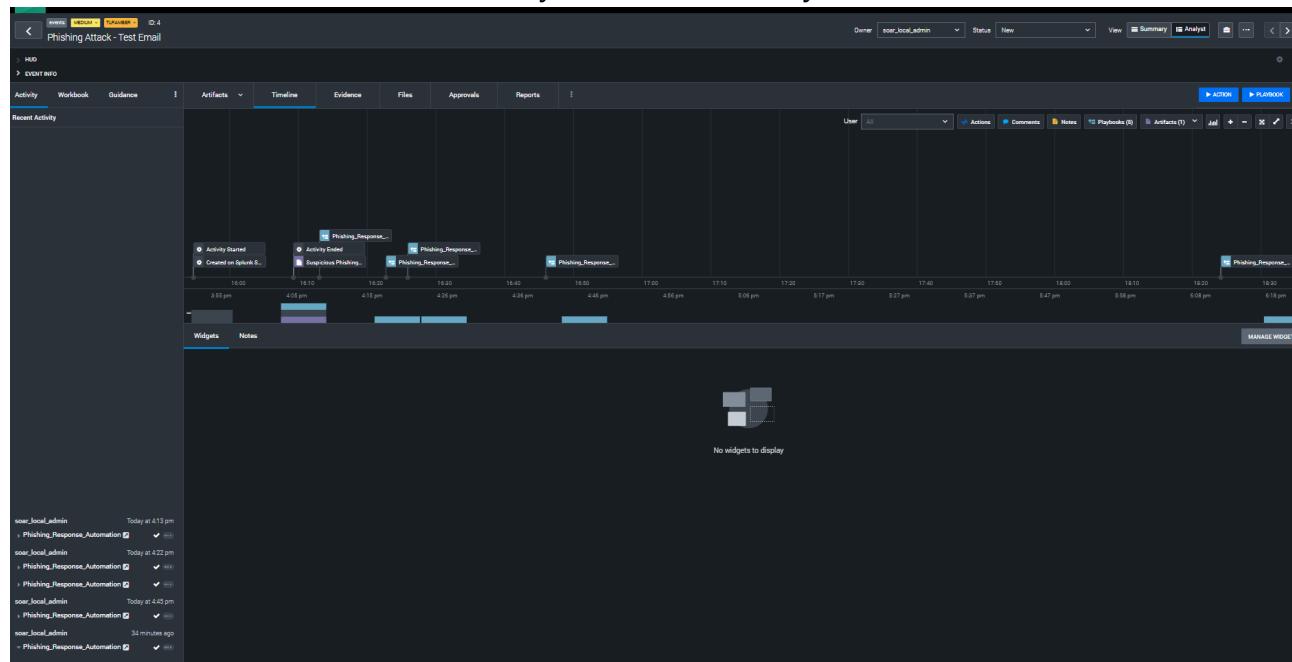
## Build out simulated phishing email to test SOAR playbook

The screenshot shows the SOAR platform interface for a "Phishing Attack - Test Email" investigation. The top navigation bar includes "splunk", "SOAR", "Search...", "INVESTIGATION", "Owner: soar\_local\_admin", "Status: New", "View: Summary", "Analyst: [empty]", and a three-dot menu. The main workspace is divided into sections:

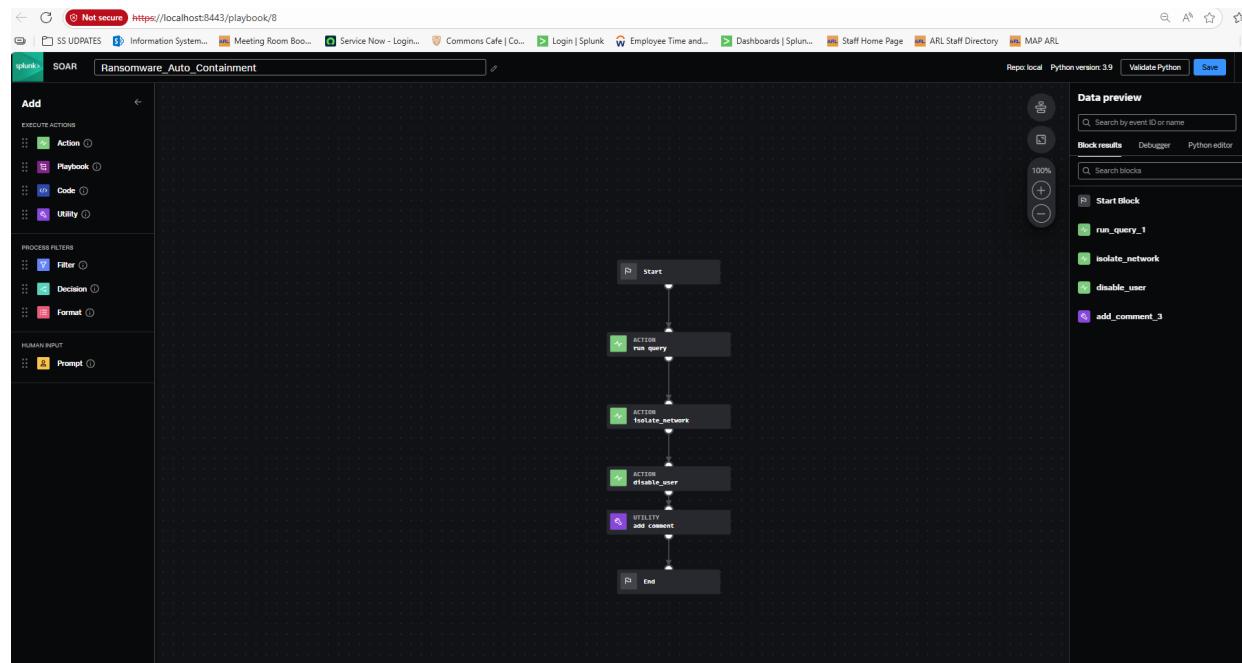
- ARTIFACTS (1)**: A table showing one artifact: ID: 13, Label: event, Name: Suspicious Phishing Email, Severity: MEDIUM, Created By: soar\_local\_admin.
- Widgets**: A section indicating "No widgets to display".

On the right side, there are buttons for "ACTION", "PLAYBOOK", and "ARTIFACT". The bottom right corner has a "MANAGE WIDGETS" link.

## Playbook ran successfully



## Ransomware Auto Containment



## Add Ransomware Attack Event in SOAR and Run Playbook

The screenshot shows a SOAR platform interface with a timeline view. The timeline displays several actions taken against a user account, categorized under a 'RANSOMWARE' event. The actions include isolating the network, running a query, and disabling the user. A modal window provides detailed configuration for the 'Ransomware\_Auto\_Containment' playbook, specifically for the 'run\_query\_1' and 'isolate\_network' steps. The 'run\_query\_1' step uses Splunk to search for specific events. The 'isolate\_network' step also uses Splunk to search for events. Both steps have a status of '0' events found. The 'disable\_user' step is also shown with a similar configuration. At the bottom of the modal, a message indicates that the ransomware has been contained. An input field at the bottom allows for comments or command invocation.

**Ransomware\_Auto\_Containment**

- run\_query\_1**
  - Splunk
  - query = index=main sourcetype="Test Ransom dat" command = search search\_mode = smart add\_raw\_field = true Sid: 1758205887.13, Total events: 0
- isolate\_network**
  - Splunk
  - query = index=main sourcetype="Test Ransom dat" command = search search\_mode = smart add\_raw\_field = true Sid: 1758205889.14, Total events: 0
- disable\_user**
  - Splunk
  - query = index=main sourcetype="Test Ransom dat" command = search search\_mode = smart add\_raw\_field = true Sid: 1758205890.15, Total events: 0

RANSOMWARE CONTAINED: Network isolated & User disabled

Enter comment or "/" to invoke command

Container (RANSOMWARE-WIN-VICTIM01)

[Start] → Provides container context

[run\_query\_1] → Queries Splunk → Finds host="WIN-VICTIM01"

[isolate\_network] → Uses host data → Simulates network isolation

[disable\_user] → Uses event data → Simulates account disable

[add\_comment] → Documents all actions taken

[End] → Playbook complete

## Splunk Enterprise Deployment Walkthrough

### Splunk Deployment!

```
splunkadmin@spl-mgr:~$ ls /mnt/hgfs/  
SplunkLabFiles  
splunkadmin@spl-mgr:~$ ls -la ~/*.tgz  
ls: cannot access '/home/splunkadmin/*.tgz': No such file or directory  
splunkadmin@spl-mgr:~$ ls SplunkLabFiles  
ls: cannot access 'SplunkLabFiles': No such file or directory  
splunkadmin@spl-mgr:~$ sudo ls SplunkLabFiles  
ls: cannot access 'SplunkLabFiles': No such file or directory  
splunkadmin@spl-mgr:~$ sudo mkdir -p /mnt/shared  
splunkadmin@spl-mgr:~$ sudo mount -t fuse.vmhgfs-fuse .host:/SplunkLabFiles /mnt/shared -o allow_other  
splunkadmin@spl-mgr:~$ ls -la /mnt/shared/  
total 4616711  
drwxrwxrwx 1 root root 4096 Aug 21 17:49 .  
drwxr-xr-x 4 root root 4096 Aug 22 12:37 ..  
-rwxrwxrwx 1 root root 1353162564 Aug 21 17:44 splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb  
-rwxrwxrwx 1 root root 70895806 Aug 21 17:48 splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.deb  
-rwxrwxrwx 1 root root 3303444480 Aug 21 17:37 ubuntu-24.04.3-live-server-amd64.iso  
splunkadmin@spl-mgr:~$ cp /mnt/shared/splunk*.deb ~/  
splunkadmin@spl-mgr:~$ ls -la ~/*.deb  
-rwxrwxr-x 1 splunkadmin splunkadmin 1353162564 Aug 22 12:39 /home/splunkadmin/splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb  
-rwxrwxr-x 1 splunkadmin splunkadmin 70895806 Aug 22 12:39 /home/splunkadmin/splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.deb  
splunkadmin@spl-mgr:~$
```

### Updating Splunk User password

```
splunkadmin@spl-mgr:~$ sudo passwd splunk  
New password:  
Retype new password:  
passwd: password updated successfully  
splunkadmin@spl-mgr:~$
```

-----

## Configuring Firewall/ports

```
splunkadmin@spl-mgr:~$ sudo usermod -aG sudo splunk
splunkadmin@spl-mgr:~$ sudo ufw --force enable
Firewall is active and enabled on system startup
splunkadmin@spl-mgr:~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
splunkadmin@spl-mgr:~$ sudo ufw allow 8000/tcp
Rule added
Rule added (v6)
splunkadmin@spl-mgr:~$ sudo ufw allow 8089/tcp
Rule added
Rule added (v6)
splunkadmin@spl-mgr:~$ sudo ufw allow 9997/tcp
Rule added
Rule added (v6)
splunkadmin@spl-mgr:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
22/tcp                      ALLOW       Anywhere
8000/tcp                    ALLOW       Anywhere
8089/tcp                    ALLOW       Anywhere
9997/tcp                    ALLOW       Anywhere
22/tcp (v6)                 ALLOW       Anywhere (v6)
8000/tcp (v6)               ALLOW       Anywhere (v6)
8089/tcp (v6)               ALLOW       Anywhere (v6)
9997/tcp (v6)               ALLOW       Anywhere (v6)

splunkadmin@spl-mgr:~$
```

## System Limits Configuration

```
splunkadmin@spl-mgr:~$ cat <<EOF | sudo tee -a /etc/security/limits.conf
# Splunk limits
splunk soft nofile 65535
splunk hard nofile 65535
splunk soft nproc 20480
splunk hard nproc 20480
EOF
```

## Disable Transparent Huge Pages (THP)

```
splunkadmin@spl-mgr:~$ echo never | sudo tee /sys/kernel/mm/transparent_hugepage/enabled
never
```

```
splunkadmin@spl-mgr:~$ echo never | sudo tee /sys/kernel/mm/transparent_hugepage/defrag
never
splunkadmin@spl-mgr:~$
```

```
splunkadmin@spl-mgr:~$ cat << 'EOF' | sudo tee /etc/systemd/system/disable-thp.service
> [Unit]
> Description=Disable Transparent Huge Pages
>
> [Service]
> Type=simple
> ExecStart=/bin/sh -c "echo never > /sys/kernel/mm/transparent_hugepage/enabled && echo never > /sys/kernel/mm/transparent_hugepage/defrag"
>
> [Install]
> WantedBy=multi-user.target
> EOF
[sudo] password for splunkadmin:
[Unit]
Description=Disable Transparent Huge Pages

[Service]
Type=simple
ExecStart=/bin/sh -c "echo never > /sys/kernel/mm/transparent_hugepage/enabled && echo never > /sys/kernel/mm/transparent_hugepage/defrag"

[Install]
WantedBy=multi-user.target
splunkadmin@spl-mgr:~$ sudo systemctl daemon-reload
splunkadmin@spl-mgr:~$ sudo systemctl enable disable-thp
Created symlink /etc/systemd/system/multi-user.target.wants/disable-thp.service → /etc/systemd/system/disable-thp.service.
splunkadmin@spl-mgr:~$ sudo systemctl start disable-thp
splunkadmin@spl-mgr:~$ cat /sys/kernel/mm/transparent_hugepage/enabled
always madvise [never]
splunkadmin@spl-mgr:~$
```

## Install Splunk Enterprise 10.0.0



spl-mgr@spl-mgr:~\$ sudo dpkg -i splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb  
[sudo] password for splunkadmin:  
Selecting previously unselected package splunk.  
(Reading database ... 86987 files and directories currently installed.)  
Preparing to unpack splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb ...  
verify that this system has all the commands we will require to perform the preflight step  
no need to run the splunk-preinstall upgrade check  
Unpacking splunk (10.0.0) ...  
Setting up splunk (10.0.0) ...  
find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory  
complete

## Enable Boot Start

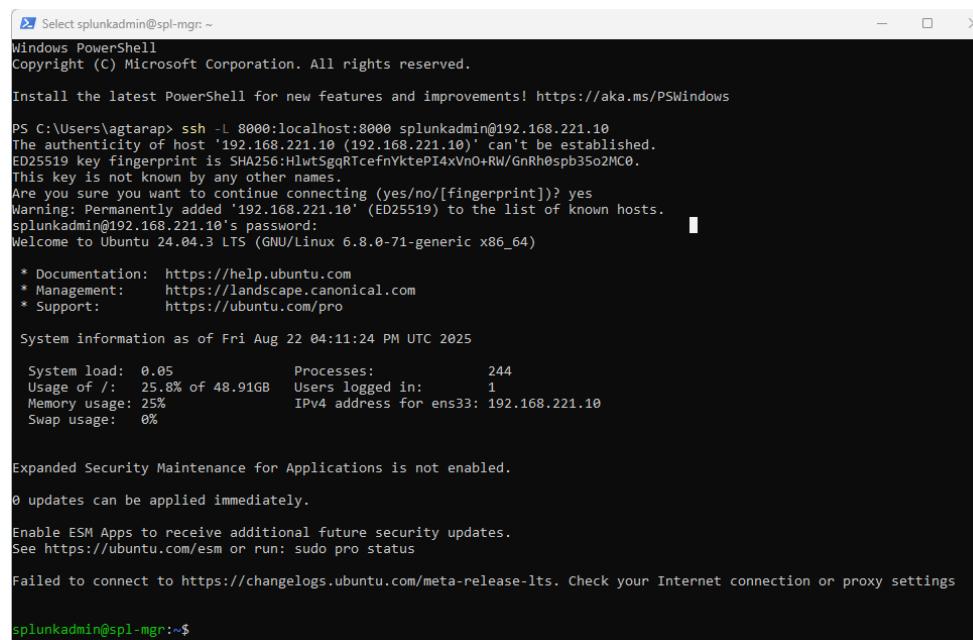
```
splunkadmin@spl-mgr:~$ ps aux | grep splunkd
splunk    40793  0.4  5.0 1078932 201504 ?        Ssl  15:30  0:10 splunkd --under-systemd --systemd-delegate=yes -p 8089 _internal_launch_under_systemd
splunk    40867  0.1  0.3 135384 15164 ?        Ss   15:30  0:00 [splunkd pid=40793] splunkd --under-systemd --systemd-delegate=yes -p 8089 _internal_launch_u
nder_systemd [process-runner]
splunk    41024  0.6  1.9 237836 77420 ?        S1   15:30  0:00 /opt/splunk/bin/splunkd instrument-resource-usage -p 8089 --with-kvstore
splunk    41379  0.3  1.8 2062392 73988 ?        S1   15:31  0:00 [splunkd pid=407 ] [search-launcher]
splunk    41380  0.0  0.3 135384 14920 ?        Ss   15:31  0:00 [splunkd pid=40793] [search-launcher] [process-runner]
splunka+  41656  0.0  0.0  6544  2304 tty1      S+   15:32  0:00 grep --color=auto splunkd
splunkadmin@spl-mgr:~$
```

## Enable HTTPS

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk set servername spl-mgr -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk set web-ssl -enable true -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Command error: 'web-ssl' is not a valid argument for the 'set' command. Please type "splunk help set" for usage and examples.
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk enable web-ssl -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
splunkadmin@spl-mgr:~$ _
```

## SSH Port Forwarding (Tunneling)



A screenshot of a Windows PowerShell window titled "Select splunkadmin@spl-mgr: ~". The window shows the following command and its output:

```
PS C:\Users\lagtarap> ssh -L 8000:localhost:8000 splunkadmin@192.168.221.10
The authenticity of host '192.168.221.10 (192.168.221.10)' can't be established.
ED25519 key fingerprint is SHA256:HwtSggQTcefnykteP14xvN+RW/GnRhospb3So2MC0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.221.10' (ED25519) to the list of known hosts.
splunkadmin@192.168.221.10's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Aug 22 04:11:24 PM UTC 2025

 System load: 0.05      Processes:          244
 Usage of /: 25.8% of 48.91GB  Users logged in:     1
 Memory usage: 25%           IPv4 address for ens3: 192.168.221.10
 Swap usage:  0%
 
 Expanded Security Maintenance for Applications is not enabled.

 0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

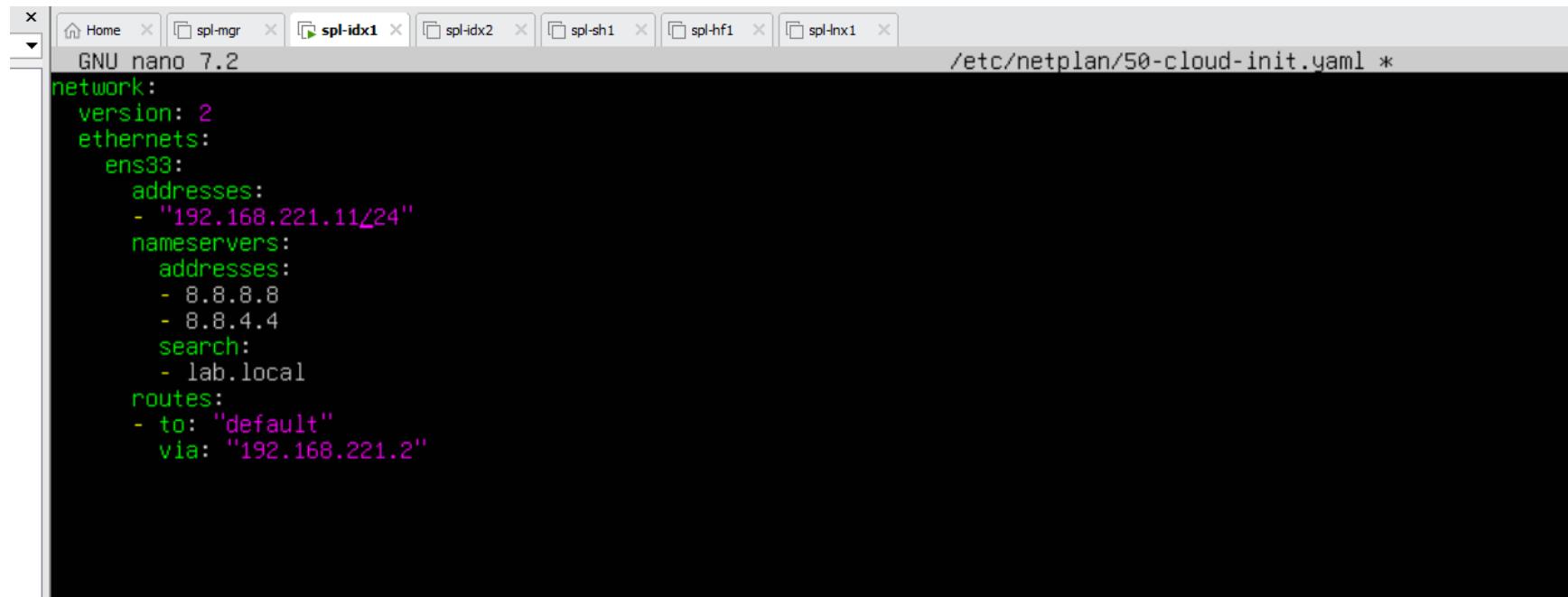
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

splunkadmin@spl-mgr:~$
```

**Build all VM's**

<b>VM Name</b>	<b>Role</b>	<b>RAM</b>	<b>CPU</b>	<b>Purpose</b>
spl-idx1	Indexer 1	8GB	4	First indexer peer
spl-idx2	Indexer 2	8GB	4	Second indexer peer
spl-sh1	Search Head	6GB	4	Search interface
spl-hf1	Heavy Forwarder	4GB	2	Data collection hub
spl-lnx1	Linux UF	2GB	1	Linux endpoint

## Configure VMS



The screenshot shows a terminal window titled "Configure VMS". The window has multiple tabs at the top: Home, spl-mgr, spl-idx1 (which is active), spl-idx2, spl-sh1, spl-hf1, and spl-lnx1. The main pane displays the contents of the file "/etc/netplan/50-cloud-init.yaml". The configuration is as follows:

```
GNU nano 7.2
network:
  version: 2
  ethernets:
    ens33:
      addresses:
        - "192.168.221.11/24"
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
        search:
          - lab.local
      routes:
        - to: "default"
          via: "192.168.221.2"
```

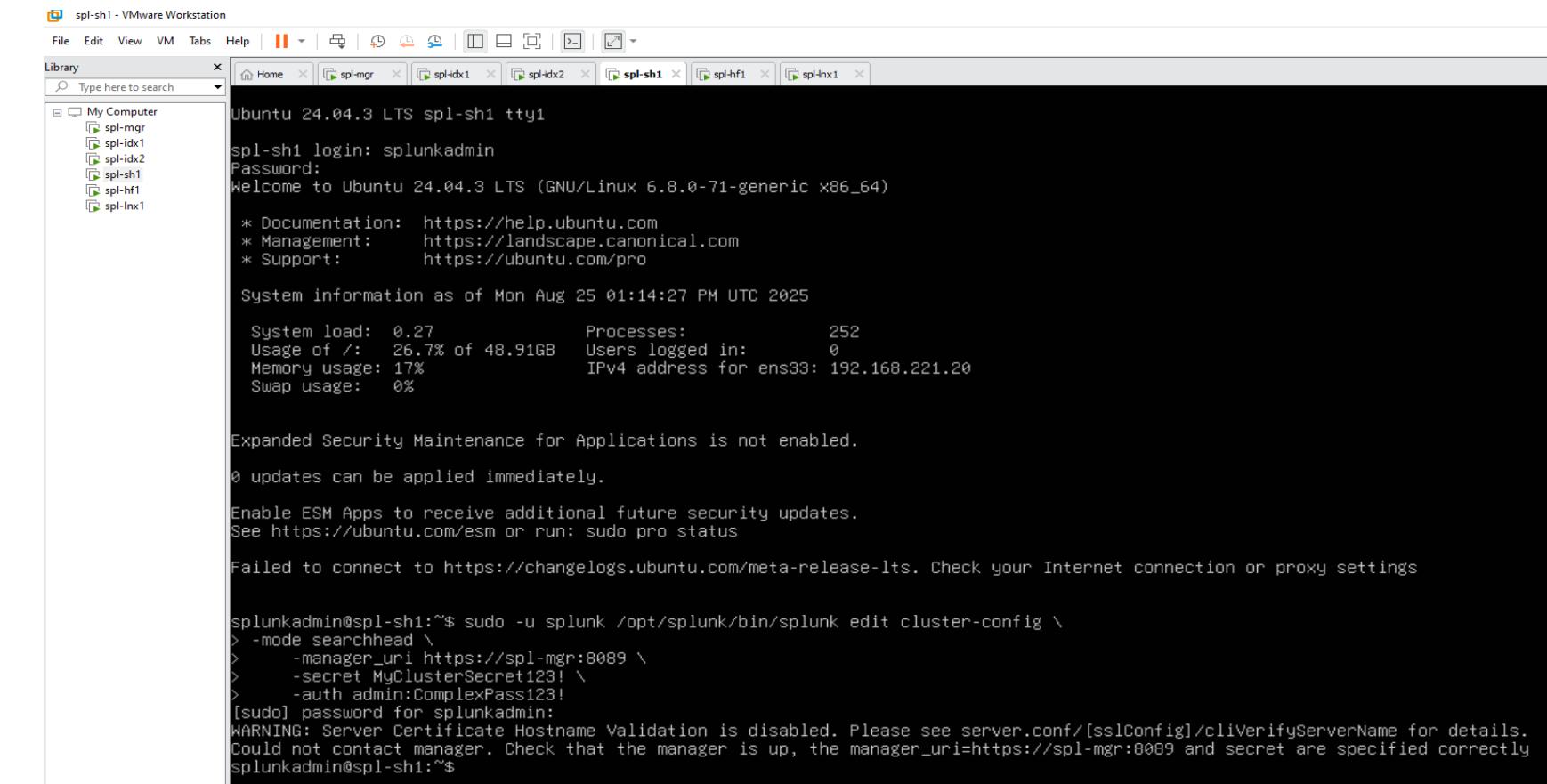
## Cluster Configuration

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk edit cluster-config \
>   -mode manager \
>   -replication_factor 2 \
>   -search_factor 2 \
>   -secret MyClusterSecret123! \
>   -cluster_label production \
>   -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
The cluster-config property has been edited.
You need to restart the Splunk Server (splunkd) for your changes to take effect.
splunkadmin@spl-mgr:~$
```

## Index Configuration's

```
splunkadmin@spl-idx1:~$ sudo -u splunk /opt/splunk/bin/splunk edit cluster-config \
> -mode peer \
>   -manager_uri https://spl-mgr:8089 \
>   -replication_port 9887 \
>   -secret MyClusterSecret123! \
>   -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Could not contact manager. Check that the manager is up, the manager_uri=https://spl-mgr:8089 and secret are specified correctly
splunkadmin@spl-idx1:~$ sudo systemctl restart Splunkd
```

## Search Head Configuration



```
splunkadmin@spl-sh1:~$ sudo -u splunk /opt/splunk/bin/splunk add search-server https://spl-idx1:8089 \
>     -auth admin:ComplexPass123! -remoteUsername admin -remotePassword ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Peer added
splunkadmin@spl-sh1:~$
```

## Heavy Forwarder Setup

```
splunkadmin@spl-hf1:~$ sudo -u splunk /opt/splunk/bin/splunk enable listen 9997 -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Listening for Splunk data on TCP port 9997.
splunkadmin@spl-hf1:~$ _
```

```
splunkadmin@spl-hf1:~$ cat << 'EOF' | sudo tee /opt/splunk/etc/system/local/outputs.conf
> [tcpout]
u> defaultGroup = indexer_cluster
>
> [tcpout:indexer_cluster]
> server = spl-idx1:9997,spl-idx2:9997
> useACK = true
> autoLB = true
> compressed = true
> EOF
[tcpout]
defaultGroup = indexer_cluster

[tcpout:indexer_cluster]
server = spl-idx1:9997,spl-idx2:9997
useACK = true
autoLB = true
compressed = true
splunkadmin@spl-hf1:~$
```

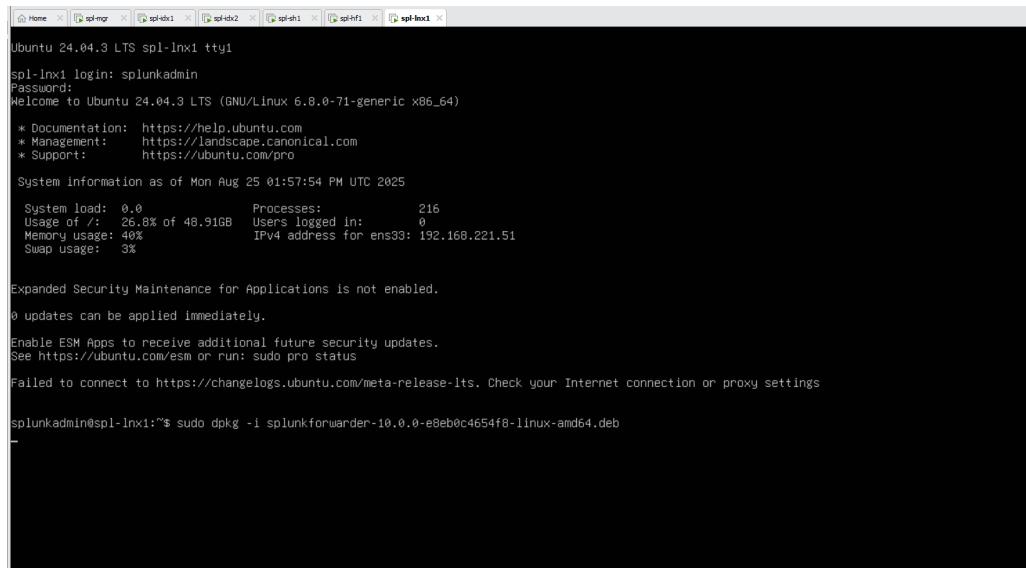
side or press Ctrl+G.

## Deployment Server

```
Home × spl-mgr × spl-idx1 × spl-idx2 × spl-sh1 × spl-hf1 × spl-lnx1 ×
splunkadmin@spl-mgr:~$ sudo -u splunk mkdir -p /opt/splunk/etc/deployment-apps/TA_base_outputs/local
splunkadmin@spl-mgr:~$ cat << 'EOF' | sudo tee /opt/splunk/etc/deployment-apps/TA_base_outputs/local/outputs.conf
> [tcpout]
> defaultGroup = heavy_forwarder
>
> [tcpout:heavy_forwarder]
> server = spl-hf1:9997
> compressed = true
> EOF
[tcpout]
defaultGroup = heavy_forwarder

[tcpout:heavy_forwarder]
server = spl-hf1:9997
compressed = true
splunkadmin@spl-mgr:~$ sudo chown -R splunk:splunk /opt/splunk/etc/deployment-apps/
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk reload deploy-server -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Reloading serverclass(es).
splunkadmin@spl-mgr:~$ _
```

## Universal Forwarder (spl-lnx1)



```
Ubuntu 24.04.3 LTS spl-lnx1 tty1
spl-lnx1 login: splunkadmin
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Mon Aug 25 01:57:54 PM UTC 2025

System load: 0.0 Processes: 216
Usage of /: 26.8% of 48.91GB Users logged in: 0
Memory usage: 40% IPv4 address for ens33: 192.168.221.51
Swap usage: 3%

Expanded Security Maintenance for Applications is not enabled.

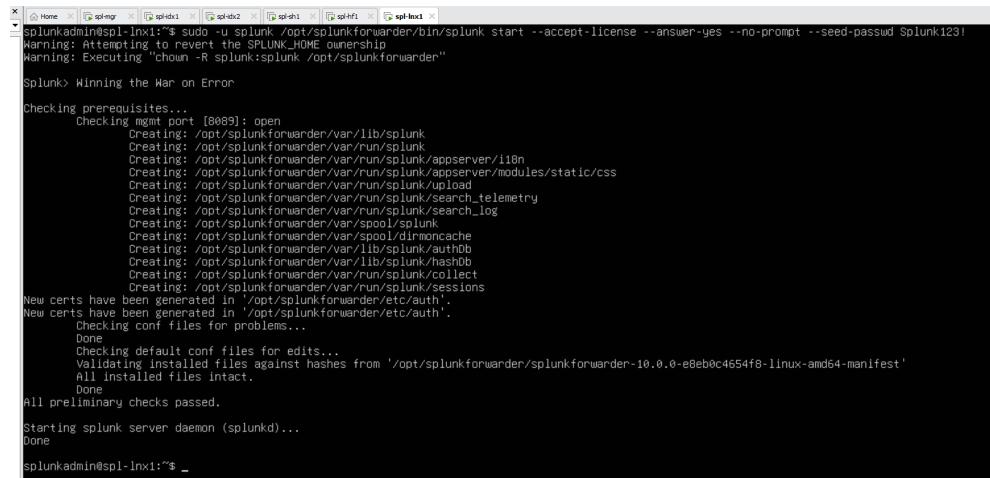
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

splunkadmin@spl-lnx1:~$ sudo dpkg -i splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.deb
```

```
[sudo] password for splunkadmin:
Selecting previously unselected package splunkforwarder.
(Reading database ... 116283 files and directories currently installed.)
Preparing to unpack splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.deb ...
verify that this system has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunkforwarder (10.0.0) ...
Setting up splunkforwarder (10.0.0) ...
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
complete
splunkadmin@spl-lnx1:~$ _
```



```
splunkadmin@spl-lnx1:~$ sudo /opt/splunkforwarder/bin/splunk start --accept-license --answer-yes --no-prompt --seed-passwd Splunk123!
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Splunk> Winning the War on Error
Checking prerequisites...
    Checking mgmt port [8089]: open
        Creating: /opt/splunkforwarder/var/lib/splunk
        Creating: /opt/splunkforwarder/var/run/splunk
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
        Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
        Creating: /opt/splunkforwarder/var/run/splunk/upload
        Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
        Creating: /opt/splunkforwarder/var/run/splunk/search_log
        Creating: /opt/splunkforwarder/var/run/splunk/management
        Creating: /opt/splunkforwarder/var/spool/dlmnoncecache
        Creating: /opt/splunkforwarder/var/lib/splunk/auth
        Creating: /opt/splunkforwarder/var/lib/splunk/hashdb
        Creating: /opt/splunkforwarder/var/run/splunk/collect
        Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
    Checking conf files for problems...
    Done
    Checking default conf files for edits...
    Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
    All installed files intact.
    Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Done
splunkadmin@spl-lnx1:~$ _
```

## Verify UF configured correctly

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk list deploy-clients -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Deployment client: 5EEC24CA-82DA-45D3-895E-76830D0CA339
    averagePhoneHomeInterval:      60
    build:                      e8eb0c4654f8
    clientName:                 5EEC24CA-82DA-45D3-895E-76830D0CA339
    dns:                         192.168.221.51
    guid:                       5EEC24CA-82DA-45D3-895E-76830D0CA339
    hostname:                   spl-lnx1
    id:                          connection_192.168.221.51_8089_192.168.221.51_spl-lnx1_linux-x86%64_5EEC24CA-82DA-45D3-895E-76830D0CA339_5EEC24CA-82DA-45D3-895E-76830D0CA339
    instanceId:                  5EEC24CA-82DA-45D3-895E-76830D0CA339
    instanceName:                spl-lnx1
    ip:                          192.168.221.51
    lastPhoneHomeTime:           1756135362
    mgmt:                        8089
    name:                        5EEC24CA-82DA-45D3-895E-76830D0CA339
    package:                     universal_forwarder
    packageType:                 deb
    serverClasses:               None
    splunkVersion:               10.0.0
    utsname:                     linux-x86_64
splunkadmin@spl-mgr:~$
```

## Verify Cluster Health

```
| Home | [spl-mgr] | [splidx1] | [splidx2] | [spl-snl] | [spl-ttl] | [splinx1] |
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk show cluster-manager-status -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Command error: 'cluster-manager-status' is not a valid argument for the 'show' command. Please type "splunk help show" for usage and examples.
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk show cluster-status -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Replication factor met
Search factor met
All data is searchable
Indexing Ready YES
HA Mode: Disabled

spl-idx2      B32D5E91-4703-40D3-9A13-8240217D378D      default
    Searchable YES
    Status Up
    Bucket Count=12

spl-idx1      B6E895B9-606E-4336-A449-463AA4A6E240      default
    Searchable YES
    Status Up
    Bucket Count=13
splunkadmin@spl-mgr:~$
```

## **Check Search Head Connectivity**

```
splunkadmin@spl-sh1:~$ sudo -u splunk /opt/splunk/bin/splunk list search-server -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Server at URI "192.168.221.11:8089" with status as "Up"
Server at URI "192.168.221.12:8089" with status as "Up"
splunkadmin@spl-sh1:~$ _
```

## **Check Universal Forwarder**

```
splunkadmin@spl-1nx1:~$ sudo -u splunk /opt/splunkforwarder/bin/splunk show deploy-poll -auth admin:Splunk123!
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Deployment Server URI is set to "spl-mgr:8089".
splunkadmin@spl-1nx1:~$
```

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk list deploy-clients -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Deployment client: 4EAF7940-C890-4799-A7F9-06CB27083623
    averagePhoneHomeInterval:      60
    build:             e8eb0c4654f8
    clientName:          4EAF7940-C890-4799-A7F9-06CB27083623
    dns:               192.168.221.51
    guid:              4EAF7940-C890-4799-A7F9-06CB27083623
    hostname:           spl-lnx1
    id:                connection_192.168.221.51_8089_192.168.221.51_spl-lnx1_linux-x86%64_4EAF7940-C890-4799-A7F9-06CB27083623_4EAF7940-C890-4799-A7F9-06CB27083623
    instanceId:         4EAF7940-C890-4799-A7F9-06CB27083623
    instanceName:       spl-lnx1
    ip:                192.168.221.51
    lastPhoneHomeTime: 1756238167
    mgmt:              8089
    name:              4EAF7940-C890-4799-A7F9-06CB27083623
    package:            universal_forwarder
    packageType:        deb
    serverClasses:     None
    splunkVersion:     10.0.0
    utsname:           linux-x86_64

splunkadmin@spl-mgr:~$
```

## Splunk Deployment Complete Validation & Testing

[Data Sources] → [Universal Forwarder] → [Heavy Forwarder] → [Indexer Cluster] → [Search Head]

### Verify Network Connectivity

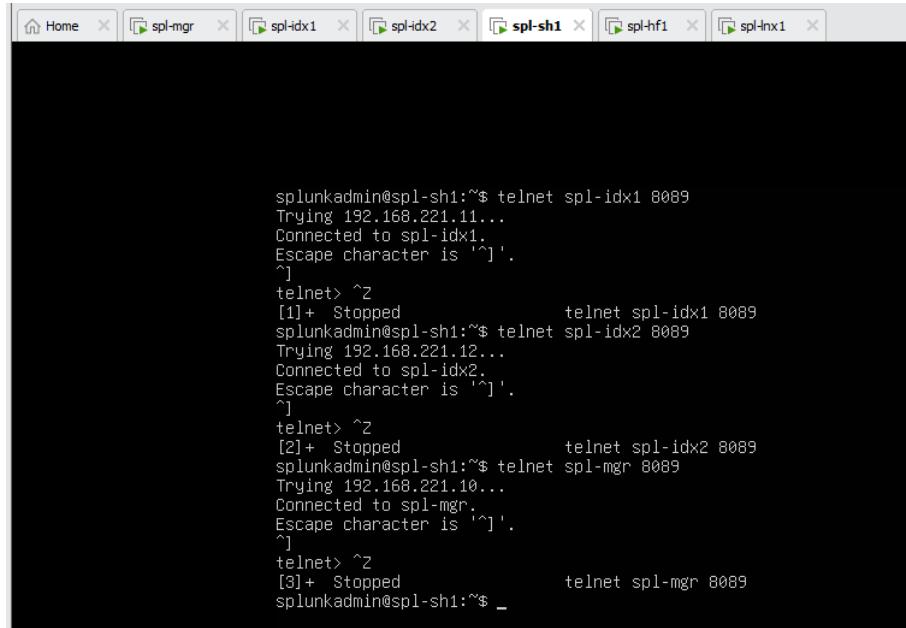
```
splunkadmin@spl-lnx1:~$ telnet spl-hf1 9997
Trying 192.168.221.30...
Connected to spl-hf1.
Escape character is '^]'.

^]
telnet>
```

```
splunkadmin@spl-lnx1:~$ telnet spl-mgr 8089
Trying 192.168.221.10...
Connected to spl-mgr.
Escape character is '^]'.

^]
telnet>
```

```
splunkadmin@spl-hf1:~$ sudo -u splunk /opt/splunk/bin/splunk list forward-server -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Active forwards:
    spl-idx1:9997
    spl-idx2:9997
Configured but inactive forwards:
    None
splunkadmin@spl-hf1:~$ _
```



A screenshot of a terminal window with a dark background and light-colored text. The window has a title bar with several tabs: Home, spl-mgr, spl-idx1, spl-idx2, spl-sh1, spl-hf1, and spl-inx1. The main area of the terminal shows a telnet session from the user's host to three different Splunk servers (spl-idx1, spl-idx2, and spl-sh1) on port 8089. The user performs a series of commands to stop and start connections, demonstrating the use of the telnet command in Splunk.

```
splunkadmin@spl-sh1:~$ telnet spl-idx1 8089
Trying 192.168.221.11...
Connected to spl-idx1.
Escape character is '^]'.
^]
telnet> ^z
[1]+  Stopped                  telnet spl-idx1 8089
splunkadmin@spl-sh1:~$ telnet spl-idx2 8089
Trying 192.168.221.12...
Connected to spl-idx2.
Escape character is '^]'.
^]
telnet> ^z
[2]+  Stopped                  telnet spl-idx2 8089
splunkadmin@spl-sh1:~$ telnet spl-mgr 8089
Trying 192.168.221.10...
Connected to spl-mgr.
Escape character is '^]'.
^]
telnet> ^z
[3]+  Stopped                  telnet spl-mgr 8089
splunkadmin@spl-sh1:~$ _
```

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk show cluster-status -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Replication factor met
Search factor met
All data is searchable
Indexing Ready YES
HA Mode: Disabled

spl-idx2      B32D5E91-4703-40D3-9A13-8240217D378D    default
    Searchable YES
    Status Up
    Bucket Count=14

spl-idx1      B6E895B9-606E-4336-A449-463AA4A6E240    default
    Searchable YES
    Status Up
    Bucket Count=15
splunkadmin@spl-mgr:~$
```

## Test Universal Forwarder → Heavy Forwarder

```
splunkadmin@spl-lnx1:~$ echo "$(date '+%Y-%m-%d %H:%M:%S') TEST_MARKER_UF: Universal Forwarder test event $$" | sudo tee -a /var/log/test_uf.log
[sudo] password for splunkadmin:
2025-08-27 12:41:19 TEST_MARKER_UF: Universal Forwarder test event 1825
splunkadmin@spl-lnx1:~$ sudo -u splunk /opt/splunkforwarder/bin/splunk add monitor /var/log/test_uf.log \
>   -index main -sourcetype test_uf -auth admin:Splunk123!
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Added monitor of '/var/log/test_uf.log'.
splunkadmin@spl-lnx1:~$ for i in {1..10}; do
>   echo "$(date '+%Y-%m-%d %H:%M:%S') TEST_MARKER_UF: Event $i from $(hostname) PID=$$ Time=$(date +%)" | sudo tee -a /var/log/test_uf.log
>   sleep 1
> done
2025-08-27 12:42:06 TEST_MARKER_UF: Event 1 from spl-lnx1 PID=1325 Time=1756298526
2025-08-27 12:42:07 TEST_MARKER_UF: Event 2 from spl-lnx1 PID=1325 Time=1756298527
2025-08-27 12:42:08 TEST_MARKER_UF: Event 3 from spl-lnx1 PID=1325 Time=1756298528
2025-08-27 12:42:09 TEST_MARKER_UF: Event 4 from spl-lnx1 PID=1325 Time=1756298529
2025-08-27 12:42:10 TEST_MARKER_UF: Event 5 from spl-lnx1 PID=1325 Time=1756298530
2025-08-27 12:42:11 TEST_MARKER_UF: Event 6 from spl-lnx1 PID=1325 Time=1756298531
2025-08-27 12:42:12 TEST_MARKER_UF: Event 7 from spl-lnx1 PID=1325 Time=1756298532
2025-08-27 12:42:13 TEST_MARKER_UF: Event 8 from spl-lnx1 PID=1325 Time=1756298533
2025-08-27 12:42:14 TEST_MARKER_UF: Event 9 from spl-lnx1 PID=1325 Time=1756298534
2025-08-27 12:42:15 TEST_MARKER_UF: Event 10 from spl-lnx1 PID=1325 Time=1756298535
splunkadmin@spl-lnx1:~$ _
```

```
splunkadmin@spl-hf1:~$ sudo lsof -i :9997 | grep spl-lnx1
[sudo] password for splunkadmin:
splunkd 41780      splunk  120u  IPv4 422380          0t0  TCP spl-hf1:9997->spl-lnx1:42808 (ESTABLISHED)
splunkadmin@spl-hf1:~$
```

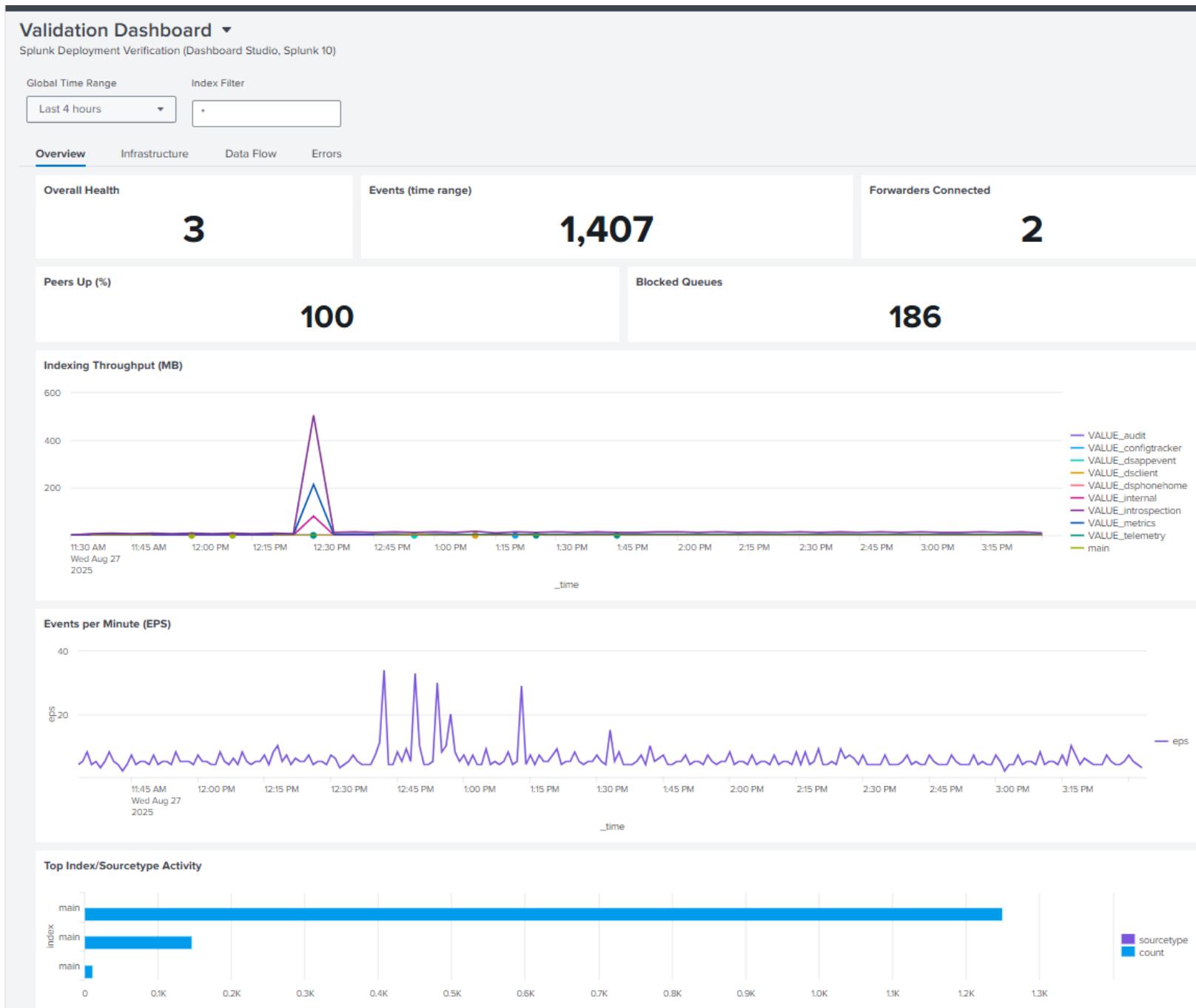
## Confirming the entire pipeline works: UF (spl-lnx1) → HF (spl-hf1) → Indexers (spl-idx1, spl-idx2) → Search Head (spl-sh1)

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** index=main DEPLOYMENT\_TEST
- Results Summary:** ✓ 2 events (8/26/25 1:00:00.000 PM to 8/27/25 1:22:27.000 PM) No Event Sampling ▾
- Event List:** Two events are listed in a table:

i	Time	Event
>	8/27/25 1:21:57:161 PM	2025-08-27T13:21:57.161836+00:00 spl-lnx1 splunkadmin: DEPLOYMENT_TEST: User login test from deployment host = spl-lnx1   source = /var/log/auth.log   sourcetype = linux_secure
>	8/27/25 1:21:53:000 PM	2025-08-27 13:21:53 DEPLOYMENT_TEST: Testing complete pipeline host = spl-lnx1   source = /var/log/syslog   sourcetype = syslog
- Side Panels:**
  - Selected Fields:** @host 1, @source 2, @sourcetype 2
  - Interesting Fields:** #date\_hour 1, #date\_mday 1, #date\_minute 1, @date\_month 1, #date\_second 2, @date\_wday 1

## Custom Built Splunk Deployment Verification Dashboard using JSON



## Validation Dashboard ▾

Splunk Deployment Verification (Dashboard Studio, Splunk 10)

Global Time Range

Index Filter

Last 4 hours

\*

Overview

**Infrastructure**

Data Flow

Errors

### Server Info

splunk_server	version	os_name	product_type
spl-mgr	10.0.0	Linux	enterprise
spl-idx1	10.0.0	Linux	enterprise
spl-idx2	10.0.0	Linux	enterprise

### Distributed Search Peers

peerName	status	build	version
spl-idx1	Up	e8eb0c4654f8	10.0.0
spl-idx2	Up	e8eb0c4654f8	10.0.0

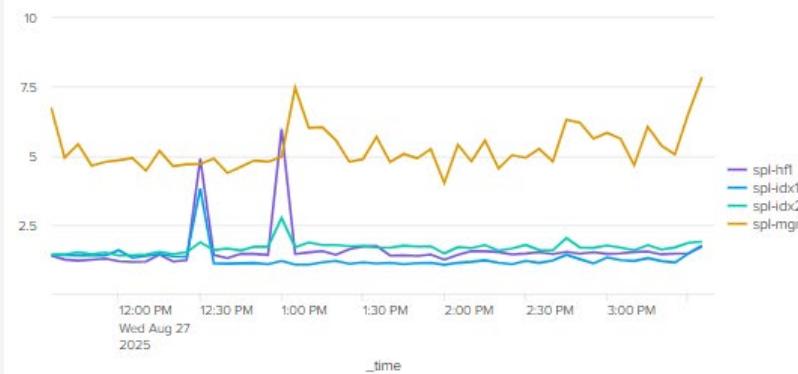
### Cluster Manager Info

mode	service_read...	indexing_rea...	replication_f...	search_factor
	1	1		

### Indexer Cluster Peers

label	status	buckets_db	consistent
spl-idx2	Up		
spl-idx1	Up		

### CPU %, by Host (\_introspection)



### Memory %, by Host (\_introspection)



### Deployment Clients

0

### HEC Tokens (enabled/total)

0

## Validation Dashboard ▾

Splunk Deployment Verification (Dashboard Studio, Splunk 10)

Global Time Range

Last 4 hours

Index Filter

\*

Overview

Infrastructure

**Data Flow**

Errors

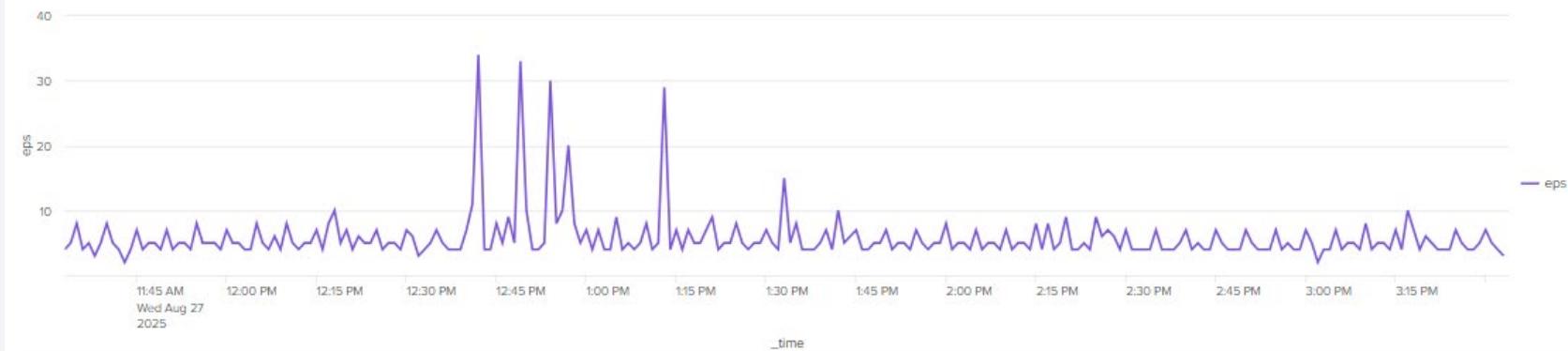
### Forwarder Connections (eps, KBps)

sourceHost	KBps	eps
192.168.221.30	16.78	11.97
192.168.221.51	0.17	0.88

### Test Marker Events

test_type	sourcetype	host	count
HF	test_hf	spl-hf1	11

### Events / 1m for \*



## **AWS - Cloud Security & Vulnerability Management Portfolio**

### **Phase 1: Security Foundation**

**IAM & Access Control** - Implemented multi-factor authentication with Duo, created IAM user 'portfolio-admin' with AdministratorAccess policy via security group, enforced password complexity requiring uppercase, lowercase, numbers, and symbols.

**Audit & Monitoring** - Deployed CloudTrail named 'portfolio-audit-trail' with multi-region coverage, KMS encryption enabled, capturing all management events while excluding data events for cost optimization.

**Budget Controls** - Created \$5 monthly budget with 80% threshold alerts to maintain cost awareness throughout testing.

### **Phase 2: Infrastructure with Intentional Vulnerabilities**

**VPC Architecture** - Built 'portfolio-vpc' (10.0.0.0/16) with 2 public and 2 private subnets across availability zones, configured route tables and internet gateway.

**S3 Bucket Issues** - Created 'portfolio-test-bucket-918689' with deliberate misconfigurations: public access allowed, no encryption, no versioning, missing SSL-only policy.

**EC2 Security Gaps** - Deployed 'portfolio-web-server' (t2.micro) with vulnerable security group 'portfolio-web-sg' having SSH open to 0.0.0.0/0, unencrypted EBS volumes.

### **Phase 3: Detection & Compliance**

**AWS Config** - Configured 10 compliance rules, detected 6 non-compliant resources including public S3, missing encryption, open SSH, achieving initial 40% compliance score.

**S3 Remediation** - Blocked all public access settings, enabled SSE-S3 encryption, activated versioning, implemented SSL-only bucket policy, achieved 90% compliance in <30 minutes.

**Security Group Fixes** - Restricted SSH from 0.0.0.0/0 to specific IP only, removed unnecessary ICMP rules, enabled EBS encryption by default for future volumes.

### **Phase 4: Incident Response & Automation**

**Compromised Key Simulation** - Created 'test-developer' IAM user, simulated unauthorized API calls, detected activity via CloudTrail within 5 minutes, disabled compromised keys.

**Lambda Auto-Remediation** - Built Python function 'S3SecurityAutoFix' that automatically enables encryption and versioning on non-compliant buckets, tested successful execution.

**EKS Deployment** - Installed eksctl in CloudShell, created 'portfolio-cluster' with proper IAM roles (ClusterRole and NodeRole), verified kubectl connectivity.

### **Phase 5: Advanced Security Tools**

**Amazon Inspector** - Activated scanning, created Ubuntu instance 'i-0887dfece8721dded', detected 101 package vulnerabilities including CVE-2025-21919 (CVSS 7.8) with no available patch.

**Zero-Day Management** - Verified patch unavailable ("work in progress" per Ubuntu), implemented compensating controls, terminated vulnerable instance as risk mitigation.

**Amazon GuardDuty** - Enabled threat detection (detector ID: 7eccb8b03cff3a081bf7dc7204c9a55c), generated sample findings including cryptocurrency mining and SSH brute force attacks.

## Add multifactor authentication using the DUO APP

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and a search bar. The main area has a blue banner at the top stating 'New access analyzers available' with the subtext 'Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization'. Below this is the 'IAM Dashboard' section with 'Security recommendations' (0). It lists two items: 'Root user has MFA' (Having multi-factor authentication (MFA) for the root user improves security for this account) and 'Root user has no active access keys' (Using access keys attached to an IAM user instead of the root user improves security).

## Create a budget

The screenshot shows the 'Create budget' page in the AWS Billing and Cost Management section. The left sidebar includes 'Billing and Cost Management', 'Choose billing view New', 'Primary view', 'Home', 'Getting Started', 'Dashboards New', 'Billing and Payments', 'Bills', 'Payments', 'Credits', 'Purchase Orders', 'Cost and Usage Analysis', 'Cost Explorer', 'Cost Explorer Saved Reports', 'Cost Anomaly Detection', 'Free Tier', 'Data Exports', 'Customer Carbon Footprint Tool', 'Cost Organization', 'Cost Categories', 'Cost Allocation Tags', 'Billing Conductor', 'Budgets and Planning', 'Budgets New', 'Budgets Reports', and 'Pricing Calculator New'. The main form is titled 'Choose budget type' with 'Budget setup' options: 'Use a template (simplified)' (selected), 'Customize (advanced)', and 'Billing View' (based on selected billing view). It also includes sections for 'Templates - new' (with 'Zero spend budget', 'Daily Savings Plans coverage budget', 'Monthly cost budget' (selected), and 'Daily reservation utilization budget'), 'Monthly cost budget - Template' (with 'Budget name' set to 'My Monthly Cost Budget' and 'Enter your budgeted amount (\$)' set to '5.00'), and 'Email recipients' (set to 'tevin.agtarap@arlut.utexas.edu').

For this portfolio lab, I used AWS's AdministratorAccess managed policy to ensure full access for security testing and configuration. In production, I would implement least-privilege custom policies based on actual job functions.

The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' wizard. A green success message at the top says 'Administrators user group created.' On the left, a vertical navigation bar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). Step 3 is highlighted with a blue circle. The main area shows 'User details' for a user named 'portfolio-admin'. It includes fields for 'Console password type' (Autogenerated) and 'Require password reset' (Yes). Below this is a 'Permissions summary' table:

Name	Type	Used as
Administrators	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

There is also a 'Tags - optional' section with an 'Add new tag' button. At the bottom right are 'Cancel', 'Previous', and a large orange 'Create user' button.

After account creation verify user is prompted for new password

The screenshot shows the AWS password change prompt. It displays the AWS account number '918689941708' and the IAM user name 'portfolio-admin'. It includes fields for 'Old password', 'New password', and 'Retype new password', all containing placeholder dots. A large blue 'Confirm password change' button is at the bottom. Below it is a link 'Sign in using root user email'. At the very bottom are language selection ('English') and legal links ('Terms of Use', 'Privacy Policy').

## Update AWS Password Security Policy to reflect industry standards

The screenshot shows the 'Edit password policy' section of the AWS IAM Account Settings. The 'Custom' option is selected, applying customized password requirements. The policy includes a minimum length of 14 characters (needs to be between 6 and 128), requiring at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character. Other requirements include turning on password expiration (90 days, needs to be between 1 and 1095 days), allowing users to change their own password, and preventing password reuse (remember 5 password(s), needs to be between 1 and 24). Buttons for 'Cancel' and 'Save changes' are at the bottom.

**Custom**  
Apply customized password requirements.

**Password minimum length.**  
Enforce a minimum length of characters.  
14 characters  
Needs to be between 6 and 128.

**Password strength**

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } | ' )

**Other requirements**

- Turn on password expiration  
Expire password in 90 day(s)  
Needs to be between 1 and 1095 days.
- Password expiration requires administrator reset
- Allow users to change their own password
- Prevent password reuse  
Remember 5 password(s)  
Needs to be between 1 and 24.

**Cancel** **Save changes**

## Create AWS CloudTrail - Complete audit log of all API calls - Evidence of security monitoring - Compliance with best practices

The screenshot shows the AWS CloudTrail landing page under Management & Governance. It features a call-to-action to 'Create a trail with AWS CloudTrail' and a brief description of its purpose: 'Continuously log your AWS account activity'. Below this, there's a diagram titled 'How it works' showing the process: Capture (record activity in AWS services as AWS CloudTrail events), Store (AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs), Act (use Amazon CloudWatch Alarms and Events to take action when important events are detected), and Review (view recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena). There are also sections for 'Pricing', 'Getting started', and 'More resources'.

**Create a trail with AWS CloudTrail**  
Get started with AWS CloudTrail by creating a trail to log your AWS account activity.  
**Create a trail**

**How it works**

- Capture**  
Record activity in AWS services as AWS CloudTrail events
- Store**  
AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs
- Act**  
Use Amazon CloudWatch Alarms and Events to take action when important events are detected
- Review**  
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena

**Pricing**

**Getting started**

**More resources**

For my portfolio, I configured CloudTrail to capture all management events while optimizing costs by excluding data events. This provides complete visibility into configuration changes and user activities without incurring charges. In production, I would selectively enable data events for sensitive buckets based on data classification.

**Step 1 Choose trail attributes**

**Step 2 Choose log events** (Selected)

**Step 3 Review and create**

### Choose log events

**Events** Info  
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

**Event type**  
Choose the type of events that you want to log.

**Management events**  
Capture management operations performed on your AWS resources.

**Data events**  
Log the resource operations performed on or within a resource.

**Insights events**  
Identify unusual activity, errors, or user behavior in your account.

**Network activity events**  
Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

**Management events** Info  
Management events show information about management operations performed on resources in your AWS account.

ⓘ No additional charges apply to log management events on this trail because this is your first copy of management events.

**API activity**  
Choose the activities you want to log.

**Read**

**Write**

Exclude AWS KMS events

Exclude Amazon RDS Data API events

[Cancel](#) [Previous](#) [Next](#)

## CloudTrail up and running and monitoring logs

**Event history (9) Info**  
Event history shows you the last 90 days of management events.

**Lookup attributes**

Read-only	Event name	Event time	User name	Event source	Resource type	Resource name
<input type="checkbox"/>	<a href="#">PutEventSelectors</a>	September 18, 2025, 14:22:10 (...)	portfolio-admin	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-2:918689941708:trail/portfolio-audit-trail
<input type="checkbox"/>	<a href="#">StartLogging</a>	September 18, 2025, 14:22:10 (...)	portfolio-admin	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-2:918689941708:trail/portfolio-audit-trail
<input type="checkbox"/>	<a href="#">CreateAlias</a>	September 18, 2025, 14:22:10 (...)	portfolio-admin	kms.amazonaws.com	AWS::KMS::Key, AWS::K...	arn:aws:kms:us-east-2:918689941708:key/a11c6e6b-60fd-4fef-af56-cf9fbafc68b8, a11c6e6b-60fd-4fef-af56-cf9fbafc...
<input type="checkbox"/>	<a href="#">CreateKey</a>	September 18, 2025, 14:22:10 (...)	portfolio-admin	kms.amazonaws.com	AWS::KMS::Key, AWS::K...	arn:aws:kms:us-east-2:918689941708:key/a11c6e6b-60fd-4fef-af56-cf9fbafc68b8, a11c6e6b-60fd-4fef-af56-cf9fbafc...
<input type="checkbox"/>	<a href="#">CreateTrail</a>	September 18, 2025, 14:22:10 (...)	portfolio-admin	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail, ...	arn:aws:cloudtrail:us-east-2:918689941708:trail/portfolio-audit-trail, portfolio-audit-trail, aws-cloudtrail-logs-9186899...
<input type="checkbox"/>	<a href="#">PutBucketPolicy</a>	September 18, 2025, 14:22:09 (...)	portfolio-admin	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-918689941708-c270cf86
<input type="checkbox"/>	<a href="#">CreateBucket</a>	September 18, 2025, 14:22:09 (...)	portfolio-admin	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-918689941708-c270cf86
<input type="checkbox"/>	<a href="#">PutBucketEncryption</a>	September 18, 2025, 14:22:09 (...)	portfolio-admin	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-918689941708-c270cf86
<input type="checkbox"/>	<a href="#">ConsoleLogin</a>	September 18, 2025, 13:55:34 (...)	portfolio-admin	signin.amazonaws.com	-	-

[Filter by date and time](#) [Clear filter](#)

## AWS Infrastructure Setup – Create VPC

**Create VPC Info**

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

**VPC settings**

**Resources to create** [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

VPC only  VPC and more

**Name tag auto-generation** [Info](#)  
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate  
portfolio-vpc

**IPv4 CIDR block** [Info](#)  
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

**IPv6 CIDR block** [Info](#)  
 No IPv6 CIDR block  Amazon-provided IPv6 CIDR block

**Tenancy** [Info](#)  
Default

**Number of Availability Zones (AZs)** [Info](#)  
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.  
1 **2** 3

**Customize AZs**

**Preview**

**VPC Show details**  
Your AWS virtual network  
portfolio-vpc

**Subnets (4)**  
Subnets within this VPC

- us-east-2a
  - portfolio-vpc-subnet-public1-us-east-2a
  - portfolio-vpc-subnet-private1-us-east-2a
- us-east-2b
  - portfolio-vpc-subnet-public2-us-east-2b
  - portfolio-vpc-subnet-private2-us-east-2b

**Route tables (3)**  
Route network traffic to resources

- portfolio-vpc-rtb-public
- portfolio-vpc-rtb-private1-us-east-2a
- portfolio-vpc-rtb-private2-us-east-2b

**vpc-02d0a11cd2dabebf6 / portfolio-vpc-vpc**

**Details** [Info](#)

<b>VPC ID</b> vpc-02d0a11cd2dabebf6	<b>State</b> Available	<b>Block Public Access</b> Off	<b>DNS hostnames</b> Enabled
<b>DNS resolution</b> Enabled	<b>Tenancy</b> default	<b>DHCP option set</b> dopt-060ca8da11caeefc7	<b>Main route table</b> rtb-075210d562b400f67
<b>Main network ACL</b> acl-0007463d77c8cd7d	<b>Default VPC</b> No	<b>IPv4 CIDR</b> 10.0.0.0/16	<b>IPv6 pool</b> –
<b>IPv6 CIDR</b> –	<b>Network Address Usage metrics</b> Disabled	<b>Route 53 Resolver DNS Firewall rule groups</b> –	<b>Owner ID</b> 918689941708

**Resource map** [Info](#)

**VPC**  
Your AWS virtual network  
portfolio-vpc-vpc  
10.0.0.0/16  
No IPv6

**Subnets (4)**  
Subnets within this VPC

- us-east-2a
  - portfolio-vpc-subnet-public1-us-east-2a  
10.0.0.0/20  
No IPv6
  - portfolio-vpc-subnet-private1-us-east-2a  
10.0.128.0/20  
No IPv6
- us-east-2b
  - portfolio-vpc-subnet-public2-us-east-2b  
10.0.16.0/20  
No IPv6
  - portfolio-vpc-subnet-private2-us-east-2b  
10.0.144.0/20  
No IPv6

**Route tables (4)**  
Route network traffic to resources

- portfolio-vpc-rtb-private1-us-east-2a
  - 1 subnet association  
2 routes including local
- portfolio-vpc-rtb-private2-us-east-2b
  - 1 subnet association  
2 routes including local
- rtb-075210d562b400f67
  - No subnet associations  
1 route including local
- portfolio-vpc-rtb-public
  - 2 subnet associations  
2 routes including local

**Network Connections (2)**  
Connections to other networks

- portfolio-vpc-igw
  - Internet routes to 2 public subnets  
0 private subnets route to the Internet
- portfolio-vpc-s3
  - Gateway endpoint to S3

## Create S3 Bucket with Security Issues! – Build with deliberate security problems that our scanning tools will detect and that I will remediate.

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The steps are as follows:

- General configuration**:
  - AWS Region**: US East (Ohio) us-east-2
  - Bucket type**: General purpose (selected)
  - Bucket name**: portfolio-test-bucket
  - Copy settings from existing bucket - optional**: Only the bucket settings in the following configuration are copied. A 'Choose bucket' button is present.
- Object Ownership**:
  - ACLs disabled (recommended)**: All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
  - ACLs enabled**: Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
- Block Public Access settings for this bucket**:
  - Block all public access**: This option is checked.
  - Turning off block all public access might result in this bucket and the objects within becoming public**: A warning message states: "AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting." A checkbox is checked: "I acknowledge that the current settings might result in this bucket and the objects within becoming public."
- Bucket Versioning**:
  - Disable** (selected)
- Tags - optional (0)**: No tags are associated with this bucket.
- Default encryption**:
  - Encryption type**: Server-side encryption with Amazon S3 managed keys (SSE-S3) (selected)
  - Bucket Key**: Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS.

## Create EC2 Instance with Security Issues! -

Screenshot of the AWS EC2 Instances page showing the creation of a new instance.

The top navigation bar includes links for "About upgrading to...", "How to upgrade Spl...", "Online Courses - Le...", "Updates for SS", "SPLunk.conf", "Search", "[Alt+S]", "All Bookmarks", "United States (Ohio)", "Account ID: 9186-8994-1708", and "portfolio-admin".

The left sidebar menu shows:

- EC2
- Dashboard
- EC2 Global View
- Events
- Instances
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
- Images
  - AMIs
  - AMI Catalog
- Elastic Block Store
  - Volumes
  - Snapshots
  - Lifecycle Manager
- Network & Security

The main content area displays the "Amazon Elastic Compute Cloud (EC2)" landing page with the heading "Create, manage, and monitor virtual servers in the cloud." It highlights "Benefits and features" such as ultimate scalability and control, and lists operating systems available: Linux, Windows, and macOS. A "Launch a virtual server" button is prominent.

The bottom section shows the "Launch an instance" wizard:

- Step 1: "Name and tags" (Info) - Name: portfolio-web-server, Add additional tags.
- Step 2: "Application and OS Images (Amazon Machine Image)" (Info) - Search bar: "Search our full catalog including 1000s of application and OS images".
- Step 3: "Quick Start" - Shows icons for Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian.
- Step 4: "Amazon Machine Image (AMI)" - Selected: "Amazon Linux 2023 kernel-6.1 AMI" (ami-0ca4d5db4872d0c28). Details: 64-bit (x86), uefi-preferred, ami-0dd755127cac9e36 (64-bit (Arm), uefi). Virtualization: hvm, ENA enabled: true, Root device type: ebs. Status: Free tier eligible.
- Step 5: "Description" - Text: "Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications."
- Step 6: "Architecture", "Boot mode", "AMI ID", "Publish Date", "Username", and "Verified provider" fields.

On the right side, there are "Additional actions" (View running instances, Migrate a server), "Pricing (US)" (EC2 pricing options, Use the AWS pricing calculator), and a "Summary" section showing 1 instance, Software Image (AMI) details, Virtual server type (t3.micro), Firewall (New security group), Storage (1 volume(s) - 8 GiB), and Launch/Preview code buttons.

## Generate key pair

Create key pair

**Key pair name**  
Key pairs allow you to connect to your instance securely.  
  
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**  
 RSA  
RSA encrypted private and public key pair  
 ED25519  
ED25519 encrypted private and public key pair

**Private key file format**  
 .pem  
For use with OpenSSH  
 .ppk  
For use with PuTTY

**When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance.** [Learn more](#)

**Create key pair**

## Network settings - BAD! INTENTIONAL TO SCAN/FIX

**Network settings** [Info](#)

**VPC - required** [Info](#)  
vpc-02d0a11cd2dabebf6 (portfolio-vpc-vpc) [Edit](#)

**Subnet** [Info](#)  
subnet-0249aa1503bec0e2 portfolio-vpc-subnet-private2-us-east-2b  
VPC: vpc-02d0a11cd2dabebf6 Owner: 918689941708 Availability Zone: us-east-2b (use2-az2)  
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.144.0/20

**Auto-assign public IP** [Info](#)  
Enable

**Firewall (security groups)** [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group  Select existing security group

**Security group name - required**  
portfolio-web-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_~!@#\$%^&\*()

**Description - required** [Info](#)  
Intentionally insecure for testing

**Inbound Security Group Rule**

**Security group rule 1 (TCP, 22, 0.0.0.0/0, BAD! INTENTIONAL TO SCAN/FIX)**

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	<input type="text" value="Add CIDR, prefix list or security group"/>	BAD! INTENTIONAL TO SCAN/FIX
0.0.0.0/0		

**Remove**

**Security group rule 2 (TCP, 80, 0.0.0.0/0, BAD! INTENTIONAL TO SCAN/FIX)**

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
HTTP	TCP	80
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	<input type="text" value="Add CIDR, prefix list or security group"/>	BAD! INTENTIONAL TO SCAN/FIX
0.0.0.0/0		

**Remove**

**Security group rule 3 (TCP, 443, 0.0.0.0/0, BAD! INTENTIONAL TO SCAN/FIX)**

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
HTTPS	TCP	443
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	<input type="text" value="Add CIDR, prefix list or security group"/>	BAD! INTENTIONAL TO SCAN/FIX
0.0.0.0/0		

**Remove**

**Security group rule 4 (ICMP, All, 0.0.0.0/0, BAD! INTENTIONAL TO SCAN/FIX)**

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
All ICMP - IPv4	ICMP	All
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	<input type="text" value="Add CIDR, prefix list or security group"/>	BAD! INTENTIONAL TO SCAN/FIX
0.0.0.0/0		

**Add security group rule**

**Advanced network configuration**

## Detect infrastructure issues via AWS Config

AWS Search [Alt+S]

AWS Config > Set up AWS Config

Step 1 Settings

Step 2 Rules

Step 3 Review

### Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

#### Recording method

Recording strategy	Default recording frequency
Record all resource types with customizable overrides	Continuous

▶ Resource types with override settings (4)

▶ Resource types with default settings (400)

#### Delivery method

S3 bucket name  
config-bucket-918689941708

▼ AWS Config rules (10)

- cloudtrail-s3-bucket-public-access-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-server-side-encryption-enabled
- s3-bucket-versioning-enabled
- s3-bucket-ssl-requests-only
- restricted-ssh
- restricted-common-ports
- ec2-security-group-attached-to-eni-periodic
- encrypted-volumes
- ec2-ebs-encryption-by-default

Cancel Previous Confirm

## AWS Config found our Noncompliant resources

[AWS Config](#) > Rules

### Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules					
Filter by compliance status					
All					
Name	Remediation action	Type	Enabled evaluation mode	Detective compliance	
cloudtrail-s3-bucket-public-access-prohibited	Not set	AWS managed	DETECTIVE	Compliant	
ec2-ebs-encryption-by-default	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
ec2-security-group-attached-to-eni-periodic	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
encrypted-volumes	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
restricted-common-ports	Not set	AWS managed	DETECTIVE	Compliant	
restricted-ssh	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
s3-bucket-public-write-prohibited	Not set	AWS managed	DETECTIVE	Compliant	
s3-bucket-server-side-encryption-enabled	Not set	AWS managed	DETECTIVE	Compliant	
s3-bucket-ssl-requests-only	Not set	AWS managed	DETECTIVE	3 Noncompliant resource(s)	
s3-bucket-versioning-enabled	Not set	AWS managed	DETECTIVE	3 Noncompliant resource(s)	

### Time to remediate!

[EC2](#) > [Security Groups](#) > [sg-0e2af90cd92470a52 - portfolio-web-sg](#) > Edit inbound rules

#### Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

##### Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	
sgr-070b1c7618accba7d	HTTPS	TCP	443	Custom	Q 0.0.0.0/0 X BAD! INTENTIONAL TO SCAN/FIX	<button>Delete</button>
sgr-02e53426d4f5ecf1d	SSH	TCP	22	Custom	Q 0.0.0.0/0 X BAD! INTENTIONAL TO SCAN/FIX	<button>Delete</button>
sgr-0e791a017e64f6ce4	All ICMP - IPv4	ICMP	All	Custom	Q 0.0.0.0/0 X BAD! INTENTIONAL TO SCAN/FIX	<button>Delete</button>
sgr-05f9c14b4e0742ae4	HTTP	TCP	80	Custom	Q 0.0.0.0/0 X BAD! INTENTIONAL TO SCAN/FIX	<button>Delete</button>

[Add rule](#)

⚠️ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#)

[Preview changes](#)

[Save rules](#)

## Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

**Inbound rules Info**

Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	Delete	
sgr-070b1c7618acca7d	HTTPS	TCP	443	Custom	Q 0.0.0.0/0 X	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-02e53426d4f5ecf1d	SSH	TCP	22	My IP	Q 146.6.208.24/32 X	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-05f9c14b4c0742ae4	HTTP	TCP	80	Custom	Q 0.0.0.0/0 X	BAD! INTENTIONAL TO SCAN/FIX	Delete

**Add rule**

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

X

Cancel Preview changes **Save rules**

## Edit Block public access (bucket settings) Info

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

**Block public access to buckets and objects granted through new access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

**Block public access to buckets and objects granted through any access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

**Block public access to buckets and objects granted through new public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

**Block public and cross-account access to buckets and objects through any public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

**Save changes**

**Issues Remediated now let's Re-evaluate rules.**

AWS Config > Rules

## Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules					
<input type="button" value="View details"/> <input type="button" value="Edit rule"/> <input type="button" value="Actions ▾"/> <input type="button" value="Add rule"/>					
<input type="button" value="Filter by compliance status"/> <input type="button" value="All"/>					
Name	Remediation action	Type	Enabled evaluation mode	Detective compliance	
cloudtrail-s3-bucket-public-access-prohibited	Not set	AWS managed	DETECTIVE	Compliant	
ec2-cbs-encryption-by-default	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
<b>ec2-security-group-attached-to-eni-periodic</b>	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
encrypted-volumes	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)	
restricted-common-ports	Not set	AWS managed	DETECTIVE	Compliant	
restricted-ssh	Not set	AWS managed	DETECTIVE	Compliant	
s3-bucket-public-write-prohibited	Not set	AWS managed	DETECTIVE	Compliant	
s3-bucket-server-side-encryption-enabled	Not set	AWS managed	DETECTIVE	Compliant	
s3-bucket-ssl-requests-only	Not set	AWS managed	DETECTIVE	3 Noncompliant resource(s)	
s3-bucket-versioning-enabled	Not set	AWS managed	DETECTIVE	3 Noncompliant resource(s)	

**portfolio-test-bucket-123456** [Info](#)

Objects | Metadata | **Properties** | Permissions | Metrics | Management | Access Points

### Bucket overview

AWS Region US East (Ohio) us-east-2	Amazon Resource Name (ARN) arn:aws:s3:::portfolio-test-bucket-123456	Creation date September 19, 2025, 07:23:47 (UTC-05:00)
----------------------------------------	-------------------------------------------------------------------------	-----------------------------------------------------------

### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**  
Enabled

**Multi-factor authentication (MFA) delete**  
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

## Fix S3 SSL Requests Only

### Edit bucket policy [Info](#)

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

**Bucket ARN**  
[arn:aws:s3:::portfolio-test-bucket-123456](#)

**Policy**

```
1▼ {
2  "Version": "2012-10-17",
3  "Statement": [
4    {
5      "Sid": "DenyInsecureConnections",
6      "Effect": "Deny",
7      "Principal": "*",
8      "Action": "s3:*",
9      "Resource": [
10        "arn:aws:s3:::portfolio-test-bucket-123456/*",
11        "arn:aws:s3:::portfolio-test-bucket-123456"
12      ],
13      "Condition": {
14        "Bool": {
15          "aws:SecureTransport": "false"
16        }
17      }
18    ]
19  ]
20 }
```

[+ Add new statement](#)

JSON Ln 11, Col 50

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

[Preview external access](#)

[Edit statement](#) [Remove](#)

**Add actions**

Choose a service

Included S3

Available AI Operations AMP API Gateway API Gateway V2 ARC Region switch ARC Zonal Shift ASC

Add a resource [Add](#)

Add a condition (optional) [Add](#)

[Cancel](#) [Save changes](#)

## Fix EBS Encryption Default

### EBS encryption Info

Manage the default encryption option of all new EBS volumes and copies of snapshots created in your account.

**Always encrypt new EBS volumes**  
Enables encryption by default for newly created EBS volumes and snapshots.  
 Enable

**Default encryption key**  
Specify the master key to encrypt your volumes.  
arn:aws:kms:us-east-2:918689941708:key/1f1500c4-92bc-49f5-b773-5ef9f42485e8

(i) The settings above only apply to the United States (Ohio) region. Choose another region to change the settings for that region. You can only launch instance types that support EBS encryption once you enable account level encryption. [Learn more about supported instance types.](#)

All Noncompliant resources fix on our bucket. The 2 Noncompliant are on the buckets AWS provides. All resources remediated!

### Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules					
Filter by compliance status					
	Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
<input type="radio"/>	cloudtrail-s3-bucket-public-access-prohibited	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	ec2-ebs-encryption-by-default	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	ec2-security-group-attached-to-eni-periodic	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	restricted-common-ports	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	restricted-ssh	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	s3-bucket-public-write-prohibited	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	s3-bucket-server-side-encryption-enabled	Not set	AWS managed	DETECTIVE	<span>Compliant</span>
<input type="radio"/>	s3-bucket-ssl-requests-only	Not set	AWS managed	DETECTIVE	<span>2 Noncompliant resource(s)</span>
<input type="radio"/>	s3-bucket-versioning-enabled	Not set	AWS managed	DETECTIVE	<span>2 Noncompliant resource(s)</span>

## Incident Response Simulation - Compromised IAM Access Keys

Let's create a test IAM user with access keys that we'll "compromise"!

The screenshot shows the AWS IAM User Details page for a user named 'test-developer'. The left sidebar shows navigation options like Identity and Access Management (IAM), Access management, and Access reports. The main content area displays the user's summary, security credentials (with one active access key listed), console sign-in details, multi-factor authentication (MFA) status (0 devices assigned), and access keys (1 key listed). The access key is described as 'Never used. Created today.' and has a 'Create access key' button.

**Summary**

- ARN: arn:aws:iam::918689941708:user/test-developer
- Console access: Disabled
- Created: September 19, 2025, 10:40 (UTC-05:00)
- Last console sign-in: -

**Security credentials**

- Access key 1: AKIASLZRQBDGEVXREMVD - Active (Never used. Created today.)
- Access key 2: Create access key

**Console sign-in**

- Console sign-in link: https://918689941708.signin.aws.amazon.com/console
- Console password: Not enabled

**Multi-factor authentication (MFA) (0)**

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

[Assign MFA device](#)

**Access keys (1)**

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

AKIASLZRQBDGEVXREMVD	Description	Status	Actions
AKIASLZRQBDGEVXREMVD			<a href="#">Actions</a>

## Simulate Attack – Configure compromised credentials via CloudShell

```
CloudShell
us-east-2 + 

~ $ aws configure --profile compromised
AWS Access Key ID [None]: AKIASLZRQBDGEVXREMVD
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-2
Default output format [None]: json
~ $ 

2025-09-19 15:16:45 portfolio-test-bucket-123456
~ $ aws s3 ls s3://portfolio-test-bucket-123456 --profile compromised
~ $ aws iam list-users --profile compromised

An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::918689941708:user/test-developer is not authorized to perform: iam>ListUsers on resource: arn:aws:iam::918689941708:user/ because no identity-based policy allows the iam>ListUsers action
~ $ aws iam get-user --profile compromised

An error occurred (AccessDenied) when calling the GetUser operation: User: arn:aws:iam::918689941708:user/test-developer is not authorized to perform: iam GetUser on resource: user test-developer because no identity-based policy allows the iam GetUser action
~ $ aws ec2 describe-instances --profile compromised

An error occurred (UnauthorizedOperation) when calling the DescribeInstances operation: You are not authorized to perform this operation. User: arn:aws:iam::918689941708:user/test-developer is not authorized to perform: ec2DescribeInstances because no identity-based policy allows the ec2DescribeInstances action
~ $ 
~ $ 
```

Now let's investigate simulated attack via CloudTrail!

Event history (2) <span style="color: #0070C0;">Info</span>						
Event history shows you the last 90 days of management events.						
Lookup attributes						
User name	Event name	Event time	User name	Event source	Resource type	Resource name
	<a href="#">DescribelInstances</a>	September 19, 2025, 11:06:57 ...	test-developer	ec2.amazonaws.com	-	-
	<a href="#">ListBuckets</a>	September 19, 2025, 11:06:26 ...	test-developer	s3.amazonaws.com	-	-

We found user test-developer actions via CloudTrail – We will now remove compromised key!

```
~ $ aws iam update-access-key \
>   --access-key-id AKIASLZRQBDGEVXREMVD \
>   --status Inactive \
>   --user-name test-developer
~ $ 
~ $ echo '/> Key disabled at $(date)'
✓ Key disabled at Fri Sep 19 04:15:48 PM UTC 2025
~ $ aws iam list-access-keys --user-name test-developer
{
  "AccessKeyMetadata": [
    {
      "UserName": "test-developer",
      "AccessKeyId": "AKIASLZRQBDGEVXREMVD",
      "Status": "Inactive",
      "CreateDate": "2025-09-19T15:49:43+00:00"
    }
  ]
~ $ aws s3 ls --profile compromised

An error occurred (InvalidAccessKeyId) when calling the ListBuckets operation: The AWS Access Key Id you provided does not exist in our records.
~ $ 
```

## Lambda Security Automation

The screenshot shows the AWS Lambda 'Get started' page. It features a dark header with the AWS logo and 'Compute' text. Below the header, there's a main section with the heading 'AWS Lambda' and the subtext 'lets you run code without thinking about servers.' A note below states: 'You pay only for the compute time that you consume — there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration.' To the right, a 'Get started' callout box contains the text 'Author a Lambda function from scratch, or choose from one of many preconfigured examples.' with a 'Create a function' button.

The screenshot shows the 'How it works' page. It has a navigation bar with tabs for '.NET', 'Java', 'Node.js' (selected), 'Python', 'Ruby', and 'Custom runtime'. Below the tabs is a code editor with a simple Node.js function:

```
1 exports.handler = async (event) => {
2   console.log(event);
3   return 'Hello from Lambda!';
4 };
5
```

Below the code editor, a 'Run' button and a link 'Next: Lambda responds to events' are visible. A note at the bottom says 'Just write the code' and 'Above is a simple Lambda function. Click "Run" to see function output before going to the next step.'

## Add Auto-Remediation Code

The screenshot shows the AWS Lambda code editor interface. On the left, the 'EXPLORER' sidebar shows a project named 'PORTFOLIO-SECURITY-AUTOREMEDIATOR' containing a file 'lambda\_function.py'. The main area displays the code for this file:

```
1 import boto3
2 import json
3 import logging
4 from botocore.exceptions import ClientError
5
6 logger = logging.getLogger()
7 logger.setLevel(logging.INFO)
8
9 def lambda_handler(event, context):
10     """
11     Auto-remediates multiple S3 security issues
12     Portfolio demonstration of security automation
13     """
14
15     s3 = boto3.client('s3')
16
17     results = {
18         'buckets_checked': 0,
19         'encryption_fixed': 0,
20         'versioning_fixed': 0,
21         'already_compliant': 0
22     }
23
24     try:
25         # Get list of all buckets
26         buckets = s3.list_buckets()
27     
```

The interface includes tabs for 'PROBLEMS', 'OUTPUT', 'CODE REFERENCE LOG', and 'TERMINAL'. At the bottom, it shows 'Request ID: 0ed17d01-7a3a-4365-96af-63cb8eb10916' and various status indicators like 'Ln 108, Col 10' and 'Layout: US'.

## Create policy via policy editor

### Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual

```
1▼ {
2    "Version": "2012-10-17",
3    "Statement": [
4        {
5            "Effect": "Allow",
6            "Action": [
7                "s3:PutEncryptionConfiguration",
8                "s3:PutBucketVersioning",
9                "s3:PutBucketPublicAccessBlock",
10               "s3:GetEncryptionConfiguration",
11               "s3:GetBucketVersioning",
12               "s3>ListBucket",
13               "s3>ListAllMyBuckets",
14               "ec2:DescribeSecurityGroups",
15               "ec2:AuthorizeSecurityGroupIngress",
16               "ec2:RevokeSecurityGroupIngress",
17               "logs>CreateLogGroup",
18               "logs>CreateLogStream",
19               "logs>PutLogEvents"
20           ],
21           "Resource": "*"
22       }
23   ]
24 }
```

+ Add new statement

JSON Ln 7, Col 14

## Run test

**Code source** [Info](#)

[Open in Visual Studio Code](#) [Upload from](#) [...](#)

EXPLORER PORTFOLIO-SECURITY-AUTOREMEDIATOR lambda\_function.py

lambda\_function.py

```
1 import boto3
```

PROBLEMS OUTPUT CODE REFERENCE LOG TERMINAL

Status: Succeeded  
Test Event Name: TestRemediation

Response:

```
{
    "statusCode": 200,
    "body": "{\"buckets_checked\": 3, \"encryption_fixed\": 0, \"versioning_fixed\": 0, \"already_compliant\": 1}"
}
```

Function Logs:

```
START RequestId: 0ed17d01-7a3a-4365-96af-63cb8eb10916 Version: $LATEST
[INFO] 2025-09-19T16:58:00.595Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Found credentials in environment variables.
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Checking bucket: aws-cloudtrail-logs-918689941708-c270cf86
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Skipping system bucket: aws-cloudtrail-logs-918689941708-c270cf86
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Checking bucket: config-bucket-918689941708
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Skipping system bucket: config-bucket-918689941708
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Checking bucket: portfolio-test-bucket-123456
[INFO] 2025-09-19T16:58:03.533Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 ✓ portfolio-test-bucket-123456 has encryption
[INFO] 2025-09-19T16:58:03.573Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 ✓ portfolio-test-bucket-123456 is fully compliant
[INFO] 2025-09-19T16:58:03.573Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Security Remediation Complete! Checked: 3 buckets. Fixed encryption: 0. Fixed versioning: 0. Already compliant: 1.
END RequestId: 0ed17d01-7a3a-4365-96af-63cb8eb10916
REPORT RequestId: 0ed17d01-7a3a-4365-96af-63cb8eb10916 Duration: 3220.09 ms Billed Duration: 3513 ms Memory Size: 128 MB Max Memory Used: 89 MB Init Duration: 292.90 ms
Request ID: 0ed17d01-7a3a-4365-96af-63cb8eb10916
```

ENVIRONMENT VARIABLES

Ln 108, Col 10 Spaces: 4 UTF-8 LF Python Lambda Layout: US

## EKS Security Portfolio Project - AWS Console & CloudShell

### Install EKS Management Tools in CloudShell

CloudShell

us-east-2 +

```
~ $ curl --silent --location "https://github.com/weaveworks/eksctl/releases/latest/download/eksctl_$(uname -s)_amd64.tar.gz" | tar xz -C /tmp
~ $ sudo mv /tmp/eksctl /usr/local/bin
~ $ eksctl version
0.214.0
~ $ curl -o kubectl https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.3/2023-11-14/bin/linux/amd64/kubectl
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total   Spent    Left  Speed
100 47.5M  100 47.5M    0     0  36.9M    0  0:00:01  0:00:01  --:-- 36.9M
~ $ chmod +x ./kubectl
~ $ sudo mv kubectl /usr/local/bin
~ $ kubectl version --client
Client Version: v1.28.3-eks-e71965b
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3
~ $
```

### Create Cluster and new NodeRole and ClusterRole!

Roles (7) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

<input type="checkbox"/>	Role name	▲ Trusted entities	Last activity	▼
<input type="checkbox"/>	<a href="#">AmazonEKSAutoClusterRole</a>	AWS Service: eks	-	
<input type="checkbox"/>	<a href="#">AmazonEKSAutoNodeRole</a>	AWS Service: ec2	-	

## Configure cluster

### Configuration options - new [Info](#)

Choose how you would like to configure the cluster.

Quick configuration (with EKS Auto Mode) - [new](#) [Info](#)

Quickly create a cluster with production-grade default settings. The configuration uses EKS Auto Mode to automate infrastructure tasks like creating nodes and provisioning storage.

Custom configuration

To change default settings prior to creation, choose this option. This configuration gives the option to use EKS Auto Mode and customize the cluster's configuration.

## Cluster configuration

### Name

Use the auto-generated name or enter a unique name for this cluster. This property cannot be changed after the cluster is created.

security-demo-cluster



The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.

### Kubernetes version [Info](#)

Select Kubernetes version for this cluster.

1.33



### Cluster IAM role [Info](#)

Select the Cluster IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This cannot be changed after the cluster is created. To create a new custom role, follow the instructions in the [Amazon EKS User Guide](#).

AmazonEKSAutoClusterRole



[Create recommended role](#)



### Node IAM role [Info](#)

Nodes need an EC2 Instance IAM Role to launch and register with a cluster. To create a new custom role, follow the instructions in the [Amazon EKS User Guide](#).

AmazonEKSAutoNodeRole



[Create recommended role](#)



### VPC [Info](#)

Select a VPC to use for your EKS cluster resources.

vpc-02d0a11cd2dabebf6 | portfolio-vpc-vpc



[Create VPC](#)



### Subnets [Info](#)

Choose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the [VPC console](#).

Select subnets



[Clear selected subnets](#)



subnet-024a9aa1503bec0e2 | portfolio-vpc-subnet-private2-us-east-2b X

us-east-2b 10.0.144.0/20 Type: Private

subnet-0b8072fb60258d52 | portfolio-vpc-subnet-private1-us-east-2a X

us-east-2a 10.0.128.0/20 Type: Private

[View quick configuration defaults](#)

[Cancel](#)

[Create](#)

## Cluster Created!

The screenshot shows the 'Clusters' section of the Amazon EKS console. On the left, there's a sidebar with navigation links for 'Amazon Elastic Kubernetes Service', 'Dashboard', 'Clusters', 'Settings', 'Amazon EKS Anywhere', 'Related services', and 'Documentation'. The main area displays the 'security-demo-cluster' details. It includes sections for 'Cluster info' (Status: Active, Kubernetes version: 1.33), 'Support period' (Standard support until July 28, 2026), 'Provider' (EKS), 'Cluster health' (0 issues), 'Upgrade insights' (5 pending), and 'Node health issues' (0 issues). Below this is a navigation bar with tabs: Overview (selected), Resources, Compute, Networking, Add-ons, Access, Observability, Update history, and Tags. The 'Details' section contains fields for 'API server endpoint' (https://87E1E797A91D0634242EE8CC9CECCD14.gr7.us-east-2.eks.amazonaws.com), 'OpenID Connect provider URL' (https://oidc.eks.us-east-2.amazonaws.com/id/87E1E797A91D0634242EE8CC9CECCD14), 'Certificate authority' (long hex string), 'Cluster IAM role ARN' (arn:aws:iam::918689941708:role/AmazonEKSAutoClusterRole), and 'Created' (27 minutes ago). There are also sections for 'Cluster ARN' (arn:aws:eks:us-east-2:918689941708:cluster/security-demo-cluster) and 'Platform version' (eks.14).

### Connect kubectl to your new cluster

```
~ $ aws eks update-kubeconfig --region us-east-2 --name security-demo-cluster
Added new context arn:aws:eks:us-east-2:918689941708:cluster/security-demo-cluster to /home/cloudshell-user/.kube/config
~ $
```

### verify access

```
~ $ kubectl get nodes
E0919 18:17:53.197581    251 [memcache.go:287] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:17:53.213734    251 [memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:17:53.219792    251 [memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:17:53.222433    251 [memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
NAME           STATUS   ROLES      AGE   VERSION
i-07a4e58d2bb0c3c48  Ready    <none>    14m  v1.33.1-eks-f5be8fb
~ $ kubectl get pods --all-namespaces
E0919 18:18:10.233291    260 [memcache.go:287] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:18:10.246051    260 [memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:18:10.248585    260 [memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:18:10.254128    260 [memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
NAMESPACE        NAME           READY   STATUS      RESTARTS   AGE
kube-system     metrics-server-7d7546bdc4-rfvdq  0/1     ImagePullBackOff  0          14m
kube-system     metrics-server-7d7546bdc4-xvh2n  0/1     ImagePullBackOff  0          14m
~ $
```

## Activate Amazon Inspector

The screenshot shows the AWS Inspector dashboard with a blue header bar containing the message: "Welcome to Inspector. To get started, activate Amazon EC2, Amazon ECR, AWS Lambda scanning for your member accounts." Below this, a green banner says: "Welcome to Inspector. Your first scan is underway." The main summary section displays environment coverage and critical findings.

**Environment coverage:**

- Instances: 0 / 0 instances
- Container repositories: 0 / 0 repositories
- Lambda functions: 0 / 0 Lambda functions
- Code repositories: 0 / 0 Code repositories

**Critical findings:**

ECR container	EC2 instance	Lambda functions
0 Critical 0 total findings	0 Critical 0 total findings	0 Critical 0 total findings

## Activate Amazon GuardDuty

The screenshot shows the AWS GuardDuty dashboard with a green banner stating: "You've successfully enabled GuardDuty." It includes a summary of security trends and a new feature notice about S3 archive file limit support.

**Summary:**

- New feature: Amazon GuardDuty Malware Protection for S3 increases archive file limit support to 10,000 files. (Amazon GuardDuty Malware Protection for S3 enhances archive processing to support up to 10,000 files per archive (up from 1,000 files). [Learn more](#))

**Overview:**

- Attack sequences - new: 0
- Total findings: 0
- Resources with findings: 0
- Accounts: 0

**Findings - new:**

Prioritize triaging and remediating topmost severity detections.

Critical	High	Medium	Low
0	0	0	0

**Introducing the new AWS Security Hub - public preview:**

The new Security Hub is your unified cloud security solution to protect your cloud environment. [Learn more](#)

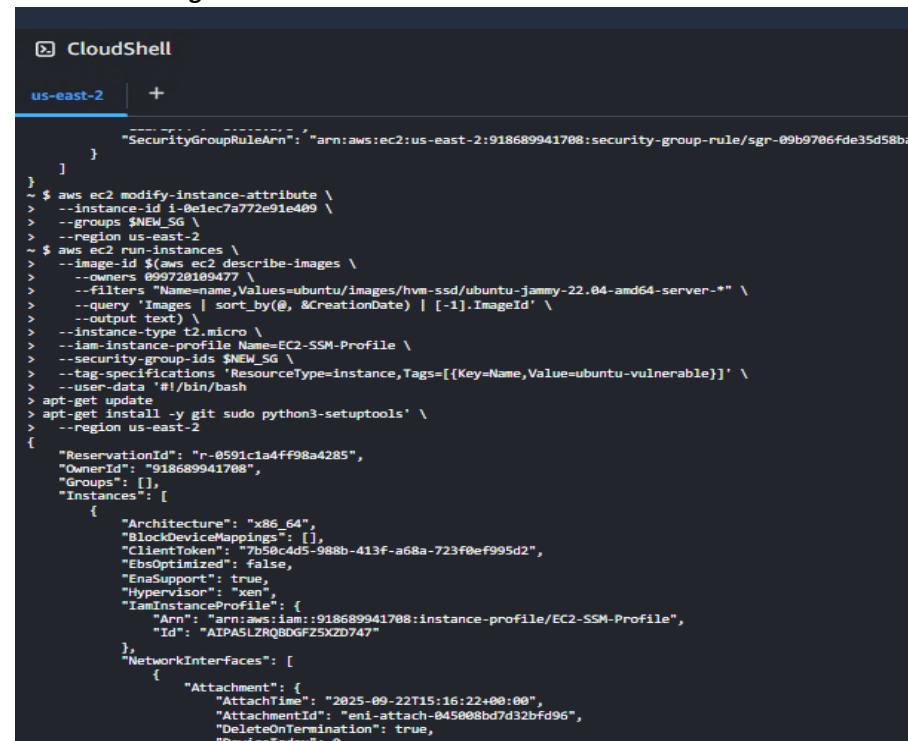
**Most common finding types:**

## Verify GuardDuty Active – Via CloudShell CLI

```
~ $ clear
~ $ kubectl logs -n amazon-guardduty aws-guardduty-agent-45nv7 --tail=20
2025-09-22T13:20:51.191788Z  INFO amzn_guardduty_agent: GuardDuty agent starting with 8 worker thread(s) and 100 max blocking threads.
2025-09-22T13:20:51.216047Z  INFO amzn_guardduty_agent: Agent fingerprint: 64b651fb444b18ae8e6813e8895ac771d9a7a55c3c58448e9b1c002d19ebb4c9
2025-09-22T13:20:51.216275Z  INFO amzn_guardduty_agent: Agent config for Component(s): AgentConfig { component_channel_size: 100, ingestion_endpoint: "socket_(EKS_Auto_Standard)_2025.9.11_(aws-k8s-1.33-standard)", os_version: OSUnknown, kernel_version: LinuxKernel16_12, region: None, stage: None, memory: 16384, pid_namespace_cache_capacity: 1024, pre_suppressor_cache_capacity: 32768, post_suppressor_cache_capacity: 32768, docker_socket_file_path: "/host/600s, scan_for_task_metadata_period: 600s, eks_cluster_name_env_var: "CLUSTER_NAME", max_file_size_to_hash: 536870912, proc_folder_path: "/host/calculation_timeout: 5s, file_open_timeout: 1.5s, mnt_ns_pids_map_capacity: 1024, pid_set_cap: 32 }

2025-09-22T13:20:51.231903Z  INFO amzn_guardduty_agent::dependency_checks: Dependency checks complete.
2025-09-22T13:20:51.235825Z  INFO amzn_guardduty_agent::dependency_checks: Health check: EXECUTABLE (connectivity OK)
2025-09-22T13:20:51.240555Z  INFO amzn_guardduty_agent_data_model::schema: Event schema rabin fingerprint = "b6ce8be84715ced5"
2025-09-22T13:20:51.240715Z  INFO amzn_guardduty_agent_data_model::schema: Container schema rabin fingerprint = "5a675cafef525a5d"
2025-09-22T13:20:51.240796Z  INFO amzn_guardduty_agent_data_model::schema: Pod schema rabin fingerprint = "8504ac7492b3cb8b"
2025-09-22T13:20:51.240877Z  INFO amzn_guardduty_agent_data_model::schema: Task schema rabin fingerprint = "195a73fa36862425"
2025-09-22T13:20:51.244256Z  INFO amzn_guardduty_agent: GuardDuty agent started ...
2025-09-22T13:20:51.244265Z  INFO amzn_guardduty_agent: Type Ctrl+C to terminate
2025-09-22T13:20:51.940027Z  INFO amzn_guardduty_agent_core::decorator: Decorator started ...
```

## Generate Package Vulnerabilities



```
CloudShell
us-east-2 + 

```sh
$ aws ec2 create-security-group \
> --group-name $NEW_SG \
> --description "New Security Group" \
> --region us-east-2
$ aws ec2 modify-instance-attribute \
> --instance-id i-0elec7a772e91e409 \
> --groups $NEW_SG \
> --region us-east-2
$ aws ec2 run-instances \
> --image-id $(aws ec2 describe-images \
> --owners 099720189477 \
> --filters "Name=name,Values=ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-*" \
> --query 'Images | sort_by(@, &CreationDate) | [-1].ImageId' \
> --output text) \
> --instance-type t2.micro \
> --iam-instance-profile Name=EC2-SSM-Profile \
> --security-group-ids $NEW_SG \
> --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=ubuntu-vulnerable}]' \
> --user-data '#!/bin/bash
apt-get update
apt-get install -y git sudo python3-setuptools' \
> --region us-east-2
{
  "ReservationId": "r-0591cia4ff98a4285",
  "OwnerId": "918689941708",
  "Groups": [],
  "Instances": [
    {
      "Architecture": "x86_64",
      "BlockDeviceMappings": [],
      "ClientToken": "7b59c4d5-988b-413f-a68a-723f0ef995d2",
      "EbsOptimized": false,
      "EnaSupport": true,
      "Hypervisor": "xen",
      "IamInstanceProfile": {
        "Arn": "arn:aws:iam::918689941708:instance-profile/EC2-SSM-Profile",
        "Id": "AIPASLZRQBDGFZ5XZD747"
      },
      "NetworkInterfaces": [
        {
          "Attachment": {
            "AttachTime": "2025-09-22T15:16:22+00:00",
            "AttachmentId": "eni-attach-045008bd7d32bfd96",
            "DeleteOnTermination": true,
            "DeviceIndex": 0
          }
        }
      ]
    }
  ]
}
```
}
```

## Check Amazon Inspector for Vulnerabilities

| By instance (1)                                                      |              |                  |                       |          |      |     |   | <a href="#">Create suppression rule</a> |
|----------------------------------------------------------------------|--------------|------------------|-----------------------|----------|------|-----|---|-----------------------------------------|
| Choose a row to view the instance's details and associated findings. |              |                  |                       |          |      |     |   | <a href="#">Add filter</a>              |
| EC2 instance                                                         | Account      | Operating system | Amazon machine image  | Critical | High | All | ▼ | ▼                                       |
| i-0887dfece8721dded                                                  | 918689941708 | UBUNTU_22_04     | ami-001209a78b30e703c | 0        | 17   | 101 |   |                                         |

## Check Remediation fix

**Inspector**

- Dashboard
- Findings
  - By vulnerability
  - By instance
  - By container image
  - By container repository
  - By Lambda function
  - All findings
- Code security
- Export SBOMs
- Suppression rules
- On-demand scans
- CIS scans

---

- Vulnerability database search
- Account management
- Resources coverage
- General settings
  - EC2 scanning settings
  - ECR scanning settings
- Usage

---

- Video tutorials
- What's New

[Switch to Inspector Classic](#)

Amazon Web Services (AWS) announces the general availability of Amazon Inspector code security capabilities, helping you secure your applications before they reach production. This new feature, with native integration to GitHub and GitLab, helps you rapidly identify and prioritize security vulnerabilities and misconfigurations across your application source-code, dependencies, and infrastructure as code (IaC). You can evaluate source-code as builders push or pull code changes in repositories, within CI/CD pipelines, or through scheduled scans. Findings from these scans are surfaced both in the Amazon Inspector console for an aggregated view across the organization and within the source code management platform as fast feedback for the developers. [Learn more](#)

**Introducing the new AWS Security Hub - public preview** The new Security Hub is your unified cloud security solution that prioritizes critical issues and helps you respond at scale to protect your cloud environment. [Learn more](#)  [Try Security Hub](#)

Inspector > Findings > By instance > i-0887dfece8721dded

**i-0887dfece8721dded** [Info](#)  
EC2 instance

| Details                                                            |                                                        |                                       |
|--------------------------------------------------------------------|--------------------------------------------------------|---------------------------------------|
| EC2 instance<br><a href="#">i-0887dfece8721dded </a>               | Launched at<br>September 22, 2025 10:16 AM (UTC-05:00) | Created by<br>918689941708            |
| Role<br>arn:aws:iam::918689941708:instance-profile/EC2-SSM-Profile | AWS account<br>918689941708                            | Security group<br>critical-vulnerable |
| Amazon machine image<br>ami-001209a78b30e703c                      |                                                        |                                       |
| Finding summary                                                    |                                                        |                                       |
| 0 Critical  17 High  84 Medium                                     |                                                        |                                       |

**Findings (101)**

Choose a row to view the finding details. All findings are related to this instance.

Filter status Filter criteria

Created at September 22, 2025 10:17 AM (UTC-05:00)

Affected packages

|                                   |                                                                    |
|-----------------------------------|--------------------------------------------------------------------|
| Name                              | linux-image-aws                                                    |
| Installed version / Fixed version | 0:6.8.0-1036.38-22.04.1.X86_64 / 0:6.8.0-1037.39-22.04.1 (pending) |
| Package manager                   | OS                                                                 |

Remediation

Upgrade your installed software packages to the proposed fixed in version and release.

- apt-get update && apt-get upgrade

Vulnerability details

|                                          |                                              |
|------------------------------------------|----------------------------------------------|
| Vulnerability ID                         | <a href="#">CVE-2025-21919 </a>              |
| Vulnerability source                     | UBUNTU_CVE                                   |
| CWEs                                     | <a href="#">CWE-787 </a>                     |
| Inspector score                          | 7.8                                          |
| Inspector scoring vector                 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| Exploit Prediction Scoring System (EPSS) | 0.00017                                      |
| CVSS 3.1                                 | 7.8 (Source: NVD)                            |
| Scoring vector                           | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CVSS 3.1                                 | 7.8 (Source: UBUNTU_CVE)                     |
| Scoring vector                           | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

Related vulnerabilities

USN-7510-6, USN-7510-5, USN-7510-4, USN-7511-3, USN-7511-2, USN-7512-1, USN-7510-3, USN-7510-8, USN-7510-7, USN-7602-1, USN-7605-1, USN-7606-1, USN-7605-2, USN-7628-1, USN-7510-2, USN-7511-1, USN-7510-1, USN-7593-1

Resource affected

|                   |                                      |
|-------------------|--------------------------------------|
| Resource ID       | <a href="#">i-0887dfece8721dded </a> |
| Type              | AWS EC2 Instance                     |
| EC2 instance type | t2.micro                             |

Verify there is a Remediation patch available if not document. ( Vulnerable, NO patch!)

|                  |                  |                                |
|------------------|------------------|--------------------------------|
| linux-aws-6.8    | 25.04 plucky     | Not in release                 |
|                  | 24.04 LTS noble  | Not in release                 |
|                  | 22.04 LTS jammy  | ✖ Vulnerable, work in progress |
|                  | 20.04 LTS focal  | Not in release                 |
|                  | 18.04 LTS bionic | Not in release                 |
|                  | 16.04 LTS xenial | Not in release                 |
|                  | 14.04 LTS trusty | Not in release                 |
| 14.04 LTS trusty |                  | Not in release                 |
| linux-hwe-6.8    | 25.04 plucky     | Not in release                 |
|                  | 24.04 LTS noble  | Not in release                 |
|                  | 22.04 LTS jammy  | ✖ Vulnerable, work in progress |
|                  | 20.04 LTS focal  | Not in release                 |
|                  | 18.04 LTS bionic | Not in release                 |
|                  | 16.04 LTS xenial | Not in release                 |
|                  | 14.04 LTS trusty | Not in release                 |

No patch so lets remove Instance

| Instances (2) <a href="#">Info</a>                                                                                            |                                     |                     |                                                          |               |                                                              |              |                   |                          |                 |            |         |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---------------------|----------------------------------------------------------|---------------|--------------------------------------------------------------|--------------|-------------------|--------------------------|-----------------|------------|---------|
| <input type="button" value="Find Instance by attribute or tag (case-sensitive)"/> <input type="button" value="All states ▾"/> |                                     |                     |                                                          |               |                                                              |              |                   |                          |                 |            |         |
| <input type="checkbox"/>                                                                                                      | Name <a href="#">🔗</a>              | Instance ID         | Instance state                                           | Instance type | Status check                                                 | Alarm status | Availability Zone | Public IPv4 DNS          | Public IPv4 ... | Elastic IP | IPv6 IP |
| <input type="checkbox"/>                                                                                                      | ubuntu-vulnerable <a href="#">🔗</a> | i-0887dfece8721dded | <span>Running</span> <a href="#">🔗</a> <a href="#">🔗</a> | t2.micro      | <span>2/2 checks passed</span> <a href="#">View alarms +</a> |              | us-east-2c        | ec2-3-145-23-120.us-e... | 3.145.23.120    | -          | -       |

| Instances (1/2) <a href="#">Info</a>                                                                                          |                                     |                     |                                                             |               |              |                               |                   |                 |                 |            |          |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---------------------|-------------------------------------------------------------|---------------|--------------|-------------------------------|-------------------|-----------------|-----------------|------------|----------|
| <input type="button" value="Find Instance by attribute or tag (case-sensitive)"/> <input type="button" value="All states ▾"/> |                                     |                     |                                                             |               |              |                               |                   |                 |                 |            |          |
| <input checked="" type="checkbox"/>                                                                                           | Name <a href="#">🔗</a>              | Instance ID         | Instance state                                              | Instance type | Status check | Alarm status                  | Availability Zone | Public IPv4 DNS | Public IPv4 ... | Elastic IP | IPv6 IPs |
| <input checked="" type="checkbox"/>                                                                                           | ubuntu-vulnerable <a href="#">🔗</a> | i-0887dfece8721dded | <span>Terminated</span> <a href="#">🔗</a> <a href="#">🔗</a> | t2.micro      | -            | <a href="#">View alarms +</a> | us-east-2c        | -               | -               | -          | -        |

## Generate Sample findings for GuardDuty

```
~ $ DETECTOR_ID=$(aws guardduty list-detectors --query 'DetectorIds[0]' --output text --region us-east-1)
~ $
~ $ echo "Detector ID: $DETECTOR_ID"
Detector ID: 7eccb8b03cff3a081bf7dc7204c9a55c
~ $ celar
-bash: celar: command not found
~ $ clear
~ $ aws guardduty create-sample-findings \
> --detector-id 7eccb8b03cff3a081bf7dc7204c9a55c \
> --finding-types \
>   "Recon:EC2/PortProbeUnprotectedPort" \
>   "UnauthorizedAccess:EC2/SSHBruteForce" \
>   "UnauthorizedAccess:EC2/MaliciousIPCaller.Custom" \
>   "CryptoCurrency:EC2/BitcoinTool.BIDNS" \
-bash: !DNS: event not found
>   "Trojan:EC2/DNSDataExfiltration" \
>   "Impact:EC2/PortSweep" \
>   "UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS" \
>   --region us-east-2
~ $
```

The screenshot shows the AWS GuardDuty Summary page. The left sidebar includes sections for Protection plan (S3, EKS, Extended Threat Detection), Runtime Monitoring, Malware Protection for EC2, RDS Protection, Lambda Protection, Accounts, Usage, Settings, and Security Hub (New). The main content area displays an overview of findings, a findings table, and various charts.

**Summary** View and analyze security trends based on GuardDuty findings in your AWS environment.

**Overview**

| Attack sequences - new | Total findings | Resources with findings | Accounts with findings |
|------------------------|----------------|-------------------------|------------------------|
| 0                      | 6              | 2                       | 1                      |

**Findings - new** Prioritize triaging and remediating top-most severity detections.

| Critical | High | Medium | Low |
|----------|------|--------|-----|
| 0        | 3    | 1      | 2   |

**Introducing the new AWS Security Hub - public preview** The new Security Hub is your unified cloud security solution that prioritizes critical issues and helps you respond at scale to protect your cloud environment. Learn more. Try Security Hub.

**Runtime Monitoring coverage**

| EKS clusters | ECS clusters | EC2 instances |
|--------------|--------------|---------------|
| No resources | No resources | 0/2 monitored |

**Most common finding types**



Impact:EC2/PortSweep   Recon:EC2/PortProbeUnprotectedPort   Trojan:EC2/DNSDataExfiltration  
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom   Others

**Resources with most findings**

All resource types ▾ All severity ▾

## Findings (6) Info

[Create suppression rule](#)[Actions ▾](#)

| <input type="checkbox"/> | Title                                                                                                                       | Severity | Finding type                                                         | Resource                                | Count | Account ID   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------|-----------------------------------------|-------|--------------|
| <input type="checkbox"/> | <a href="#">[SAMPLE] The EC2 instance i-99999999 is communicating with an IP address on a custom threat list.</a>           | Medium   | UnauthorizedAccess:EC2/MaliciousIPCaller.Custom                      | EC2 Instance: i-99999999                | 1     | 918689941708 |
| <input type="checkbox"/> | <a href="#">[SAMPLE] An unprotected port on EC2 instance i-99999999 is being probed.</a>                                    | Low      | Recon:EC2/PortProbeUnprotectedPort                                   | EC2 Instance: i-99999999                | 1     | 918689941708 |
| <input type="checkbox"/> | <a href="#">[SAMPLE] Credentials for instance role GeneratedFindingUserName were used from an external IP address.</a>      | High     | UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS | Access Key: GeneratedFindingAccessKeyId | 1     | 918689941708 |
| <input type="checkbox"/> | <a href="#">[SAMPLE] 198.51.100.0 is performing SSH brute force attacks against i-99999999.</a>                             | Low      | UnauthorizedAccess:EC2/SSHBruteForce                                 | EC2 Instance: i-99999999                | 1     | 918689941708 |
| <input type="checkbox"/> | <a href="#">[SAMPLE] The EC2 instance i-99999999 is probing a port on a large number of publicly routable IP addresses.</a> | High     | Impact:EC2/PortSweep                                                 | EC2 Instance: i-99999999                | 1     | 918689941708 |
| <input type="checkbox"/> | <a href="#">[SAMPLE] Data exfiltration through DNS queries from the EC2 instance i-99999999.</a>                            | High     | Trojan:EC2/DNSDataExfiltration                                       | EC2 Instance: i-99999999                | 1     | 918689941708 |

## Azure Security Portfolio

End-to-end Azure cloud build demonstrating secure tenant hardening (MFA, break-glass admin, RBAC), SIEM on boarding with Microsoft Sentinel (Log Analytics + Azure Activity), and full Microsoft Defender plan enablement. I intentionally deployed a vulnerable storage resource to validate detection and guided remediation via Defender for Cloud and network segmentation.

Detection coverage is mapped to MITRE ATT&CK, with KQL hunting for rapid/suspicious resource creation, alert to incident workflows, and documented investigations. I operationalized threat intelligence by creating test IoCs, modeling spear-phishing and simulated APT activity, and confirming enterprise-wide visibility through Threat Analytics and analyst reports—showcasing a complete loop from prevention and detection to response and intel.

## Create and enable MFA on Azure account

All services > Default Directory | Overview > Users >

### Per-user multifactor authentication ...

Bulk update Got feedback?

Users Service settings

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. [Learn more](#)

Before you begin, take a look at the [multifactor authentication deployment guide](#).

Enable MFA  Disable MFA  Enforce MFA  User MFA settings

Status : All View : Sign-in allowed users Reset filters

| <input checked="" type="checkbox"/> Name ↑        | UPN                                                         | Status   |
|---------------------------------------------------|-------------------------------------------------------------|----------|
| <input checked="" type="checkbox"/> Tevin Agtarap | agtaraptevin_gmail.com#EXT#@agtarpetingmail.onmicrosoft.com | disabled |

| <input type="checkbox"/> Name ↑        | UPN                                                         | Status  |
|----------------------------------------|-------------------------------------------------------------|---------|
| <input type="checkbox"/> Tevin Agtarap | agtaraptevin_gmail.com#EXT#@agtarpetingmail.onmicrosoft.com | enabled |

## Create emergency Admin account – just in case!

All services > Default Directory | Overview > Users >

### Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create

#### Basics

|                     |                                                 |  |
|---------------------|-------------------------------------------------|--|
| User principal name | emergency-admin@agtarpetingmail.onmicrosoft.com |  |
| Display name        | Emergency Access Admin                          |  |
| Mail nickname       | emergency-admin                                 |  |
| Password            | *****                                           |  |
| Account enabled     | Yes                                             |  |

#### Properties

|           |        |
|-----------|--------|
| User type | Member |
|-----------|--------|

#### Assignments

Administrative units

Groups

Roles

## Add Assigned role – Global Admin

Emergency Access Admin | Assigned roles

User

Search + Add assignments Remove assignments Refresh Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems Custom security attributes

Administrative roles Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Search by name or description Add filters

| Role                                                     | Description                                                                                              | Resource Name | Resource Type | Assignment Path | Type     |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------|---------------|-----------------|----------|
| <input checked="" type="checkbox"/> Global Administrator | Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities. | Directory     | Organization  | Direct          | Built-in |

## Create Resource groups for the use in Microsoft Sentinel & Defender

Home >

Resource groups

Default Directory ([agtaraptevin@gmail.onmicrosoft.com](#))

+ Create Manage view Refresh Export to CSV Open query Assign tags

ⓘ You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field... Subscription equals all Location equals all + Add filter

| Name                                                      | Subscription             | Location |
|-----------------------------------------------------------|--------------------------|----------|
| <input checked="" type="checkbox"/> rg-defender-resources | ... Azure subscription 1 | East US  |
| <input checked="" type="checkbox"/> rg-security-portfolio | ... Azure subscription 1 | East US  |
| <input checked="" type="checkbox"/> rg-sentinel-workspace | ... Azure subscription 1 | East US  |

## Create Log Analytics Workspace (Required for Sentinel)

Microsoft Azure

Home > Microsoft.LogAnalyticsOMS | Overview

Deployment

Search Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

>Your deployment is complete

Deployment name : MicrosoftLogAnalyticsOMS  
Subscription : Azure subscription 1  
Resource group : rg-sentinel-workspace

Deployment details

| Resource               | Type                    | Status | Operation details                 |
|------------------------|-------------------------|--------|-----------------------------------|
| law-security-portfolio | Log Analytics workspace | OK     | <a href="#">Operation details</a> |

Next steps

[Go to resource](#)

[Give feedback](#)  
[Tell us about your experience with deployment](#)

Cost management  
Get notified to stay within your budget and prevent unexpected charges on your bill.  
[Set up cost alerts >](#)

Microsoft Defender for Cloud  
Secure your apps and infrastructure  
[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials  
[Start learning today >](#)

Work with an expert  
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

## Add Sentinel to Workspace

[portal.azure.com/#view/Microsoft\\_Azure\\_Security\\_Insights/MainMenuBlade/~/NewsAndGuides/subscriptionId/f73fcad7-e519-46f8-9142-a387884a6c5b/resourceGroup/rg-sentinel-workspace/workspaceName/law-security-portfolio](#)

About upgrading to... How to upgrade Splunk Online Courses - Learn Updates for SS \$Plunk.conf

Microsoft Azure

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | Guides

Selected workspace: 'law-security-portfolio'

Search Documentation

General Overview Logs Guides Search Threat management Content management Configuration

**Microsoft Sentinel free trial activated**  
The free trial is active on this workspace from 9/22/2025 to 10/23/2025 at 11:59:59 PM UTC. During the trial, up to 10 GB/day are free for both Microsoft Sentinel and Log Analytics. Data beyond the 10 GB/day included quantity will be billed. [Learn more](#).

OK

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

Install your first content hub solution

Notifications

More events in the activity log → Dismiss all

Successfully added Microsoft Sentinel  
Successfully added Microsoft Sentinel to workspace 'law-security-portfolio', it might take a few minutes for your workspace to appear in Microsoft Sentinel workspaces list.

a few seconds ago

## Install Azure Activity

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Data connectors >

Content hub

Refresh Install/Update Delete + SIEM Migration Guides & Feedback

424 Solutions 322 Standalone contents 0 Installed 0 Updates

Did you find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. [Learn more](#)

Search... Status: All Content type: Data connector (335) Support: All Provider: All Category: All Content sources: All

| Content title             | Status                 | Content source | Provider        | Support   | Category                                     | Content type                           |
|---------------------------|------------------------|----------------|-----------------|-----------|----------------------------------------------|----------------------------------------|
| AWS Amazon Web Services   | FEATURED Not installed | Solution       | Amazon Web S... | Microsoft | Security - Cloud Security                    | Analytics rule (58) Data connector (3) |
| Azure Activity            | FEATURED In progress   | Solution       | Microsoft       | Microsoft | IT Operations                                | Analytics rule (14) Data connector (2) |
| Cisco Cloud Security      | FEATURED Not installed | Solution       | Cisco           | Microsoft | Security - Automation (SOAR), Security - ... | Analytics rule (10) Data connector (2) |
| Google Cloud Platform     | FEATURED Not installed | Solution       | Google          | Microsoft | Cloud Provider, Identity                     | Analytics rule (10) Data connector (4) |
| Microsoft Defender for... | FEATURED Not installed | Solution       | Microsoft       | Microsoft | Security - Threat Protection                 | Analytics rule Data connector (2)      |

Provider: Microsoft Support: Microsoft Version: 3.0.3

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.

Data Connectors: 1, Workbooks: 2, Analytic Rules: 14, Hunting Queries: 15

[Learn more about Microsoft Sentinel](#) [Learn more about Solutions](#)

Content type: 14 Analytics rule 1 Data connector 2 Workbook 15 Hunting query

## Add Rules through Microsoft Defender Configuration Analytics dashboard

Analytics

Manage all your rules in one place

Now you can manage all your rules on one page, providing a centralized and streamlined approach to rule management. This enhancement not only simplifies your workflow but also ensures that you can easily access, modify, and oversee all your rules in one convenient location.

Go to unified rules page

2 Active rules More content at Content hub

Rules by severity

High (0) Medium (1) Low (1) Informational (0)

LEARN MORE About analytics rules

Active rules Rule templates Anomalies

+ Create Analytics workbooks Enable Disable Delete Import Export Columns

Rare subscription-level operations i... Add filter

| Severity | Name                                        | Rule type | Data sources   | Tactics              | Techniques | Sub techniques | Source name    |
|----------|---------------------------------------------|-----------|----------------|----------------------|------------|----------------|----------------|
| Low      | Rare subscription-level operations in Azure | Scheduled | Azure Activity | Credential Access +1 | T1003 +1   |                | Azure Activity |

Microsoft Defender | Default Directory

Analytics > Analytics rule wizard

Validation passed.

Analytics rule wizard - Create a new Scheduled rule

Rare subscription-level operations in Azure

Analytics rule details

Name: Rare subscription-level operations in Azure

Description: This query looks for a few sensitive subscription-level events based on Azure Activity Logs. For example, this monitors for the operation name 'Create or Update Snapshot', which is used for creating backups but could be misused by attackers to dump hashes or extract sensitive information from the disk.

MITRE ATT&CK

> Credential Access (1)

> Persistence (1)

Severity: Low

Status: Enabled

Analytics rule settings

Rule query:let starttime = 14d; let endtime = 1d; // The number of operations above which an IP address is considered an unusual source of role assignment operations let alertOperationThreshold = 5; // Add or remove operation names below as per your requirements. For operations list, please refer to <https://learn.microsoft.com/en-us/Azure/role-based-access-control/resource-provider-operations#all> let SensitiveOperationList = dynamic(["microsoft.compute/snapshots/write", "microsoft.network/networksecuritygroups/write", "microsoft.storage/storageaccounts/listkeys/action"]); let SensitiveActivity = AzureActivity | where OperationNameValue in= (SensitiveOperationList) or OperationNameValue hasuffix "listkeys/action" | where ActivityStatusValue == "Success"; SensitiveActivity | where TimeGenerated between (ago(starttime)..ago(endtime)) | summarize count() by CallerIpAddress, Caller, OperationNameValue, binTimeGenerated, id | where count\_ >= alertOperationThreshold // Returns all the records from the right side that don't have matches from the left join kind = rightanti (SensitiveActivity | where TimeGenerated >= ago(alertTime)) | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStamp = make\_list(TimeGenerated), ActivityStatusValue = make\_list(ActivityStatusValue), CorrelationIds = make\_list(CorrelationId), ResourceGroups = make\_list(ResourceGroup), ResourceIds = make\_list(ResourceId), ActivityCountByCallerAddress = sum(count) by CallerIpAddress, Caller, OperationNameValue | where ActivityCountByCallerIpAddress > alertOperationThreshold on CallerIpAddress, Caller, OperationNameValue | extend Name = toString(split(Caller, '@')[0]), UPNSuffix = toString(split(Caller, '@')[1])[]

Rule frequency: Run query every 1 day

Rule period: Last 14 days data

< Previous Next Cancel

## Activate 6 various rules to help cover portions of the MITRE ATT&CK frame work

Active rules Rule templates Anomalies

+ Create Analytics workbooks Rule runs (Preview) Enable Disable Import Export Columns

Search by ID, name, tactic or technique Add filter

| Severity | Name                                                            | Rule type | Status  | Tactics              | Techniques | Sub techniques | Source name    | Last modified       |
|----------|-----------------------------------------------------------------|-----------|---------|----------------------|------------|----------------|----------------|---------------------|
| Low      | New CloudShell User                                             | Scheduled | Enabled | Execution            | T1059      |                | Azure Activity | 9/23/2025, 10:31... |
| Medium   | NRT Microsoft Entra ID Hybrid Health AD FS New Server           | NRT       | Enabled | Defense Evasion      | T1578      |                | Azure Activity | 9/23/2025, 10:30... |
| Low      | Creation of expensive computes in Azure                         | Scheduled | Enabled | Defense Evasion      | T1578      |                | Azure Activity | 9/23/2025, 10:27... |
| Low      | Rare subscription-level operations in Azure                     | Scheduled | Enabled | Credential Access +1 | T1003 +1   |                | Azure Activity | 9/23/2025, 10:26... |
| Medium   | Suspicious number of resource creation or deployment activities | Scheduled | Enabled | Impact               | T1496      |                | Azure Activity | 9/23/2025, 10:24... |
| Low      | Suspicious Resource deployment                                  | Scheduled | Enabled | Impact               | T1496      |                | Azure Activity | 9/23/2025, 10:22... |

## Activate all Defender plans

Microsoft Azure Upgrade

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans Azure subscription 1

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/billable resource/month. Foundation CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

| Plan              | Pricing*                              | Resource quantity | Monitoring coverage | Status |
|-------------------|---------------------------------------|-------------------|---------------------|--------|
| Foundational CSPM | Free Details >                        |                   | Full                | Off On |
| Defender CSPM     | \$5/billable resource/Month Details > | 1 resources       | Full Settings >     | Off On |

Cloud Workload Protection (CWPP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

| Plan             | Pricing*                                                                                             | Resource quantity                          | Monitoring coverage | Status |
|------------------|------------------------------------------------------------------------------------------------------|--------------------------------------------|---------------------|--------|
| Servers          | Plan 2 (\$15/Server/Month) Change plan                                                               | 0 servers                                  | Full Settings >     | Off On |
| App Service      | \$15/instance/Month Details >                                                                        | 0 instances                                | Full                | Off On |
| Databases        | Selected: 4/4 Select types >                                                                         | 0 instances                                | Full                | Off On |
| Storage          | \$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Scanning (configurable) Details > | 1 storage accounts                         | Full Settings >     | Off On |
| Containers       | \$6.8693/VM core/Month Details >                                                                     | 0 container registries; 0 kubernetes cores | Full Settings >     | Off On |
| AI Services      | \$0.0008/1K tokens/month Details >                                                                   | 0 AI resources                             | Partial Settings >  | Off On |
| Key Vault        | \$0.25/Vault/Month Details >                                                                         | 0 key vaults                               | Full                | Off On |
| Resource Manager | \$3/Subscription/Month Details >                                                                     |                                            | Full                | Off On |

## Deploy a Storage account with vulnerabilities so we can use Azure to find and then remediate them!

Home > Storage center | Storage accounts (Blobs) >

### Create a storage account

|                                                              |                              |
|--------------------------------------------------------------|------------------------------|
| Allow cross-tenant replication                               | Disabled                     |
| Access tier                                                  | Hot                          |
| Enable large file shares                                     | Enabled                      |
| <strong>Security</strong>                                    |                              |
| Secure transfer                                              | Disabled                     |
| Blob anonymous access                                        | Disabled                     |
| Allow storage account key access                             | Enabled                      |
| Default to Microsoft Entra authorization in the Azure portal | Disabled                     |
| Minimum TLS version                                          | Version 1.0                  |
| Permitted scope for copy operations (preview)                | From any storage account     |
| <strong>Networking</strong>                                  |                              |
| Public network access                                        | Enabled                      |
| Public network access scope                                  | Enabled from all networks    |
| Default routing tier                                         | Microsoft network routing    |
| <strong>Data protection</strong>                             |                              |
| Point-in-time restore                                        | Disabled                     |
| Blob soft delete                                             | Disabled                     |
| Container soft delete                                        | Disabled                     |
| File share soft delete                                       | Disabled                     |
| Versioning                                                   | Disabled                     |
| Blob change feed                                             | Disabled                     |
| Version-level immutability support                           | Disabled                     |
| <strong>Encryption</strong>                                  |                              |
| Encryption type                                              | Microsoft-managed keys (MMK) |
| Enable support for customer-managed keys                     | Blobs and files only         |
| Enable infrastructure encryption                             | Disabled                     |

[Previous](#) [Next](#) [Create](#)

## Confirm deployment

The screenshot shows the Azure portal's deployment overview page. The deployment name is 'stvulnportfolio123\_1758642357992'. Deployment status: Complete. Deployment details: Deployment name: stvulnportfolio123\_1758642357992, Subscription: Azure subscription 1, Resource group: rg-security-portfolio. Start time: 9/23/2025, 10:50:29 AM. Correlation ID: 2831d406-9b9a-42cf-b1b6-c39e8d3b3f0c. Next steps: Go to resource.

Verify we are now connected with Azure Activity

**Microsoft Sentinel | Data connectors**

Selected workspace: 'low-security-portfolio'

Search Refresh Guides & Feedback

General Overview Logs Guides Search Threat management Incidents Workbooks Hunting Notebooks Entity behavior Threat intelligence MITRE ATT&CK (Preview) SOC optimization Content management Content hub Repositories Community Workspace manager (Preview) Data connectors Analytics Summary rules Watchlist Automation

Device specific AMA connectors have been deprecated. Learn more >

Starting June 2, 2025, the Codeless Connector Platform (CCP) will be renamed to the Codeless Connector Framework (CCF).

Onboarded Connectors 8 Connected 8 Updates 0 More content at Content Hub

Search by name or provider Providers : Microsoft Data Types : All Status : Connected (8)

| Status    | Connector name                                  | Content Source             | Updates |
|-----------|-------------------------------------------------|----------------------------|---------|
| Connected | Azure Activity                                  | Solution<br>Azure Activity | ...     |
| Connected | Microsoft 365 Insider Risk Management (Preview) | Microsoft                  | ...     |
| Connected | Microsoft Defender for Cloud Apps               | Microsoft                  | ...     |
| Connected | Microsoft Defender for Endpoint                 | Microsoft                  | ...     |
| Connected | Microsoft Defender for Identity                 | Microsoft                  | ...     |
| Connected | Microsoft Defender for Office 365 (Preview)     | Microsoft                  | ...     |
| Connected | Microsoft Defender XDR                          | Microsoft                  | ...     |
| Connected | Microsoft Entra ID Protection                   | Microsoft                  | ...     |

Azure Activity

Connected Microsoft Provider Last Log Received  
Status operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received 9/23/2025, 12:46:59 PM

Content source Azure Activity Version 2.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Related content Workbooks Queries Analytics rules templates

Data received Go to log analytics

Open connector page

**Use Microsoft Defender for Cloud to check for our Vulnerabilities**

**Microsoft Defender for Cloud | Overview**

Showing subscription 'Azure subscription 1'

Search Subscriptions What's new

You may be viewing limited information. To get tenant-wide visibility, click here →

**Security posture**

- Critical recommendations: 0
- Attack paths: 0
- Overdue recommendations: 0/0

Environment risk and secure score: 0%

All recommendations by risk (7): Critical 0 | High 0 | Medium 0 | Low 7 | Not evaluated 0

Total secure score: 0%

Azure - AWS - GCP -

Explore your security posture >

**Regulatory compliance**

Microsoft cloud security benchmark: 59 of 63 controls passed

Lowest compliance standards by controls passed: No additional standards are currently monitored.

Open security policies to manage additional compliance standards

Improve your compliance >

**Workload protections**

Resource coverage: 100% For full protection, enable 4 resource plans

Alerts by severity: High 0 | Medium 0 | Low 0

No security alerts

**Inventory**

Total Resources: 2

Unhealthy (2) | Healthy (0) | Not applicable (0)

Utilize the Permissions Management capability in Defender CSPM

CIEM empowers security admins to identify overprovisioned, unused and super identities to facilitate the implementation and enforcement of least privilege across multi-cloud environments. Explore the CIEM dashboard, to get granular, contextual visibility into all identities, configurations, access policies, and permissions across your multi-cloud estate all at one place.

Upgrade to new Defender CSPM plan

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

Click here to upgrade >

Defender for Cloud community

Join the Defender for Cloud community on GitHub to share knowledge and interact with other customers and experts. The community is a great place to learn and provide feedback.

View Defender for Cloud Community >

## Several found let's Remediate

**stvulnportfolio123**  
storage account

4 Active recommendations | 0 Active alerts

**Resource information**

|                                      |                                         |
|--------------------------------------|-----------------------------------------|
| Subscription<br>Azure subscription 1 | Resource Group<br>rg-security-portfolio |
| Environment<br>Azure                 | Location<br>eastus                      |

**Security value**

Microsoft Defender for Storage  
On

**Recommendations** Alerts

Search: Status == Unhealthy Risk level == All

| Risk level ↑ | Description                                                                                                              | Status ↑    |
|--------------|--------------------------------------------------------------------------------------------------------------------------|-------------|
| Low          | Storage accounts should restrict network access using virtual network rules <span style="color: #0072bc;">Preview</span> | ● Unhealthy |
| Low          | Storage accounts should prevent shared key access <span style="color: #0072bc;">Preview</span>                           | ● Unhealthy |
| Low          | Secure transfer to storage accounts should be enabled                                                                    | ● Unhealthy |
| Low          | Storage account should use a private link connection <span style="color: #0072bc;">Preview</span>                        | ● Unhealthy |

**Storage accounts should restrict network access using virtual network rules** ...

---

Open query View policy definition View recommendation for all resources

.ow risk level
stvulnportfolio... Resource
Unassigned Status
«

**Take action** Graph

Take one of the the following actions in order to mitigate the threat:

Remediate

To protect your storage account from potential threats using virtual network rules:

1. In the Azure portal, open your storage account.
2. From the left sidebar, select 'Networking'.
3. From the 'Allow access from' section, select 'Selected networks'.
4. Add a Virtual network under the 'Virtual networks' section. Do not add allowed IP ranges/ or addresses in the firewall. This i prevent public IPs from accessing your storage account. For details, see: <https://aka.ms/storagenetworksecurity>.

Recommendation owner and set due date

Assign owner and set due date by which recommendation should be implemented.

Assign owner & set due date

Exempt

Exempt the entire recommendation, or disable specific findings using disable rules. Exempted resources appear as not applicable and do not affect secure score.

Exempt

Workflow automation

Set a logic app which you would like to trigger with this security recommendation.

Trigger logic app

Prevention

Enforce remediation for future resources or Deny creation of misconfigured resources

Deny

## Per remediation step create Virtual Network

Copilot         

### Create virtual network

Name \*  ✓

Address space \*  10.0.0.0 - 10.0.255.255 (65536 addresses)

Subscription \*  Azure subscription 1

Resource group \*  rg-security-portfolio [Create new](#)

Location \*  East US

Subnet

Name \*  default

Address range \*  10.0.1.0 - 10.0.1.255 (256 addresses)

DDoS protection  Basic  Standard

Service endpoint  Microsoft.Storage

Firewall  Disabled  Enabled

[Create](#)

1:37 PM  
9/23/2025

**Assigned to me and remediated!**

Storage accounts should restrict network access using IP-based filtering.

[Open query](#) [View policy definition](#) [View recommendation for all resources](#)

| Risk level | Resource                   | Status  |
|------------|----------------------------|---------|
| Low        | vnet-security-portfolio... | On time |

Description

This method is preferred over IP-based filtering, which can leave your storage accounts vulnerable to threats if public IPs gain access. If IP-based filtering is not disabled, your storage accounts could be exposed to potential threats, compromising the security of your data.

General details

|                                                                                                          |                                                                                            |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Scope                                                                                                    | Ticket ID                                                                                  |
|  Azure subscription 1 | -                                                                                          |
| Last change date                                                                                         | Freshness                                                                                  |
| 9/23/2025                                                                                                |  30 Min |

Attack Paths

 0

Risk

Risk factors

Governance

Recommendation owner  agtaraptevin@gmail.com Due date  9/23/2025

Was this recommendation useful?  Yes  No

Search

## Advanced Hunting with KQL in Microsoft Defender

### Rapid Resource Creation Pattern (Potential Cloud Abuse)

|                          |                 |     |                      |         |
|--------------------------|-----------------|-----|----------------------|---------|
| <input type="checkbox"/> | rg-test-hunt-01 | ... | Azure subscription 1 | East US |
| <input type="checkbox"/> | rg-test-hunt-02 | ... | Azure subscription 1 | East US |
| <input type="checkbox"/> | rg-test-hunt-03 | ... | Azure subscription 1 | East US |
| <input type="checkbox"/> | rg-test-hunt-04 | ... | Azure subscription 1 | East US |

### Advanced hunting

Detect Encoded PowerShell Commands\* | New query | +

Schema Functions Queries ...

Search

Favorites

Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"

Shared queries

> Microsoft Sentinel

My queries

Detect Encoded PowerShell Commands

Community queries

> Campaigns

> Discovery

> Impact

> Microsoft Sentinel

> Protection events

> Ransomware

Run query Set in query Save Share link Create summary rule Create detection rule

```
// Detect Rapid Cloud Resource Deployment - Potential Account Takeover
let time_window = 24h;
let threshold = 3;
AzureActivity
| where TimeGenerated > ago(time_window)
| where ActivityStatusValue == "Success"
| where OperationNameValue has_any ("write", "create", "Microsoft.Resources")
| summarize
    TotalOperations = count(),
    UniqueResourceTypes = dcount(ResourceProviderValue),
    ResourcesCreated = make_set(Resource),
    FirstAction = min(TimeGenerated),
    LastAction = max(TimeGenerated)
    by Caller, bin(TimeGenerated, 15m)
| extend DurationMinutes = datetime_diff('minute', LastAction, FirstAction)
| where TotalOperations >= threshold
| extend RiskScore = case(
    TotalOperations >= 10, "Critical",
    TotalOperations >= 5, "High",
    TotalOperations >= 3, "Medium",
    "Low"
)
| project TimeGenerated, Caller, TotalOperations, DurationMinutes, RiskScore, ResourcesCreated
| order by TotalOperations desc
```

Results Query history

Export Show empty columns 4 items Search 00:01:425 Low Chart type Full screen

Filters: Add filter

| TimeGenerated          | Caller                 | TotalOperations | DurationMinutes | RiskScore | ResourcesCreated |
|------------------------|------------------------|-----------------|-----------------|-----------|------------------|
| > Sep 23, 2025 1:30... | agtaraptevin@gmail.com | 5               | 1               | High      | [ ]              |
| > Sep 23, 2025 2:15... | agtaraptevin@gmail.com | 4               | 1               | Medium    | [ ]              |
| > Sep 23, 2025 1:00... | agtaraptevin@gmail.com | 3               | 10              | Medium    | [ ]              |
| > Sep 23, 2025 1:45... | agtaraptevin@gmail.com | 3               | 10              | Medium    | [ ]              |

### Investigate Alert! Suspicious Resource deployment!

Microsoft Defender | Default Directory

Home Exposure management Investigation & response Incidents & alerts Incidents Alerts

Alerts

Export 1 Week

Filter set: Status: New, In progress Add filter Reset all

| Suspicious Resource deployment | Severity | Investigation state | Status | Category            | Detection source   | Product name | Impacted assets |
|--------------------------------|----------|---------------------|--------|---------------------|--------------------|--------------|-----------------|
|                                | Low      | New                 | Impact | Scheduled detection | Microsoft Sentinel | 2 Accounts   |                 |

### Convert Alert to Incident

Home Exposure management Investigation & response Incidents & alerts Incidents Alerts Hunting Advanced hunting Custom detection rules

Incidents

Most recent incidents and alerts

Export Copy list link Refresh

1 Week 1 Incident Search for name or ID Customize columns

Filter set: Save

| Incident name                                        | Incident Id | Tags | Severity | Investigation state | Categories | Impacted assets | Active alerts | Service sources    |
|------------------------------------------------------|-------------|------|----------|---------------------|------------|-----------------|---------------|--------------------|
| > Suspicious Resource deployment involving multip... |             |      | Low      | New                 | Impact     | 2 Accounts      | 1/1           | Microsoft Sentinel |

## Start Incident/Alert Investigation

Incidents > Suspicious Resource deployment involving multiple users

### Suspicious Resource deployment involving multiple users

[Manage incident](#) [Tasks](#) ...

Low | Active | [agtaraptevin@gmail.com](#)

(i) Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Attack story Alerts (1) Assets (2) Investigations (0) Evidence and Response (2) Summary

Alerts

Play attack story Unpin all Show all

Sep 10, 2025 10:18 AM • New  
**Suspicious Resource deployment**  
agtaraptevin@gmail.com

Attack story

Incident graph Layout Group similar nodes

2 Users

2 IPs

Incident details

Assigned to agtaraptevin@gmail.com Incident ID 2

Classification Not set Categories Impact

First activity Sep 10, 2025 Last activity Sep 24, 2025 10:18:00 AM 10:18:00 AM

Workspaces law-security-portfolio

Incident description Identifies when a rare Resource and ResourceGroup deployment occurs by a previously unseen caller.

Impacted assets

Users (2)

agtaraptevin@gmail.com

0382bd81-b553-4960-8b19-ab205bbdd4d

## Verify Queries and IPs

2 Users

Query results

View query

| CallerIpAddress            | Caller                                                                                                                                                                                                 | OperationNameValue    | StartTimeUtc            | EndTimeUtc              | ActivityTimeStamp                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------|
| 146.6.208.44               | agtaraptevin@gmail.com                                                                                                                                                                                 | MICROSOFT.RESOURCE... | Sep 23, 2025 1:01:49 PM | Sep 23, 2025 2:29:22 PM | ["2025-09-23T18:00:00Z", "2025-09-23T18:01:51.2543386Z", "2025-09-23T19:28:20.9223557Z", "2025-09-23T19:28:22.485Z"] |
| CallerIpAddress            | 146.6.208.44                                                                                                                                                                                           |                       |                         |                         |                                                                                                                      |
| Caller                     | agtaraptevin@gmail.com                                                                                                                                                                                 |                       |                         |                         |                                                                                                                      |
| OperationNameValue         | MICROSOFT.RESOURCES/SUBSCRIPTIONS/RESOURCEGROUPS/WRITE                                                                                                                                                 |                       |                         |                         |                                                                                                                      |
| StartTimeUtc               | Sep 23, 2025 1:01:49 PM                                                                                                                                                                                |                       |                         |                         |                                                                                                                      |
| EndTimeUtc                 | Sep 23, 2025 2:29:22 PM                                                                                                                                                                                |                       |                         |                         |                                                                                                                      |
| ActivityTimeStamp          | ["2025-09-23T18:01:49.5667959Z", "2025-09-23T18:01:51.2543386Z", "2025-09-23T19:28:20.9223557Z", "2025-09-23T19:28:22.485Z"]                                                                           |                       |                         |                         |                                                                                                                      |
| ActivityStatusValue        | ["Start", "Success"]                                                                                                                                                                                   |                       |                         |                         |                                                                                                                      |
| CorrelationIds             | ["d21a0e66-f452-448f-ab7661b90d5d", "69563523-76a7-4455-ac9b-ac520461234c", "355eb4b1-dd5a-40c6-a9de-80c669e                                                                                           |                       |                         |                         |                                                                                                                      |
| ResourceGroups             | ["LOGANALYTICSDEFAULTRESOURCES", "RG-TEST-HUNT-01", "RG-TEST-HUNT-02", "RG-TEST-HUNT-03", "RG-TEST-HUNT-04"]                                                                                           |                       |                         |                         |                                                                                                                      |
| ResourceIds                | ["/subscriptions/f73fcad7-e519-46f8-9142-a387884a6c5b/resourcegroups/loganalyticsdefaultresources", "/subscriptions/f73fcad7-e519-46f8-9142-a387884a6c5b/resourcegroups/loganalyticsdefaultresources"] |                       |                         |                         |                                                                                                                      |
| ActivityCountByCallerIP... | 10                                                                                                                                                                                                     |                       |                         |                         |                                                                                                                      |
| Name                       | agtaraptevin                                                                                                                                                                                           |                       |                         |                         |                                                                                                                      |
| UPNSuffix                  | gmail.com                                                                                                                                                                                              |                       |                         |                         |                                                                                                                      |
| > 146.6.208.44             | agtaraptevin@gmail.com                                                                                                                                                                                 | MICROSOFT.RESOURCE... | Sep 23, 2025 1:39:10 PM | Sep 23, 2025 1:39:22 PM | ["2025-09-23T18:00:00Z", "2025-09-23T18:01:51.2543386Z", "2025-09-23T19:28:20.9223557Z", "2025-09-23T19:28:22.485Z"] |
| > 52.253.160.11            | 0382bd81-b553-4960-8b19-ab205bbdd4d                                                                                                                                                                    | MICROSOFT.RESOURCE... | Sep 23, 2025 1:39:21 PM | Sep 23, 2025 1:39:22 PM | ["2025-09-23T18:00:00Z", "2025-09-23T18:01:51.2543386Z", "2025-09-23T19:28:20.9223557Z", "2025-09-23T19:28:22.485Z"] |

**Suspicious Resource deployment**

Low | Unknown | New

Manage alert Move alert to another incident

146.6.208.44 Suspicious

52.253.160.11 Suspicious

Alert description

Identifies when a rare Resource and ResourceGroup deployment occurs by a previously unseen caller.

Analytics rule details

Rule name Suspicious Resource deployment

Rule description Identifies when a rare Resource and ResourceGroup deployment occurs by a previously unseen caller.

View rule in Sentinel

Incident details

Incident Suspicious Resource deployment involving multiple users

Incident severity Low

Active alerts 1/1 Devices 0 Users 2 Mailboxes 0 Apps 0

Impacted assets

## Manage Alert/Incident – Moved to incident to investigate verified test and marked accordingly

The screenshot shows the Microsoft Defender interface for managing alerts. On the left, a large window displays a single alert titled "Suspicious Resource deployment involving multiple users". The alert status is "Low" (blue) and "Active". A note at the top says: "Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days". Below the alert title are tabs: "Attack story", "Alerts (1)", "Assets (2)", "Investigations (0)", "Evidence and Response (2)", and "Summary". Under "Alerts (1)", there are buttons for "Export", "6 Months", "Manage alerts", and "Move alerts". A "Filter set" section includes dropdowns for "Status: New, In progress", "Tags", "Severity", "Investigation state", "Status", and "Category". A specific filter for "Suspicious Resource deployment" is selected. At the bottom right of the alert window are "Save" and "Cancel" buttons.

**Manage alerts**

Status: Resolved

Assign to: agtaraptevin@gmail.com

Classification: Informational, expected activity - Security testing

Comment: Test to verify Suspicious Resource deployment Alert triggers.

## Threat analytics - View current threat campaigns and emerging threats. We need to know our threats!

The screenshot shows the Microsoft Threat Analytics dashboard. The left sidebar contains navigation links: Home, Exposure management, Investigation & response (selected), Threat intelligence, Threat analytics, Intel management, Intel profiles, Intel explorer, Intel projects, Microsoft Sentinel, Email & collaboration, Cases, SOC optimization, and Reports. The main content area has a title "Threat analytics" and a summary bar with counts: Attack campaigns (378), Tools & techniques (178), Activity groups (261), Vulnerabilities (158), and Attack surfaces (6). Below this are two sections: "Latest threats" and "High-impact threats". The "Latest threats" section lists recent activity profiles: "Activity Profile: Void Blizzard impersonates Microsoft in credential phishing campaign" (0/0), "Actor Profile: Storm-2246" (0/0), "Activity Profile: Storm-2026 using fake Microsoft Ads policy violation lure in OAuth p..." (0/0), and "Actor Profile: Storm-0301" (0/0). The "High-impact threats" section lists high-impact profiles: "Technique Profile: Simulated threat" (0/0), "Tool Profile: WannaCrypt" (0/0), "Tool Profile: BadRabbit" (0/0), and "Activity Profile: Smoke Loader (Dofoil) mines coin" (0/0). At the bottom is a search bar and a table with columns: Threat, Alerts, Impacted assets, Report type, Published, and Last updated. The first row shows "Activity Profile: Void Blizzard i..." with 0 active / 0 alerts, categorized as an "Attack campaigns" report, published on Sep 15, 2025 9:26 PM. The second row shows "Actor Profile: Storm-2246" with 0 active / 0 alerts, categorized as an "Activity groups" report, published on Sep 15, 2025 7:27 PM. The third row shows "Activity Profile: Storm-2026 usi..." with 0 active / 0 alerts, categorized as an "Attack campaigns" report, published on Sep 9, 2025 5:24 PM.

## Check enterprise for related incidents and overview including Analyst report.

Microsoft Defender | Default Directory

Threat analytics > Activity Profile: Void Blizzard impersonates Microsoft in credential phishing campaign

Search

Overview Analyst report Related incidents Impacted assets Recommended actions

Analyst report

Please take a moment to provide feedback on this Threat Intelligence profile [here](#).

Microsoft Threat Intelligence observed Russian threat actor **Void Blizzard** conducting a global credential phishing campaign impersonating Microsoft Teams. The actor primarily targeted non-governmental organizations (NGO) in Europe that focus on civil society in the region and in countries neighboring Russia that could hold intelligence value for Moscow.

Microsoft Defender for Endpoint detects this actor's activity with the alert **Void Blizzard Activity**. Organizations can further defend themselves by hardening identity and authentication and email security.

[Read the full analyst report](#)

Related incidents

0 active incidents

Incidents severity

No Active Incidents

Alerts over time

0 08/31 09/07 09/14 09/21

View all related incidents

Active alerts Resolved alerts

Report details

Report type: Attack campaigns Published: Sep 15, 2025 9:26 PM Threat tags: Phishing Last updated: Sep 15, 2025 9:26 PM

Recommended actions

Action status: 0%

0/0 points achieved

100% 50% 0%

Breakdown points by: Category

Points achieved Opportunity

08/09 08/10 08/11 08/12 08/13 08/14 08/15 08/16 08/17 08/18 08/19 08/20 08/21 08/22 08/23 08/24 08/25

Threat analytics > Activity Profile: Void Blizzard impersonates Microsoft in credential phishing campaign

Overview Analyst report Related incidents Impacted assets Recommended actions

### Executive summary

Please take a moment to provide feedback on this Threat Intelligence profile [here](#).

Microsoft Threat Intelligence observed Russian threat actor **Void Blizzard** conducting a global credential phishing campaign impersonating Microsoft Teams. The actor primarily targeted non-governmental organizations (NGO) in Europe that focus on civil society in the region and in countries neighboring Russia that could hold intelligence value for Moscow.

Microsoft Defender for Endpoint detects this actor's activity with the alert **Void Blizzard Activity**. Organizations can further defend themselves by hardening identity and authentication and email security.

### Activity Overview

In July 2025, Russian threat actor Void Blizzard conducted a credential phishing campaign posing as Microsoft likely with the end goal to conduct remote email collection. Credential phishing is designed to deceive a target into entering their account details into an actor-controlled application or website for the purpose of directly using and/or reselling stolen information. The campaign targeted nearly a dozen think tanks and NGOs in Europe that focus on security issues and democracy. Microsoft did not observe any successful compromises, which could be due to public exposure of previous **Void Blizzard** activity as well as other Russian threat actors targeting organizations in similar sectors, increased implementation of automated email protections, and user awareness of this actor's phishing tactics, techniques, and procedures (TTPs). The actor also used domains, such as *office365online[.]co*, that spoof Microsoft services. This domain is not a Void Blizzard-registered domain and is possibly acquired through fraud services, such as offshore domain or phishing kits used in the cybercriminal ecosystem.

The actor used a well-crafted phishing lure using authentic Microsoft graphics and convincing text informing users that their organization is implementing a Microsoft Teams integration effort. The email body contained a malicious link fronted by Cloudflare, allowing the traffic to obfuscate the actual Evilginx attack server behind it. Microsoft has observed Void Blizzard using Evilginx, which is an open-source phish kit used by other threat groups to facilitate adversary-in-the-middle (AitM) attacks, in previous campaigns.

Threat analytics > Activity Profile: Void Blizzard impersonates Microsoft in credential phishing campaign

Overview Analyst report Related incidents Impacted assets Recommended actions

#### Devices with alerts over time

No data available

No data

Devices with active alerts  
Devices with resolved alerts

#### Users with alerts over time

No data available

No data

Users with active alerts  
Users with resolved alerts

#### Mailboxes with alerts over time

No data available

No data

Mailboxes with active alerts  
Mailboxes with resolved alerts

#### Apps with alerts over time

No data available

No data

Apps with active alerts  
Apps with resolved alerts

# Intel Management (Threat Indicators)

## Create Test IoC!

The screenshot shows the Microsoft Defender interface with the 'Intel management' blade selected. The main pane displays a message: '(⌚) No threat intelligence data has been found in your workspace'. Below it are sections for 'What is threat intelligence?' and 'How does it work?'. The right pane is a 'New TI object' dialog for creating an Indicator. It includes fields for 'IPv4 address' (192.168.100.100), 'Domain name' (malicious-test-site.com), and a dropdown for 'All of' or 'Any of' observable types.

## New TI object

This screenshot shows the 'New TI object' form on the left. It includes sections for 'Name' (Test Malicious Infrastructure - Portfolio Demo), 'Indicator types' (Compromised, Malicious activity), 'Kill chains' (Mitre, CommandAndControl), 'Valid from' (9/25/2025, 7:11:00 AM), 'Valid until' (10/25/2025, 12:00:00 AM), 'Source' (Microsoft Sentinel), 'Created' (9/25/2025, 7:11:00 AM), 'Modified' (9/25/2025, 7:11:00 AM), and 'Created by reference'. A green bar at the bottom indicates 'No conflict found.'

## New TI object

This screenshot shows the 'New TI object' form on the right. It includes sections for 'Modified' (9/25/2025, 7:11:00 AM), 'Created by reference' (Select identity), 'Description' (Test threat indicator for portfolio demonstration. Simulated malicious C2 infrastructure used for security testing. Part of threat hunting exercise.), 'Tags' (C2, Demo, Portfolio, Test), 'Revoked' (unchecked), 'Confidence' (0, Is null), 'Traffic light protocol' (empty), 'Severity level' (4), and 'Relationship' (Relationship type: Related to, Target reference: Select TI object). A note states: 'Asserts a non-specific relationship between two SDOs. This relationship can be used when none of the other predefined relationships are appropriate, and a user-defined one is not needed.' A green bar at the bottom indicates 'No conflict found.'

No conflict found.

Add Cancel

Add and duplicate

Add and duplicate

## Add attack Pattern – Spear Phising

### Intel management

Recently, we've upgraded our threat hunting experience by updating the threat intelligence tables schema to incorporate threat actors, attack patterns, and additional objects. For more details on actions required, check out the public docs.

**Filters**

**Indicators (1) Attack patterns (1) Identities (0) Threat actors (0) Relationships (0)**

**+ New Add tags Delete Columns**

| Name                                     | Aliases      | Source             | Confidence | Tags     | Created               | Modified              |
|------------------------------------------|--------------|--------------------|------------|----------|-----------------------|-----------------------|
| Spear Phishing with Malicious Attachment | T1566.001 +1 | Microsoft Sentinel | --         | Email +3 | 9/25/2025, 7:11:00 AM | 9/25/2025, 7:11:00 AM |

## Add Threat actors – APT Group

### Intel management

Recently, we've upgraded our threat hunting experience by updating the threat intelligence tables schema to incorporate threat actors, attack patterns, and additional objects. For more details on actions required, check out the public docs.

**Filters**

**Indicators (1) Attack patterns (1) Identities (0) Threat actors (1) Relationships (0)**

**+ New Add tags Delete Columns**

| Name           | Aliases | Source             | Confidence | Tags        | First seen            | Last seen              |
|----------------|---------|--------------------|------------|-------------|-----------------------|------------------------|
| APT-DEMO-GROUP | +2      | Microsoft Sentinel | --         | APT Demo +2 | 1/1/2024, 12:00:00 AM | 9/25/2025, 12:00:00 AM |

**Generate demo logs to show APT Threat Actor - Simulated threat data was used to safely demonstrate detection capabilities without introducing actual malicious indicators into the environment.**

Microsoft Defender | Default Directory

Advanced hunting

New query +

Run query Last 24 hours Save Share link

Selected workspace: law-security-portfolio Help resources ...

Create summary rule Create detection rule

**Query**

```

1 let ThreatDetections = datatable(
2     TimeGenerated:datetime,
3     ThreatActor:string,
4     SourceIP:string,
5     Operation:string,
6     Severity:string,
7     MITRETechnique:string
8 )
9 [
10     datetime(2025-09-23 10:00:00), "APT-DEMO-GROUP", "192.168.100.100", "Initial Access - Phishing Email", "Critical", "T1566",
11     datetime(2025-09-23 10:05:00), "APT-DEMO-GROUP", "192.168.100.100", "Valid Account Compromise", "High", "T1078",
12     datetime(2025-09-23 10:10:00), "APT-DEMO-GROUP", "192.168.100.100", "Privilege Escalation", "High", "T1068",
13     datetime(2025-09-23 10:15:00), "APT-DEMO-GROUP", "malicious-test-site.com", "Command & Control", "Critical", "T1071",
14     datetime(2025-09-23 10:20:00), "APT-DEMO-GROUP", "10.10.10.10", "Data Exfiltration Started", "Critical", "T1048",
15     datetime(2025-09-23 10:25:00), "APT-DEMO-GROUP", "10.10.10.10", "500MB Data Exported", "Critical", "T1048"
16 ];
17 ThreatDetections
| extend Detection = strcat("⚠️ ALERT: ", ThreatActor, " - ", Operation)
18 | extend ResponseAction = case(
19     Severity == "Critical", "IMMEDIATE: Isolate system, disable accounts",
20     Severity == "High", "URGENT: Investigate and contain",
21     "Monitor and analyze"
22 )
23 | project TimeGenerated, ThreatActor, Operation, SourceIP, Severity, MITRETechnique, ResponseAction

```

**Results**

Query history

Export Show empty columns

6 items Search 0:00:123 Low Chart type Full screen

Filters: Add filter

| TimeGenerated                         | ThreatActor                   | Operation               | SourceIP | Severity | MITRETechnique             | ResponseAction |
|---------------------------------------|-------------------------------|-------------------------|----------|----------|----------------------------|----------------|
| > Sep 23, 2025 5:00... APT-DEMO-GROUP | Initial Access - Phishing ... | 192.168.100.100         | Critical | T1566    | IMMEDIATE: Isolate syst... |                |
| > Sep 23, 2025 5:05... APT-DEMO-GROUP | Valid Account Comprom...      | 192.168.100.100         | High     | T1078    | URGENT: Investigate an...  |                |
| > Sep 23, 2025 5:10... APT-DEMO-GROUP | Privilege Escalation          | 192.168.100.100         | High     | T1068    | URGENT: Investigate an...  |                |
| > Sep 23, 2025 5:15... APT-DEMO-GROUP | Command & Control             | malicious-test-site.com | Critical | T1071    | IMMEDIATE: Isolate syst... |                |
| > Sep 23, 2025 5:20... APT-DEMO-GROUP | Data Exfiltration Start...    | 10.10.10.10             | Critical | T1048    | IMMEDIATE: Isolate syst... |                |

## Create query to show simulated threat data to match Attack pattern of Spear Phishing

Saved

Search

Selected workspace: law-security-portfolio Help resources ...

**Advanced hunting**

New query +

Run query Last 24 hours Save Share link Create summary rule Create detection rule

**Query**

```

1 let AttackPatternDetection = datatable(
2     TimeGenerated:datetime,
3     AttackPattern:string,
4     Phase:string,
5     Technique:string,
6     Evidence:string,
7     Severity:string
8 )
9 [
10     datetime(2025-09-23 12:00:00), "Spear Phishing with Malicious Attachment", "Initial Access", "T1566.001", "Weaponized PDF detected", "Critical",
11     datetime(2025-09-23 12:05:00), "Spear Phishing with Malicious Attachment", "Execution", "T1204.002", "User clicked malicious link", "High",
12     datetime(2025-09-23 12:10:00), "Spear Phishing with Malicious Attachment", "Persistence", "T1547.001", "Registry key created", "High",
13     datetime(2025-09-23 12:15:00), "Spear Phishing with Malicious Attachment", "Defense Evasion", "T1055", "Process injection detected", "Critical",
14     datetime(2025-09-23 12:20:00), "Spear Phishing with Malicious Attachment", "Command & Control", "T1071.001", "HTTPS C2 channel established", "Critical"
15 ];
16 AttackPatternDetection
17 | extend Detection = strcat("Attack Pattern Matched: ", AttackPattern)
18 | extend KillChainProgress = case(
19     Phase == "Command & Control", "Attack successful - Immediate action required",
20     Phase == "Initial Access", "Attack attempted - Monitor closely",
21     "Attack in progress - Containment needed"
22 )
23 | project TimeGenerated, AttackPattern, Phase, Technique, Evidence, Severity, KillChainProgress

```

**Results** Query history

Export Show empty columns 5 items 00:00:706 Search Chart type Full screen

Filters: Add filter

| TimeGenerated          | AttackPattern                            | Phase             | Technique | Evidence                     | Severity | KillChainProgress                             |
|------------------------|------------------------------------------|-------------------|-----------|------------------------------|----------|-----------------------------------------------|
| > Sep 23, 2025 7:00... | Spear Phishing with Malicious Attachment | Initial Access    | T1566.001 | Weaponized PDF detected      | Critical | Attack attempted - Monitor closely            |
| > Sep 23, 2025 7:05... | Spear Phishing with Malicious Attachment | Execution         | T1204.002 | User clicked malicious link  | High     | Attack in progress - Containment needed       |
| > Sep 23, 2025 7:10... | Spear Phishing with Malicious Attachment | Persistence       | T1547.001 | Registry key created         | High     | Attack in progress - Containment needed       |
| > Sep 23, 2025 7:15... | Spear Phishing with Malicious Attachment | Defense Evasion   | T1055     | Process injection detected   | Critical | Attack in progress - Containment needed       |
| > Sep 23, 2025 7:20... | Spear Phishing with Malicious Attachment | Command & Control | T1071.001 | HTTPS C2 channel established | Critical | Attack successful - Immediate action required |

## All Threat intelligence/Intel management working together

Advanced hunting

Selected workspace: law-security-portfolio Help resources Query resources report Schema reference

New query +

Run query Last 24 hours Save Share link Create summary rule Create detection rule

**Query**

```

1 let CombinedDetection = datatable(
2     TimeGenerated:datetime,
3     DetectionType:string,
4     Detail:string,
5     ThreatActor:string,
6     Severity:string,
7     ResponseTaken:string
8 )
9 [
10     datetime(2025-09-23 09:00:00), "Indicator", "192.168.100.100 detected in logs", "APT-DEMO-GROUP", "High", "IP Blocked",
11     datetime(2025-09-23 09:15:00), "Attack Pattern", "Spear Phishing Email Received", "APT-DEMO-GROUP", "Critical", "Email Quarantined",
12     datetime(2025-09-23 09:30:00), "Indicator", "malicious-test-site.com accessed", "APT-DEMO-GROUP", "High", "Domain Sinkholed",
13     datetime(2025-09-23 09:45:00), "Attack Pattern", "Credential Harvesting Attempted", "APT-DEMO-GROUP", "Critical", "Session Terminated",
14     datetime(2025-09-23 10:00:00), "Threat Actor", "APT-DEMO-GROUP TTps Confirmed", "APT-DEMO-GROUP", "Critical", "Incident Response Activated",
15     datetime(2025-09-23 10:15:00), "Indicator", "Data Exfiltration to 10.10.10.", "APT-DEMO-GROUP", "Critical", "Connection Blocked"
16 ];
17 CombinedDetection
18 | summarize
19     TotalDetections = count(),
20     CriticalAlerts = countif(Severity == "Critical"),
21     IndicatorsBlocked = countif(DetectionType == "Indicator"),
22     PatternsDetected = countif(DetectionType == "Attack Pattern")
23 | extend IncidentSummary = "APT-DEMO-GROUP attack successfully detected and contained"
24 | extend ResponseTime = "15 minutes from initial detection to full containment"

```

**Results** Query history

Export Show empty columns 1 item 00:01:378 Search Chart type Full screen

Filters: Add filter

| TotalDetections   | CriticalAlerts | IndicatorsBlocked | PatternsDetected | IncidentSummary                                           | ResponseTime                                          |
|-------------------|----------------|-------------------|------------------|-----------------------------------------------------------|-------------------------------------------------------|
| 6                 | 4              | 3                 | 2                | APT-DEMO-GROUP attack successfully detected and contained | 15 minutes from initial detection to full containment |
| TotalDetections   | 6              |                   |                  |                                                           |                                                       |
| CriticalAlerts    | 4              |                   |                  |                                                           |                                                       |
| IndicatorsBlocked | 3              |                   |                  |                                                           |                                                       |
| PatternsDetected  | 2              |                   |                  |                                                           |                                                       |