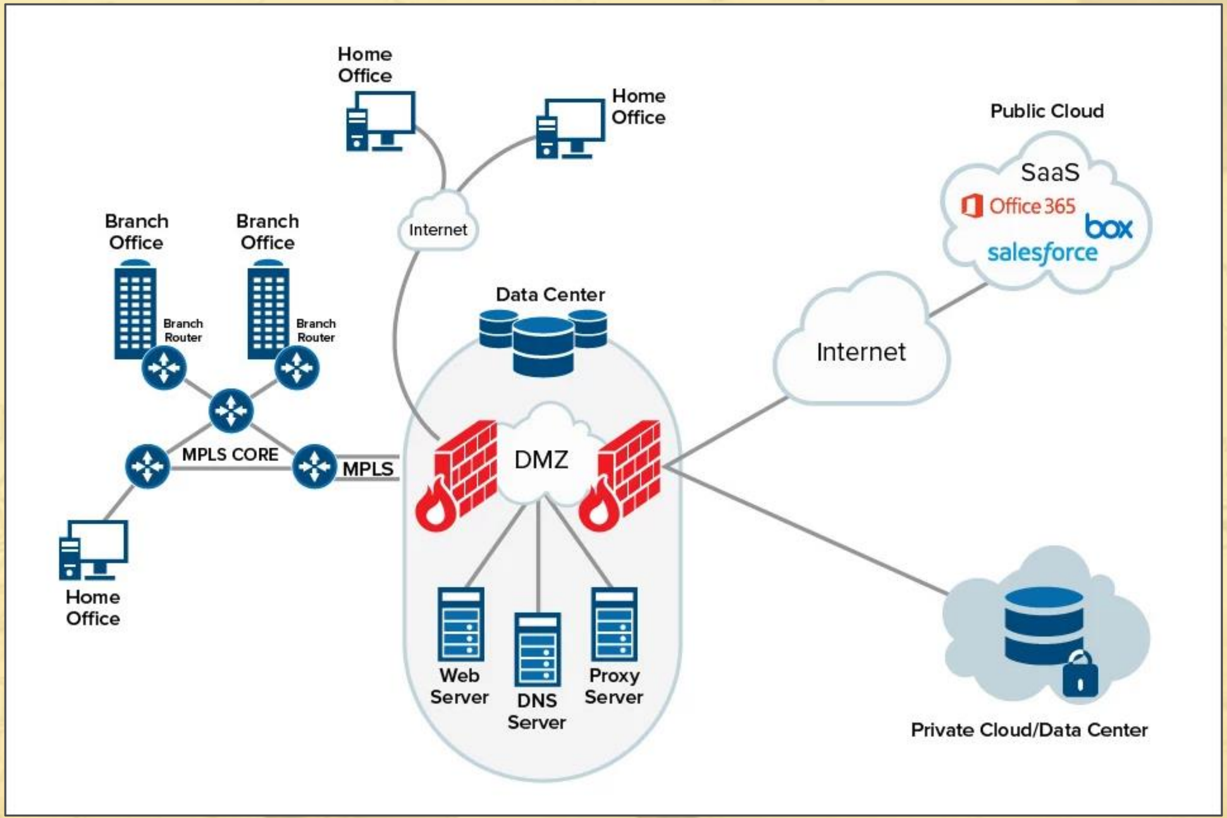
Enterprise Auditing and Logging

Ankur Chowdhary | @lucifer8931 | DevilSec

Index

- Enterprise Network Setup
- Threat Vectors
- Logs
- Windows Events and Auditing
- Automation Using PowerShell
- Linux Logs
- Unified Log Management Tools - Splunk

Enterprise Network Setup



Threat Vectors

Network - Perimeter of the network usually protected by the Firewall.

User – Social Engineering and Social Networking to gather information about users, tricking them into opening pathway for attack.

Email – Phishing attempts and malicious attachments target email threat vector.

Threat Vectors

Web Applications – Inadequately protected web applications being targeted by SQL Injection and Cross Site Scripting (XSS) attacks.

Remote Access – A host/device trying to access secured and unauthorized segments of the network.

Mobile – Smartphones, tablets, and other mobile devices can be used for malware propagation, attacking corporate network.

Threat Vectors

Phishing

Rootkit

Trojan

Botnets

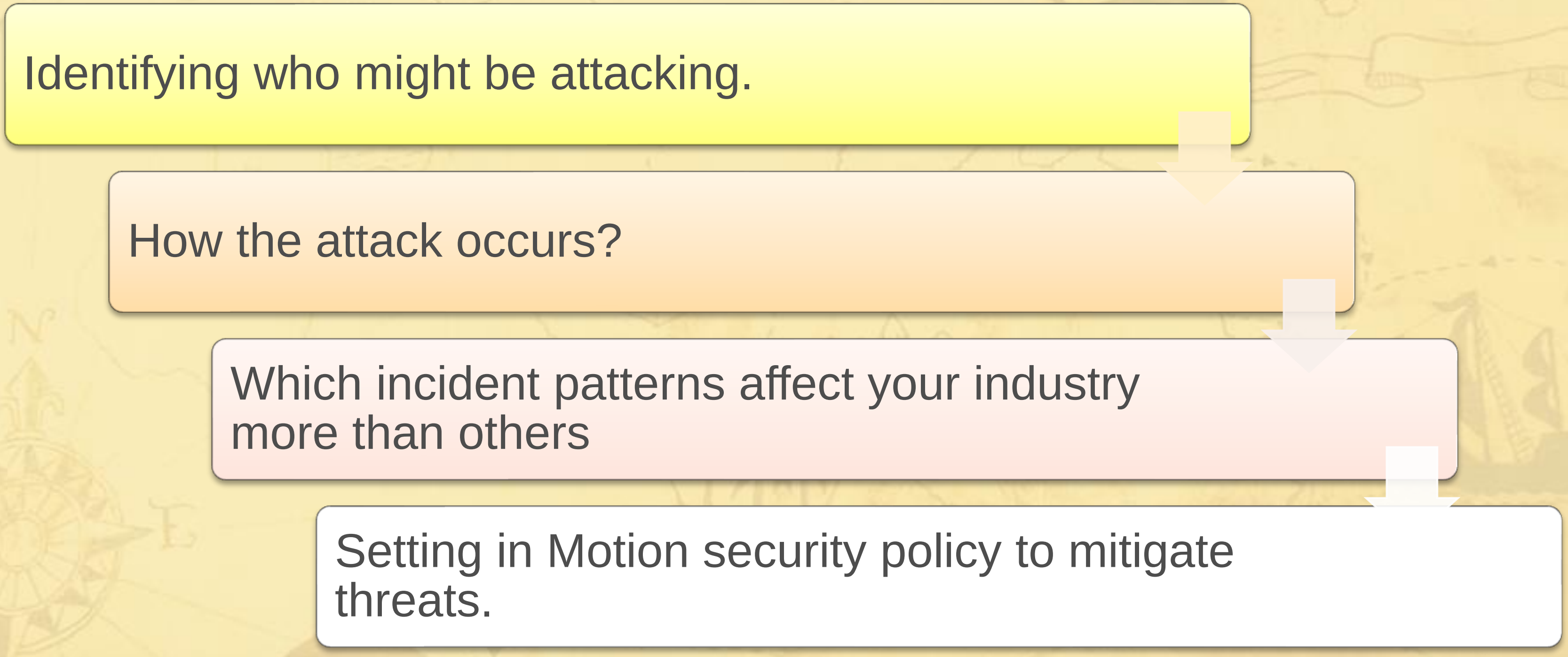
Keylogger

Spyware

Social Engineering

Pharming

Goals



Identifying who might be attacking.

How the attack occurs?

Which incident patterns affect your industry more than others

Setting in Motion security policy to mitigate threats.

Security Information and Event Management (SIEM)

The product capabilities of gathering, analyzing and presenting information from network and security devices

Vulnerability management and policy-compliance tools

Operating-system, database and application logs

External threat data

SIEM Components

- Data Collection – Log Management
- Dashboards – Activities and Patterns
- Alerting – Automated analysis of correlated events
- Compliance – reports adhering to government and security standards
- Retention – Correlation with historical data
- Forensic Analysis – Search over data based on different incident criteria.

Logs

Log Sources

- Server and Workstation OS Log
- Application Logs – Web Server, Database Server
- Security Tool Logs - AV, HIDS, NIDS
- Outbound proxy logs, end-user application logs
- Firewall Logs

Log Locations

- Linux - /var/log
- Windows – System, Security, Application Event Logs
- Network Devices – Syslog, proprietary locations and formats

Windows Events and Incidents

- User Log-on, Log-Off
- User Account Changes
- Password Changes
- Service Started/ Stopped/ Errors
- Registry entries modified
- Object Access Attempts
- Audit, Event Logs Cleared

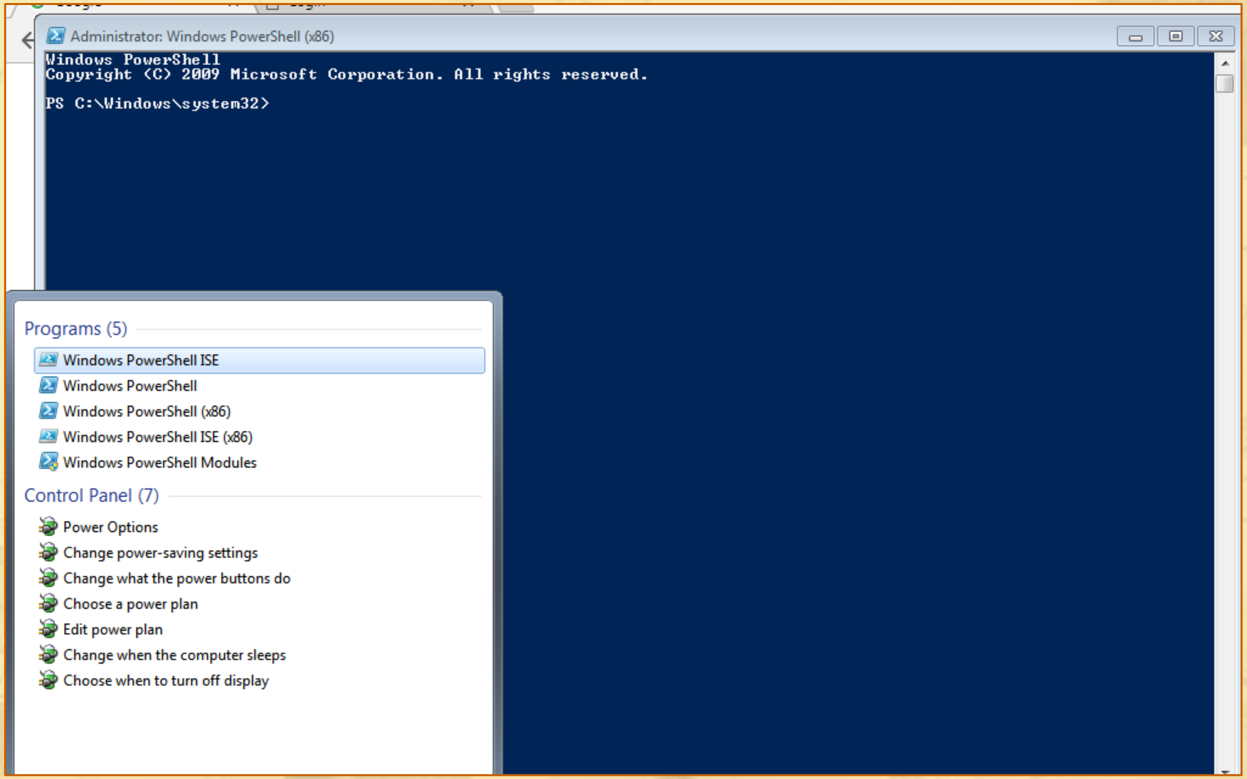
Windows Events and Incidents

Windows Activity	Source	Event ID
App Crash	Application	1001
Application Error	Application	1000
New process Created	Security	4688
Service Installed on the System	Security	4697
Successful Logon	Security	528, 540
Failed Logon	Security	529-537

PowerShell

- Windows PowerShell since version 1 was released in 2006.
- Command-line shell where you run command-line utilities.
- Scripting capabilities.
- Automation for complex tasks.

PowerShell



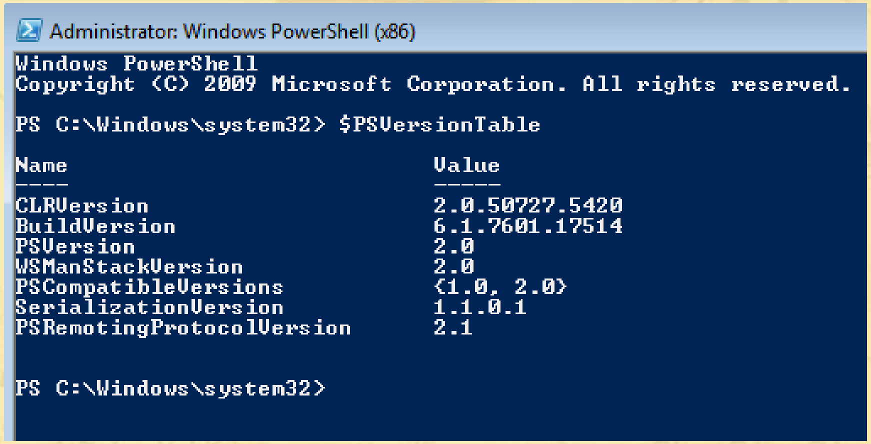
Administrator: Windows PowerShell (x86)

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

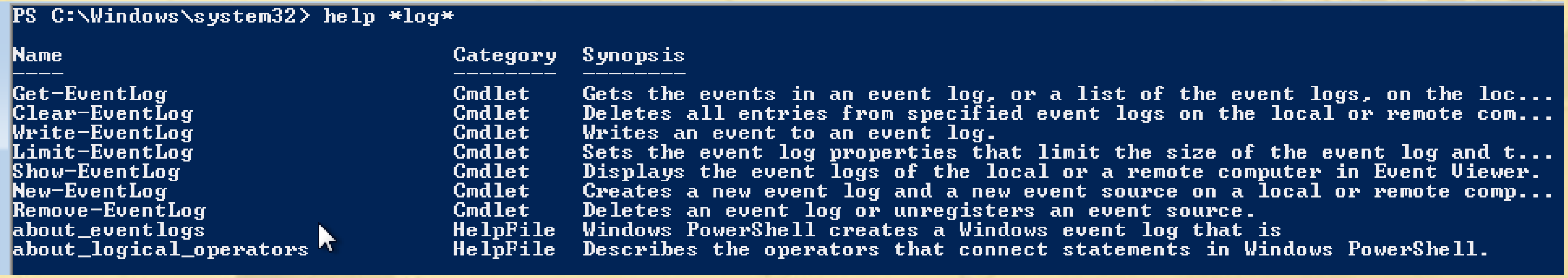
Programs (5)
Windows PowerShell ISE
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE (x86)
Windows PowerShell Modules
Control Panel (7)
Power Options
Change power-saving settings
Change what the power buttons do
Choose a power plan
Edit power plan
Change when the computer sleeps
Choose when to turn off display

PowerShell Basics

- $PSVersionTable
- help Get-Service
- help *log*
- help *event*

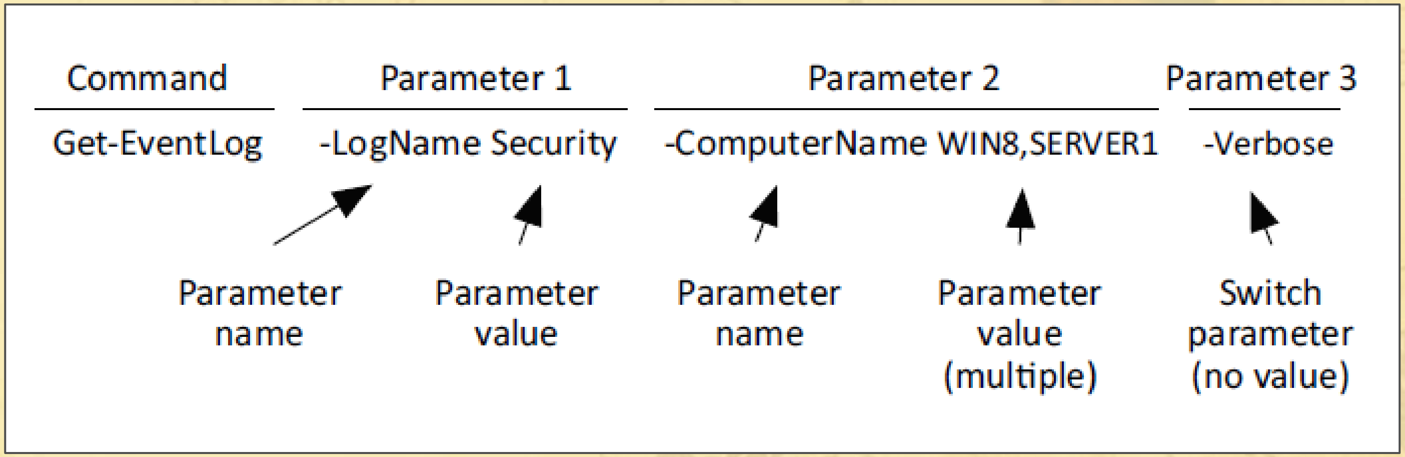


```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $PSVersionTable

Name                           Value
----                           -----
CLRVersion                     2.0.50727.5420
BuildVersion                   6.1.7601.17514
PSVersion                      2.0
WSManStackVersion              2.0
PSCompatibleVersions           {1.0, 2.0}
SerializationVersion           1.1.0.1
PSRemotingProtocolVersion      2.1


PS C:\Windows\system32>
```



```
PS C:\Windows\system32> help *log*

Name                              Category  Synopsis
----                              --------  --------
Get-EventLog                      Cmdlet    Gets the events in an event log, or a list of the event logs, on the loc...
Clear-EventLog                    Cmdlet    Deletes all entries from specified event logs on the local or remote com...
Write-EventLog                    Cmdlet    Writes an event to an event log.
Limit-EventLog                    Cmdlet    Sets the event log properties that limit the size of the event log and t...
Show-EventLog                     Cmdlet    Displays the event logs of the local or a remote computer in Event Viewer.
New-EventLog                      Cmdlet    Creates a new event log and a new event source on a local or remote comp...
Remove-EventLog                   Cmdlet    Deletes an event log or unregisters an event source.
about_eventlogs                   HelpFile  Windows PowerShell creates a Windows event log that is
about_logical_operators           HelpFile  Describes the operators that connect statements in Windows PowerShell.
```

PowerShell Basics



Command

Parameter 1

Parameter 2

Parameter 3

```
Get-EventLog -LogName Security -ComputerName WIN8,SERVER1 -Verbose
```

Parameter name

Parameter value

Parameter name

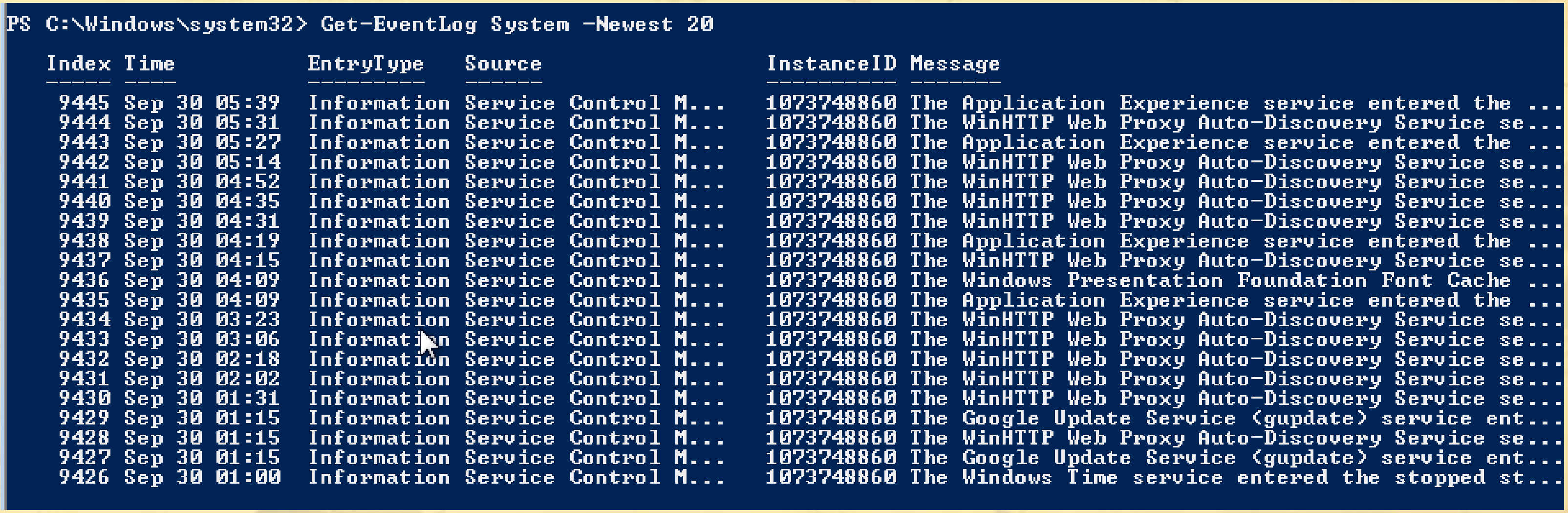
Parameter value (multiple)

Switch parameter (no value)

PowerShell

- Get Newest 20 system event logs

> Get-EventLog System -Newest 20

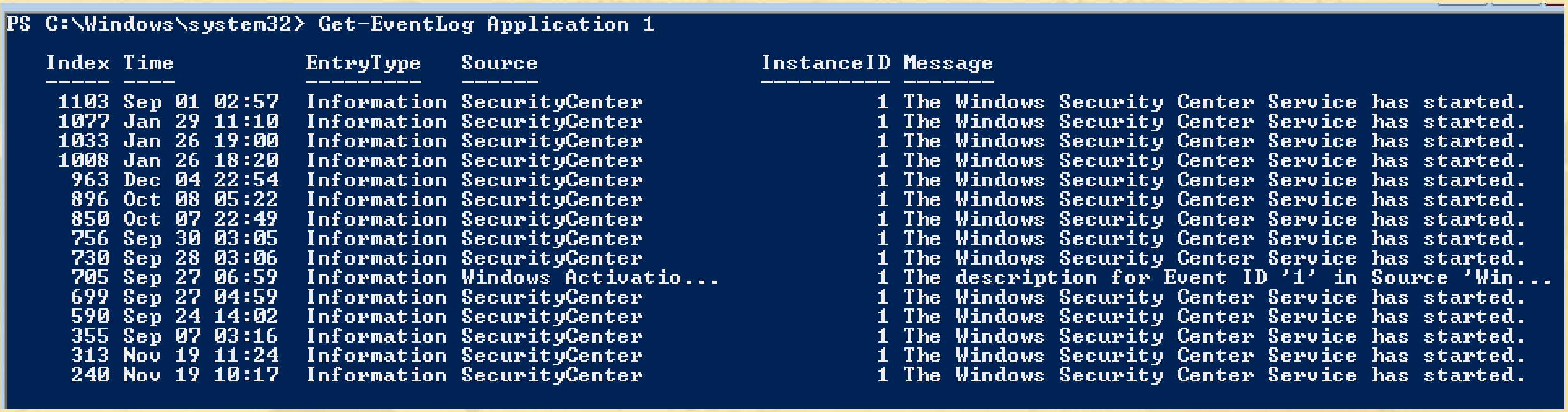


```
PS C:\Windows\system32> Get-EventLog System -Newest 20

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    9445 Sep 30 05:39  Information Service Control M...   1073748860 The Application Experience service entered the ...
    9444 Sep 30 05:31  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9443 Sep 30 05:27  Information Service Control M...   1073748860 The Application Experience service entered the ...
    9442 Sep 30 05:14  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9441 Sep 30 04:52  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9440 Sep 30 04:35  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9439 Sep 30 04:31  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9438 Sep 30 04:19  Information Service Control M...   1073748860 The Application Experience service entered the ...
    9437 Sep 30 04:15  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9436 Sep 30 04:09  Information Service Control M...   1073748860 The Windows Presentation Foundation Font Cache ...
    9435 Sep 30 04:09  Information Service Control M...   1073748860 The Application Experience service entered the ...
    9434 Sep 30 03:23  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9433 Sep 30 03:06  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9432 Sep 30 02:18  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9431 Sep 30 02:02  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9430 Sep 30 01:31  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9429 Sep 30 01:15  Information Service Control M...   1073748860 The Google Update Service (gupdate) service ent...
    9428 Sep 30 01:15  Information Service Control M...   1073748860 The WinHTTP Web Proxy Auto-Discovery Service se...
    9427 Sep 30 01:15  Information Service Control M...   1073748860 The Google Update Service (gupdate) service ent...
    9426 Sep 30 01:00  Information Service Control M...   1073748860 The Windows Time service entered the stopped st...
```

PowerShell

- Positional parameters
- Event with a particular InstanceID

> Get-EventLog Application 1

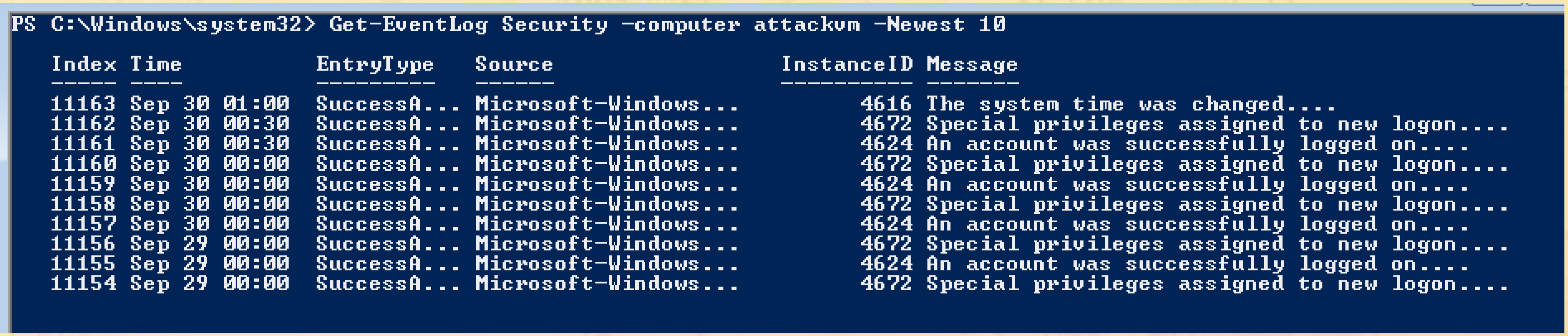


```
PS C:\Windows\system32> Get-EventLog Application 1

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    1103 Sep 01 02:57  Information SecurityCenter                  1 The Windows Security Center Service has started.
    1077 Jan 29 11:10  Information SecurityCenter                  1 The Windows Security Center Service has started.
    1033 Jan 26 19:00  Information SecurityCenter                  1 The Windows Security Center Service has started.
    1008 Jan 26 18:20  Information SecurityCenter                  1 The Windows Security Center Service has started.
     963 Dec 04 22:54  Information SecurityCenter                  1 The Windows Security Center Service has started.
     896 Oct 08 05:22  Information SecurityCenter                  1 The Windows Security Center Service has started.
     850 Oct 07 22:49  Information SecurityCenter                  1 The Windows Security Center Service has started.
     756 Sep 30 03:05  Information SecurityCenter                  1 The Windows Security Center Service has started.
     730 Sep 28 03:06  Information SecurityCenter                  1 The Windows Security Center Service has started.
     705 Sep 27 06:59  Information Windows Activatio...            1 The description for Event ID '1' in Source 'Win...
     699 Sep 27 04:59  Information SecurityCenter                  1 The Windows Security Center Service has started.
     590 Sep 24 14:02  Information SecurityCenter                  1 The Windows Security Center Service has started.
     355 Sep 07 03:16  Information SecurityCenter                  1 The Windows Security Center Service has started.
     313 Nov 19 11:24  Information SecurityCenter                  1 The Windows Security Center Service has started.
     240 Nov 19 10:17  Information SecurityCenter                  1 The Windows Security Center Service has started.
```

PowerShell

- Security Event Logs of a host

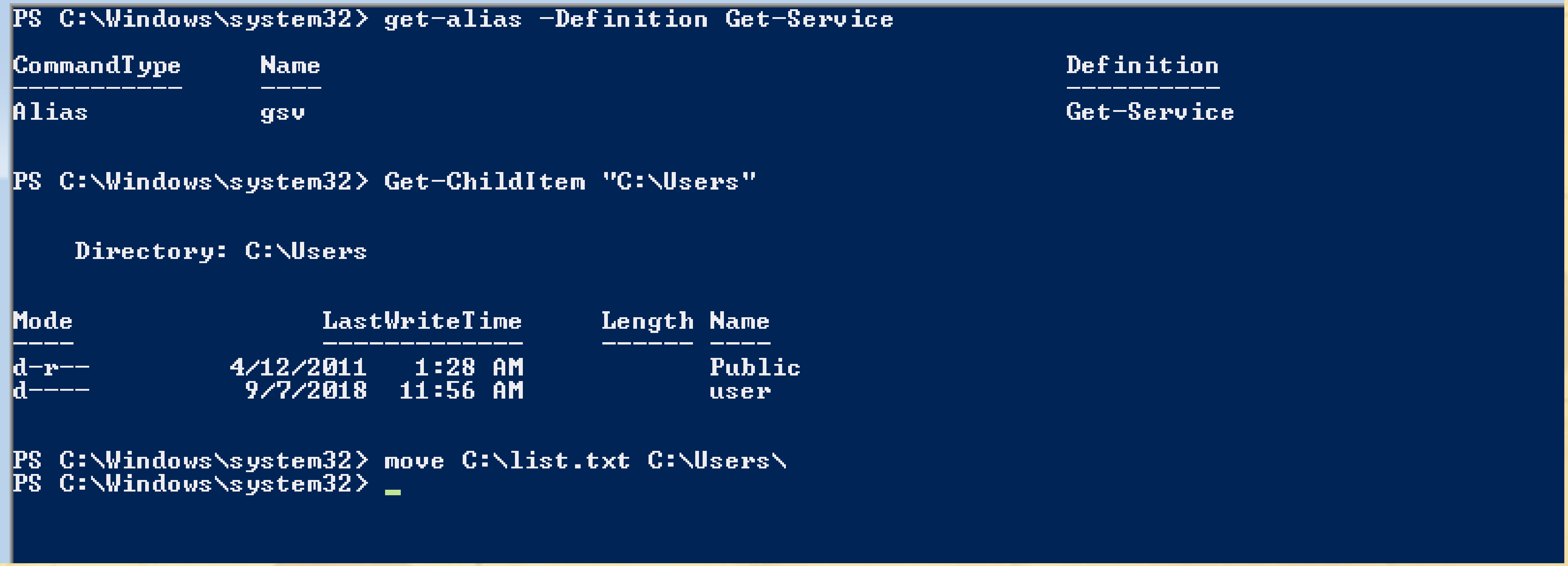
> Get-EventLog Security –computer attackvm –Newest 10



```
PS C:\Windows\system32> Get-EventLog Security -computer attackvm -Newest 10

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
   11163 Sep 30 01:00  SuccessA... Microsoft-Windows...         4616 The system time was changed....
   11162 Sep 30 00:30  SuccessA... Microsoft-Windows...         4672 Special privileges assigned to new logon....
   11161 Sep 30 00:30  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   11160 Sep 30 00:00  SuccessA... Microsoft-Windows...         4672 Special privileges assigned to new logon....
   11159 Sep 30 00:00  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   11158 Sep 30 00:00  SuccessA... Microsoft-Windows...         4672 Special privileges assigned to new logon....
   11157 Sep 30 00:00  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   11156 Sep 29 00:00  SuccessA... Microsoft-Windows...         4672 Special privileges assigned to new logon....
   11155 Sep 29 00:00  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   11154 Sep 29 00:00  SuccessA... Microsoft-Windows...         4672 Special privileges assigned to new logon....
```

PowerShell

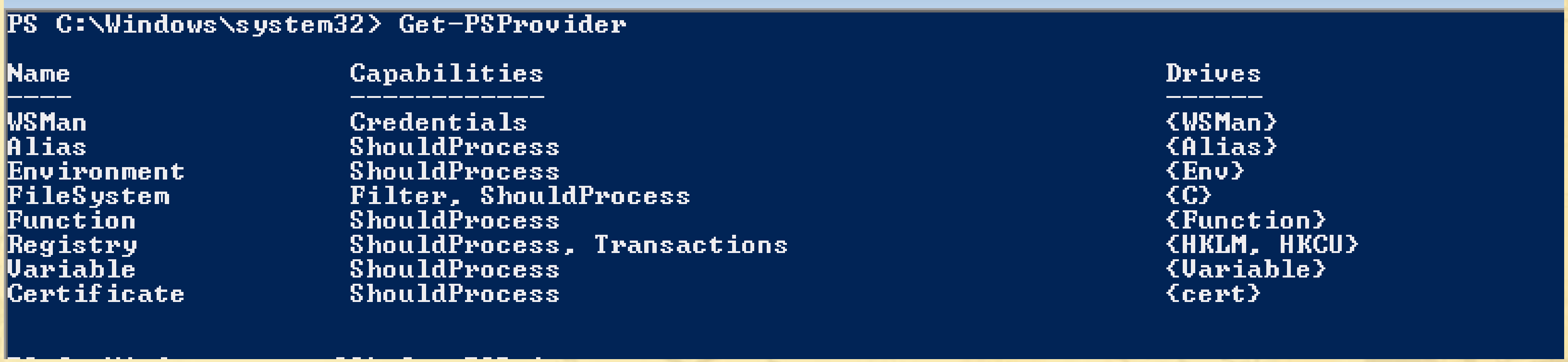
- Shortcuts – alias
- Directory Contents
- Moving Objects



```
PS C:\Windows\system32> get-alias -Definition Get-Service

CommandType     Name                                                      Definition
-----------     ----                                                      ----------
Alias           gsv                                                       Get-Service


PS C:\Windows\system32> Get-ChildItem "C:\Users"


    Directory: C:\Users


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-r--         4/12/2011   1:28 AM            Public
d----          9/7/2018  11:56 AM            user


PS C:\Windows\system32> move C:\list.txt C:\Users\
PS C:\Windows\system32> _
```

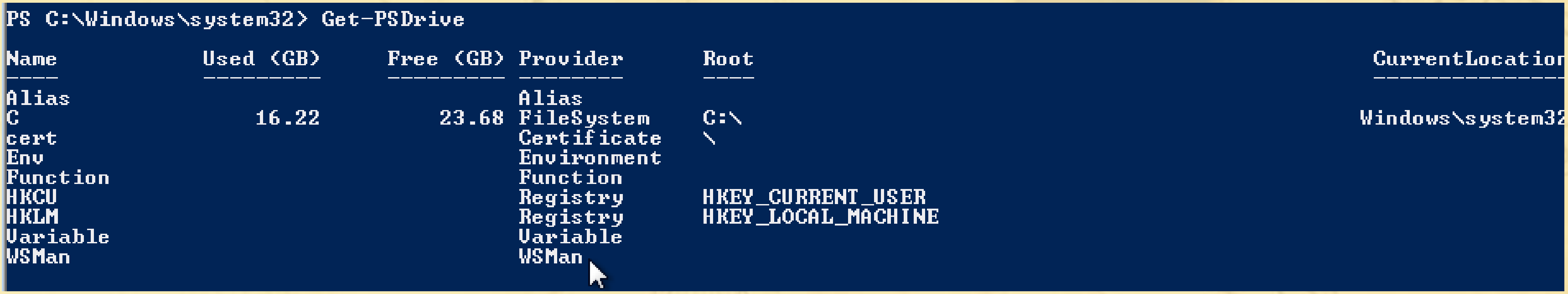
PowerShell Providers

- Adapter that makes data-storage unit looks like a disk drive



```
PS C:\Windows\system32> Get-PSProvider

Name                 Capabilities                                      Drives
----                 ------------                                      ------
WSMan                Credentials                                       {WSMan}
Alias                ShouldProcess                                     {Alias}
Environment          ShouldProcess                                     {Env}
FileSystem           Filter, ShouldProcess                             {C}
Function             ShouldProcess                                     {Function}
Registry             ShouldProcess, Transactions                       {HKLM, HKCU}
Variable             ShouldProcess                                     {Variable}
Certificate          ShouldProcess                                     {cert}
```

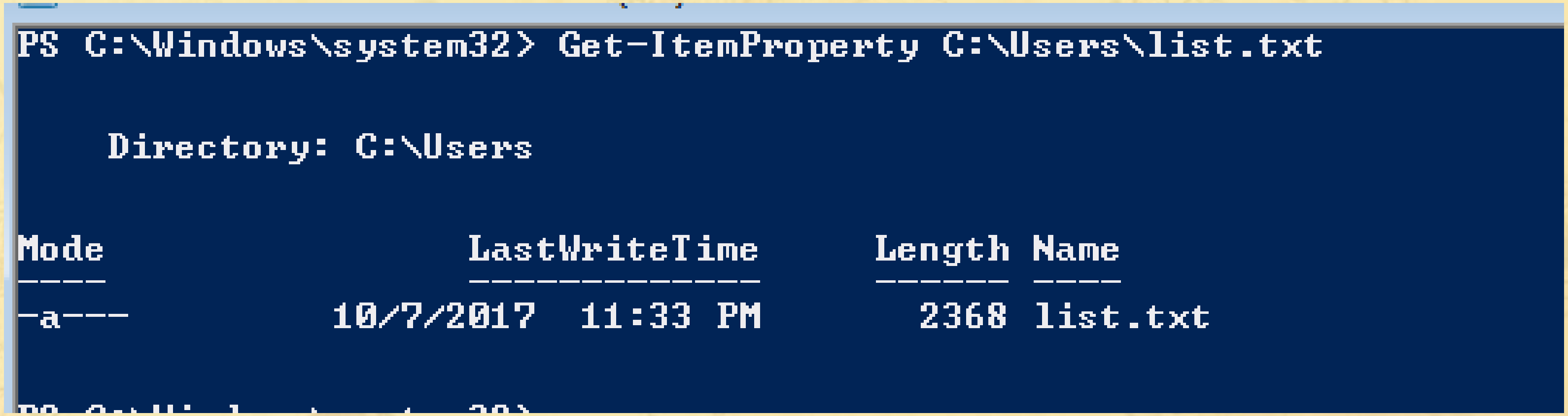
PowerShell PSDrive



```
PS C:\Windows\system32> Get-PSDrive

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Alias                                  Alias
C                  16.22         23.68 FileSystem    C:\                                               Windows\system32
cert                                   Certificate   \
Env                                    Environment
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USER
HKLM                                   Registry      HKEY_LOCAL_MACHINE
Variable                               Variable
WSMan                                  WSMan
```

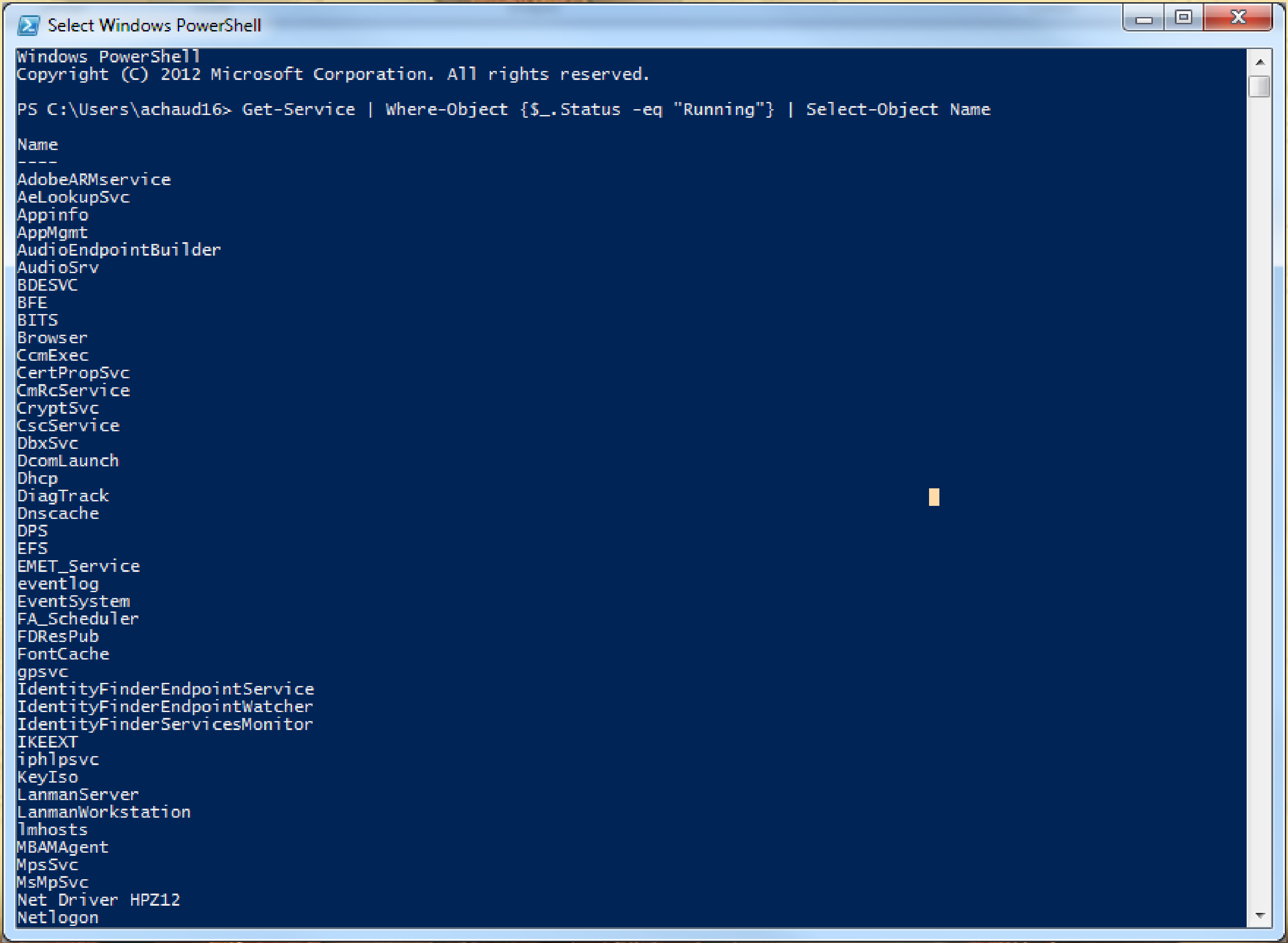
PowerShell

- Clear, Copy, Get, Move, New, Remove, Rename, and Set -Verbs
- Item – Files, Folders
- ItemProperty – Read, Creation Time, Length
- ChildItem
- >Get-ItemProperty C:\Users\list.txt



```
PS C:\Windows\system32> Get-ItemProperty C:\Users\list.txt


    Directory: C:\Users


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         10/7/2017  11:33 PM       2368 list.txt


PS C:\Windows\system32>
```

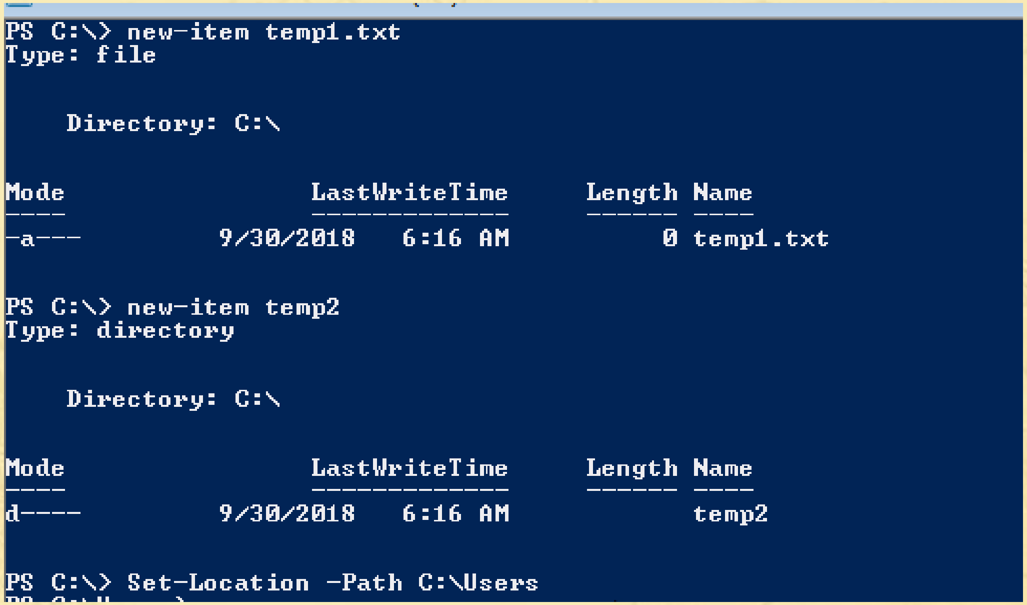
Filter name of the running services



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\achaud16> Get-Service | Where-Object {$_.Status -eq "Running"} | Select-Object Name

Name
----
AdobeARMservice
AeLookupSvc
Appinfo
AppMgmt
AudioEndpointBuilder
AudioSrv
BDESVC
BFE
BITS
Browser
CcmExec
CertPropSvc
CmRcService
CryptSvc
CscService
DbxSvc
DcomLaunch
Dhcp
DiagTrack
Dnscache
DPS
EFS
EMET_Service
eventlog
EventSystem
FA_Scheduler
FDResPub
FontCache
gpsvc
IdentityFinderEndpointService
IdentityFinderEndpointWatcher
IdentityFinderServicesMonitor
IKEEXT
iphlpsvc
KeyIso
LanmanServer
LanmanWorkstation
lmhosts
MBAMAgent
MpsSvc
MsMpSvc
Net Driver HPZ12
Netlogon
```

PowerShell

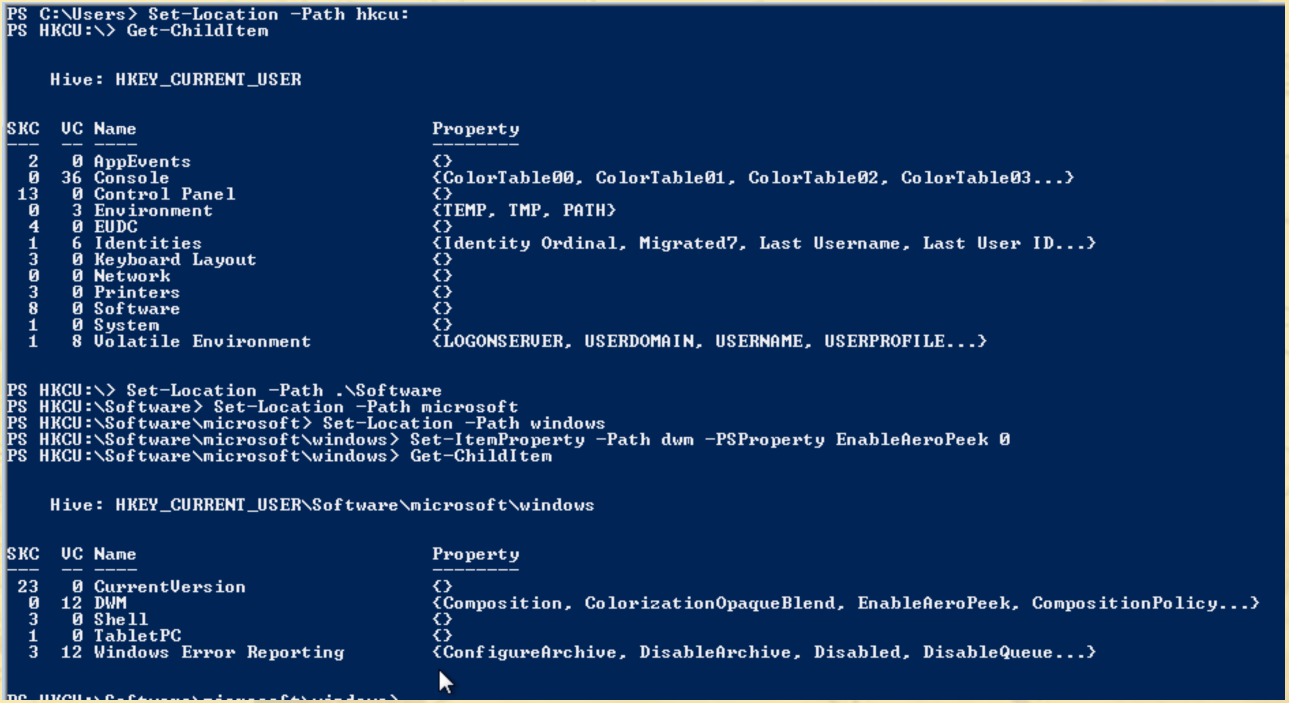
- Creating new files, folders
- Changing Directory



```
PS C:\> new-item temp1.txt
Type: file


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         9/30/2018   6:16 AM          0 temp1.txt


PS C:\> new-item temp2
Type: directory


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         9/30/2018   6:16 AM            temp2


PS C:\> Set-Location -Path C:\Users
```

PowerShell

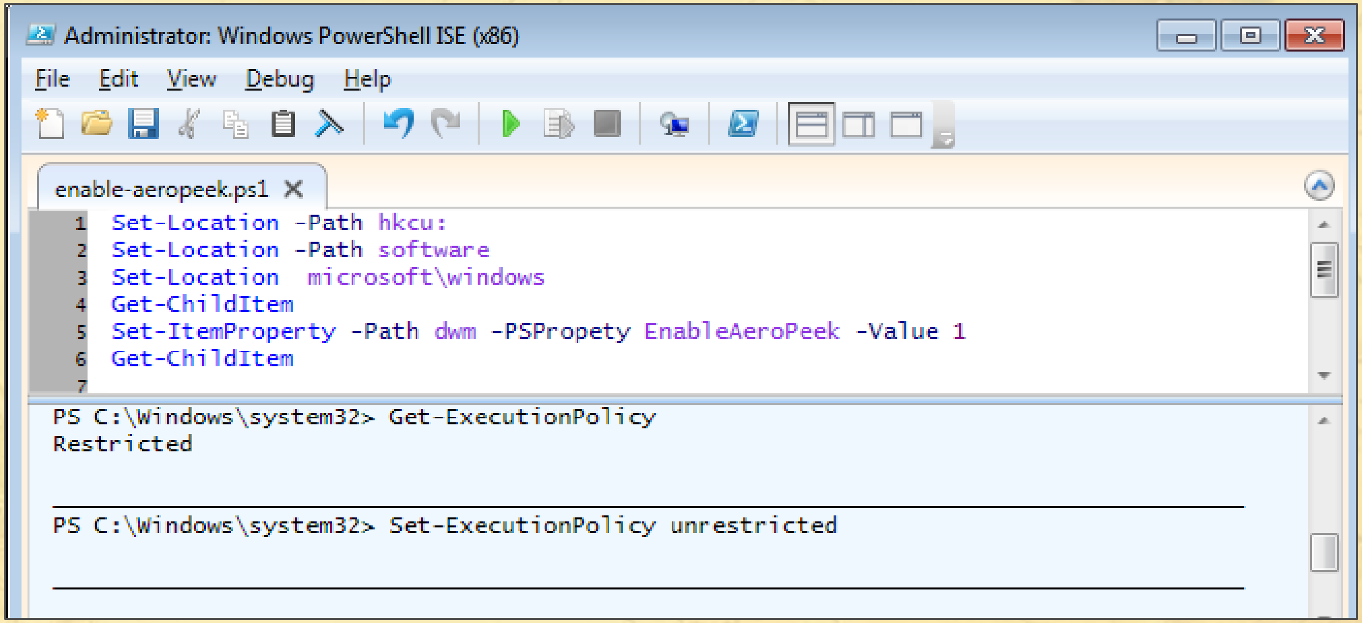
- Changing Registry Values
- Turn Off AeroPeek Feature



```
PS C:\Users> Set-Location -Path hkcu:
PS HKCU:\> Get-ChildItem


    Hive: HKEY_CURRENT_USER


SKC  VC Name                           Property
---  -- ----                           --------
  2   0 AppEvents                      {}
  0  36 Console                        {ColorTable00, ColorTable01, ColorTable02, ColorTable03...}
 13   0 Control Panel                  {}
  0   3 Environment                    {TEMP, TMP, PATH}
  4   0 EUDC                           {}
  1   6 Identities                     {Identity Ordinal, Migrated7, Last Username, Last User ID...}
  3   0 Keyboard Layout                {}
  0   0 Network                        {}
  3   0 Printers                       {}
  8   0 Software                       {}
  1   0 System                         {}
  1   8 Volatile Environment           {LOGONSERVER, USERDOMAIN, USERNAME, USERPROFILE...}


PS HKCU:\> Set-Location -Path .\Software
PS HKCU:\Software> Set-Location -Path microsoft
PS HKCU:\Software\microsoft> Set-Location -Path windows
PS HKCU:\Software\microsoft\windows> Set-ItemProperty -Path dwm -PSProperty EnableAeroPeek 0
PS HKCU:\Software\microsoft\windows> Get-ChildItem


    Hive: HKEY_CURRENT_USER\Software\microsoft\windows


SKC  VC Name                           Property
---  -- ----                           --------
 23   0 CurrentVersion                 {}
  0  12 DWM                            {Composition, ColorizationOpaqueBlend, EnableAeroPeek, CompositionPolicy...}
  3   0 Shell                          {}
  1   0 TabletPC                       {}
  3  12 Windows Error Reporting        {ConfigureArchive, DisableArchive, Disabled, DisableQueue...}


PS HKCU:\Software\microsoft\windows>
```

PowerShell Scripting

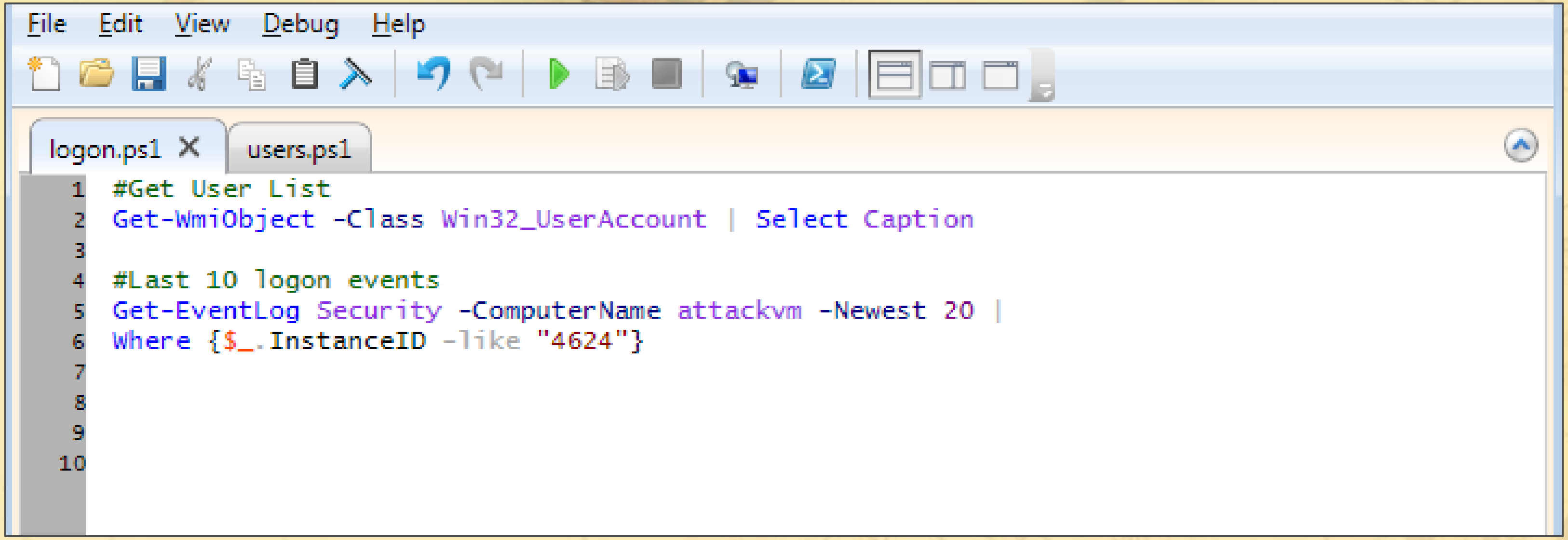
- Set-ExecutionPolicy



```
Set-Location -Path hkcu:
Set-Location -Path software
Set-Location  microsoft\windows
Get-ChildItem
Set-ItemProperty -Path dwm -PSPropety EnableAeroPeek -Value 1
Get-ChildItem
```

```
PS C:\Windows\system32> Get-ExecutionPolicy
Restricted

PS C:\Windows\system32> Set-ExecutionPolicy unrestricted
```

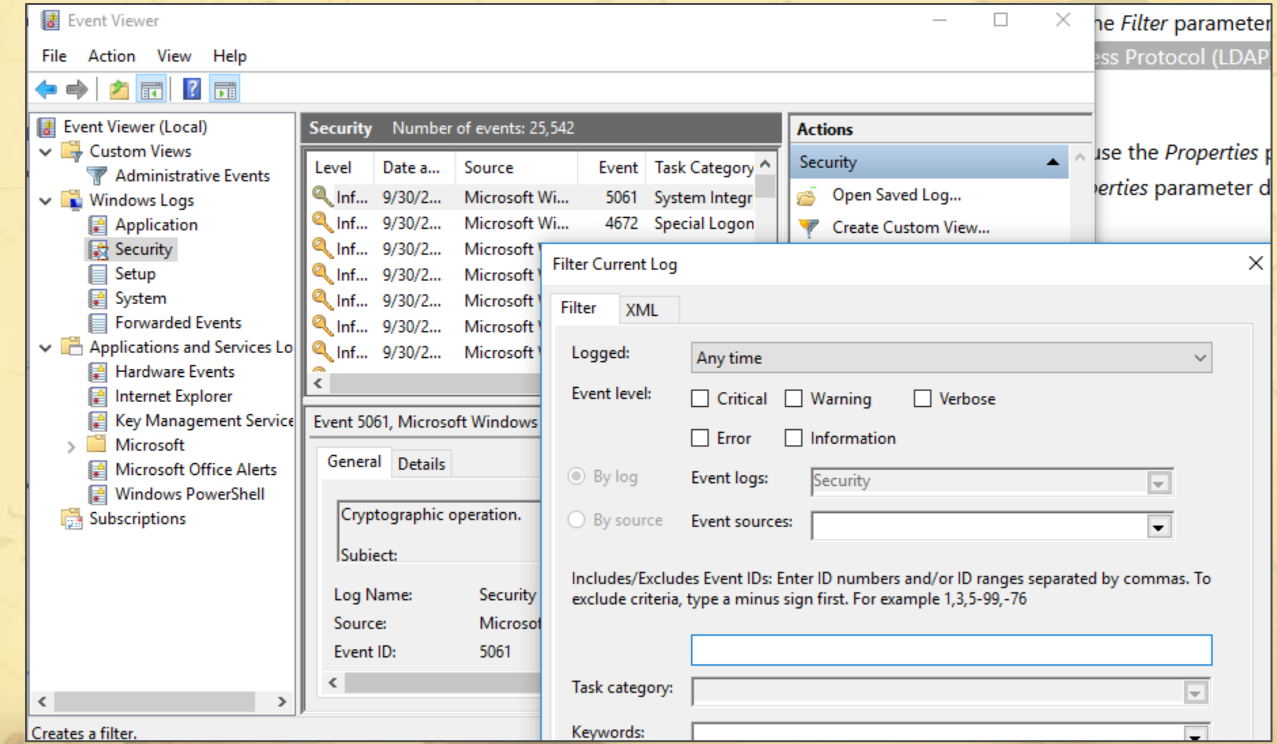
PowerShell Scripts



```
#Get User List
Get-WmiObject -Class Win32_UserAccount | Select Caption

#Last 10 logon events
Get-EventLog Security -ComputerName attackvm -Newest 20 |
Where {$_.InstanceID -like "4624"}
```

Windows Event Viewer

- Shows windows application logs and system messages.
- Useful tool for security assessment and troubleshooting



Security Number of events: 25,542

Level	Date a...	Source	Event	Task Category
Inf...	9/30/2...	Microsoft Wi...	5061	System Integr
Inf...	9/30/2...	Microsoft Wi...	4672	Special Logon
Inf...	9/30/2...	Microsoft		
Inf...	9/30/2...	Microsoft		
Inf...	9/30/2...	Microsoft		
Inf...	9/30/2...	Microsoft		
Inf...	9/30/2...	Microsoft		

Event 5061, Microsoft Windows

General Details

Cryptographic operation.

Subject:

Log Name: Security
Source: Microsof
Event ID: 5061

Filter Current Log

Filter XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

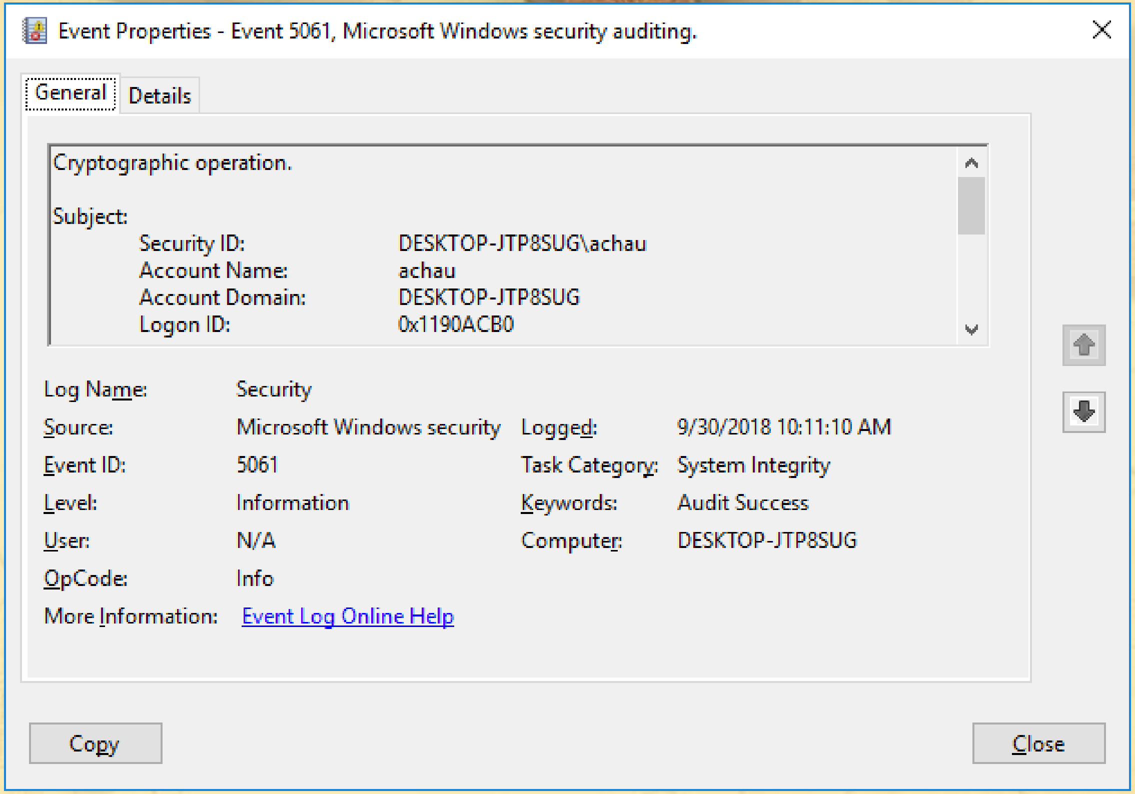
○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

Task category:

Keywords:

Windows Event Viewer



Event Properties - Event 5061, Microsoft Windows security auditing.

```
Cryptographic operation.

Subject:
        Security ID:        DESKTOP-JTP8SUG\achau
        Account Name:       achau
        Account Domain:     DESKTOP-JTP8SUG
        Logon ID:           0x1190ACB0
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/30/2018 10:11:10 AM
Event ID:	5061	Task Category:	System Integrity
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-JTP8SUG
OpCode:	Info		
More Information:	Event Log Online Help		

Auditing

- Information security is not only compromised by individuals outside the company, but those inside as well.
- Does your company have internal auditing?
- Do they think audits are necessary?
- Auditing is a very important process that will uncover any holes in network security.
- Auditing can be done through informal self audits and formal information technology (IT) audits.

Auditing Types

- Self Audits – Scope, Compliance with govt. standards, PCI, HIPPA
- IT Audits
- Determine the threats and vulnerabilities creating a risk to the business environment.
- IT auditors will create several individual test cases towards testing the security of the server and its environment.
- Audit Reports

Linux Logs

- /var/log/messages

-Global system messages including the messages logged during system startup

- /var/log/dmesg

Information on hardware devices detected by the kernel during boot phase.

- /var/log/auth.log

Authorization information including user-logins and authentication mechanism used.

Linux Logs

- /var/log/daemon.log

Log file for processes running in the background

- /var/log/lastlog

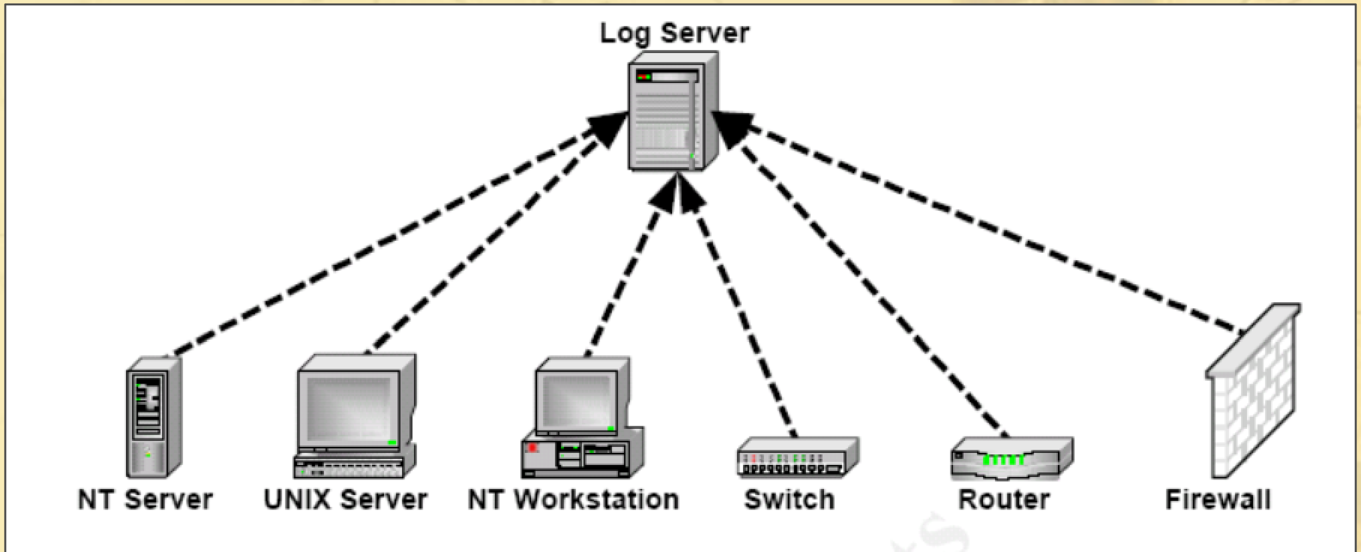
Login information for all users

- /var/log/mail.log

Mail Server Logs

- Application Logs - /var/log/httpd, /var/log/apache2, /var/log/mysql.log

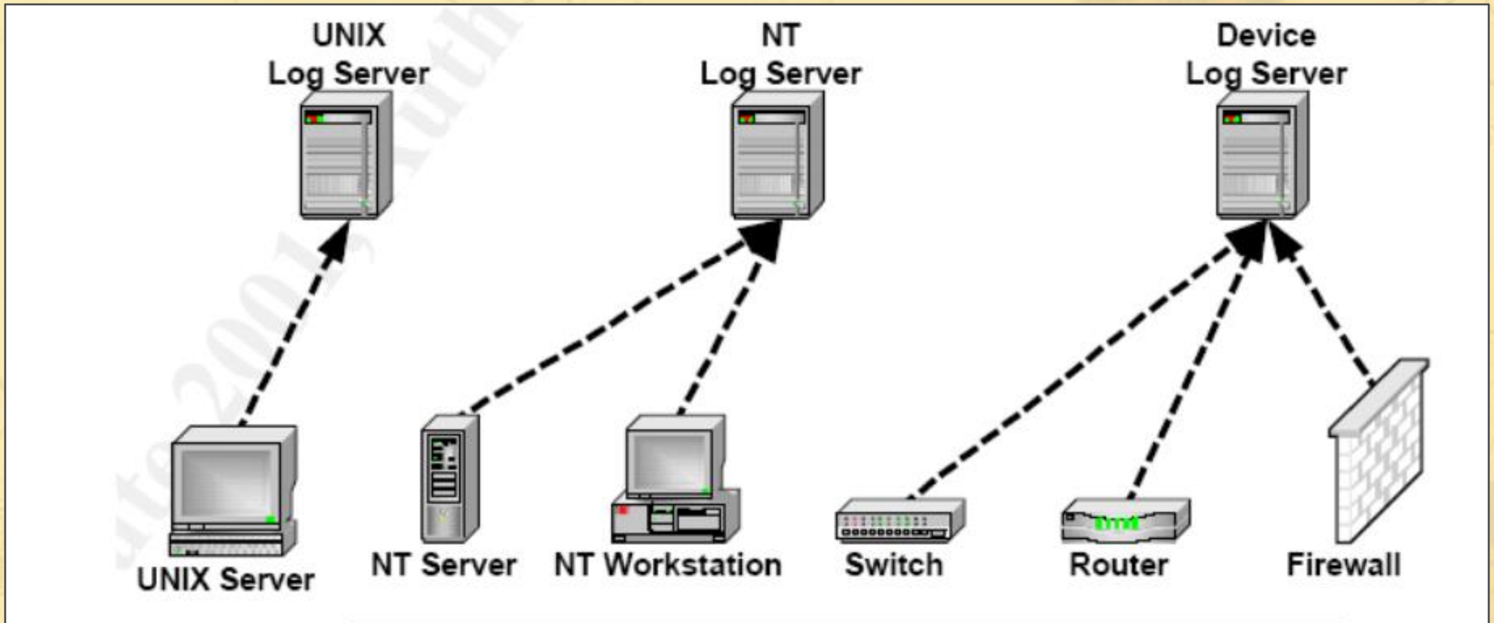
Logging Mechanism – Centralized Logging



Logging Scenario A

All devices report back to a common central logging server.

Logging Mechanism – Distributed Logging

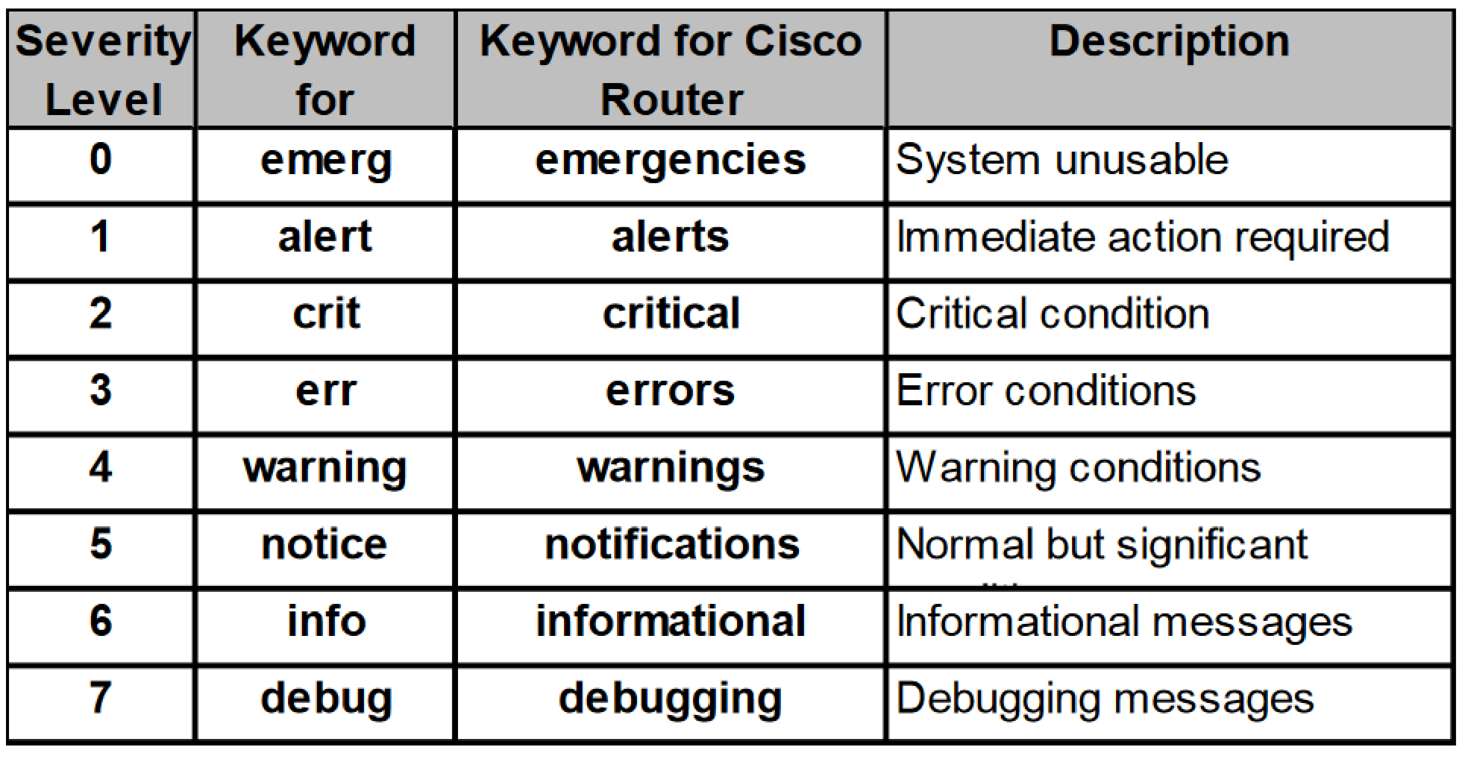


Logging Scenario B
All similar devices report back to a designated logging server.

Syslog

- Syslog is a utility for tracking and logging all manner of system messages from the merely informational to the extremely critical.
- Each msg sent to the syslog server has two descriptive labels:
- Function Facility for the application that generated it, e.g., mail, cron, auth (security logs).
- Severity Level of the message.

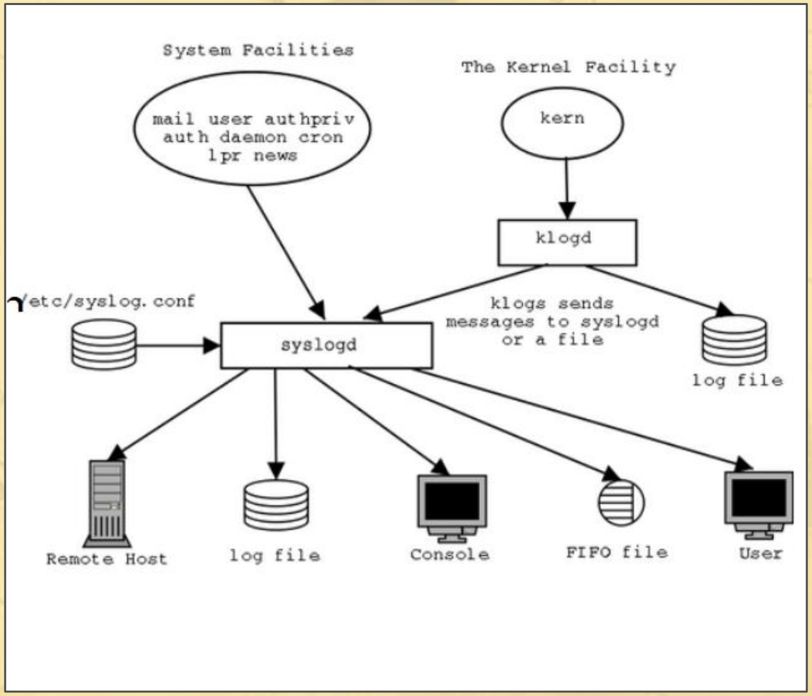
Syslog Severity Levels



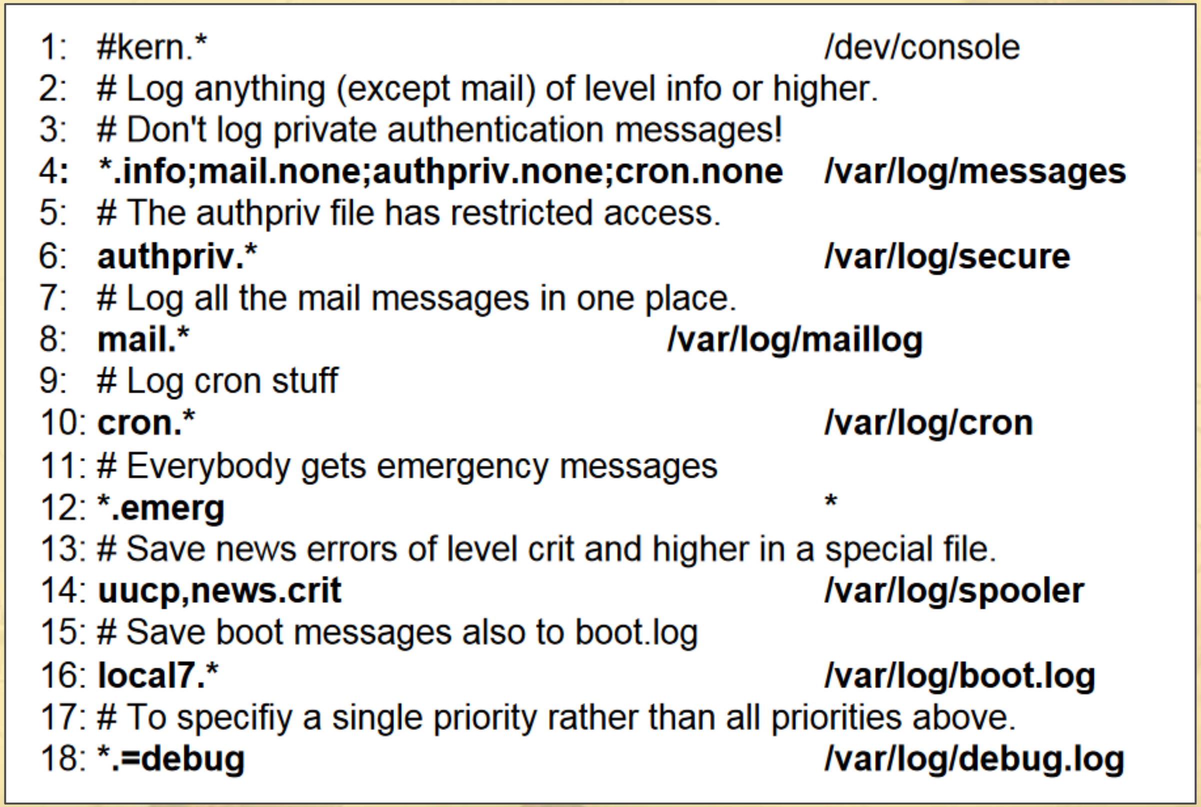
Severity Level	Keyword for	Keyword for Cisco Router	Description
0	emerg	emergencies	System unusable
1	alert	alerts	Immediate action required
2	crit	critical	Critical condition
3	err	errors	Error conditions
4	warning	warnings	Warning conditions
5	notice	notifications	Normal but significant
6	info	informational	Informational messages
7	debug	debugging	Debugging messages

Syslog

- **syslogd** collects the logs from various agents in a centralized manner.
- Logging is configured in /etc/syslog.conf files containing names and locations for your system log files.
- **klogd** takes care of kernel log messages



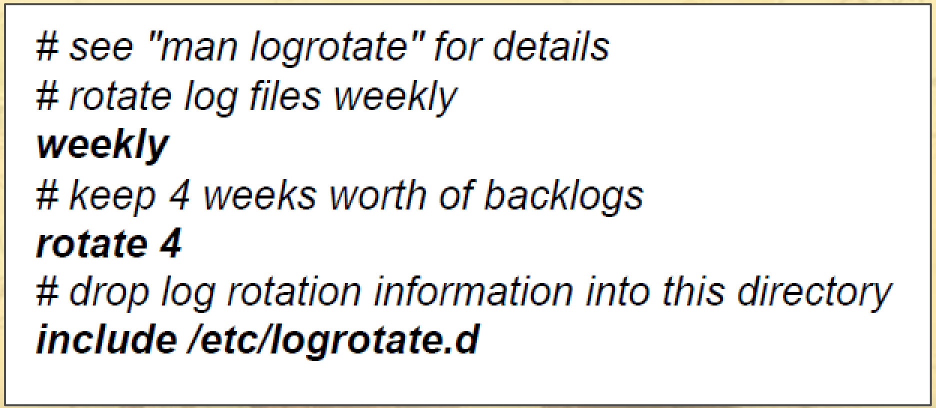
Sample syslog.conf



```
#kern.*                                          /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none         /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                       /var/log/secure
# Log all the mail messages in one place.
mail.*                                   /var/log/maillog
# Log cron stuff
cron.*                                           /var/log/cron
# Everybody gets emergency messages
*.emerg                                          *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                   /var/log/spooler
# Save boot messages also to boot.log
local7.*                                         /var/log/boot.log
# To specifiy a single priority rather than all priorities above.
*.=debug                                         /var/log/debug.log
```

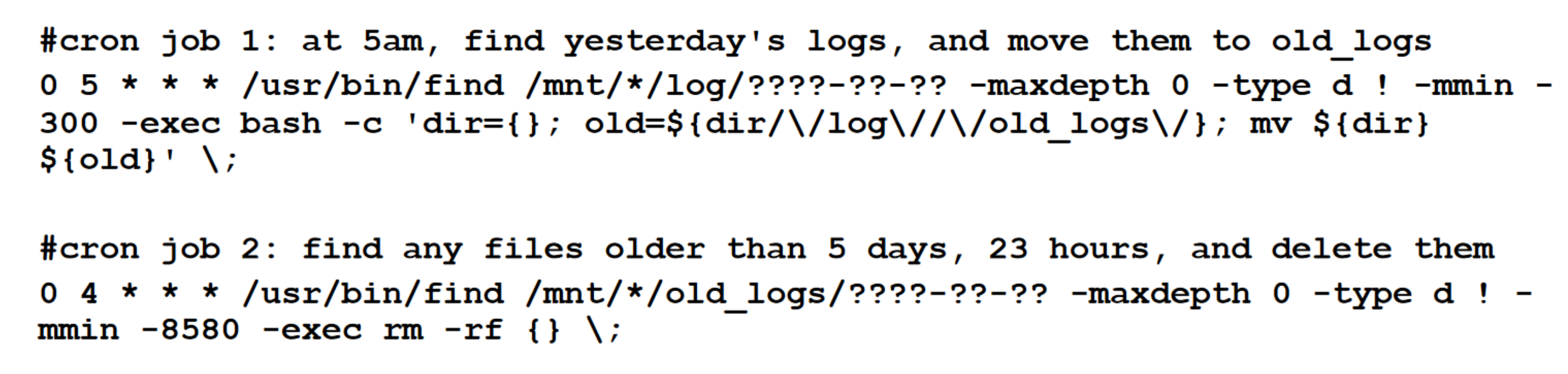
Log Rotation

- Log Files can grow a lot and become useless.
- Logrotate service rotates log files, conserving only compressed logs under a specified age.
- Logrotate is executed by the crond in regular basis and its main configuration file is /etc/logrotate.conf



```
# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# drop log rotation information into this directory
include /etc/logrotate.d
```

Log Rotation

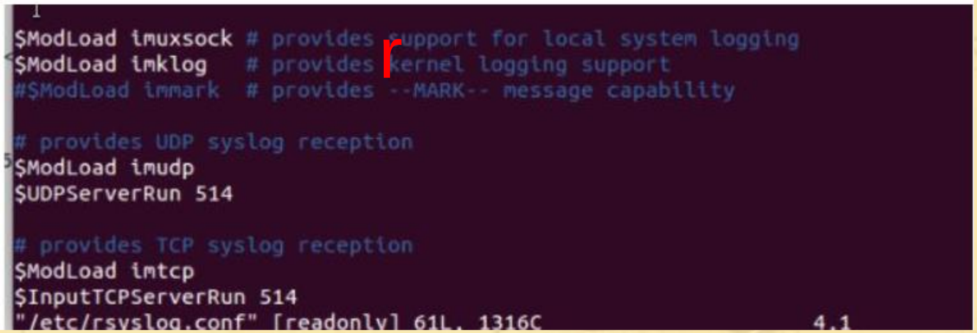


```
#cron job 1: at 5am, find yesterday's logs, and move them to old_logs
0 5 * * * /usr/bin/find /mnt/*/log/????-??-?? -maxdepth 0 -type d ! -mmin -
300 -exec bash -c 'dir={}; old=${dir/\/log\//\/old_logs\/}; mv ${dir}
${old}' \;

#cron job 2: find any files older than 5 days, 23 hours, and delete them
0 4 * * * /usr/bin/find /mnt/*/old_logs/????-??-?? -maxdepth 0 -type d ! -
mmin -8580 -exec rm -rf {} \;
```

Configuring the Remote Syslog Server

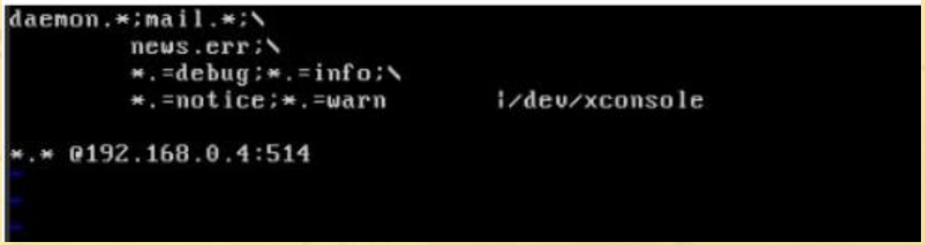
- Edit /etc/rsyslog.conf
- Restart the service- service rsyslog restart
- Add iptables rule if required *iptables –A INPUT –m state –state NEW –m tcp –p tcp --dport 514 –j ACCEPT*
- Restart iptables service.

Server



```
$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
"/etc/rsyslog.conf" [readonly] 61L, 1316C                          4,1
```

Client



```
daemon.*;mail.*;\
        news.err;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole

*.* @192.168.0.4:514
~
~
~
```

Defense Against Log and Accounting File Attacks

- Active Logging
- Set proper permissions
- Keep a separate log server
- Encrypt the log files - Core Labs tools at http://www.core-sdi.com/english/freesoft.html
- Make Log files append only; $ chattr +a [logname]
- Protecting log files with write-once media, such as CD-ROM

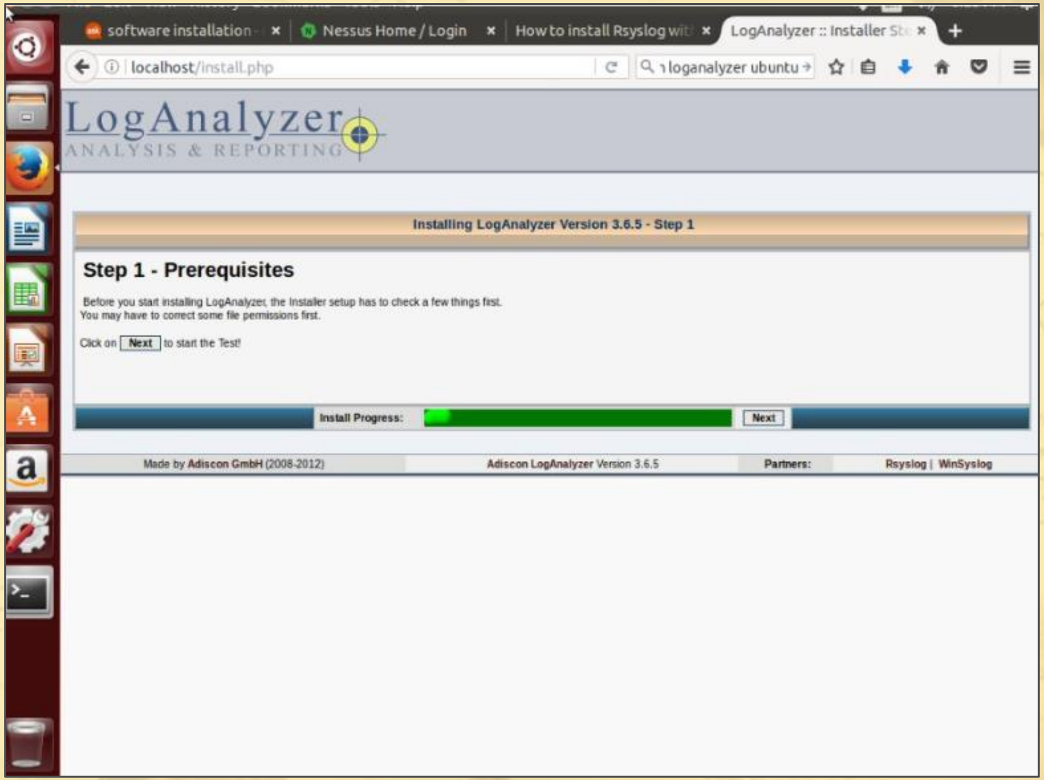
Dashboards

- Log Analyzer
- Splunk
- Graylog
- ELK Stack

Log Analyzer

- Logs are saved in a mysql database.
- Configured with rsyslog server and LAMP stack.
- Provides visualization and log configuration options.
- Provides basic search and filtering capability.
- Doesn’t have a rich query interface for performing analytics.

Log Analyzer



Installing LogAnalyzer Version 3.6.5 - Step 1

Step 1 - Prerequisites

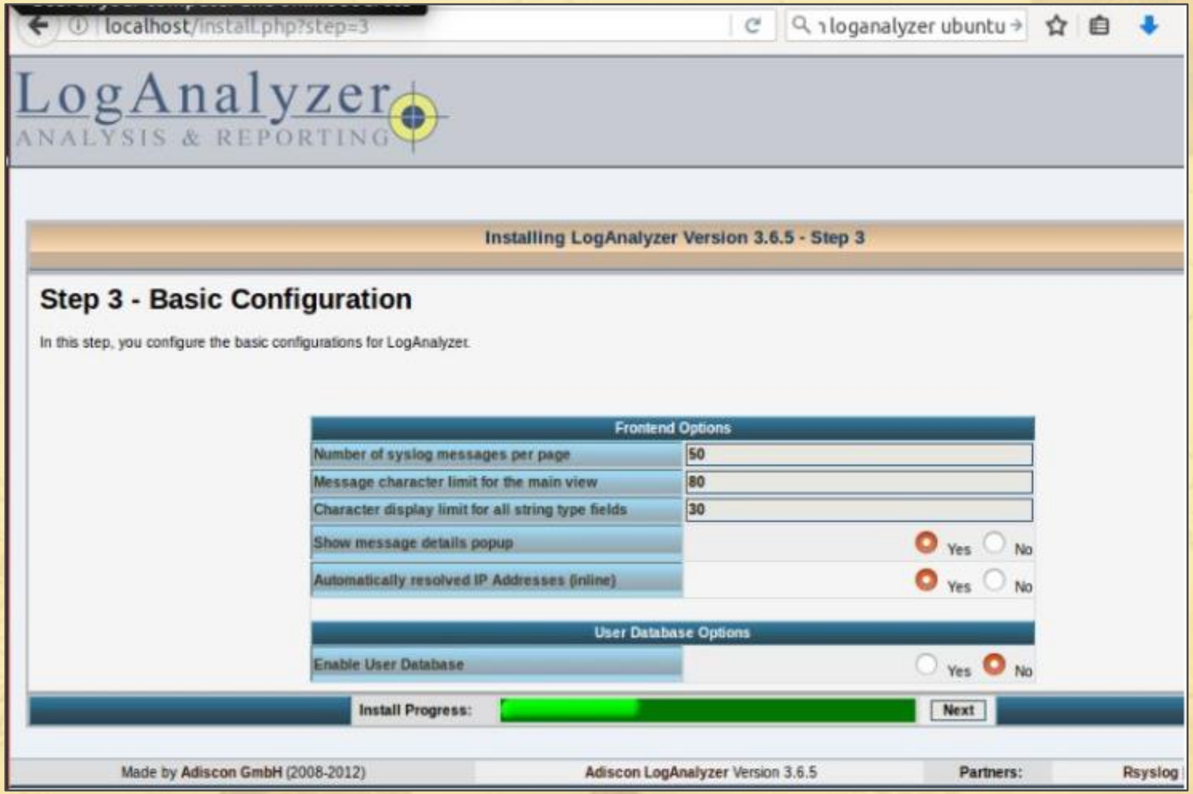
Before you start installing LogAnalyzer, the Installer setup has to check a few things first.
You may have to correct some file permissions first.

Click on Next to start the Test!

Install Progress: Next

Made by Adiscon GmbH (2008-2012) | Adiscon LogAnalyzer Version 3.6.5 | Partners: | Rsyslog | WinSyslog

Log Analyzer



Installing LogAnalyzer Version 3.6.5 - Step 3

Step 3 - Basic Configuration

In this step, you configure the basic configurations for LogAnalyzer.

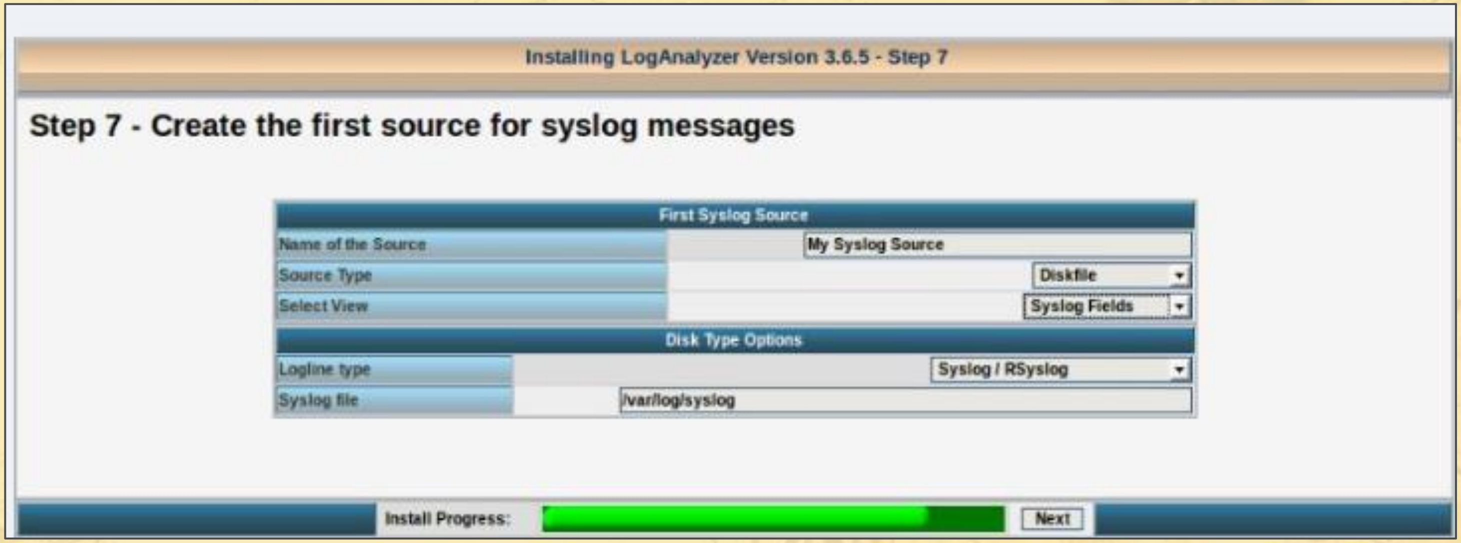
Frontend Options	
Number of syslog messages per page	50
Message character limit for the main view	80
Character display limit for all string type fields	30
Show message details popup	● Yes ○ No
Automatically resolved IP Addresses (inline)	● Yes ○ No

User Database Options	
Enable User Database	○ Yes ● No

Install Progress: Next

Made by Adiscon GmbH (2008-2012) Adiscon LogAnalyzer Version 3.6.5 Partners: Rsyslog

Log Analyzer

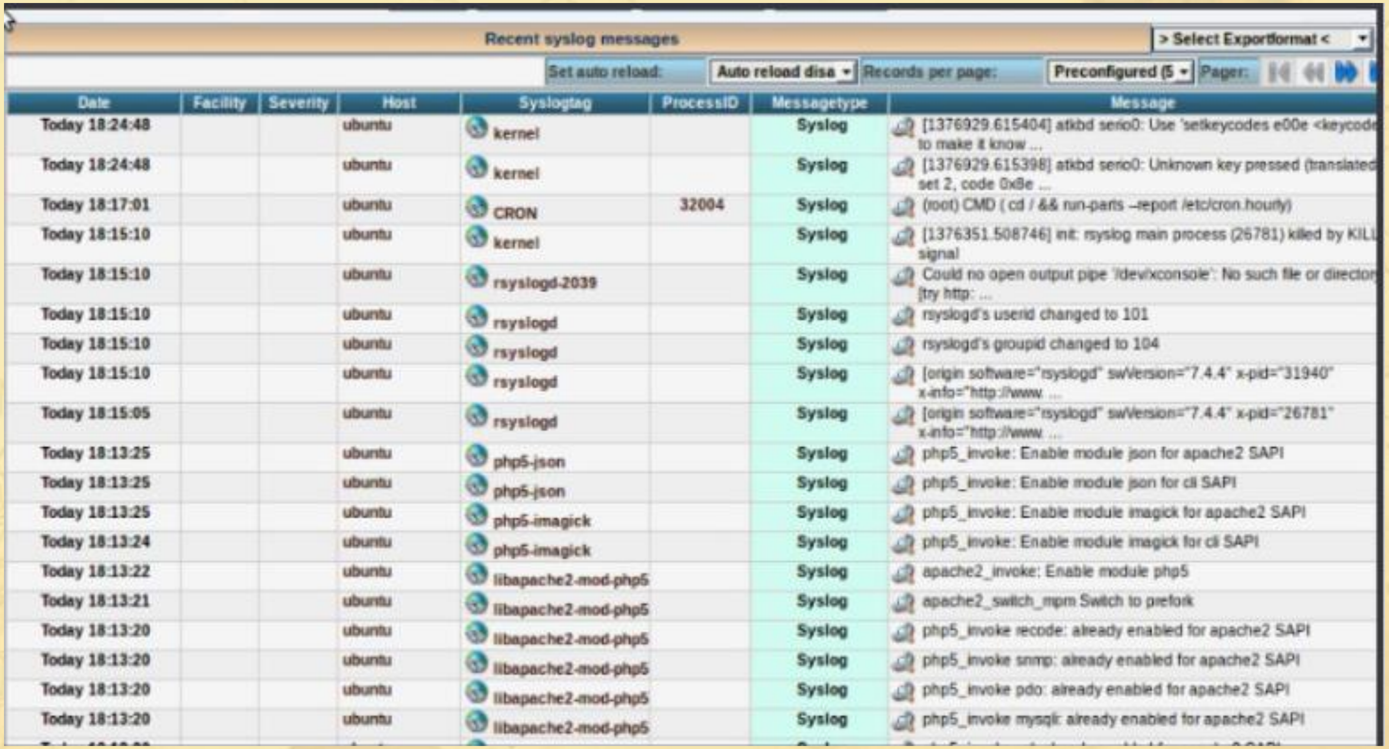


Step 7 - Create the first source for syslog messages

First Syslog Source	
Name of the Source	My Syslog Source
Source Type	Diskfile
Select View	Syslog Fields

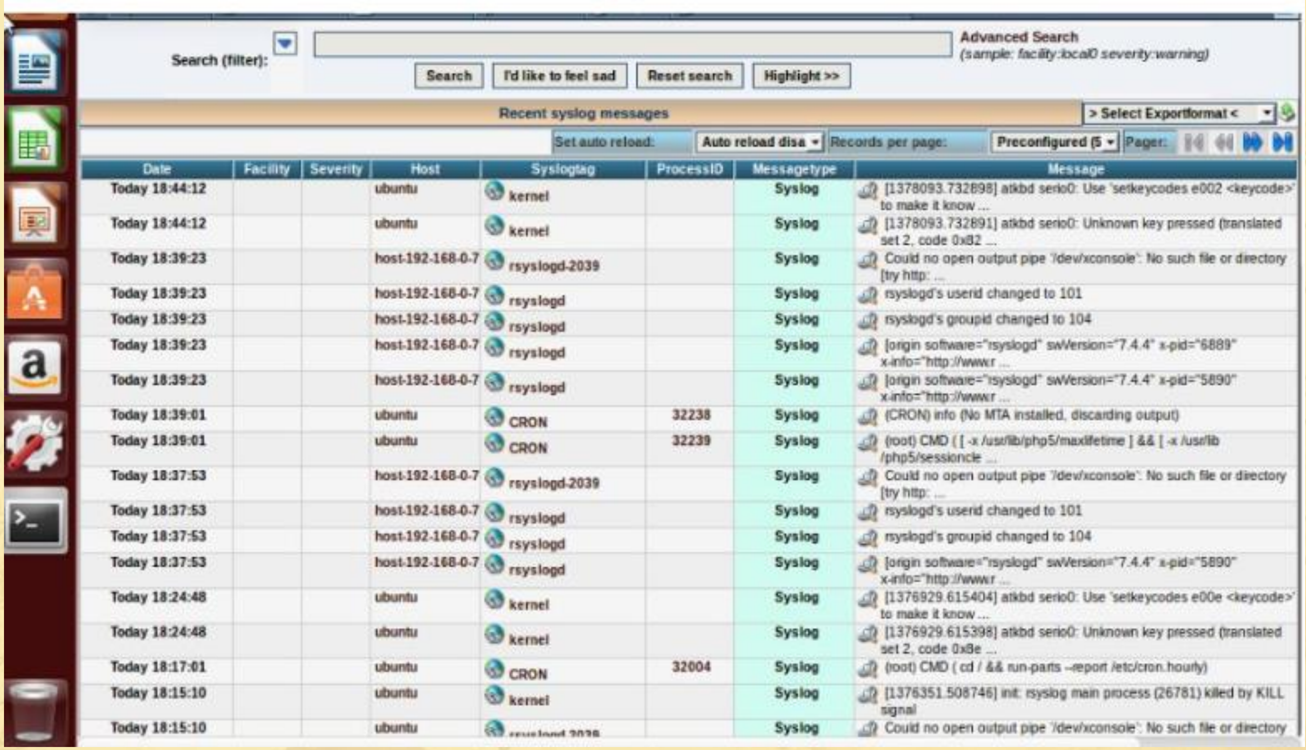
Disk Type Options	
Logline type	Syslog / RSyslog
Syslog file	/var/log/syslog

Log Analyzer



Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 18:24:48			ubuntu	kernel		Syslog	[1376929.615404] atkbd serio0: Use 'setkeycodes e00e <keycode to make it know ...
Today 18:24:48			ubuntu	kernel		Syslog	[1376929.615398] atkbd serio0: Unknown key pressed (translated set 2, code 0x8e ...
Today 18:17:01			ubuntu	CRON	32004	Syslog	(root) CMD (cd / && run-parts –report /etc/cron.hourly)
Today 18:15:10			ubuntu	kernel		Syslog	[1376351.508746] init: rsyslog main process (26781) killed by KILL signal
Today 18:15:10			ubuntu	rsyslogd-2039		Syslog	Could no open output pipe '/dev/xconsole': No such file or director [try http: ...
Today 18:15:10			ubuntu	rsyslogd		Syslog	rsyslogd's userid changed to 101
Today 18:15:10			ubuntu	rsyslogd		Syslog	rsyslogd's groupid changed to 104
Today 18:15:10			ubuntu	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="31940" x-info="http://www. ...
Today 18:15:05			ubuntu	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="26781" x-info="http://www. ...
Today 18:13:25			ubuntu	php5-json		Syslog	php5_invoke: Enable module json for apache2 SAPI
Today 18:13:25			ubuntu	php5-json		Syslog	php5_invoke: Enable module json for cli SAPI
Today 18:13:25			ubuntu	php5-imagick		Syslog	php5_invoke: Enable module imagick for apache2 SAPI
Today 18:13:24			ubuntu	php5-imagick		Syslog	php5_invoke: Enable module imagick for cli SAPI
Today 18:13:22			ubuntu	libapache2-mod-php5		Syslog	apache2_invoke: Enable module php5
Today 18:13:21			ubuntu	libapache2-mod-php5		Syslog	apache2_switch_mpm Switch to prefork
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke recode: already enabled for apache2 SAPI
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke snmp: already enabled for apache2 SAPI
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke pdo: already enabled for apache2 SAPI
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke mysqli: already enabled for apache2 SAPI

Log Analyzer



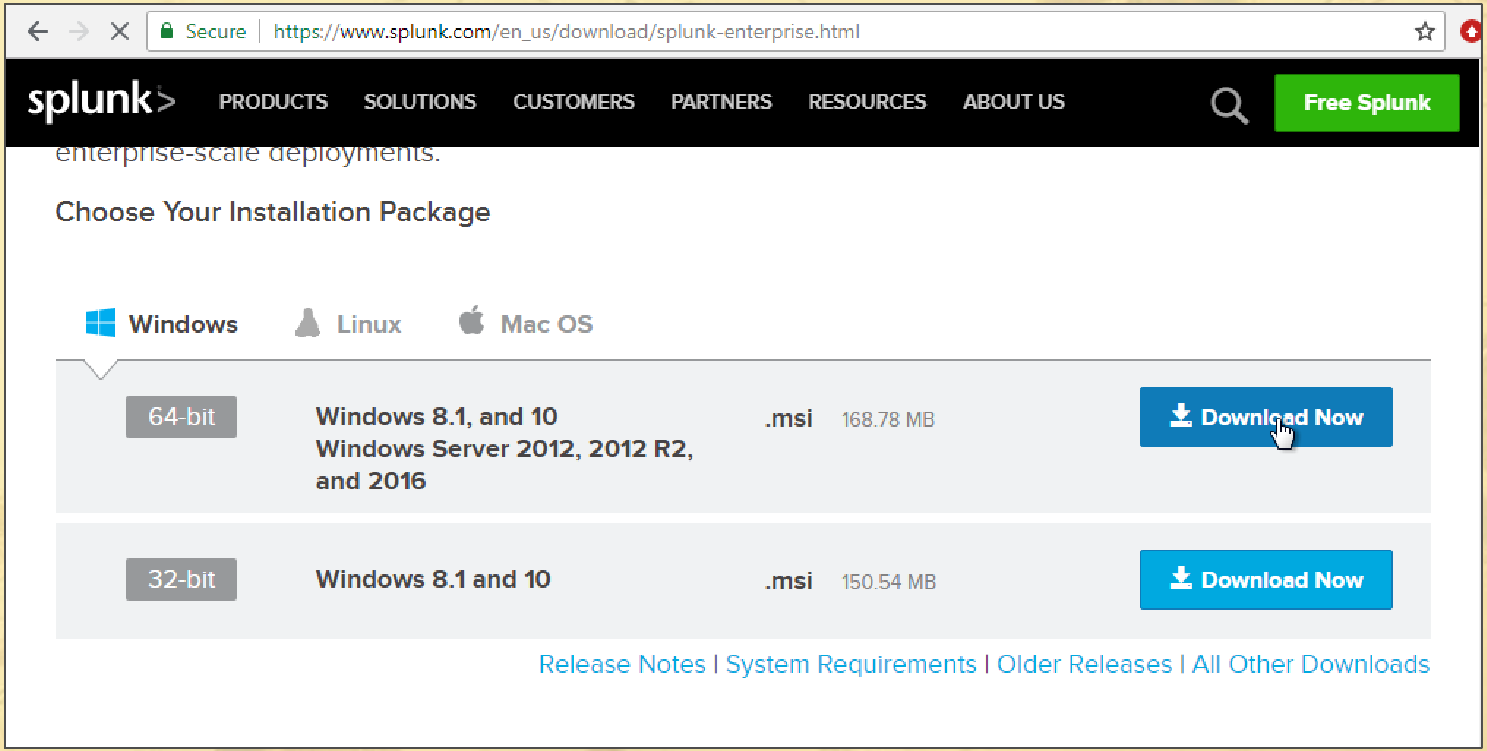
Search (filter): Advanced Search
(sample: facility:local0 severity:warning)

Recent syslog messages

Set auto reload: Auto reload disa Records per page: Preconfigured (5

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 18:44:12			ubuntu	kernel		Syslog	[1378093.732898] atkbd serio0: Use 'setkeycodes e002 <keycode>' to make it know ...
Today 18:44:12			ubuntu	kernel		Syslog	[1378093.732891] atkbd serio0: Unknown key pressed (translated set 2, code 0x82 ...
Today 18:39:23			host-192-168-0-7	rsyslogd-2039		Syslog	Could no open output pipe '/dev/xconsole': No such file or directory [try http: ...
Today 18:39:23			host-192-168-0-7	rsyslogd		Syslog	rsyslogd's userid changed to 101
Today 18:39:23			host-192-168-0-7	rsyslogd		Syslog	rsyslogd's groupid changed to 104
Today 18:39:23			host-192-168-0-7	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="6889" x-info="http://www.r ...
Today 18:39:23			host-192-168-0-7	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="5890" x-info="http://www.r ...
Today 18:39:01			ubuntu	CRON	32238	Syslog	(CRON) info (No MTA installed, discarding output)
Today 18:39:01			ubuntu	CRON	32239	Syslog	(root) CMD ([-x /usr/lib/php5/maxlifetime] && [-x /usr/lib /php5/sessionclе ...
Today 18:37:53			host-192-168-0-7	rsyslogd-2039		Syslog	Could no open output pipe '/dev/xconsole': No such file or directory [try http: ...
Today 18:37:53			host-192-168-0-7	rsyslogd		Syslog	rsyslogd's userid changed to 101
Today 18:37:53			host-192-168-0-7	rsyslogd		Syslog	rsyslogd's groupid changed to 104
Today 18:37:53			host-192-168-0-7	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="5890" x-info="http://www.r ...
Today 18:24:48			ubuntu	kernel		Syslog	[1376929.615404] atkbd serio0: Use 'setkeycodes e00e <keycode>' to make it know ...
Today 18:24:48			ubuntu	kernel		Syslog	[1376929.615398] atkbd serio0: Unknown key pressed (translated set 2, code 0x8e ...
Today 18:17:01			ubuntu	CRON	32004	Syslog	(root) CMD (cd / && run-parts --report /etc/cron.hourly)
Today 18:15:10			ubuntu	kernel		Syslog	[1376351.508746] init: rsyslog main process (26781) killed by KILL signal
Today 18:15:10			ubuntu	rsyslogd-2039		Syslog	Could no open output pipe '/dev/xconsole': No such file or directory

Splunk



https://www.splunk.com/en_us/download/splunk-enterprise.html

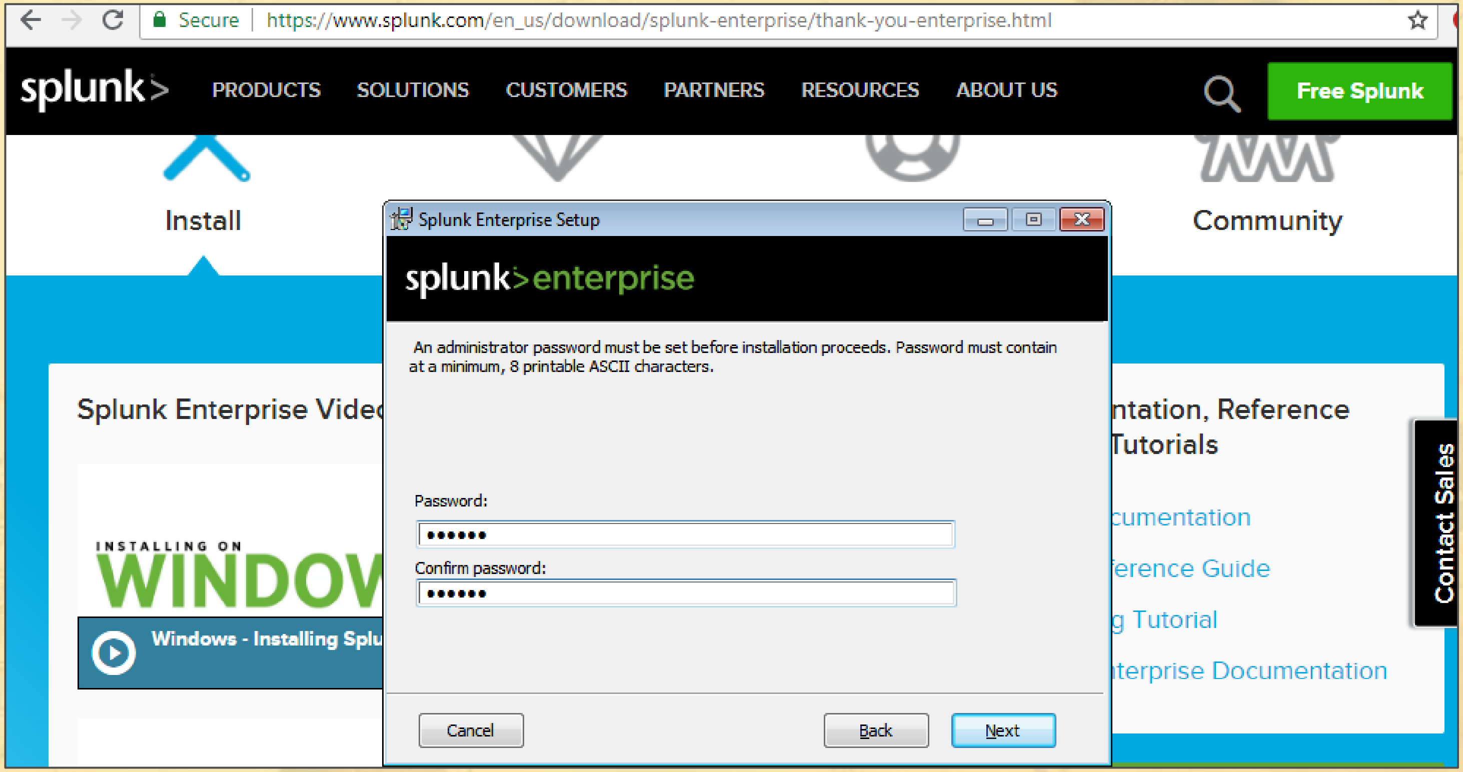
enterprise-scale deployments.

Choose Your Installation Package

64-bit	Windows 8.1, and 10 Windows Server 2012, 2012 R2, and 2016	.msi	168.78 MB	Download Now
32-bit	Windows 8.1 and 10	.msi	150.54 MB	Download Now

Release Notes | System Requirements | Older Releases | All Other Downloads

Splunk Installation Windows

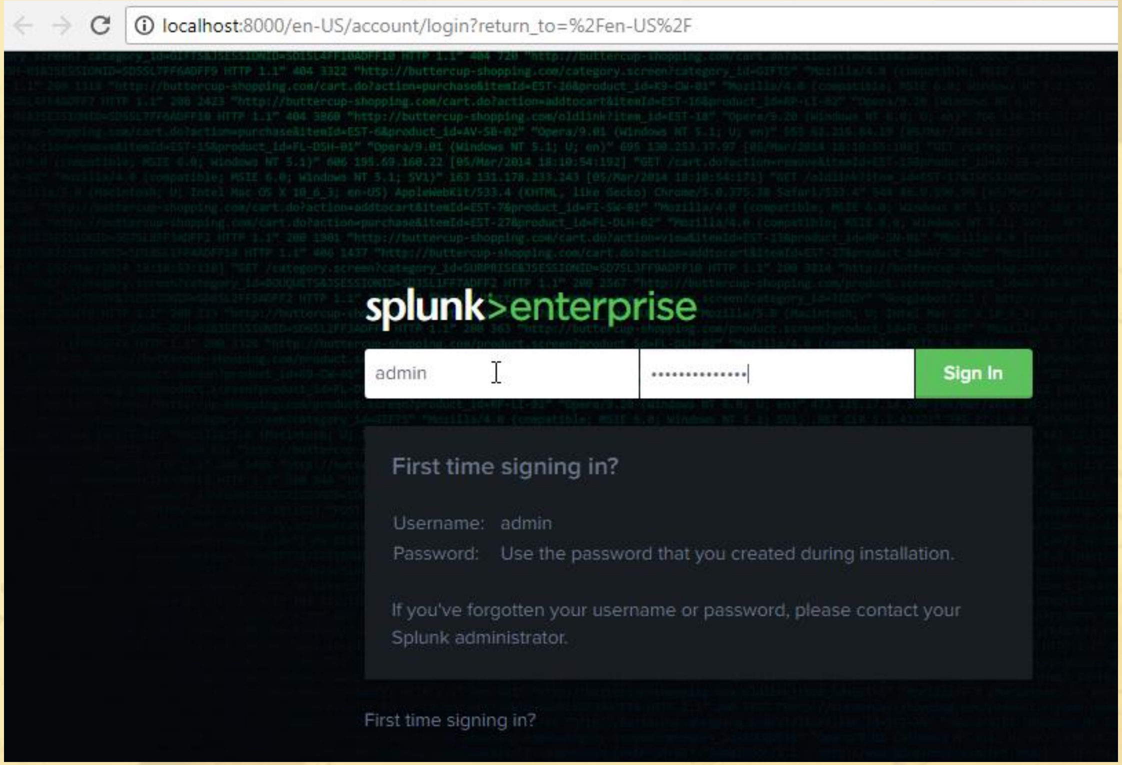


An administrator password must be set before installation proceeds. Password must contain at a minimum, 8 printable ASCII characters.

Password: ••••••

Confirm password: ••••••

Splunk Server Dashboard



localhost:8000/en-US/account/login?return_to=%2Fen-US%2F

admin

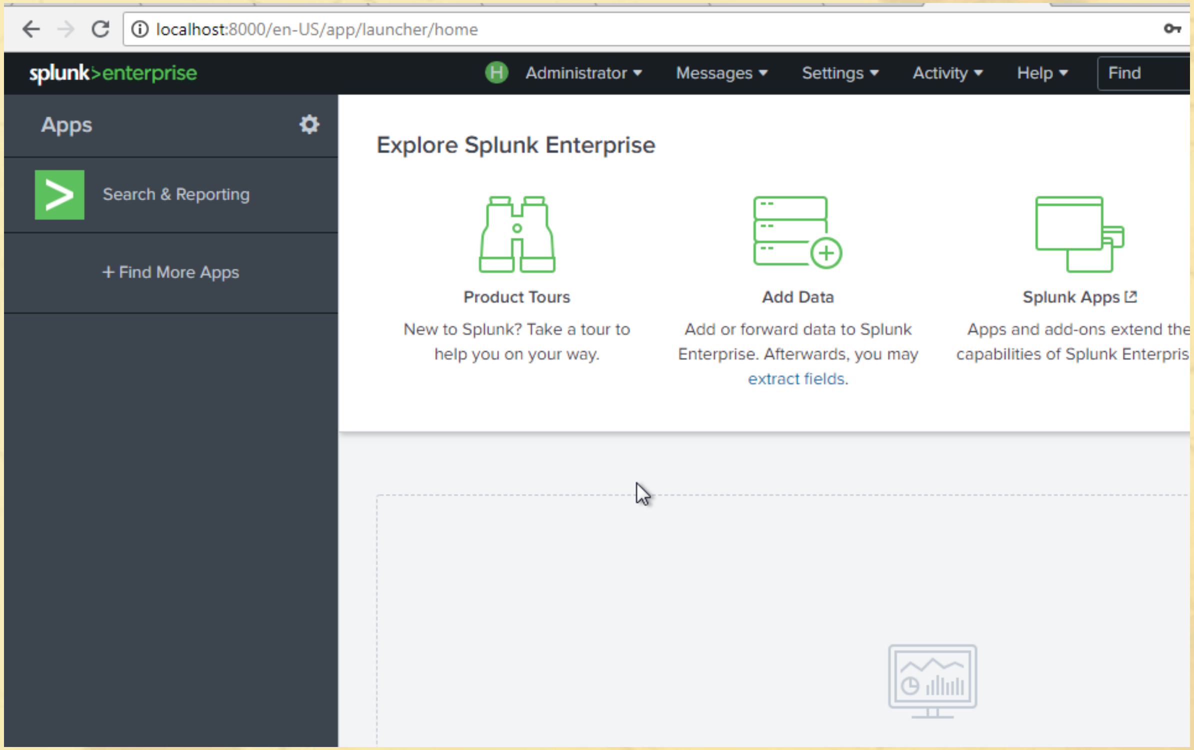
First time signing in?

Username: admin
Password: Use the password that you created during installation.

If you've forgotten your username or password, please contact your Splunk administrator.

First time signing in?

Splunk Dashboard



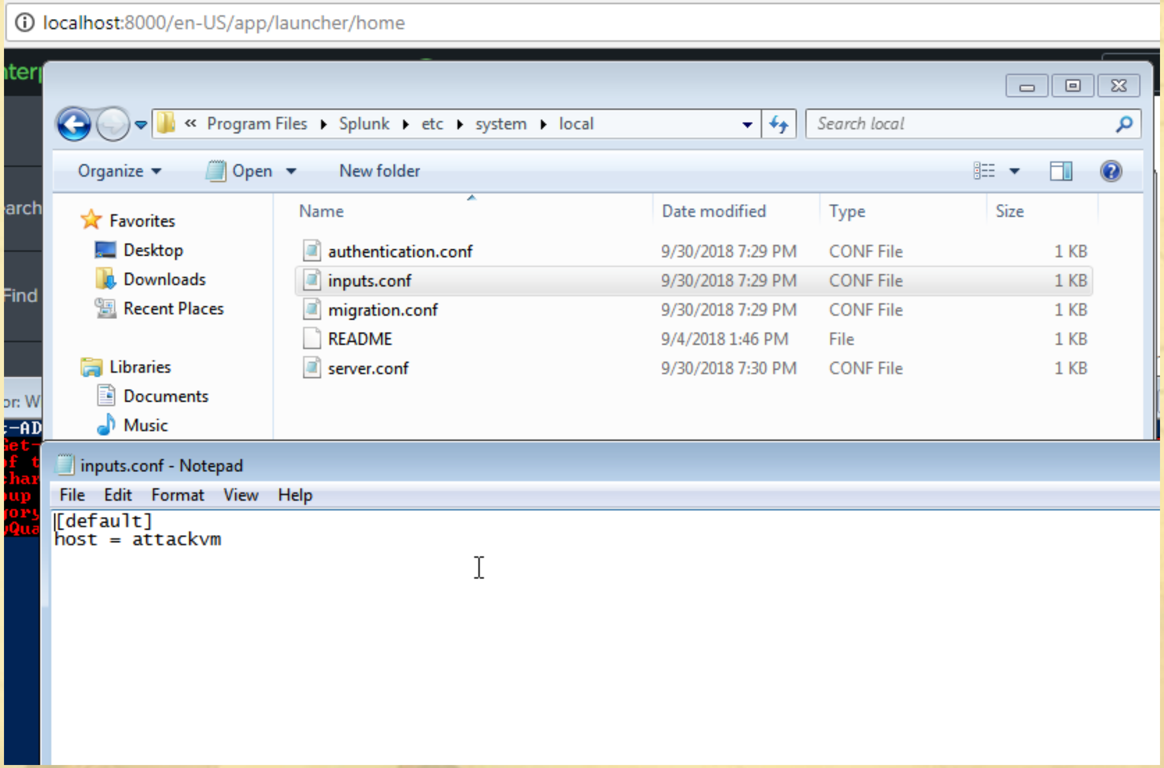
Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterpris

Splunk – Getting Input Data



localhost:8000/en-US/app/launcher/home

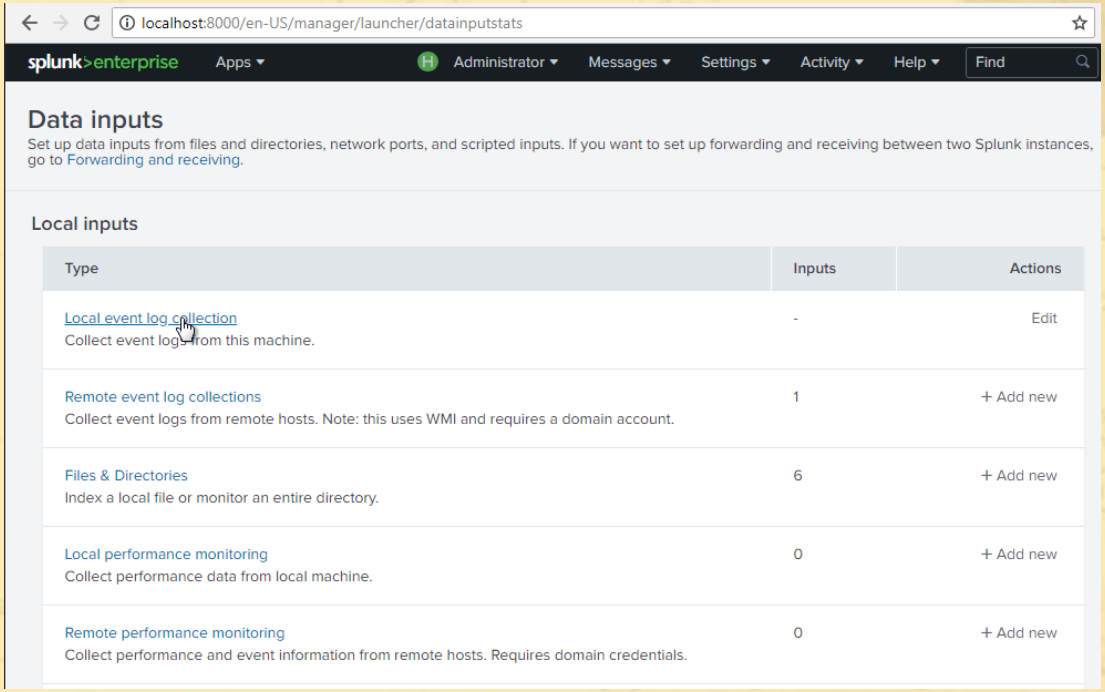
« Program Files ▸ Splunk ▸ etc ▸ system ▸ local

Name	Date modified	Type	Size
authentication.conf	9/30/2018 7:29 PM	CONF File	1 KB
inputs.conf	9/30/2018 7:29 PM	CONF File	1 KB
migration.conf	9/30/2018 7:29 PM	CONF File	1 KB
README	9/4/2018 1:46 PM	File	1 KB
server.conf	9/30/2018 7:30 PM	CONF File	1 KB

inputs.conf - Notepad

```
[default]
host = attackvm
```

Splunk Getting Data



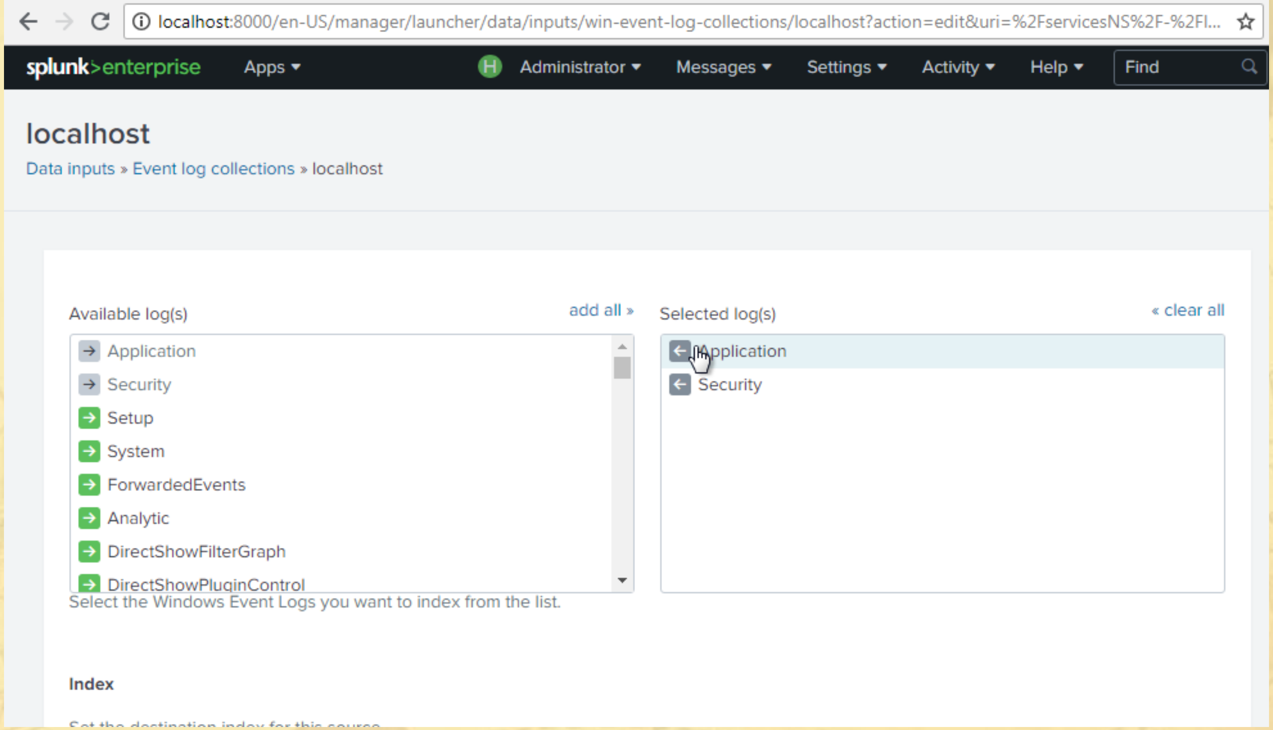
Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	6	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new

Splunk Getting Data



localhost:8000/en-US/manager/launcher/data/inputs/win-event-log-collections/localhost?action=edit&uri=%2FservicesNS%2F-%2Fl...

localhost

Data inputs » Event log collections » localhost

Available log(s) add all »

- Application
- Security
- Setup
- System
- ForwardedEvents
- Analytic
- DirectShowFilterGraph
- DirectShowPluginControl

Selected log(s) « clear all

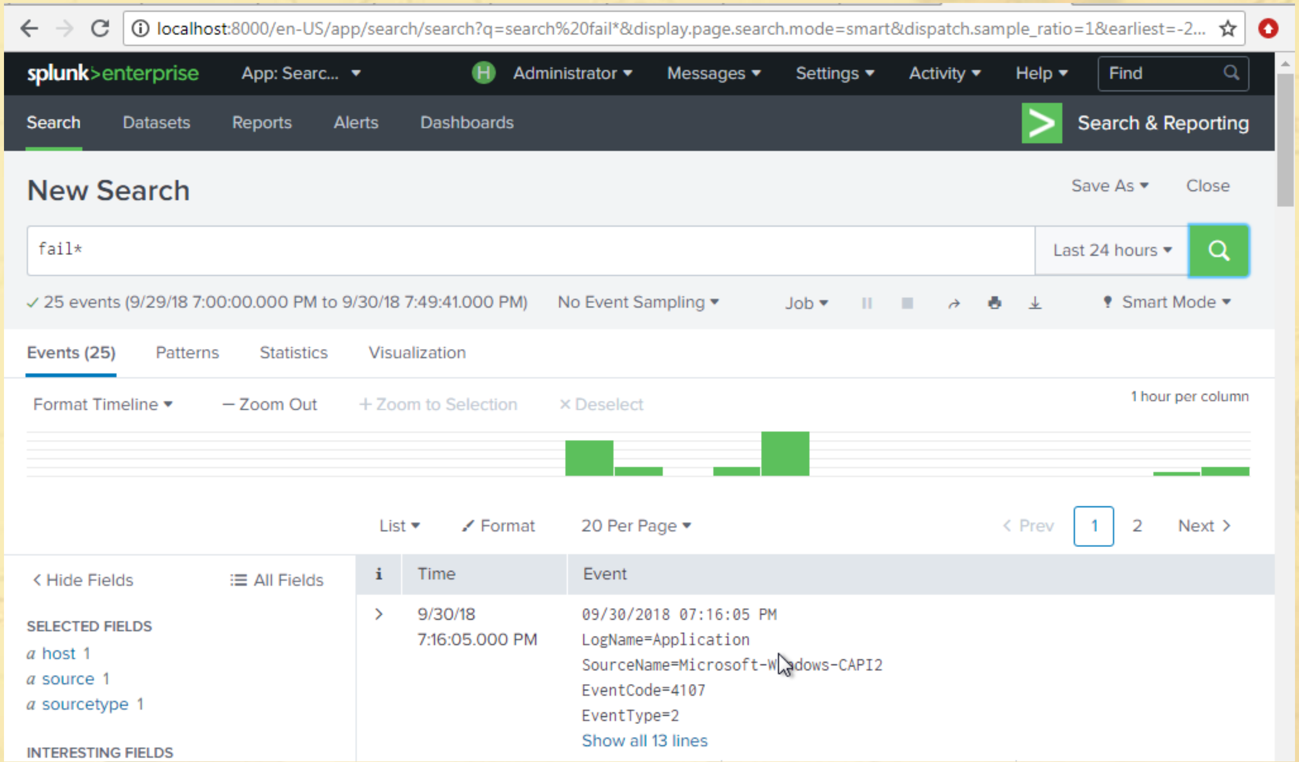
- Application
- Security

Select the Windows Event Logs you want to index from the list.

Index

Set the destination index for this source.

Splunk Fail Events

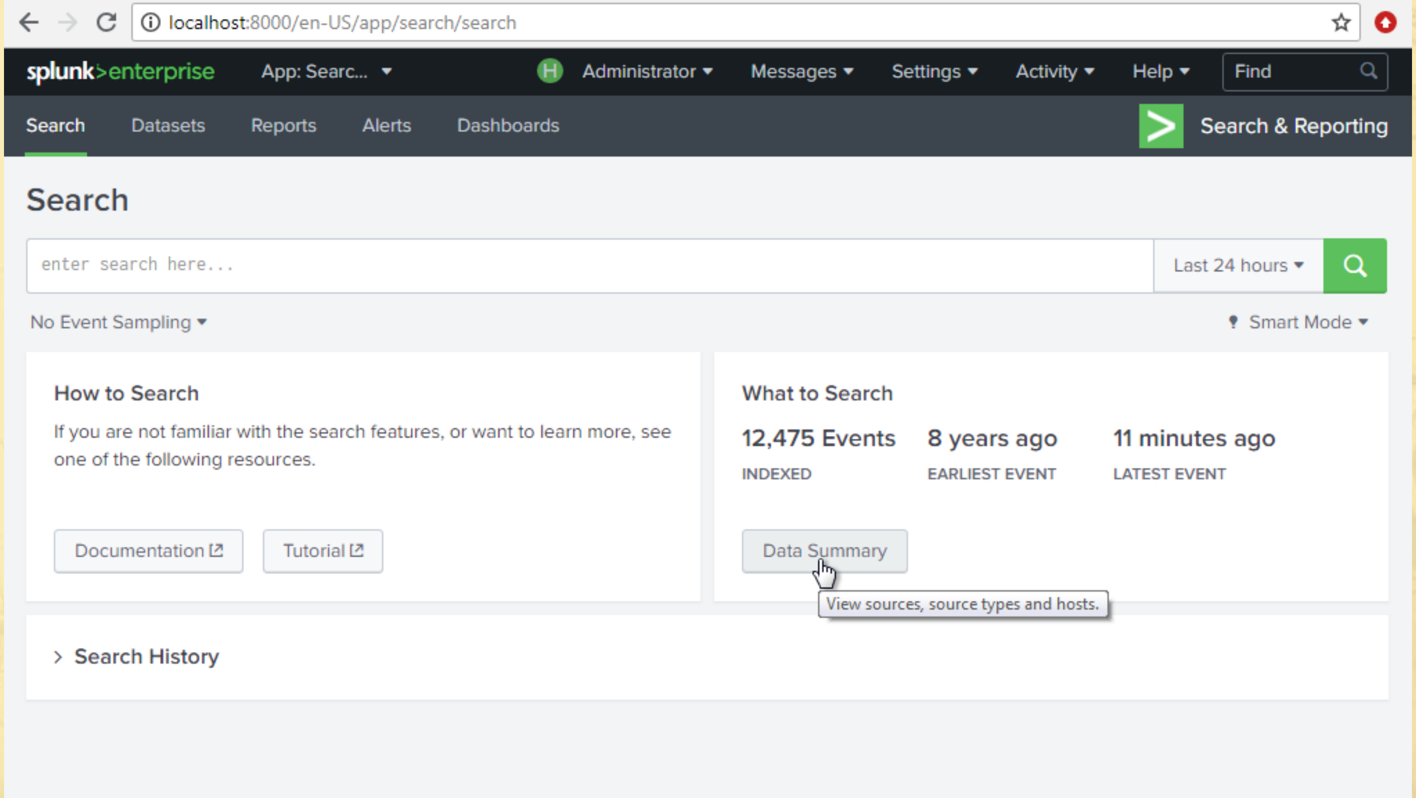


```
fail*
```

✓ 25 events (9/29/18 7:00:00.000 PM to 9/30/18 7:49:41.000 PM)

```
09/30/2018 07:16:05 PM
LogName=Application
SourceName=Microsoft-Windows-CAPI2
EventCode=4107
EventType=2
```

Splunk Indexed Data



Search

enter search here...

Last 24 hours

No Event Sampling

Smart Mode

How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

Documentation

Tutorial

What to Search

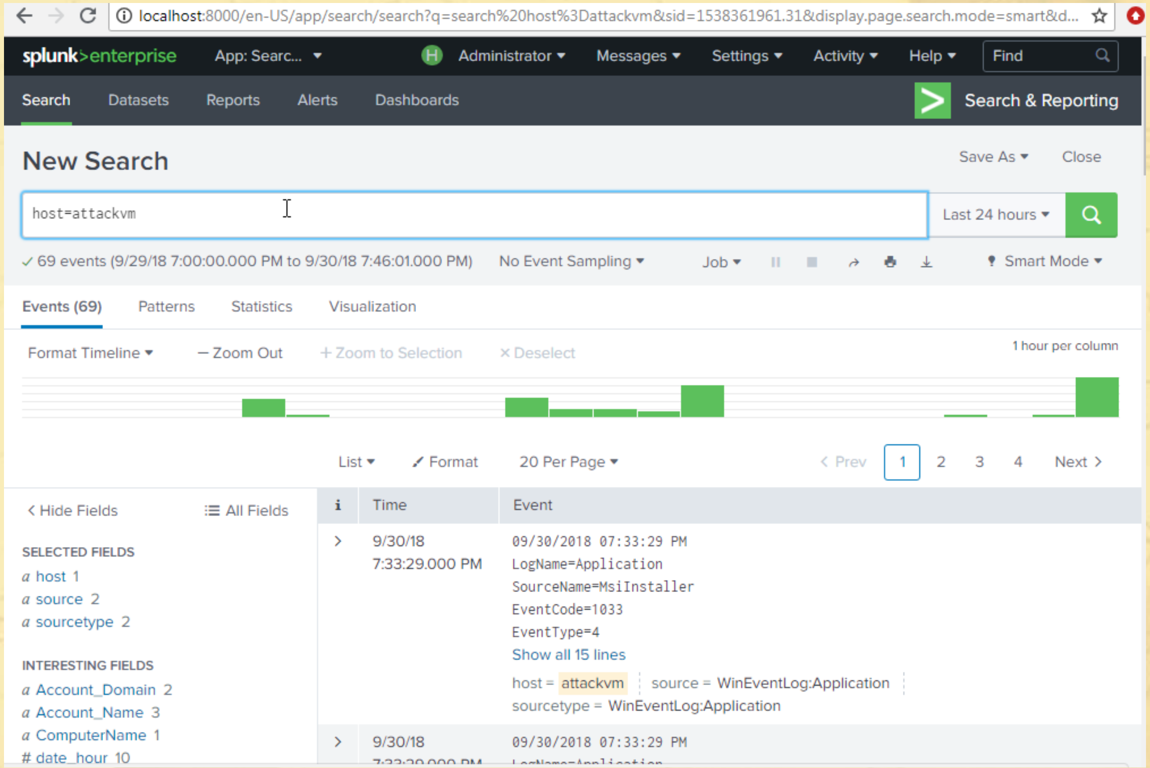
12,475 Events	8 years ago	11 minutes ago
INDEXED	EARLIEST EVENT	LATEST EVENT

Data Summary

View sources, source types and hosts.

Search History

Splunk Search



localhost:8000/en-US/app/search/search?q=search%20host%3Dattackvm&sid=1538361961.31&display.page.search.mode=smart&d...

New Search

```
host=attackvm
```

✓ 69 events (9/29/18 7:00:00.000 PM to 9/30/18 7:46:01.000 PM)

SELECTED FIELDS
- a host 1
- a source 2
- a sourcetype 2

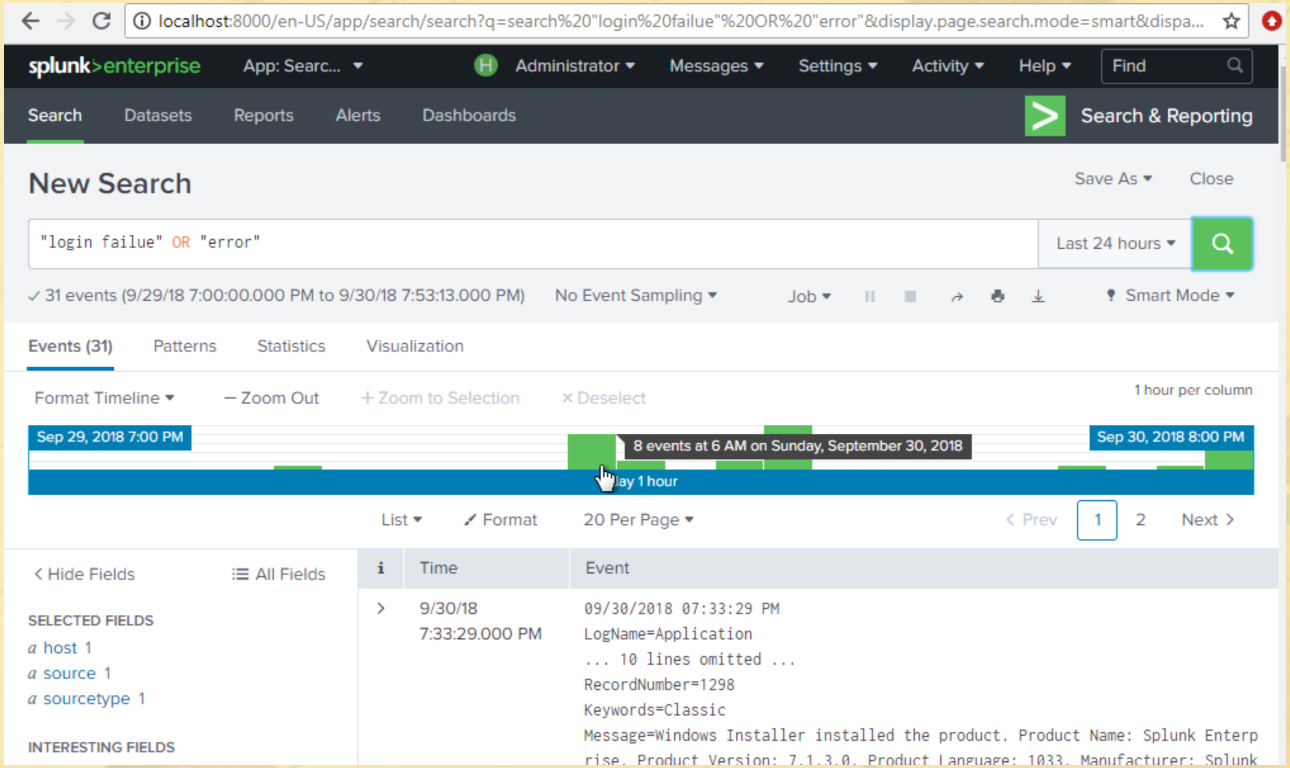
INTERESTING FIELDS
- a Account_Domain 2
- a Account_Name 3
- a ComputerName 1
- # date_hour 10

Time	Event

9/30/18 7:33:29.000 PM	09/30/2018 07:33:29 PM
	LogName=Application
	SourceName=MsiInstaller
	EventCode=1033
	EventType=4
	Show all 15 lines
	host = attackvm source = WinEventLog:Application
	sourcetype = WinEventLog:Application

9/30/18 7:33:29.000 PM	09/30/2018 07:33:29 PM LogName=Application

Splunk Search Queries



```
"login failue" OR "error"
```

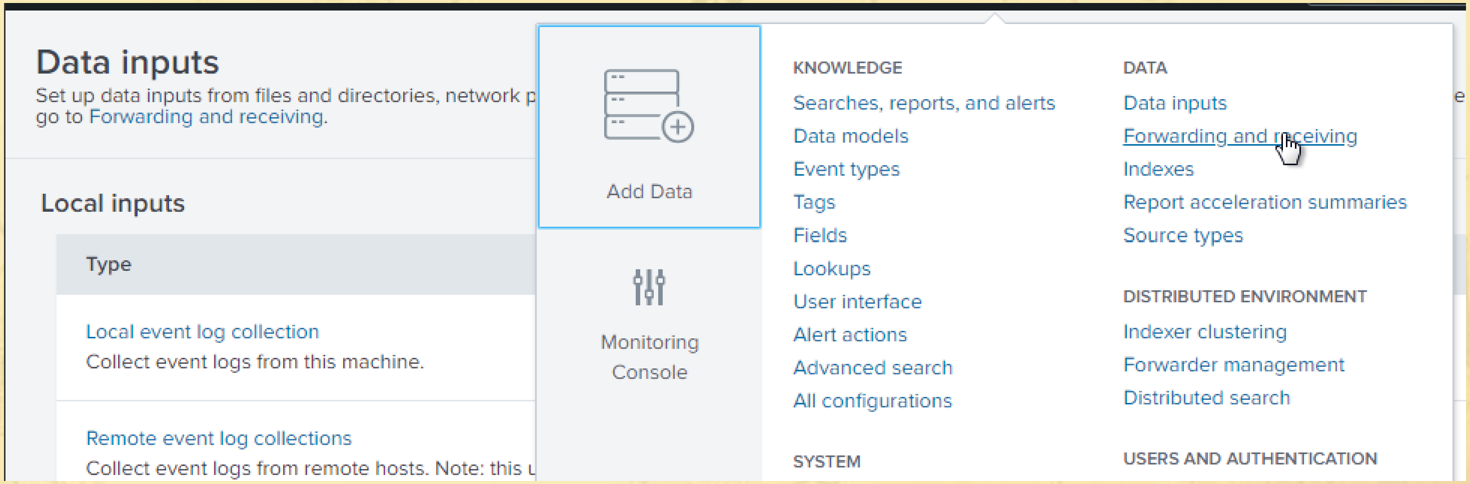
✓ 31 events (9/29/18 7:00:00.000 PM to 9/30/18 7:53:13.000 PM)

i	Time	Event

›	9/30/18
	7:33:29.000 PM
		09/30/2018 07:33:29 PM
		LogName=Application
		... 10 lines omitted ...
		RecordNumber=1298
		Keywords=Classic
		Message=Windows Installer installed the product. Product Name: Splunk Enterprise. Product Version: 7.1.3.0. Product Language: 1033. Manufacturer: Splunk

Splunk Received Port

- Add new receiving port



Data inputs

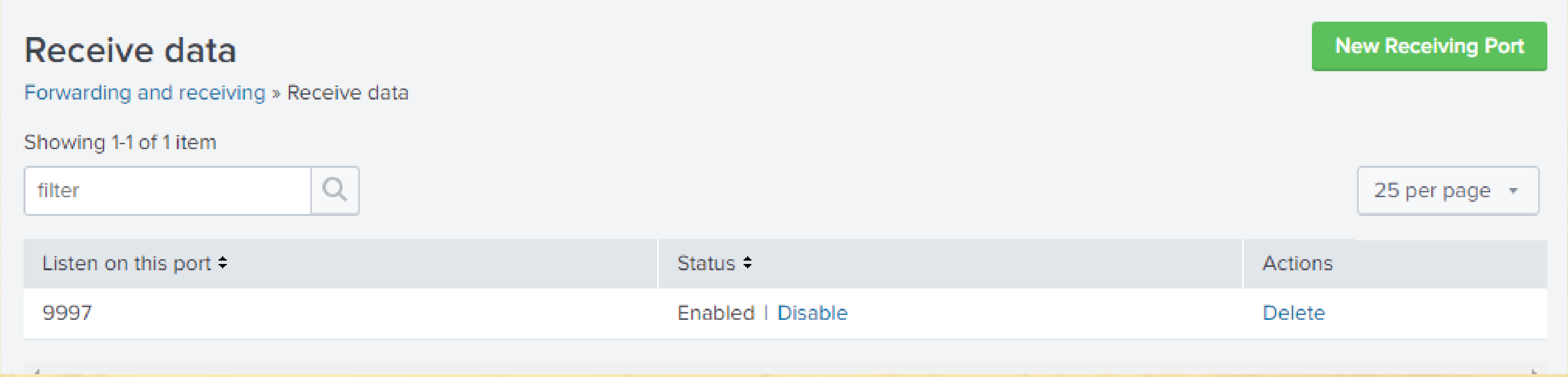
Set up data inputs from files and directories, network p
go to Forwarding and receiving.

Local inputs

Type
Local event log collection Collect event logs from this machine.
Remote event log collections Collect event logs from remote hosts. Note: this u

Splunk Receiving Port

- Forwarding and Receiving -> Configure Receiving -> New Receiving Port



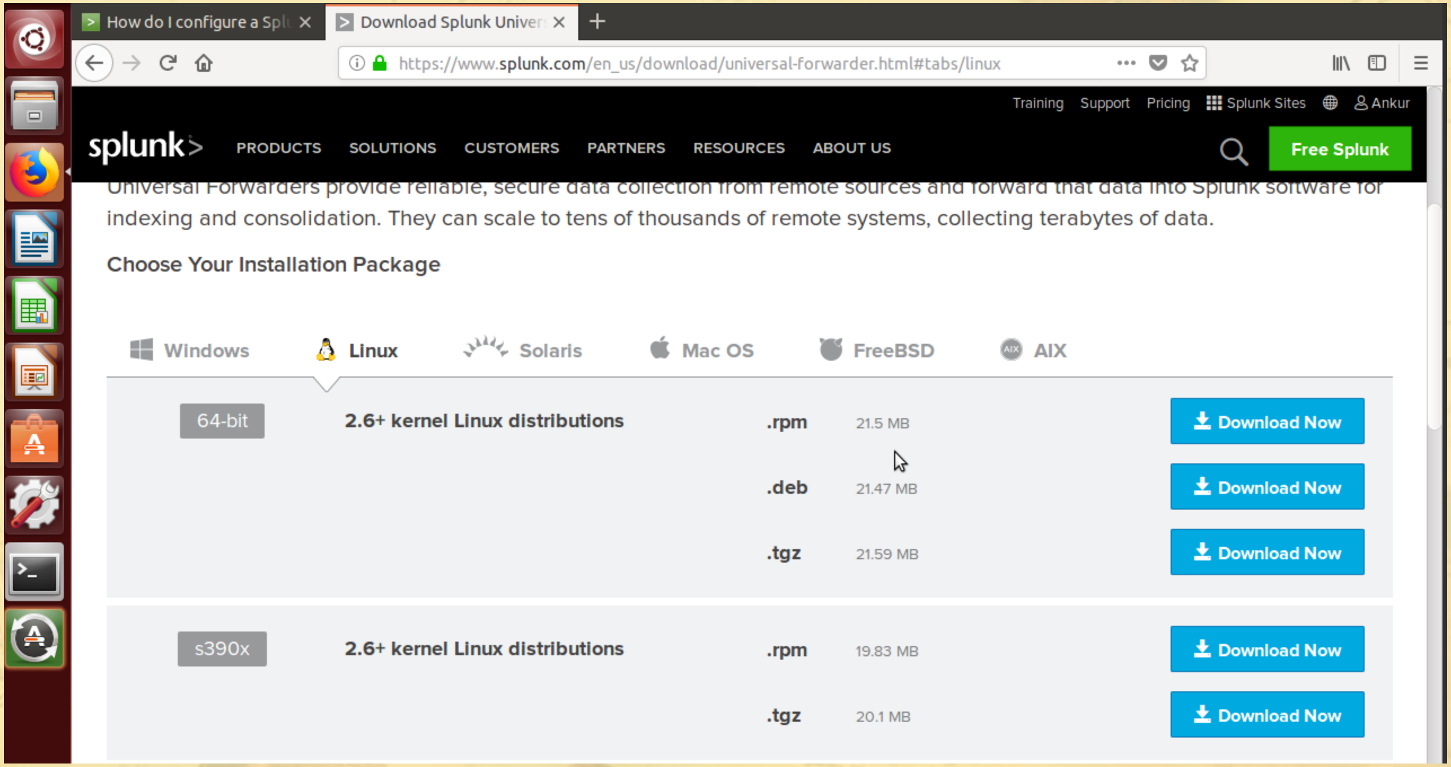
Receive data

Forwarding and receiving » Receive data

Showing 1-1 of 1 item

Listen on this port ⬍	Status ⬍	Actions
9997	Enabled | Disable	Delete

Splunk Universal Forwarder (Client)



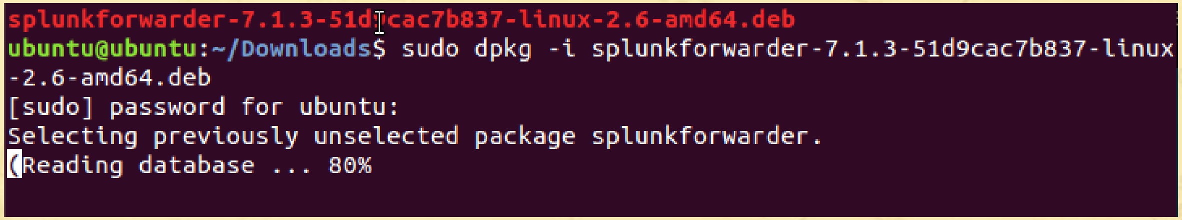
Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

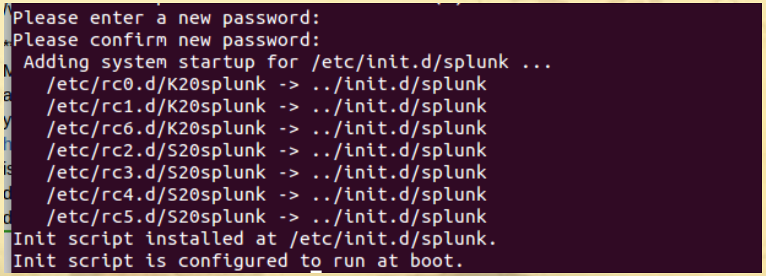
64-bit	2.6+ kernel Linux distributions	.rpm	21.5 MB	Download Now
		.deb	21.47 MB	Download Now
		.tgz	21.59 MB	Download Now
s390x	2.6+ kernel Linux distributions	.rpm	19.83 MB	Download Now
		.tgz	20.1 MB	Download Now

Splunk Universal Forwarder

- Download the Universal Forwarder
- Install using appropriate package (Windows/ Linux)
- $sudo /opt/splunkforwarder/bin/splunk enable boot-start



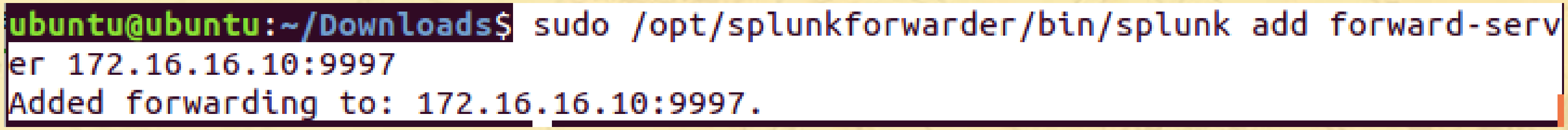
```
splunkforwarder-7.1.3-51d9cac7b837-linux-2.6-amd64.deb
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i splunkforwarder-7.1.3-51d9cac7b837-linux
-2.6-amd64.deb
[sudo] password for ubuntu:
Selecting previously unselected package splunkforwarder.
(Reading database ... 80%
```



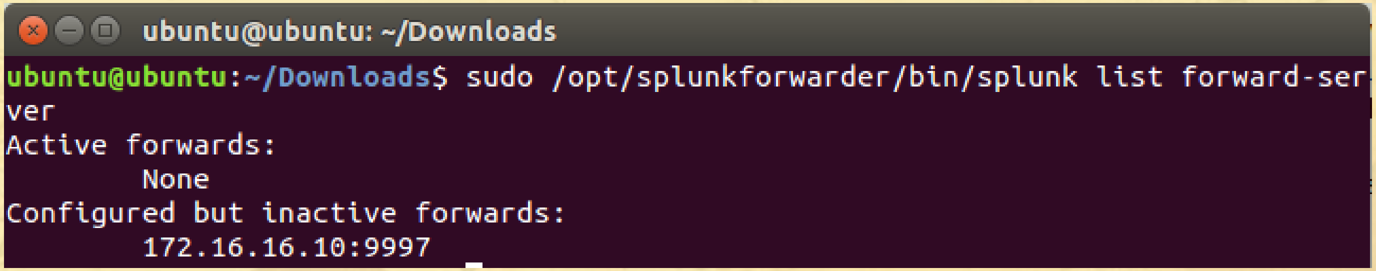
```
Please enter a new password:
Please confirm new password:
 Adding system startup for /etc/init.d/splunk ...
   /etc/rc0.d/K20splunk -> ../init.d/splunk
   /etc/rc1.d/K20splunk -> ../init.d/splunk
   /etc/rc6.d/K20splunk -> ../init.d/splunk
   /etc/rc2.d/S20splunk -> ../init.d/splunk
   /etc/rc3.d/S20splunk -> ../init.d/splunk
   /etc/rc4.d/S20splunk -> ../init.d/splunk
   /etc/rc5.d/S20splunk -> ../init.d/splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
```

Splunk Universal Forwarder

- Add server IP and Port on the client
- $ sudo vim /opt/splunkfowarder/etc/system/local/output.conf
- $ sudo /opt/splunkforwarder/bin/splunk list forward-server



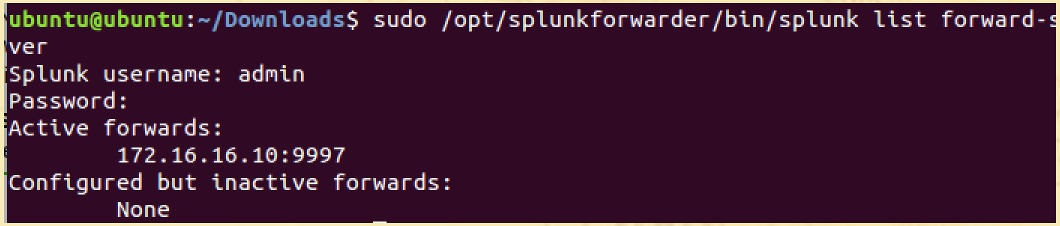
```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk add forward-serv
er 172.16.16.10:9997
Added forwarding to: 172.16.16.10:9997.
```



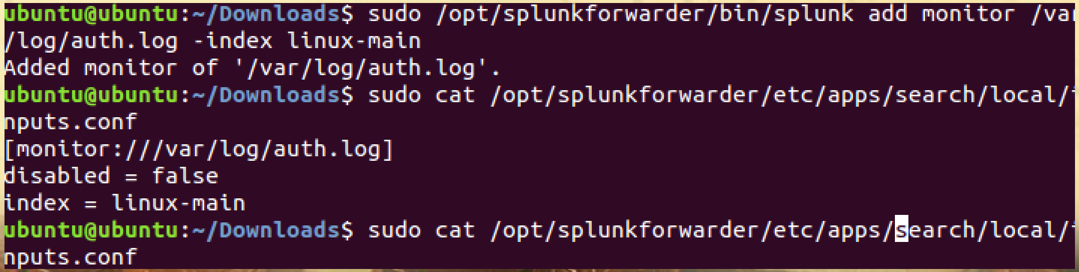
```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk list forward-ser
ver
Active forwards:
        None
Configured but inactive forwards:
        172.16.16.10:9997
```

Splunk Forwarder Start

- $sudo /opt/splunkforwarder/bin/splunk start
- Add monitor
- $sudo /opt/splunkforwarder/bin/splunk add monitor –index splunk-main
- $sudo cat /opt/splunkforwarder/etc/apps/search/local/inputs.conf

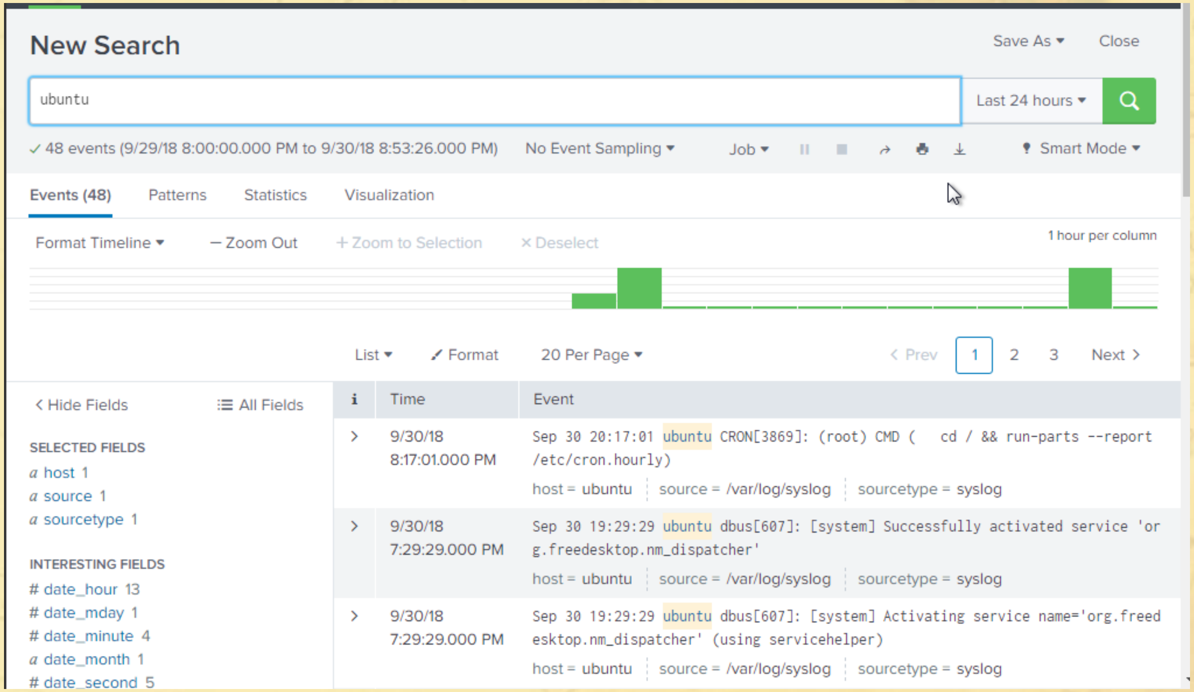


```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk list forward-s
ver
Splunk username: admin
Password:
Active forwards:
        172.16.16.10:9997
Configured but inactive forwards:
        None
```



```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk add monitor /va
/log/auth.log -index linux-main
Added monitor of '/var/log/auth.log'.
ubuntu@ubuntu:~/Downloads$ sudo cat /opt/splunkforwarder/etc/apps/search/local/
nputs.conf
[monitor:///var/log/auth.log]
disabled = false
index = linux-main
ubuntu@ubuntu:~/Downloads$ sudo cat /opt/splunkforwarder/etc/apps/search/local/
nputs.conf
```

Check Forwarder Data on Splunk Server



```
ubuntu
```

✓ 48 events (9/29/18 8:00:00.000 PM to 9/30/18 8:53:26.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 13
# date_mday 1
# date_minute 4
a date_month 1
# date_second 5

	Time	Event

›	9/30/18
	8:17:01.000 PM
		`Sep 30 20:17:01 ubuntu CRON[3869]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)`
		host = ubuntu source = /var/log/syslog sourcetype = syslog

›	9/30/18
	7:29:29.000 PM
		`Sep 30 19:29:29 ubuntu dbus[607]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'`
		host = ubuntu source = /var/log/syslog sourcetype = syslog

›	9/30/18
	7:29:29.000 PM
		`Sep 30 19:29:29 ubuntu dbus[607]: [system] Activating service name='org.freedesktop.nm_dispatcher' (using servicehelper)`
		host = ubuntu source = /var/log/syslog sourcetype = syslog

References

- https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995
- https://en.wikipedia.org/wiki/Security_information_and_event_management
- http://yallalabs.com/linux/how-to-setup-loganalyzer-with-rsyslog-on-ubuntu-16-04-lts-ubuntu-18-04-lts/
- https://answers.splunk.com/answers/50082/how-do-i-configure-a-splunk-forwarder-on-linux.html