

ב-5/11 בשעה 11:01 בבוקר ArcSight נתנה לנו אזהרת Web Site Crawling.
Web-crawler - הוא רובוט חיפוש שמנתח את התוכן של דף אינטרנט.

The screenshot shows the McAfee ESM console interface. At the top, there's a navigation bar with tabs for Database Performance Statistics, ArcSight User Status, ESM System Information, Connector Connection and Cache Status, and Event Throughput. Below this is a sub-navigation bar with buttons for System Events Last Hour, Connector Overview, ESM Overview, All last day, Fired Rules, DSM - Rules Fired, Current Event Sources, and McAfee Alerts. The main content area displays a table titled 'All Rules Fired'.

End Time	Name	Source Address	Destination Address	Source User Name	Destination User Name	Device Address	Host/DNS Name	Reporter Server
5/11 11:01:57	--Web Site Crawling	199.203.100.178	172.16.100.4			192.168.66.1		ArcsightESM

הייתה בעיה באחד השרתים שלנו ב-172.16.100.4 שבו מאוחסן tech.com. תוקף עם כתובת IP 199.203.100.178 תקף אותנו באמצעות פורט 80.

ה-IP התוקף גרם להרבה בקשות GET לדפי האתר בו זמנית

The screenshot displays the ArcSight Console 6.11.0.2339.0 interface. The top menu bar includes File, Edit, View, Windows, Tools, System, and Help. The main window is divided into several panes:

- Navigator:** Shows a tree view of the system structure, including Resources, Packages, Use Cases, and All Use Cases.
- Viewer:** Displays a table of events. The table has columns for Name, Source Address, Destination Address, Source User Name, Destination User Name, Device Address, HostName, and Reporter Server. The first event is named "SS action" and has a source address of "192.168.1.1".
- Inspect/Event Inspector:** Provides a detailed view of the selected event. It includes tabs for Event, Details, Annotations, and Payload. The Event tab is active, showing the event's name, message, type, and various attributes like End Time, Application Protocol, Transport Protocol, Vulnerability Resource, Bytes In, Bytes Out, Generator Resource, Customer Resource, Domain, Domain ID, Domain URI, Domain External ID, Domain Resource, Domain Name, Aggregated Event Count, Correlated Event Count, and Category.

הכנסנו את הכתובת של האתר הזה לדפדפן וקיבלנו שגיאה 404, במקביל יכולנו לגשת באופן חופשי דרך IP, מה שאומר שהמסקנה שלנו הייתה ש-DNS (Domain Name System) הממיר בקשות שמות לכתובות IP, מה שמספק סוף חיבור משתמש עם שרת מסוים בעת הזנת שם דומיין בדפדפן האינטרנט של המשתמש הותקף. נכנסנו ל-Zenoss. שרת ה-DNS היה מושבת.

Zenoss

Dashboard
Events
Infrastructure
Reports
Advanced

Devices
Networks
Processes
IP Services
Windows Services
Network Map
Manufacturers

CNT-DC1
Server/Windows/WinRM/Active Directory
192.168.200.1

Up
Production
Normal

DEVICE STATUS
PRODUCTION STATE
PRIORITY

Overview
Events
Components
Network Routes (5)
File Systems (2)
Processors (1)
Interfaces (16)
Graphs
Modeler Plugins
Configuration Properties

Windows Services

Events	Service Name	Caption	Start Mode	Start Name	Status	Monitored
	BEF	Base Filtering ...	Auto	NT AUTHORITY\...	Unknown	<input type="checkbox"/>
	BES	Background Int...	Manual	LocalSystem	Unknown	<input type="checkbox"/>
	Browse	Computer Brow...	Disabled	LocalSystem	Unknown	<input type="checkbox"/>
	COM+ SysApp	COM+ System...	Manual	LocalSystem	Unknown	<input type="checkbox"/>
	CertProcSvc	Certificate Prop...	Manual	LocalSystem	Unknown	<input type="checkbox"/>
	CredSsp	Cryptographic ...	Auto	NT Authority\N...	Unknown	<input type="checkbox"/>
	DFS	DFS Replication	Auto	LocalSystem	Unknown	<input type="checkbox"/>
	DNS	DNS Server	Auto	LocalSystem	Down	<input checked="" type="checkbox"/>

הכתובת של שרת זה היא 192.168.200.1

The screenshot displays the Zenoss Core web interface for configuring device CNT-DC1 (192.168.200.1). The interface is organized into a sidebar and a main content area. The sidebar contains navigation links for Overview, Events, Components, Graphs, Modeler Plugins, Configuration Properties, Custom Properties, Administration, and Monitoring Templates. The main content area is divided into several sections: Overview (showing device ID, uptime, first seen, last change, model time, locking, and memory/swap), Device Information (title, production state, priority, tag, serial number), Rack Slot, Systems, Groups, Location, Links, Comments, and SNMP configuration (SysName, Location, Contact, Description, Community, Version). The device status is shown as 'Up' and 'Production'.

הפעלנו מחדש את השרת

The screenshot shows the 'Shut Down Windows' dialog box in Windows Server 2012 R2. The dialog box has a title bar 'Shut Down Windows' and a Windows logo. It asks 'What do you want the computer to do?' with a dropdown menu set to 'Restart'. Below this, it says 'Closes all apps, turns off the computer, and then turns it on again.' There is a 'Shutdown Event Tracker' section with a dropdown menu set to 'Hardware: Maintenance (Planned)' and a checkbox for 'Planned' checked. Below this, it says 'A restart or shutdown to service hardware on the system.' There is a 'Comment' text box. At the bottom, there are 'OK' and 'Cancel' buttons.

לאחר אתחול השרת, היו עוד 2 שירותים שהיינו צריכים להפעיל.

