HP ArcSight Logger in 2 Hours

An introduction to conducting forensic investigations Using ArcSight Logger 6

Failed Logons Use Case



Reducing complexity, cost and risk in your security infrastructure

By: Brian Wolff CISSP, MBA HP ArcSight ArcSight Architect, Americas

December 16, 2014

Table of Contents

1.	Summary	3
1.1.	Document History	3
1.2.	Current models of Logger	4
2.	ArcSight Logger Trial, Downloads and Demos	5
3.	Deployment Scenarios	7
4.	Logger Appliance Configuration	8
5.	Introduction to Logger	.13
5.1.	One set is a test because been been been a	.15
6. 7	Connecting to the Logger User Interface	.16
7.1	Configuring Logger to accept the Windows Unified Connector Events	.23
7.2.	Configuring the Windows Unified Connector to collect and send events to a Log appliance	gger .25
7.3.	Installing the Windows Unified Connector to collect and send events to a Softw Logger	are .28
8.	USE CASE Step by Step	.33
8.1.	Search / Analyze	.33
8.2.	Categorization	.35
8.3.	Viewing a Live Feed	.42
8.4.	Dashboards	.43
8.5.	Reporting	.48
8.6.	Running a default report	.49
8.7.	Creating a report, by customizing default report	.51
9.	Pipeline Operators:	.60
10.	Selected Examples:	.61
11.	Reporting Example	.68



1. Summary

Secure Your Data, Enforce Compliance, and Defeat Cybercrime

Get Started in Minutes!

ArcSight Logger is available as free downloadable software that brings true enterprise-class log management functionality to everyone. Users can download, install and start getting instant value out of their logs within minutes. Using this version, you can collect up to 750 MB of log data per day and store up to 500 GB of uncompressed logs (assuming average compression 10:1). It also comes with 90 days of phone and email support followed by access to the ArcSight Logger user community. As shown below, the downloadable version of ArcSight Logger provides access to all enterprise features for a full 12 months. Anytime during that period, you can upgrade to an enterprise version.

What It Does

ArcSight Logger collects information from any system that generates log data. It can process that information as much or as little as desired, and can produce ultra-fast searching across the data. As a result, organizations of any size can use this high performance log data repository to aid in faster forensic analysis of IT operations, application development, and cyber security issues, and to simultaneously address multiple regulations.

How It's Different

Until now, log analysis was asset-centric and organizations purchased one product for security and compliance reporting, a different product for IT operations search and yet another one for application development. Today, the questions that need to be answered through log analysis are increasingly user-centric and can span any and all infrastructure. Traditional log management tools cannot be expanded to analyze logs across the enterprise because they are limited by the type of sources; have restricted search/reporting capabilities and are not scalable.

ArcSight Logger is a universal log management solution that can capture and analyze ALL enterprise log data to answer questions of individual teams and can easily be expanded into an enterprise-wide log management solution when needed.

1.1. Document History

Initial Release Based on ArcSight Logger 5.2

Update: 2012/11/08 Modified for Windows 2008 logs

Please refer any documentation changes or suggestions to brian.wolff@hp.com

Update: 2014/04/10 for Logger 5.5 Update: 2015/12/17 for Logger 6



1.2. Current models of Logger

ArcSight Logger is available as Software or as an Appliance.

http://www8.hp.com/us/en/software-solutions/arcsight-logger-log-management/tech-specs.html

The current models of the Logger Software available are:

ArcSight Logger Software Specifications

Model (E-LTU)	Max log volume	Max Online Storage	Max data colume/instance	Max instances in peering	Max data volume
HP ARST Logger 5GB/d SW (Base +	5 GB/ day each	8 TB	250 GB/ day	20	5 TB/ day

Software Generic Specs	
Supported OS	Red Hat Enterprise Linux v6.5, 64-bit CentOS v 6.5 64-bit
Recommended Hardware	CPU: 2 x Intel Xeon Quad Core or equivalent Memory: 12 - 24 GB (24 GB recommended) Disk Space: 65 GB (minimum) in the software Logger installation directory. If you allocate more space, you can store more data. Root partition: 400 GB Temp directory: 1 GB
Storage	Average compression of 10:1 (depending on the data type and source)

The current models of the Logger Appliance available are:

ArcSight Logger Appliance Specifications

Model	L3505	L7505-SAN	L7505s	L7505x
Daily Data Limits (not expandable)	30 GB/day	160 GB/day	80 GB/day	160 GB/day
Capacity (Compressed Data)	800 GB	8TB	8TB	8TB
Hardware Spec	1x Intel Xeon, E5-2620 2.0GHz, 6-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor	2x Intel Xeon, 2648L, 1.8, GHZ 8-core Processor
Memory	32 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM	64 GB, 1600 MHz RAM
Storage	4 x 500 GB (1.5 TB RAID- 5	External – SAN	4 x 3 TB (9 TB - RAID 5)	4 x 3 TB (9 TB - RAID 5)
Host Bus Adapter	N/A	2 x 2-port 16 GB Emulex HBA	N/A	N/A
Dimensions (DxWxH)	27.5" x 17.1" x 1.7"	27.5" x 17.1" x 1.7"	29.5" x 17.1" x 1.7"	29.5" x 17.1" x 1.7"
Connector Management	Yes	N/A	N/A	N/A

Generic Specs	
Management	Web browser, CLI, Web Services API
Operating System	Red Hat Enterprise Linux v6.5, 64-bit
Supported Sources	Raw Syslog (TCP/UDP), Raw File based logs (FTP, SCP, SFTP) Analysis optimized collection using HP ArcSight SmartConnectors FlexConnector framework for legacy event sources HP ArcSight CEF (Common Event Format), HP ArcSight ESM
Storage	Average compression of 10:1 (dependent on data type and data source)
Power	2 x 460W CS Platinum Power Supply
Ethernet Interfaces	4 x 10/100/1000
Chassis	10

2. ArcSight Logger Trial, Downloads and Demos

Logger is delivered in several formats

- 1. Appliance Logger
- 2. Software Logger
- 3. Trial Logger 6.0 for Linux
- 4. Trial Logger 6.0 on VMware VM

Below is the link for the free trial license of (2) Software Logger.

ArcSight Logger is now available as a Limited Period, no cost demo. You can locate it at the following link, which is also seen in the screen-shot that follows:

http://www8.hp.com/us/en/software-solutions/arcsight-logger-log-management/try-now.html

For Home	For Work	Support		Search HP.com	۹ (For Home	For Work Support		Search HP.com	
A Software Harre	Security Ser	🔊 🕉	Automation & Busine Cloud Mana	ត់រ៍ [] ex Service Mable agement	Q App Litecycle	Denview > 2) The ArcSig	ent Niel, Ansight Logger arms of service > ③ Deventoed ht Logger 6.0 Eng	glish SW E-Media		
Download A	ARCSIGHT FreSight Logger	LOGGER TRIAL, [trial software to experience the limited period	DOWNLOADS e unique advantages of lat no cost.	AND DEMOS	nt for a	ownload the trial FREE 6 Completensive log co sources Utha-fast searching of Stripfiled formations	or 1 year. Hection and sitrage from over 350 Yags in full-text estigation	Tell us about yourself First came *	Last name *	
Overslaw	Tech Specia	Get Started Now	Contact Us 🗠		d. Free Irial	 Support IT operations Detext subjictors between the store years' worth of a to 10:1 Scale to 	ppliance and regulatory requirements l'analytics svice late through high compression facts of up	✓ H ² may small me ● Flans for using this software *	Desiness phone *	
jet Universal Lo et out-of-the-box, u nd conditions, and bi Downlood Now	ig Managem niversal log mar egin the downlo	ent in 15 Minutes! agement with this free trial of ad, You can install on RHEL v6.	ArcSight Logger softwa 5 ar CentOS v6.5,	are. Just click the link, agre	e to the terms	j koat more 		Press selectore Cancel Continue III Phicey Subtract	U Danny* long	Pas*



For Home	For Work Suppo	n (Searcempation					Search Her.com	4
Log Management 7	Trial, AvcSigtr Logger				Software / Log Man	ogement Trial, ArcSight Logger				
riew > 👩 Terms	s of service > ③ Dev	mload			1 Overview > (Terms of service > () Download				
rcSight	Logger 6	0 English SV	V E-Media		HP ArcSi	ight Logger 6.0 E	nglish SW E-M	ledia		
ownload Terms of	Use				You may now downly For License keys or to	oad your software and supporting materia o downtbad content again, please refer to p	ls. Il drivertoad confirmation email sen	to brian worthin	Rep. com.	
s ticense agreement	REA : (the "Agreement") state	CAREFULLY BEFORE DOWNLO is the terms between you ("You	ADING THE SOFTWARE. " or "Your") and Hewlett-Packard Cor	npany and its subsidiaries (*HP*)	* Review our FAQ for m	scre beipful information.				
the software that V coment, if You do r use the Software.	fou download from HP's v not agree to be bound b	vebsite (the "Software"). By do y the terms of this Agreement,	wnioading, copying, or using the So , do not click on "I Agree" below and	ftware You agree to this I do not download, install, copy,	Name		FileSt	te .	Using HP Download Man	ga 🗸
ms . This Agreement horizations, softwa	it includes supporting ter are specifications, publish	ms and information referenced red warranties, supplier terms,	by HR, which may be software licens open source software licenses and s	e information, additional license imilar content ("Supporting	HP ArcSight Tile	Logger 6.00 for Linux	206 M	8	Download	
erial"). Additional 6 horization. If you a prevable against Yo	icense authorizations an agree to this Agreement su and any entity for whi	e available at: www.tp.comugor on behalf of another person or h you download, install or use!	SWLICENSING. entity, you warrant you have authori the Product.	ty to do so. This Agreement will be	e IIP ArcSight Smar	tConnectors for Logger Trial	340 M	ú	Download	
isamer Rights. If yo	ou obtained the Software	as a consumer, nothing in this	Agreement affects your statutory rig	bis.						
AGREE AND USING THE OWNLOAD AGREEMENT	I SOFTWARE YOU INDICATE Y	DUR ACCEPTANCE OF THE HE SOFTM ED ACCESS TO THE SOFTWARE, YOU I	ARE DOWN, DAD AGREEMENT, IF YOU (LICK ARE NOT AUTHORIZED TO USE THE SOFTWA	I DISAGALE AND DO NOT ACCEPT THE M RE, AND YOU MAY NOT DOWNLOAD THE	You might also like th	ne following: mmsnihe subsort for ArrSishi Losper		er Started with A	ir Sitht Longert	
				I DISAGREE TAG	GREE	menul select in model cello		Watch ArcSight	Logger in action. (4:48 minutes	
					Learn more about the	ese products				
States					We United States					
h20392.	.www2.hp.cor	n/ecommerce/ak	am/tableviewpopup.	html?language=en	8tr=0.57696071650022178	kurls=http%3A%2F%2Fh	30537.www3.hp.com	n%2Fprdo	wnloads%2FHP_A	rcSight_Sm 👔
	Progress	Size	Status	Filename						
mm								a a a tara f		
	52.3%	348.12 MB	DOWNLOADING	HP ArcSight S	martConnectors for	Logger Trial HP-Arc	Sight-SmartConr	lectors-r	or-Logger-Trial.	zip
	52.3%	348.12 MB	DOWNLOADING	HP_ArcSight_S	martConnectors_for_	Logger_Trial_HP-Arc	Sight-SmartConr	lectors-r	or-Logger-Trial.	zıp
	52.3%	348.12 MB	DOWNLOADING	HP_ArcSight_S	imartConnectors_for_	Logger_Trial_HP-Arc	Sight-SmartConr	Tectors-I	or-Logger-Triai.	Exit
A 1 20202	52.3%	348.12 MB	DOWNLOADING	HP_ArcSight_S	imartConnectors_for_	Logger_Trial_HP-Arc	Sight-SmartConr	iectors-i	or-Logger-Inal	Exit
h20392	52.3%	348.12 MB m/ecommerce/a	DOWNLOADING kam/tableviewpopu	HP_ArcSight_S	en&r=0.02493160096048	Logger_Trial_HP-Arc	Sight-SmartConr 62Fh30537.www3.h	p.com%2	Fprdownloads%2	Exit
h20392	52.3%	348.12 MB m/ecommerce/a	DOWNLOADING kam/tableviewpopu Status	HP_ArcSight_S	en&r=0.024931600%048	Logger_Trial_HP-Arc	Sight-SmartConr 62Fh30537.www3.h	p.com%2	or-Logger-Irial. Fprdownloads%2	Exit
A 20392	52.3%	348.12 MB m/ecommerce/a Size	DOWNLOADING kam/tableviewpopu Status	HP_ArcSight_S	en&r=0.024931600.0048	Logger_Trial_HP-Arc	62Fh30537.www3.h	p.com%2	Fprdownloads%2	Exit
h20392	52.3% 2.www2.hp.co Progress 13.7%	348.12 MB m/ecommerce/a Size 702.96 MB	DOWNLOADING	HP_ArcSight_S	en&r=0.024931600.0048 _Trial_Logger_6.00_c	Logger_Trial_HP-Arc 941&urls=http%3A%2F pn_VMware_VM_HP-	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo	p.com%2 ogger-60	Fprdownloads%21	Exit THP_ArcSig i /M.zip
h20392	52.3%	348.12 MB m/ecommerce/a Size 702.96 MB	DOWNLOADING kam/tableviewpopu Status DOWNLOADING	HP_ArcSight_S	en&r=0.024931600.6048	Logger_Trial_HP-Arc 941&urls=http%3A%2F on_VMware_VM_HP-	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo	p.com%2	Fprdownloads%21	Exit HP_ArcSig
 h20392 m 	52.3%	348.12 MB m/ecommerce/a Size 702.96 MB	DOWNLOADING kam/tableviewpopu Status DOWNLOADING	HP_ArcSight_S	en&r=0.02493160096048	Logger_Trial_HP-Arc 941&urls=http%3A%2F9 9n_VMware_VM_HP-	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo	p.com%2	Fprdownloads%21	zıp Exit FHP_ArcSig i /M.zip Exit
 h20392 h20392 h20392 	52.3% 2.www2.hp.co Progress 13.7%	348.12 MB m/ecommerce/a Size 702.96 MB	DOWNLOADING kam/tableviewpopu Status DOWNLOADING	HP_ArcSight_S	en&r=0.024931600.0048	Logger_Trial_HP-Arc 941&urls=http%3A%2F on_VMware_VM_HP-	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lc	p.com%2	Fprdownloads%21	ZIP Exit FHP_ArcSig 7 (M.zip Exit
 h20392 h20392 h20392 h20392 	52.3%	348.12 MB m/ecommerce/a Size 702.96 MB	DOWNLOADING	HP_ArcSight_S	martConnectors_for_ en&r=0.024931600.0048 _Trial_Logger_6.00_c	Logger_Trial_HP-Arc 941&urls=http%3A%2F on_VMware_VM_HP- 62630865&urls=http%	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lc 3A%2F%2Fh30537.	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow	zıp Exit HP_ArcSig 👔 /M.zip Exit nloads‰ 👔
 h20392 h20393 h20393 h20393 h20393 	52.3% 2.www2.hp.co Progress 13.7% 22.www2.hp.a	348.12 MB m/ecommerce/a Size 702.96 MB	DOWNLOADING kam/tableviewpopu Status pownLoADING e/akam/tableviewp	HP_ArcSight_S	en&r=0.024931600.6048 _Trial_Logger_6.00_c	Logger_Trial_HP-Arc 941&urls=http%3A%2F9 on_VMware_VM_HP- 62630865&urls=http%	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537	p.com%2 ogger-60	Fprdownloads%2 00-on-VMware-V p.com%2Fprdow	zıp Exit HP_ArcSig (*) /M.zip Exit
 h20392 h20392 h20392 h20392 h2039 	52.3% Progress 13.7% Progress 13.7% Progress Progress	348.12 MB m/ecommerce/a Size 702.96 MB com/ecommerce s Size	DOWNLOADING	HP_ArcSight_S	en&r=0.024931600.60483	Logger_Trial_HP-Arc 941&urls=http%3A%2F9 pn_VMware_VM_HP- 62630865&urls=http%	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537.	p.com%2 ogger-60	Fprdownloads%2 00-on-VMware-N p.com%2Fprdow	zıp Exit HP_ArcSig î /M.zip Exit nloads% î
 h20392 h20392 h20392 h2039 h2039 	52.3% Progress 13.7% 2.www2.hp.co Progress 13.7% 2.www2.hp.co 3.3% 2.www2.hp.co 3.3% 2.www2.hp.co 3.3% 3.4%	348.12 MB × commerce/a 5 ze 702.96 MB × v × s 5 Size 286.03 M	DOWNLOADING karr/tableviewpopu Status DOWNLOADING e/akarr/tableviewp Status Status B DOWNLOAD	HP_ArcSight_S	en&tr=0.7835580	Logger_Trial_HP-Arc 941&urls=http%3A%2F9 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lc 3A%2F%2Fh30537.	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-1 0.com%2Fprdow	zıp Exit HP_ArcSig ? (M.zip Exit nloads‰ ? zip
 h20392 h20392 h20392 h2039 h2039 	52.3% Progress 13.7% Progress 2.www2.hp.co Progress 34%	348.12 MB m/ecommerce/a 702.96 MB com/ecommerce/ s Size 286.03 MI	DOWNLOADING kam/tableviewpopu Status DOWNLOADING e/akam/tableviewpopu status Status Status B	HP_ArcSight_S	e cight_Trial_Logger_6.00_c	Logger_Trial_HP-Arc 941&urls=http%3A%2F 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537.	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux.	zıp Exit HP_ArcSig i /M.zip Exit nloads% i zip
 h20392 h20392 h2039 h2039 h2039 	52.3% 2.www2.hp.co Progress 13.7% 2.www2.hp.co Progress 34%	348.12 MB w/ecommerce/a 702.96 MB w/ecommerce/a s Size 286.03 MI	DOWNLOADING	HP_ArcSight_S	e sight_Trial_Logger_6.00_c	Logger_Trial_HP-Arc 941&urls=http%3A%2F 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux.	zıp Exit HP_ArcSig (*) /M.zip Exit nloads‰ (*) zip Exit
 h20392 h20392 h2039 <l< td=""><td>52.3% Progress 13.7% Progress 13.7% Progress 34% WinZi</td><td>348.12 MB m/ecommerce/a Size 702.96 MB com/ecommerce s Size 286.03 Mi p [HP_ArcS</td><td>DOWNLOADING</td><td>HP_ArcSight_S</td><td>e Sight_Trial_Logger_6.00_c e Sight_Trial_Logger_ e</td><td>Logger_Trial_HP-Arc 941&urls=http%3A%2F3 on_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log</td><td>Sight-SmartConr (2Fh30537.www3.h) ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-</td><td>p.com%2 ogger-60 .www3.h Logger-</td><td>Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux.</td><td>zıp Exit HP_ArcSig (*) /M.zip Exit nloads‰ (*) zip Exit</td></l<>	52.3% Progress 13.7% Progress 13.7% Progress 34% WinZi	348.12 MB m/ecommerce/a Size 702.96 MB com/ecommerce s Size 286.03 Mi p [HP_ArcS	DOWNLOADING	HP_ArcSight_S	e Sight_Trial_Logger_6.00_c e Sight_Trial_Logger_ e	Logger_Trial_HP-Arc 941&urls=http%3A%2F3 on_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr (2Fh30537.www3.h) ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-	p.com%2 ogger-60 .www3.h Logger-	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux.	zıp Exit HP_ArcSig (*) /M.zip Exit nloads‰ (*) zip Exit
 h20392 h20392 h2039 h2039 h2039 h2039 	52.3% Progress 13.7% Progress 34% WinZi Ai	348.12 MB m/ecommerce/a Size 702.96 MB com/ecommerce s Size 286.03 MI p [HP_ArcS rcSight-log	DOWNLOADING	HP_ArcSight_S p.html?language=r p.html?language=r p.html?language=r p.html?langu p	e Sight_Trial_Logger_6.00_c e Sight_Trial_Logger_6.00_c e	Logger_Trial_HP-Arc 941&urls=http%3A%2F9 on_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr 42Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-1	p.com%2 ogger-60 .www3.h Logger-	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 6000-for-Linux. zip]	zıp Exit HP_ArcSig (*) /M.zip Exit nloads%(*) zip Exit
 h20392 h20392 h2039 <l< td=""><td>52.3% Progress 13.7% 2.www2.hp.co 13.7% 2.www2.hp.co 34% WinZi An An An An An An An A</td><td>348.12 MB m/ecommerce/a Size 702.96 MB com/ecommerce s Size 286.03 MI p [HP_ArcS rcSight-log rcSight-log</td><td>DOWNLOADING</td><td>HP_ArcSight_S p.html?language= Filename HP_ArcSight_ HP_ArcSight_ PHP_ArcSight_ Filename DING HP_ArcS gger_6.00_fo 5.0.trial.bin 5.0.trial.bin</td><td>en&r=0.02493160096048 _Trial_Logger_6.00_c uage=en&r=0.783 580 e Sight_Trial_Logger_ or_Linux_HP_Arc</td><td>Logger_Trial_HP-Arc 941&urls=http%3A%2F9 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log</td><td>Sight-SmartConr 42Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-</td><td>p.com%2 ogger-60 .www3.h Logger-</td><td>Fprdownloads%21 00-on-VMware-N p.com%2Fprdow 600-for-Linux. zip]</td><td>zıp Exit HP_ArcSig î /M.zip Exit nloads%2 î zip</td></l<>	52.3% Progress 13.7% 2.www2.hp.co 13.7% 2.www2.hp.co 34% WinZi An An An An An An An A	348.12 MB m/ecommerce/a Size 702.96 MB com/ecommerce s Size 286.03 MI p [HP_ArcS rcSight-log rcSight-log	DOWNLOADING	HP_ArcSight_S p.html?language= Filename HP_ArcSight_ HP_ArcSight_ PHP_ArcSight_ Filename DING HP_ArcS gger_6.00_fo 5.0.trial.bin 5.0.trial.bin	en&r=0.02493160096048 _Trial_Logger_6.00_c uage=en&r=0.783 580 e Sight_Trial_Logger_ or_Linux_HP_Arc	Logger_Trial_HP-Arc 941&urls=http%3A%2F9 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr 42Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-	p.com%2 ogger-60 .www3.h Logger-	Fprdownloads%21 00-on-VMware-N p.com%2Fprdow 600-for-Linux. zip]	zıp Exit HP_ArcSig î /M.zip Exit nloads%2 î zip
 h20392 h20392 h2039 h2039 h2039 	52.3% 2.www2.hp.co Progress 13.7% 2.www2.hp.c Progress 34% WinZi Ai	348.12 MB m/ecommerce/a Size 702.96 MB s Size 286.03 MI p [HP_ArcS rcSight-log rcSig	bownLOADING	HP_ArcSight_S	e sight_Trial_Logger_6.00_c age=en&r=0.783_580 e sight_Trial_Logger_ pr_Linux_HP_Arc sig	Logger_Trial_HP-Arc 941&urls=http%3A%2F 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-	p.com%2 ogger-60 .www3.h Logger-	Fprdownloads%21 00-on-VMware-1 0.com%2Fprdow 600-for-Linux. zip]	zıp Exit HP_ArcSig i /M.zip Exit nloads‰ i zip
 h20392 h20392 h2039 h2039	52.3% Progress 13.7% 2.www2.hp.co Progress 34% WinZi Ai Ai Ai	348.12 MB m/ecommerce/a 702.96 MB Toz.96 MB som/ecommerce s Size 286.03 MI p [HP_ArcS rcSight-log rcSight-log	DOWNLOADING kam/tableviewpopu Status DOWNLOADING e/akam/tableviewp e/akam/tableviewp ger-6.0.0.7285 ger-6.0.0.7285 ger-6.0.0.7285	HP_ArcSight_S	e Sight_Trial_Logger_6.00_c age=en&r=0.783 Sight_Trial_Logger_ or_Linux_HP_Arc Sig urce.tgz	Logger_Trial_HP-Arc 941&urls=http%3A%2Ff 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr 62Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-1	p.com%2 ogger-60 .www3.h Logger-	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux. zip]	zıp Exit HP_ArcSig () /M.zip Exit nloads‰ () zip Exit
 h20392 h20392 h2039 h2039	52.3% Progress 13.7% Progress 13.7% Progress 34% WinZi Ai Ai Ai Lc	348.12 MB m/ecommerce/a 702.96 MB m/ecommerce/a s s s s s s s s s	DOWNLOADING kam/tableviewpopu Status DOWNLOADING e/akam/tableviewp e/akam/tableviewp ger-6.0.0.728! ger-6.0.0.728! ger-6.0.0.728! ger-6.0.0.728! ger-6.0.0.728!	HP_ArcSight_S	en&r=0.02493160006048 _Trial_Logger_6.00_c uage=en&r=0.7830580 e Sight_Trial_Logger_ or_Linux_HP-Arc sig urce.tgz	Logger_Trial_HP-Arc 941&urls=http%3A%2Ff on_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr 42Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux. zip]	zıp Exit HP_ArcSig T /M.zip Exit nloads‰ T zip
 h20392 h20392 h2039 h2039	52.3% Progress 13.7% 22.hp.co Progress 34% 2.hp.co Progress 34% 2.hp.co 2	348.12 MB m/ecommerce/a TO2.96 MB com/ecommerce s Size 286.03 M p [HP_ArcS rcSight-log	DOWNLOADING	HP_ArcSight_S	imartConnectors_for_ en&r=0.024931600.0048 _Trial_Logger_6.00_c iage= en&r=0.783.580 e Sight_Trial_Logger_ or_Linux_HP_Arc sig urce.tgz	Logger_Trial_HP-Arc 941&urls=http%3A%2F3 9n_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr (2Fh30537.www3.h) ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 600-for-Linux. zip]	zıp Exit HP_ArcSig () /M.zip Exit nloads‰ () zip
 h20392 h20392 h2039 h2039	52.3% Progress 13.7% 13.7% Progress 34% WinZi Ai	348.12 MB m/ecommerce/a T02.96 MB T02.96 MB som/ecommerce s Size 286.03 MI p [HP_ArcS rcSight-log	DOWNLOADING	HP_ArcSight_S	imartConnectors_for_ en&r=0.024931600.0048 _Trial_Logger_6.00_c iage= en&r=0.783.580 e Sight_Trial_Logger_ or_Linux_HP-Arc sig urce.tgz	Logger_Trial_HP-Arc 941&urls=http%3A%2F3 on_VMware_VM_HP- 62630865&urls=http% 6.00_for_Linux_HP Sight-Trial-Log	Sight-SmartConr 42Fh30537.www3.h ArcSight-Trial-Lo 3A%2F%2Fh30537. ArcSight-Trial-I ger-600-for-1	p.com%2 ogger-60 .www3.h	Fprdownloads%21 00-on-VMware-V p.com%2Fprdow 6000-for-Linux. zip]	zıp Exit HP_ArcSig () /M.zip Exit nloads% () zip Exit



3. Deployment Scenarios

Typically, Logger is deployed inside the perimeter firewall with a high degree of physical security to prevent tampering with the collected event information. Logger does not require other ArcSight products. It receives and forwards syslog and log file events created by a wide variety of hardware and software network products. Logger also interoperates with ArcSight ArcSight's Enterprise Security Manager (ESM) correlation product as shown in the following figures. A typical use of Logger is to collect firewall or other data and forward a subset of the data to ArcSight ESM for real-time monitoring and correlation, as shown below. Logger can store the raw firewall data for compliance or service level agreement purposes.



In the following illustrations ArcSight Logger can be the Logger appliance or the software version of Logger that is installed on a supported platform of your choice.



Logger can act as a funnel, forwarding selected events to ArcSight ESM.



Logger can store events sent by ArcSight ESM.



4. Logger Appliance Configuration

These are some common configuration tasks that should be understood when setting up a Logger Appliance.

4.1.1. Configure Network Settings on a Logger

Below are instructions on how to set an IP address and a default gateway on a Logger Appliance.

1) Attach a KVM or Keyboard, Monitor and Mouse to the appliance after it is fully booted and login as the default user interface credentials:

Username: admin

Password: password



2) Type "help" if you want to display a help screen with a list of commands and descriptions.



3) Set the IP address: You can show the usage of how to set the IP by simply typing "set IP".

logger> set ip Usage: set ip <interface> <ip address>[∕prefix] [netmask]



4) Set the IP address based on the usage output. This example below sets the IP of the eth0 interface to 10.0.187.38 with a netmask of 255.255.255.0.

logger> set ip eth0 10.0.187.38 255.255.255.0

5) Type "show ip" to verify the IP is set properly for eth0.

logger>	show ip eth0
eth0	Link encap:Ethernet HWaddr 98:4B:E1:74:A9:30
	inet addr:10.0.187.38
	inet6 addr: fe80::9a4b:e1ff:fe74:a930/64 Scope:Link
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:38 errors:0 dropped:0 overruns:0 frame:0
	TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:3472 (3.3 KiB) TX bytes:3132 (3.0 KiB)
	Interrupt:162 Memory:f4000000-f4012800

6) **Set the default gateway:** You can type "set defaultgw" to show usage on how to set the default gateway.



7) Based on the usage info, set the default gateway. This example sets the default gateway to 10.0.187.1 for interface eth0.

ogger> set defaultgw 10 Р

8) Verify the default gateway by typing "show defaultgw".

logger≻ show	defaultgw						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	10.0.187.1	0.0.0	UG	0	0	0	eth0

9) Connect to the Logger from a workstation to confirm the configuration.

https://10.0.187.38 (in this example only)



4.1.2. Installing a license on Logger Appliance

*Note the Limited Use Free License is automatically deployed, you do not need to do this step

1 Connect to the appliance's user interface.

https://10.0.187.38 (in this example)

Default ID and Password: admin/password

You will need to read through the user agreement before checking the "Accept" box.

- 2 Click System Admin from the top-level menu bar.
- 3 Click License & Update from the System section.
- 4 Click Browse to locate the file.
- 5 Click Upload Update.



4.1.3. Configuring Date & Time zone

Configuring the date and time zone properly is important so that timestamps on events will come in properly. You can setup the date using an NTP server or set the date & time zone manually here in the user interface:

- 1. Click System Admin from the top-level menu bar.
- 2. Click Network from the System section.
- 3. May need to change the Time Zone by clicking the "Change Time Zone" button and supplying the correct time zone. This will require a reboot.
- 4. Click the **Time/NTP** tab and enter in your settings. If you use an NTP server it will automatically update the date/time.
- 5. Click "save" to save your entries.



ime/NTP Setting	gs		
WARNING: Therefore, mod	If you must configure system lifying system time can resu	time locally, D0 NOT modify it after it has been initially set. Events are time st t in unpredictable behavior on your system, and may lead to data integrity issued.	amped using system time. es.
ArcSight s	trongly recommends that yo	use Network Time Protocol (NTP) for system time instead of locally configuring	g it.
Date/Time Sel	ttings		
urrent Time Zone	America/Los Angeles	G Change Time Zone	
Current Time	03/23/2012 02:17:20 PM	Schange Date/Time	
NTP Servers —			
Enable as NTP set	erver 🕡		
NTP Servers			

4.1.4. Configure DNS Settings

- 1. Click System Admin from the top-level menu bar.
- 2. Click Network from the System section.
- 3. In the **System DNS** tab, enter new values for the IP address of the primary and secondary DNS servers and edit the list of search domains (6 search domains entries is a limit imposed by the OS).
- 4. Click "Save" to save your entries.

System DNS	Hosts 🕘 NICs 📑 Sta	tic Routes	
DNS Settings			
DNS Settings			
Primary DNS	0.0.0.0		
Secondary DNS			
- DNS Search Dr	mains		
DNS Search Domai	ins		
localdomain			



4.1.5. Setup Hosts file entries

Setting up hosts file entries is especially important when configuring Connectors on Connector Appliance with an ESM or Express destination. This is because those destinations usually have certs configured that use a hostname. To configure the hosts file entries, follow these steps:

- 1 Click System Admin from the top-level menu bar.
- 2 Click Network from the System section.
- 3 In the Hosts tab, enter in your hosts entries with the following format:

<ip-address> <hostname>

Example below shows an entry for "esm" host

Network Settings	
🙀 System DNS 🔯 Hosts 💌 NICs 🗃 Static Routes 💽 Time/NTP	
Hosts Settings	
A System Hosts	Import from Local File
10.10.10 esm	



5. Introduction to Logger

ArcSight Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events.

Logger is available in two form factors: an appliance and software. The appliance-based solution is a hardened, dedicated, enterprise-class system that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis.

Supported Platforms

You can install software Loggers on platforms with the hardware specifications and supported operating systems outlined below, according to the indicated deployment scenarios. This information applies to both physical and virtual machines.

VM installation on the operating systems listed in the table below is supported. Additional information about installing Logger on VMware is available in the Logger for VMware VM Quick Start Guide.

Note

HP strongly recommends allocating 4 GB RAM per VM instance.
 The sum of memory configurations of the active VMs on a VM serve

not exceed the total physical memory on the server.	

Specification	Details
Supported Operating Systems	 Red Hat Enterprise Linux (RHEL) versions 6.2 and 6.5 (64-bit) CentOS versions 5.5 and 6.5 (64-bit) Notes: HP ArcSight recommends RHEL 6.5 for fresh installs. If you are planning to upgrade your current OS and the Logger at the same time, HP ArcSight recommends upgrading the Logger application first followed by the OS. For example, upgrade from Logger 5.3 SP1 to Logger 5.5 followed by an upgrade from RHEL 6.2 to 6.5.
CPU, Memory, and Disk Space	 For the Trial Version and VM Instances CPU: 1 or 2 x Intel Xeon Quad Core or equivalent Memory: 4 - 12 GB (12 GB recommended) Disk Space: 10 GB (minimum) Temp directory: 1 GB For the Enterprise Version CPU: 2 x Intel Xeon Quad Core or equivalent Memory: 12 - 24 GB (24 GB recommended) Disk Space: 65 GB (minimum) in the software Logger installation directory. If you allocate more space, you can store more data. Root partition: 400 GB Temp directory: 1 GB Note: Using NFS as primary event storage on software Logger is not recommended.
Other Applications	For optimal performance, make sure no other applications are running on the system on which you install Logger.

For a detailed capacity planning guide, see the Capacity Planning for Software Version of Logger document that is available for download from the Protect 724 Community at https://protect724.arcsight.com.



Connecting to Logger

The Logger user interface (UI) is a web browser application using Secure Sockets Layer (SSL) encryption. Users must log in and be authenticated before they can access the Logger UI.

Logger 6.0 supports access through the following browsers:

- Firefox: Version ESR 31
- Internet Explorer: Versions 10 and 11
- Chrome: Latest version
- Safari: version 7.0 (on OSX 10.9)

An Adobe Flash Player plug-in is required for Internet Explorer and Firefox browsers that access Logger. (Chrome includes a Flash player, and so does not need an additional one.) Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is available for free at http://www.adobe.com/products/flashplayer.html

JavaScript and cookies must be enabled.

Logger stores time-stamped text messages, called events, at high and sustained input rates. Logger compresses raw data, but can always retrieve unmodified data on demand, for forensics-quality litigation data.

O 🗸 All Fields							admin
	Last 10 minu	tes 🖃					
h querý				🖌 Go	Advanced		
nts (Scanned: 63,358 events	s 00:01.094) 🛎						
							1 bar = 5 second
15:59:21	16:00:21	16:01:21	16:02:21 16:0	03:21 16:04:21	16:05:21	16:06:21	
Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	de	viceEventClassId
2014/11/22 16:07:58 PST	10.0.0.18 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	OW	тм
2014/11/22 16:07:58 P5T	10.0.0.17 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	051	rs
2014/11/22 16:07:58 PST	10.0.0.18 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	MS	та
2014/11/22 16:07:58 PST	10.0.0.17 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	PO	sc
2014/11/22 16:07:58 PST	10.0.0.18 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	PR	EG
2014/11/22 16:07:58 PST	10.0.0.17 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	DR	GW
2014/11/22 16:07:58 PST	10.0.0.18 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	ME	RR
2014/11/22 16:07:58 PST	10.0.0.17 [PCI_events]	Local	Symantec	Critical System Protection	5.0.5.64	PN	ÊŢ
2014/11/22 16:07:58 P5T	10.0.0.18 [PCI_events]	Local	Symantec	Critical System Protection	5.1.0.214	DFI	ww
2014/11/22 16:07:58 PST	10.0.0.17 [PCI_events]	Local	Symantec	Critical System Protection	5.1.0.214	DFI	ww
2014/11/22 16:07:58 PST	10.0.0.18 [PCI_events]	Local	Symantec	Critical System Protection	5.1.0.214	DFI	ww
2014/11/22 16:07:58 PST	10.0.0.17 [PCI_events]	Local	Symantec	Critical System Protection	5.1.0.214	DF	ww
	ts (Scanned: 63,358 event 15:59:21 Time (Event Time) 1014/11/22 16:07:58 PST 1014/11/22 16:07:58 PST 1014/11/24 16:07:58 PST 1014/11/24 16:07:58 PST 1014/11/24 16:0	ts: (Scanned: 63,358 events, 00.01.094) 15:59:21 36:00:21 Time (Devent Time) Bevice 1014/11/22 16:07:58 PST 10.0.0.18 [PC]_events] 1014/11/22 16:07:58 PST 10.0.0.17 [PC]_events] 1014/11/22 16:07:58 PST 10.0.0.18 [PC]_events] 2014/11/22 16:07:58 PST 10.0.0.17 [PC]_events] 2014/11/22 16:07:58 PST 10.0.0.18 [PC]_events] 2014/11/22 16:07:58 PST 10.0.0.17 [PC]_events] 2014/11/22 16:07:58 PST 10.0.0.18 [PC]_events] 2014/11/22 16:07:58 PST 10.0.0.17 [PC]_event	tis (Scanned: 63,358 events, 00:01.094) 15:59:21 16:00:21 16:01:21 16:01:21 Time (Devet Time) Device Logger 1014/11/22 16:07:58 PST 10:0.0.18 (PCL,events) Local 1014/11/22 16:07:58 PST 10:0.0.17 (PCL,events) Local 1014/11/22 16:07:58 PST 10:0.0.18 (PCL,events) Local	sts (Scanned: 63,358 events, 00:01.094) 35:59:23 16:00:21 86:01:23 16:02:21 16:01:23 Time (Devent Time) Device Logger devicativender 1014/11/22 16:07:58 PST 10:0.0.18 (PC)_events] Local Symantec 1014/1	tis (Scanned: 63,358 events, 00:01:094) 35:59:21 16:00:21 36:01:23 16:02:21 16:03:23 16:04:23 Time (Devent Time) Device Logger devicablender deviceProduct 01/41/1/22 16:07:58 PST 10:0.0.18 (PC)_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.17 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.18 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.0.17 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.0.17 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.0.17 (PC]_events] Local Symantice Critical System Protection 01/41/1/22 16:07:58 PST 10:0.0.17 (PC]_events] Local Symanti	Partie Science: 63,358 events, 00.01.094] 15:59:23 16:00:21 16:01:21 16:02:21 16:03:23 16:04:23 16:05:21 Time (Devent Time) Device Logger device/Fender device/Fender device/Version 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64 1014/11/22 16:07:58 PST 10.0.0.18 (PC)_events] Local Symantice Critical System Protection 5.0.5.64	rist (Scanned: 63,358 events, 00:01.094) ● 15:59:21 16:00:21 16:01:21 16:02:23 16:03:21 16:09:21 16:05:22 16:06:23 Time (Device Time) Device Logger device/Vendor device/Pedict device/Vendor device/Ve

Logger can receive structured events that are parsed and unstructured RAW events, for which no parser is involved. Both types of events are searched for from a common interface.

Logger leverages the ArcSight SmartConnector framework to collect events. Logger can receive normalized CEF events from the SmartConnectors.

Multiple Loggers can work together for scalability purposes, supporting extremely high event volumes. Loggers can be configured as a peer network, with search queries distributed across all loggers.



Syslog is a loose standard (characterized, not defined, in RFC 3164) for event messages.

Although Logger is message-agnostic, it can do more with messages that adhere to the Common Event Format (CEF), an industry standard for the interoperability of event- or log-generating devices currently supported by many technology providers.

Raw Events consist of a receipt time, event time, a source (host name or IP address), and an un-parsed message portion. Logger displays events in a tabular form, as shown above.

Analyzing Events

Events can be searched, yielding a table of events that match a particular query. Queries can be executed manually or automatically, entered into the search field by clicking on terms in the event table. Queries can be based on plain English keywords (full-text search), predefined fields, or specified as regular expressions. Logger supports a flow-based search language that allows you to specify multiple search commands in a pipeline format.

By default, Logger queries only its primary data store even if peer Loggers are configured. However, you can configure Logger to distribute a query across peer Loggers of your choice.

Queries can be saved as a Filter or as a Saved Search. Saved filters can be used to select events for forwarding or to query events again later. For ease of use, Saved Filters and Saved Searches can be quickly called upon by typing "\$" into a search box at any time. This is an enhancement in Logger 6.0 which can collectively save a great amount of time when running multiple queries. A Saved Search is used to export selected events or save results to a file, typically as a scheduled task.

These saved searches are also leveraged to provide dashboards that can be customized to each individual user.

5.1. Introduction to the interface



Browser Requirements

Logger works with most modern browsers, including Internet Explorer (versions 10 and 11), Mozilla Firefox (version ESR 31), and Safari (version 7.0 - on OSX 10.9). Javascript and cookies must be enabled. An Adobe Flash Player plug-in is required for Internet Explorer browsers that access the Logger user interface. Some redundant monitoring features will be unavailable if the Flash Player plug-in is not installed. The Flash Player plug-in is

available for free at http://www.adobe.com/products/flashplayer/. Please look to the most current Release Notes to find the browser versions supported for your particular release.



6. Connecting to the Logger User Interface

Because the user interface of the software Logger uses SSL, make sure you connect using https, as seen in the following URL:

https://<hostname or IP address>:<configured_port>

Where hostname or IP address is of the system on which you installed Logger software.

Once you use the URL specified above, the following Login screen is displayed.

ArcSight Logger			
This is a private system Unauthorized access or limitation under 18 USC	, explicit authorizati use may result in se Sections 1030 et se	ion from the system o evere civil and/or crim rg. All rights whatsoe	owner is required for access or use. Inal liability, including without wer are reserved.
		🛃 l Accept	
WP	ArcSight	Logger	
Username	-		*
Password	1		*
	🗍 Use Local Au	thentication	
	Login	Reset	
	Copyright © 2001-2 Confidential comme	014 Hewlett-Packard D rcial computer software	levelopment Company, L.P. e, Valid license required.

Note that your system may have the disclosure enabled, which must be accepted before the login fields are available. This is a configurable option.

For the Logger Limited Use Free Version, use the following information:

Username: admin

Password: password

(Please change after first use)

Navigating the User Interface

As shown below, a consistent navigation and information band runs across the top of every page in the user interface.

			Menu T	abs			Navigation Box		Gauges	Optic	ins Dropdown
🍈 ArcSight Logger	Summary	Analyze 🗸	Dashboards	Reports	Configuration 🗸	System Admin	(Take me to (Alt+o)	EPS In: 0	EPS Out: D	CPU: 1%	(14:5-1) admin 🗸

Real-time counters, located at the top of the screen, provide an indication of the throughput and CPU usage information, as well as the current time, which are available in more detail on the Monitor Dashboard ("Dashboards" on page 22). The current user-name is also displayed immediately below the time in the top-right corner of the screen.



<u>Help</u>

A help link is found under the admin drop-down, which provides context-sensitive online help related to the currently displayed window-pane.

In addition, Search Helper, a search-specific utility is available that provides search history, search operator history, examples, suggested next operators, and list of fields and operators. Search Helper is available and enabled by default. This helper automatically displays relevant information based on the query currently entered in the Search text box.

Options

The **Options** page enables you to set the default start page (home page) for all users and specific start pages for individual users.

System		
EPS input rate gauge max	100K	•
EPS output rate gauge max	100K	•
Default start page for all users	Summary	•
Upload a logo (PNG file)	Browse No file selected.	
Show default logo		
Personal		
Default start page for admin	Use default for all users	•

Logger 6 also added the option to add your own logo. I added this as my logo. Feel free to use this or your own company logo.



Logout

Click the Logout link on any page to return to the Login screen. Logging out is good security practice, to eliminate the chance of unauthorized use of an unattended Logger session.

Logger automatically logs you out after a user-configurable length of time (15 minutes by default). To change this length of time, see the Logger Administrator's Guide.

Summary

The Summary page is a global dashboard that provides summarized event information about your Logger in one screen. It enables you to gauge incoming events activity and the status of indexing.



ArcSight Logger Summary Analy	ze 🗸 Dashboards Reports	Configuration 🗸 System Ad	min Take me to (Alt+o)	EPS In: 105 EPS Out	:C CPU: 3% admin
Global Summary					
There are 378,487 events indexed from 2014/1	1/20 14:09:32:915 PST to 2014/11/	22 17:28:57:044 PST. Add Data			
Event Summary by Receiver			Event Summary by Device		
Receiver	Count -	Most Recent	Device	Count ~	Most Recent
demo_events	167,473	2014/11/22 17:28:45 P5T	10.0.0.11	167,512	2014/11/22 17:28:45 PST
PO_events	100,957	2014/11/22 17:28:57 PST	10.0.0.12	167,512	2014/11/22 17:28:45 PST
raw_syslog	63,756	2014/11/22 17:28:32 P5T	10.0.0.17	101,007	2014/11/22 17:28:57 PST
Now_data	25,200	2014/11/22 17:28:28 PST	10.0.0.18	101,006	2014/11/22 17:28:57 PST
SOK_events	18,000	2014/11/22 17:28:28 PST	10.0.0.14	63,765	2014/11/22 17:28:32 PST
Logger Internal Event Device	3,091	2014/11/22 17:27:08 PST	10.0.0.13	63,765	2014/11/22 17:28:32 PST
			10.0.0.19	25,200	2014/11/22 17:28:28 PST
			10.0.0.20	25,200	2014/11/22 17:28:28 PST
			10.0.0.15	18,000	2014/11/22 17:28:28 PST
			10.0.0.16	18.000	2014/11/22 17:28:28 P5T
Displaying 1 - 6 of 6] ((Page 1 of 1 ≥)]	Displaying 1 - 10 of 11		jii i Page 1 of 2
Event Summary by Agent Severity			Event Summary by Agent Type		
Agent Severity	Count -	Most Recent	Agent Type	Count -	Most Recent
Unknown	240,787	2014/11/22 17:28:57 PST	golaya	164,382	2014/11/22 17:28:45 PST
Medium	129,662	2014/11/22 17:28:57 PST	symantercsp_db	36,027	2014/11/22 17:20:46 PST
High	90,600	2014/11/22 17:28:45 PST	oracle_db	33,092	2014/11/22 17:25:56 PST
Low	88,787	2014/11/22 17:28:57 PST	syslog_file	20,521	2014/11/22 17:26:26 PST
Very-High	58,479	2014/11/22 17:28:45 PST	syslog_pipe	17,628	2014/11/22 17:28:45 PST
1	3,011	2014/11/22 17:27:08 PST	nt_advanced	16,814	2014/11/22 17:26:26 PST
3	39	2014/11/22 17:25:44 PST	sigtserver_audit_db	13,120	2014/11/22 17:21:31 PST
2	38	2014/11/22 17:25:44 PST	multisgiserver_audit_db	11,800	2014/11/22 17:28:57 PST
	17	2014/11/22 17:22:52 PST	Other	9,686	2014/11/22 17:29:35 PST
7	3	2014/11/22 15:38:54 PST	siteorotector dh	9.090	2014/11/22 17:20:05 PST
Displaying 1 - 10 of 10		14 4 Page 1 of 1 5 51	Displaying 1 - 10 of 30		Page 1 of 3

Dashboards

Dashboards are an all-in-one view of the Logger information of interest to you. You can assemble various search queries that match events of interest to you, status of Logger components such as receivers, forwarders, storage, CPU, and disk, or a combination of both on a single dashboard for status at-a-glance.

Each Dashboard contains one or more panels of these types: Search Results and Monitor.

The Search Results panel displays events that match the query associated with the panel.

The Monitor panel displays the real-time and historical status of various Logger components such as receivers, forwarders, storage, CPU, and disk.

For more details about Dashboards, see the Logger Administrator's Guide.

Example:







Searching and Analyzing Events

The Process of Searching Events through stored events is very simple and intuitive on Logger. It uses a flow-based search language that allows you to specify multiple search commands in a pipeline format. In addition, you can customize the display of search results, view search results as charts, and, as always, access saved searches and filters with "\$".

🗃 🛗 关 🗘 🗸 🖌 All Fields	*	Custom time range 💌 Start 🏦 11/22/2014	16:03:27 Dynamic End 🏦 11/22/2014 16:13					
"john" AND message STARTSWITH "click"	\$							
\$action=monitor	4,827	Examples	Help 🛃					
\$btime=2005-12-31	4,827	error alert	The Indexed search uses Logger's indexing capability to					
\$cat=others	4,877	message CONTAINS "Between"	quickly and efficiently search for relevant data, and					
\$cnt=1	4,579	(name="lohn Doe" OR name="lane Doe") AND	enables you to specify keywords, indexed, and					
\$devicename=test	4,827	message!="success"	non-indexed fields in a boolean expression.					
\$devicetype=netkeeper	4,827		more »					
\$dstip=192.168.168.254	4,253		Suggested Next Search Operators					
\$dstport=0	4,253		cef , rex , extract , regex					
\$etime=2005-12-31	4,827							
\$filter\$Configuration - Configuration Chang	es (Unified)							
\$filter\$Configuration - System Configuratio format)	n Changes (CEF							
\$filter\$Events - CEF								
\$filter\$Events - Event Counts by Destinatio	n							
\$filter\$Events - Event Counts by Source								
\$filter\$Events - High and Very High Severity	CEF Events	Auto-open is ON						
\$ifno=0	4,253							
\$ori=built-in	4,893							
\$ruleid=1048909	4 253							

Next, enter the keywords or information you are searching for (referred to as queries) in the Search text box, select the time range, and click Go, as shown in the previous figure. Logger searches for the data that matches the criteria you specified and will display the results on the same user interface page where you entered your query.

A query can be as simple as a keyword; for example, hostA.companyxyz.com. Or a complex query that includes Boolean expressions of keywords and indexed fields, and regular expressions; for example:

```
_storageGroup IN ["Default Storage Group"] _deviceGroup IN
["192.168.22.120 [TCPC]"] name="*[4924TestAlert]*" AND ("192.168.*" OR
categoryBehavior CONTAINS Stop) | REGEX=":\d31" | cef name
deviceEventCategory | chart _count by name
```

Additionally, a query can include constraints that limit the search to specific device groups and storage groups.

Logger offers several convenient ways to enter a search query:

- typing the query in the Search text box
- using Logger's Search Builder tool to create a query, or
- using a previously saved query (referred to as filter or saved search)
- Retrieving saved searches and filters with "\$", followed by its name

When you type a query, the auto-suggest facility in the user interface provides suggestions and possible matches for the fields you are entering and the applicable operators for those fields, thus enabling you to quickly build a query expression. The auto-suggest facility is available only for fields in the Logger schema, metadata terms (_storageGroup, _deviceGroup, _peerLogger), and the regular expression term (|REGEX=). Although a search query on Logger is as simple as entering a keyword to match, you will utilize the full potential of Logger's search operation if you are familiar with all elements of a query, as described in the following section.

Building a Query



When you build a query, the following elements need to be specified:

- Query Expression—search conditions that are used to select or reject an event.
- **Time range**—the time range within which events should be searched.
- Field Set—fields of an event that should be displayed for matching events; for example, you can select to display only the deviceAddress and deviceReceiptTime fields of matching events.

🗃 🗎 👯 🔅 🗸 🛛 All Fields	•	Custom time range 🔹 Start SCurrentWeek 🖉 Dynamic End SNow	🔽 Dyn	amic	
enter search query			~	Go!	Advanced

Saving Queries for Later Use

If you need to run the same query regularly, you can save it in two ways:

- Saved filter Save the query expression, but not the time range or field set information.
- Saved search Save the query expression and the time range.

For more information about saving queries and using them again, see the Logger Administrator's Guide.

Query Building Tools

Logger offers the following tools to assist you in building queries that are complex:

□ Search Builder

The Search Builder tool, as shown in the following figure, is a Boolean-logic conditions-editor that enables you to quickly and accurately build search queries. The tool provides a visual representation of the conditions you are including in a query. You can specify keywords, field-based conditions, and regular expressions using this tool. In addition, the tool enables you to specify search constraints such as device groups and storage groups.

Click Advanced Search below the Search text box to access this tool. (For information about how to use this tool, see the Logger Administrator's Guide)



🗌 Regex Helper**Tool** 🧾

쳵 ArcSight Logger	Summary Analyz	e 🗸 Dashboa	rds Reports Configuration 🗸 System Adm	in
Take me to (Alt+o)		🗟 Extract Fie	lds	? 🗆 🗙
🗃 🗎 💐 🔷 🗸 🗛	l Fields	Raw Event	<13>Aug 6 12:24:36 centos65 root: Aug 4 17:06:24 centos65 sshd[identification string from 15.1.237.141	25979]: Did not receive
_deviceGroup IN ["n127-(D-O-h16.my.company.cor 321 events, 00:00.930)	n (Regex	\<{? <number_1>\d+)\>{?<timestamp_1>\S++\d+\d+\d+\d+\d+\d+\d+\d+\d+\d+\d+\d+\d</timestamp_1></number_1>	Vord_1>\S+) /ord_2>\S+) >\S+) (? <word_6>\S+) >\d+\.\d+\.\d+\.\d+)</word_6>
200 150 100 50				
12:24:20		Field Nam Number_2	e Value 25979	*
? «	Time (Ev	ent Word_4	Did	
Selected Fields (0)		Word_5	not	
No fields to display	I 5 2014/08/	Word_6	receive	
		06 Word_7	identification	
		Word_8	string	=
	☐ 7 2014/08/	06 🔲 Word_9	from	
	RAW 📆 <13>A	ug IPAddress_	1 15.1.237.141	-
		06	ОК	Cancel

The Regex Helper tool enables you to create regular expressions that can be used with the rex pipeline operator to extract fields of interest from an event. This tool not only simplifies the task of creating regular expressions for the rex operator but also makes it efficient and error-free. For details about this tool, see the Logger Administrator's Guide.

Search Helper

deviceEventCla	ssld Field	Search History	
deviceEventCa	egory Field	logger cef deviceEventCategory name	
deviceExternal	d Field	Search Operator History	Help 🗹
		cef deviceEventCategory cef deviceEventCategory name Examples	Extracts values for specified fields from matching CEF events. If an event is non-CEF, the field value is set to NULL. more » Suggested Next Search Operators
		categorySignificance STARTSWITH "Norma" AND agentType STARTSWITH "testalert" cef categorySignificance agentType logger cef deviceEventCategory name	rex , extract , regex , top , fields , sort
		Auto anno in ON	



Search Helper is a search-specific utility that provides the following features:

- **Search History**—Displays the recently run queries on Logger, thus enabling you to select and reuse previously run queries without typing them again.
- Search Operator History Displays the fields used previously with the search operator that is currently typed in the Search text box.
- **Examples**—Lists examples relevant to the latest query operator you have typed in the Search text box.
- **Suggested Next Operators**—List of operators that generally follow the currently typed query. For example, if you type logger |, the operators that often follow are cef, rex, extract, or regex.
- **Help**—Provides context-sensitive help for the last-listed operator in the query that is currently typed in the Search text box.
- List of Fields and Operators—Depending on the current query in the Search text box, a complete list of fields that possibly match the field name you are typing or a list of operators that are available on Logger is displayed.

System Filters (Predefined Filters)

Your Logger ships with a number of predefined filters, also known as system filters. These filters define queries for commonly searched events. For example: unsuccessful login attempts or the number of events by source.

To use a system filter, follow the steps provided below:

- 1. Click **Analyze** > **Search**
- 2. Click the Load a Saved Filter icon (i) to view a list of all system filters.



- 3. Click Close
- 4. Select filter
- 5. Click Load+Close.
- 6. Click Go to run the query.



7. Prepare System for Use Case Below

7.1. Configuring Logger to accept the Windows Unified Connector Events

Note: Some Logger Appliances have integrated connectors; other models require external Smart Connectors. Both require you to enable a receiver on the logger to receive the processed events.

From the Logger Menu, mouse over **Configuration**, under the **Data** column and select **Receivers** within the drop-down menu. Once at the devices page, Click the "**Add**" button.

ArcSight Logger Summary	Analyze 🐱 Dashboar	rds Reports	Configuration 🗸	System Admin	Take me to (Alt+o)			EPS In: 105	EPS Out:	CPU: 4%	ad	8:05 Imin 🗸
Receivers												
Add												
Once you enable the Apache URL Access En	ror Log receiver, Logger will	start storing entries I	from the <install_di< td=""><td>r>/userdata/logs/ap</td><td>ache/http_error_log file.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></install_di<>	r>/userdata/logs/ap	ache/http_error_log file.							
Logger can also store entries from the mes Administrators guide for details.	sages and audit.log files in t	the /var/log/* folders	s. Before enabling th	e receivers for these	files, consult the Logge	6						
Name			Туре				IP Address		Port			
Name Mail Logs			Type File Receiver				IP Address		Port		/ >	0
Name Mail Logs Apache URL Access Error Log			Type File Receiver Folder Follower R	leceiver			IP Address		Port		/ >	2
Name Mail Logs Apache URL Access Error Log Audit Log			Type File Receiver Folder Follower R Folder Follower R	leceiver			IP Address		Port		/ >	0
Name Mail Logs Apache URL Access Error Log Audit Log Var Log Messages			Type File Receiver Folder Follower R Folder Follower R Folder Follower R	leceiver leceiver leceiver			IP Address		Port		/ >	
Name Mail Logs Apache URL Access Error Log Audit Log Var Log Messages demo_events			Type File Receiver Folder Follower R Folder Follower R Folder Follower R UDP Receiver	leceiver leceiver leceiver			IP Address		Port 519		/ >	
Name Mail Logs Apache URL Access Error Log Audit Log Var Log Messages demo_events fiow_data			Type File Receiver Folder Follower R Folder Follower R Folder Follower R UDP Receiver UDP Receiver	tecelver Lecelver Lecelver			IP Address All All		Port 519 518		/ > / > / > / > / >	
Name Mail Logs Apache URL Access Error Log Audit Log Var Log Messages demo_events flow_data PO_events			Type File Receiver Folder Follower R Folder Follower R Folder Follower R UDP Receiver UDP Receiver	lecelver lecelver lecelver			IP Address All All All		Port 519 518 517		/ > / > / > / > / > / > / >	
Name Mail Logs Apache URL Access Error Log Audit Log Var Log Messages demo_events flow_data PCL_events raw_syslog			Type File Receiver Folder Follower R Folder Follower R Folder Follower R UDP Receiver UDP Receiver UDP Receiver	leceiver leceiver leceiver			IP Address All All All All All		Port 519 518 517 515		/ > > > > > > > > > > > > > > > > > > >	

Next, add a receiver with the the name of "Windows" and select SmartMessage Receiver from the available type options.

Name	Windows	
Туре	SmartMessage Receiver	
	Shart Estige Receiver	
	Next Cancel	

Now, click Next



source type that	you need does not exist in the Source Type dropdown list below, go to the Source Types page to add it.
Name	Windows
Encoding	UTF-8
Source Type	CEF

Choose the default Encoding (UTF-8), a source type of CEF and choose Save

Windows	SmartMessage Receiver	1	×	
Note that the receive	er is not enabled upon configuration			
Click on the disabled	l symbol 🖉 to enable the connector			
Notice that the disable enabled and ready to	led symbol 🖉 now shows a checkmark 💙 and the rece preceive events.	viver is n	ЭW	
Windows	SmartMessage Receiver		×	✓



7.2. Configuring the Windows Unified Connector to collect and send events to a Logger appliance

Below are screenshots showing the general configuration of a Connector on a Connector Appliance. If you have the Software Logger <u>goto section 7.3</u>

If your logger supports onboard connectors:

Choose Configuration > Manage Connectors to reveal the connector menus.

ArcSight	Logg	jer			
Summary A	nalyze [Dashboards Reports	Configuration	System Admin	
		« Connectore	Settings		
∢ System		connectors	Manage Conne	ctors	
🖃 🐽 Default		Default -> Local	Repositories		
⊡	⊡-¶_Localhost └── <mark>ॄ</mark> Container 1		i 🙀 🗞 🛞		
		Name		Path	Туре
		Delete Runti	me Parameters	Destinations	Parameters

1) Click the add Connector icon (🍫) to start the process of adding a Connector.

Monitor Manage Setu	ıp				5K - 155K		
(w)	Connectors						
© System → Default → Quocalhost → Container 1 ⊕ Container 2 → Container 3	Default -> Localho	ost -> Container	1 (Connected)	FPS In	FPS Out	Cache	
- Container 5			. i pe	1.5.1	No item is available for this o	peration.	
Container 6	Delete	Runtime Paramet	De	estinations	Parameters		

2) Click Next.



his process allows you to add a connector. The wizard guides you through the following steps: - Choosing type of the connector to be created. Define connector parameters. - Define destination parameters (select from exisiting ones or create new one). - Define connector details	nnector Setup			
 Choosing type of the connector to be created. Define connector parameters. Define destination parameters (select from exisiting ones or create new one). Define connector details 	This process allows you to a	dd a connector. The wizard g	uides you through the follo	owing steps:
 Define destination parameters (select from exisiting ones or create new one). Define connector details 	- Choosing type of the connec	or to be created. Define connect	or parameters.	
	 Define destination parameter Define connector details 	s (select from exisiting ones or o	reate new one).	
	- Define connector details	• • • • • • • • • • • • • • • • • • •		

- 3) Choose the Connector Type you want to configure. This example chooses "Microsoft Windows Event-Log-Unified"
- 4) Run through the Connector Setup and choose "Microsoft Windows Event Log Unified"

Select the type of connector you wish to confi	gure	
Type Microsoft Windows Event Log - Unified	•	

5) This next screen is only required if you will be using the Windows Host Browser. Since we will enter devices manually, you can skip this step and click Next.

nter Connector Details		
Domain Name		
Domain User Name		
Domain User Password		
Active Directory Server		
Active Directory Base DN	ou= <organizational unit="">,dc=<domain component:<="" td=""><td></td></domain></organizational>	
Active Directory Filter	(&(cn=*)(operatingsystem=*)(whencreated=*))	
Active Directory User Name		
ctive Directory User Password		
Active Directory Protocol	non_ssl 🔹	
Active Directory Port	389	
ctive Directory Max Page Size	300	
Global Catalog Server		
Global Catalog Base DN		
Global Catalog User Name		
Global Catalog User Password		

6) Choose to "Enter Devices Manually"



elect how you want to browse for devi	es	
PPE Enter Devices Manually	•	

7) Click "Add Row" for each host that you want to collect events from.

Domain Name	Host Name	User Name	Password	Security	System	Application	Microsoft OS Version	locale	
arcnet.com	testhost	arcsight				Г	Windows Server 2008 R2 👻	en_US	1

Fill in the following parameters for each host you want to collect events from:

Domain Name - Name of the domain to which the host belongs. If you are using a Domain User account for a target host, fill in the Domain Name field. If you are using a Local User account for the target host, leave the Domain Name field blank. If the target host is a Workgroup host that does not belong to a domain, leave the Domain Name field blank.

Host Name - Host name or IP address of the target Windows host.

User Name - Name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain. Windows Server 2003 can utilize a standard domain user account. Windows 2008 servers can also utilize a standard Domain User Account and choose the new "Event Log Readers" builtin. See the MicrosoftWindowsEventLogUnified.pdf document for further details.

Password - Password for the user specified in User Name.

Security Logs - Select the check box for security events to be collected from this host; unselect the check box if you do not want to collect security events. The default value is checked (true)

System Logs - Select the check box for system events to be collected from this host; unselect the check box if you do not want to collect system events. The default value is unchecked (false)

Application - Select the check box for application events to be collected from this host; unselect the check box if you do not want to collect application events. The default value is unchecked (false)

Microsoft OS Version - Select the Microsoft Operating System version this host is running.

locale - Enter the code for your locale; possible values are 'en_US' (United States English),' ja_JP' (Japanese), 'zh_CN' (Simplified Chinese), 'zh_TW' (Traditional Chinese), 'fr_CA' (French). The default value is 'en_US'.

8) Click Next and continue on with the installation

9) Choose "ArcSight Logger SmartMessage" as the Destination Type.



nector Setup		
Choose Destina	ation Type	
Destination Type	ArcSight Logger SmartMessage (encrypted)	

10) Enter in the "**Hostname/IP**" of the Logger and the "**Receiver Name**" (note: A receiver should have already been created on the Logger). In our case the receiver is named "Windows"

V	/izard	
Co	nnector Setup	
	Enter these paran	neters
	Host Name/IP	10.10.10
	Port	443
	Receiver Name	Windows
	Compression Mode	Disabled •
	Cancel	Previous Next

7.3. Installing the Windows Unified Connector to collect and send events to a <u>Software Logger</u>

Obtain a current version of the ArcSight Smart Connectors.

For example if you download the Trial Logger you will have the following version

				10
Marcinet E 27 6EM 0 Compositor Developedable Longer Win eve	Annelination	1/22/2012 4:40 DM	172 241 022	0.0/
Arcsight-3.2.7.0344.0-Connector-Downloadable-Logger-Win.exe	Application	1/25/2015 4:49 PIVI	1/0.041.902	0.76

Or you may have the full version. As of this date the current version is 7.0.7

ArcSight-7.0.7.7279.0-Connector-Linux.bin	12/5/2014 4:16 PM	BIN File	171,445 KB
ArcSight-7.0.7.7279.0-Connector-Linux64.bin	12/5/2014 4:12 PM	BIN File	165,301 KB
ArcSight-7.0.7.7279.0-Connectors.aup	12/5/2014 4:08 PM	AUP File	584,383 KB
ArcSight-7.0.7.7279.0-Connector-Win.exe	12/9/2014 4:35 PM	Application	161,102 KB
ArcSight-7.0.7.7279.0-Connector-Win64.exe	12/5/2014 4:07 PM	Application	160,741 KB

As you can see there are multiple platforms that the connectors can be installed on.

In this example I am installing the ArcSight-7.0.7.7279.0-Connector-Win.exe on Windows 7 workstation.





Just click OK to continue the installation.

In this case I choose to install the connector in C:\my_data\Arcsight\Connectors\WUC







TIP: Resize the screen for better view ability



Click Add, Enter the appropriate Values and click "Next"



If validation and logon to the device passes you will get the following screen, if not resolve the user/pass and domain entries as needed

Select ArcSight Logger SmartMessage (encrypted)



Constructions		and the second		1000 Contraction
Configure	Zone the type of devicements			
	1101949 - 1000 - 100			
			 Comparison of a second s	
			· Eventsen Johnson and and	
			0.1970	
			0.073498	
			 GP (introductioning SAP) 	
			 On the 	
and the second se			 Row type) 	
Andunhalt				
Arcsigniz				
				Comment of the second s

Next

Enter the hostname and receiver name

In my case the address is 172.16.100.100 and the Receiver Name was set to "Windows" which is case sensitive

You will get the following screen, if an error occurs follow the guidance given



Recommendation for testing is to leave as a standalone application, then once it is verified you can change it to a service.



Choose Next then Exit

Start a command window in windows

Change directory to C:\my_data\Arcsight\Connectors\WUC\current\bin where I installed the connector

C:\my_data\Arcsight\Connectors\WUC\current\bin>arcsight	agents

You will see something like the following

[Tue	Dec	16	23:54:11	CST	2014]	LINFO] Agent	upgrad	e sta	tus o	check	threa	d sta	arted						
[Tue	Dec	16	23:54:11	CST	2014]	LINEO	1 Device	conne	ction	to	EWOLFE	FB2.1 u	p.(Co	onnec	ted to	Host)				
[Tue	Dec	16	23:54:13	CST	20141	LINEO	1 First	event	from	[Arc8	Sight	ArcSi	ght 1	16.21	4.228.	205 I wa	1ffb21	receiv	ved.	
[Tue	Dec	16	23:54:13	CST	2014]	LINEO] First	event	from	[Mici	rosoft	Hicr	ösoft	; Win	dowsii	wolffl	2.amer	icas.hp	ogcorp.net]	received.
I GC	1088:	17K-	->16403K<	2457	60K), (0.01642	44 secs													

Indicates the connector is up and the events are being sent to logger.

To confirm, go to the "Analyze" tab of the logger

Enter your machine name, in my case WOLFFB2

earch # siem	Sommary	Analyze 🐱 Dashbo	ards Reports Cooff	guration 🖌	System Ad	min Take me to.	. (Alt+o)				EPS In: IOS EPS Out: O	CPU: 1%	2 1:56 dmin 🗸
M 4 0 V A	Fields	Last 10	minutes 🔽					Got: Advanced					
events (Scanned: 62;	978 events, 0	0:00.6941										1 ber - 1 se	econd
							21(54)21						
él.		Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEvent(TassId	name	agentAddress	agentilastName	agentType	ager
cced Fields (5) ceEventClassId 10	¥ 1	2014/12/16 21:54:21 PST	172.16.100.1 [Windows]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security- Auditing:4688	Microsoft-Windows-Security-Auditing	16.214.228.205	W00111132 americas: hpc: orp. vet	windowstg	/AIL Add Equi
eProduct 2 eVendor 2 eVersion 1	# 2	2014/12/16 21:54:21 PST	172.16.100.1 [Windows]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security- Auditing:4688	Microsoft-Windows-Security-Auditing	16,214,228,205	WOLFTB2 anvectors hppp or pinel	windowslg	/All. Add Equ
1	# 3	2014/12/16 21:54:21 PST	172.16.100.1 [Windows]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security- Audting#688	Microsoft-Windows-Security-Auditing	16,214,228,205	WCCFFTIC: american lippo or pinet	windowslg	/AIC Add Equi
	a 4	2014/12/16 21:54:21 PST	172.16.100.1 [Windown]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security- Auditing/4688	Microsoft-Windows-Security-Auditing	16,214,228,205	And Hild American Space poor	windowslg	/All: Addr Equi
	⊯ 5	2014/12/16 21:54:21 PST	172.16.100.1 [Windows]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security- Auditiog2668	Microsoft-Windows-Security-Auditing	16,214,228,205	WUTTER american bogsorp. Art	windowslg	/AIL Addr Equi
	-a 6	2014/12/16 21:54:21 PST	172.16.100.1 [Windows]	Local	Mcrosoft	Microsoft Windows		Microsoft-Windows-Security- Audtings/658	Nicrosoft-Windows-Security-Auditing	16.214.228.205	WHIPPersonal standards	windowsfg	/All Add Equi
	-27	2014/17/16 21-64-21 DCT	172.16 100.1 falloctrue1	Local	Mirneda	Ministel Minister		Microsoft, Mindows, Saroritos	Miccourd Mindows, Sacority, Audition	16.216.228.205		wintracts	. /ai
	Destau	and the office is the second	. 25									CONTRACTOR OF	1.1

We can see that I received 56 events from the connector.



8. USE CASE Step by Step

We are interested in any activities surrounding **FAILED** logon attempts in Microsoft Windows

First we need to know how Microsoft Classifies Failed Logon Attempts

- 529 Logon Failure Unknown user name or bad password
- **530** Logon Failure Account logon time restriction violation
- 531 Logon Failure Account currently disabled
- 532 Logon Failure The specified user account has expired
- 533 Logon Failure User no allowed to logon at this computer
- 534 Logon Failure The user has not been granted the requested logon type at this machine
- 535 Logon Failure The specified account's password had expired
- 536 Logon Failure The NetLogon component is not active
- **537** Logon Failure The logon attempt failed for other reasons.
- 538 User Logoff
- 539 Logon Failure
- 540 Successful Network Logon

675 – Pre-authentication failed

Windows 2008R2

- 4624 An account was successfully logged on
- 4625 An account failed to logon
- 4634 An account was logged off

As an administrator of Microsoft products you are already aware of the hundreds of codes that Microsoft uses to define their event codes. In this case we will conduct a simple text search for the entry "Security:529" or for Windows 2008 "Microsoft-Windows-Security-Auditing:4625"

Thankfully ArcSight recognizes that not everyone is an expert in security codes for dozens of products and uses categorization to eliminate the need to know specific codes.

Read more about Categorization in section 7.2 below.

8.1. Search / Analyze

Mouse over "Analyze", and select "Search" from the menu

And in the Search area enter: "Security:529" OR for Windows 2008:"Microsoft-Windows-Security-Auditing:4625

l	ArcSight Logger Summary	Analyze 💙	Dashboards	Reports	Configuration 🗸	System Admin	(Take me to (Alt+o)			
l	🗃 🛅 💐 🗘 🗸 All Fields	(*)	Last 10 minutes	[\$]						
l	"security:529"							~	Go!	Advanced

As you can see the events that meet the query have been returned and are displayed for further revision and/or analysis.



m ArcSight Logger	Summary	Analyze V Dashboard	is Reports Configuration	 System Admin 	Take me to (Alt+o)		EPS In: 106 EPS Out: 1	CPU: 13% admin
■ H 🍕 O 🗸 🕫	All Fields	¢ Last 10 min	utes ()					
"security:529"					*	Gol Advanced		
24 events (Scanned: 6	0,285 events, 0	0:01.648) 🐳						1 bar = 5 second
6 4 2								
20:08:03		20:08:43	20:09	23	20:10:03	20:10:43		20:11:23
2 (4)		Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId
elected Fields (4) eviceEventClassId 1	¥ 1	2014/12/14 20:11:46 PST	10.0.0.12 (demo_events)	Local	Microsoft	Microsoft Windows		SECURIS/1920
eviceProduct 1 eviceVendor 1	≝ 2	2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Nicrosoft	Microsoft Windows		STREET STREET
ame 1	≡ 3	2014/12/14 20:11:46 PST	10.0.0.12 [demo_events]	Local	Microsoft	Microsoft Windows		500007850
	. 4	2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Microsoft	Microsoft Windows		2000000000

You can change the presentation of the results by choosing or creating a display set in the Fields: portion.

To change the Field set click the Select the "Categories" field



drop down box next to "Fields:" set.

	Time (Event Time)	Device	Logger	deviceEventClassId	name	deviceVendor	deviceProduct	categoryBehavior	categoryDeviceGroup
1	2014/12/14 20:11:46 PST	10.0.0.12 [demo_events]	Local	SR00157529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
2	2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
3	2014/12/14 20:11:46 PST	10.0.0.12 [demo_events]	Local	SINULITY STOL	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
4	2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	Security 529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System
5	2014/12/14 20:11:46 PST	10.0.0.11 [demo_events]	Local	STRUCTURE	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System

Minimize the Field Summary at this time by clicking on the 🦉 We will discuss this shortly

? «
Selected Fields (9)
categoryBehavior 1
categoryDeviceGroup 1
categoryObject 1
categoryOutcome 1
categorySignificance 2
deviceEventClassId 1
deviceProduct 1
deviceVendor 1
name 1



8.2. Categorization

As you can see the **Security:529** has been returned but I am now focusing on the fields related to categorization. First notice that the **Security:529** appears under the field name **deviceEventClassId**.

ArcSight SmartConnectors normalize, categorize and prioritize all events as they are being obtained from the logging systems. This eliminates the need to understand each vendor's individual coding of events and allows you to use categorization to find the nature of the information you are looking for.

As you can see Security:529 is categorized as:

categoryBehaviour /Authentication/Verify categoryDeviceGroup/Operating System CategoryObject /Host/Operating System CategoryOutcome /Failure CategorySignficance /Information/Warning

For Windows 2008 you see that **Microsoft-Windows-Security-Auditing:4625** is categorized in exactly the same way

Logger	deviceEventClassId	name	deviceVendor	deviceProduct	categoryBehavior	categoryDeviceGroup	categoryObject
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
Local	Security:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System

Now modify the search and look for /Authentication/Verify AND /Failure instead.

Delete "Security:529 " from the Search area and replace with: *"/Authentication/Verify and /Failure*" and click "**Go**"



Ø	ArcS	ight Logger Summar	y Analyze 🗸 Dasht	idards F	teports Configuration	System Admin (Take me to (A	it+o}	E	rs In: 105 EPS Out: 0	CPU: 14
in 1	n 4	O 🗸 Categories	() (Last 1	minutes	•					
/Aut	henti	cation/Verify AND /Failure					~	Gol Advanced		
1,15	i0 eve	nts (Scanned: 52,594 ever	nts, 00:01.081) 🗸							1
D 6 2 8 4 0 20 8	14	20:21:54 2	0.22:34 20:23:14	20:23	54 20:24:34	20:25:14 20:25:54 2	2:26:34 20:3	17:14 20:2	7:54 20:28:34	20:29
		Time (Event Time)	Device	Logger	deviceEventClassId	name	deviceVendor	deviceProduct	categoryBehavior	category
	7	2014/12/14 20:29:02 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	(Authoritics) (with	/Operating
	8	2014/12/14 20:28:54 PST	10.0.0.16 (SOX_events)	Local	arcsight:10:30	Failed password	Unix	Unix	Mathematica Weilly	/Operating
а	9	2014/12/14 20:28:54 PST	10.0.0.15 (50X_events)	Local	arcsight:10:30	Failed password	Unix	Unix	(Sotherstation/Werlfy)	/Operating
	10	2014/12/14 20:28:52 PST	10.0.0.11 [demo_events]	Local	arcsight:38:0	Login failure	Unix	Unix	Mithentication/Weilly	/Operating
3	11	2014/12/14 20:28:52 PST	10.0.0.12 [demo_events]	Local	arcsight:47:0	PAM Error Message - Authentication failed	Unix	Unix	(Anthonikasion Antily)	/identity M
э	12	2014/12/14 20:28:51 PST	10.0.0.11 [demo_events]	Local	arcsight:35:7	pam_authenticate: Authentication failed	Unix	Unix	(Contraction Vinter	/Operating
з	13	2014/12/14 20:28:51 PST	10.0.0.11 (demo_events)	Local	arcsight:35:5	Login incorrect	Unix	Unix	Samerican write	/Operating
	14	2014/12/14 20:28:51 PST	10.0.0.12 [demo_events]	Local	arcsight:35:5	Login incorrect	Unix	Unix	Contraction of the	/Operating
а	15	2014/12/14 20:28:49 PST	10.0.0.15 (SOX_events)	Local	arcsight:10:30	Failed password	Unix	Unix	(Mathentication/World)	/Operating
a	16	2014/12/14 20:28:47 PST	10.0.0.11 (demo_events)	Local	t_auth_attempt	auth_attempt	Secure Computing	Sidewinder	Mathematication/Weatly	/Firewall
	17	2014/12/14 20:28:46 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	(Authoritantian/World)	(Operating

Instead of being limited to Authentication Failures specific to Microsoft, I now see ALL events classified as Authentication Failures regardless of Vendor. Here we see UNIX and Sidewinder.

Notice that any time the search criteria are met, the display highlights that entry for fast location visually.

By hovering over an entry, in this case "Unix" all matching events are highlighted.

a 11	2014/12/14 20:28:52 PST	10.0.0.12 [demo_events]	Local	arcsight:47:0	PAM Error Message - Authentication failed	Unix	Unix	/Authentication/Verify	/identity Management/AAA
a 12	2014/12/14 20:28:51 PST	10.0.0.11 [demo_events]	Local	arcsight:35:7	pam_authenticate: Authentication failed	Unix	Unix	lausnen Henrien Weitz,	/Operating System
13	2014/12/14 20:28:51 PST	10.0.0.11 [demo_events]	Local	arcsight:35:5	Login incorrect	Unix	Unix	/Authentication/Verify	/Operating System
14	2014/12/14 20:28:51 PST	10.0.0.12 [demo_events]	Local	arcsight:35:5	Login incorrect	Unix	Unix	Authentication/Weilly	/Operating System
15	2014/12/14 20:28:49 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Verify	/Operating System
16	2014/12/14 20:28:47 PST	10.0.0.11 [demo_events]	Local	t_auth_attempt	auth_attempt	Secure Computing	Sidewinder	(Authentication Verify	/Firewall
17	2014/12/14 20:28:46 PST	10.0.0.15 [S0X_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Vecify	/Operating System
18	2014/12/14 20:28:44 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	(Authonicston/Wesley	/Operating System
19	2014/12/14 20:28:40 PST	10.0.0.15 [SOX_events]	Local	arcsight:10:30	Failed password	Unix	Unix	/Authentication/Verify	/Operating System
20	2014/12/14 20:28:39 PST	10.0.0.11 [demo_events]	Local	Failed Login Attempt	Failed Login Attempt	Nortel	VPN	/Authentication/Verify	/VPN

If you click "UNIX" under deviceProduct column, the search is modified. Note that we are now adding a Structured Search Element to the free form text search. The normalized column name now appears in the search. If instead you choose ALT-Click you can automatically insert a NOT condition into the search string.

ArcSight Logger	Summary	Analyze 🗸	Dashboards	Reports
🗃 🗎 🔍 🗸 Cat	egories		Last 10 minutes	\$
/Authentication/Verify AN	D /Failure AND	deviceProduct CC)NTAINS "Unix"	

This narrows the previous search further to only those events that contain Unix as the deviceProduct. Let's change our focus back to Microsoft Events, by replacing "Unix" with "Microsoft" in the Search Area.



Your entry should look like this:

/Authentication/Verify and /Failure AND deviceProduct CONTAINS "Microsoft"

🅼 ArcSi	ight Logger Summar	y Analyze 🗸 Dashb	oards Repo	orts Configura	ition 🗸 System /	idmin (Take me to	(Alt+o)	EPS In:		20:42 admin -
🖮 🖿 🔫	O 🗸 Categories	\$ Last 10	0 minutes (\$)							
/Authentia	cation/Verify AND /Failure A	ND deviceProduct CONTAINS	"Microsoft"				×	Gol Advanced		
35 events	Gcanned: 59,134 events,	00:01.459)								1 bar = 5 second
6										
20:32:21	20:33:01	20:33:41	20:34	21	20:35:01	20:35:41	20:35:21	20:37:01	20:37:41	20:38:21
8	Time (Event Time)	Device	Logger d	leviceEventClassId	name	deviceVendor	deviceProduct	categoryBehavior	categoryDeviceGroup	categoryObject
. 1	2014/12/14 20:38:42 PST	10.0.0.12 [demo_events]	Local S	ecurity:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
_ 2	2014/12/14 20:38:42 PST	10.0.0.11 [demo_events]	Local 5	ecurity:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
3	2014/12/14 20:38:42 PST	10.0.0.12 [demo_events]	Local S	ecurity:529	Logon Failure	Microsoft	Microsoft Windows	/Authentication/Verify	/Operating System	/Host/Operating System
	2014/12/14 20-20-42 DET	10.0.0.11 [damo_avents]	Local c	anulture 20	Longo Fallura	Missocoft	The days	Mush antication Reads	(Oncerting Sustam	Next Operating Surtage

At this point I want to save this query for future use. Press the 🛅 to save the search.



Give it the name "Microsoft Authentication Failures"

My suggestion is to personalize your Saved Queries by adding your initials to the description.

Click the "Saved Search" radio button to the right of "Save as"

Click Save

Field Summary

You have noticed the field summary in the past, but let us explore what it does.

You can rapidly find additional information about the events returned without having to manually count the items you are interested in.

Expand the Field Summary window by clicking on the arrow Por the Field Summary Window

Click on deviceEventClassId in the Field Summary



7 44		Time (Event Time)	Device		Logger	deviceEven
Selected Fields (9)	⊞ 1	2014/12/14 20:38:42 PST	10.0.0.12 [demo_e	vents]	Local	Security:529
categoryBehavior 1	⊒ 2	2014/12/14 20:38:42 PST	10.0.0.11 [demo_e	vents]	Local	Security:52
categoryDeviceGroup 2 categoryObject 2	B 3	2014/12/14 20:38:42 P5T	10.0.0.12 [demo_e	vents]	Local	Security:525
categoryOutcome 1	⊞ 4	2014/12/14 20:38:42 PST	10.0.0.11 [demo_e	vents]	Local	Security:529
categorySignificance 2	a 5	2014/12/14 20:38:42 PST	10.0.0.12 [demo_e	vents]	Local	Security:681
deviceEventClassId 4	devices	EventClassId (4)				×
deviceProduct 1 deviceVendor 1 name 3	Display Chart of	events containing deviceEventCla	assid			
	Field va	-520	24	70	-	
	Security	:681	7	20%		
	Security	:533	3	8.571%		
	IA5:2		1	2.857%		

Notice that we have 4 different values that appear in our return set. These statistics help me focus on the information I am interested in.

Say I am only interested in Security:533, just click on that value. As you would expect the query was automatically changed to: (/Authentication/Verify and /Failure AND deviceProduct CONTAINS "Microsoft") and deviceEventClassId = "Security:533"

Delete the addition "and deviceEventClassId = "Security:533" to get to our original query and click on deviceEventClassId again. This time choose "**Values by time**"

deviceEventClassId 3	deviceEventClassId (3)			×
deviceProduct 1	Display events containing deviceEventClassid			
deviceVendor 1	Chart on: Values by time Top values			
name 3	Field Value	Count	%	
	Security:529	14	70%	
	Security:681	5	25%	
	IAS:2	1	5%	
	32.04	'	376	

A succedur rabbu	Summary Analyze -	Dashboards R	parts Configurad	on 👻 System Admin	(bianess, 00+)	\Box	EPS in	ICB IPS Out: D	092 26%	20:53 admin 🖵
= m 4 0~ 1	Camportes E	Gen 10 emilian								
(Authentication/Verify	AND JTallure AND deviceProduct CD	NTANS "Meresoft")	where deviceEventOr	essid is not null. I chart cour	nt by deviceEventClassid	span-1er 🗸 🚧 🖦				
Plevents Scinnet 5	4.071 events, 00:02:071 1 🛔									
										Chart Setting
				Search Resi	eits					
1	4 4	/	li	11		11 11	t	al.	4	
		20012								
initationald	space, an end Tame									
initationtCasts ecuity:529 ecuity:641	1014/1214 20400 PS1	,0000 1								
initativentOxaald esarily:129 esarily:181	1244/1274 20400915 2014/1274 20400915 2014/1274 20400955 2014/1274 20400955	,00011 4 3								
lookad vertiCavaid scurity-129 scurity-181 5,2 varity-181	1944, HVMITTING 2014/12/14 2044 00 PS1 2014/12/14 2044 00 PS1 2014/12/14 2045 00 PS1 2014/12/14 2045 00 PS1	,0000 4 1 1								
lockal-wetCounted accurity 129 occurity 181 52 accurity 181 accurity 129	1994, Intel®Time 2014/12/14 (2014) 00 PS1 2014/12/14 (2014) 00 PS1 2014/12/14 (2015) 00 PS1 2014/12/14 (2015) 00 PS1 2014/12/14 (2015) 00 PS1	,00001 4 3 1								
teritari wertCaustal ecurity 529 ecurity 681 652 ecurity 1881 ecurity 128 652	9946, jonal Time 2014/12/14 2044:00/951 2014/12/14 2044:00/951 2014/12/14 2044:00/951 2014/12/14 2044:00/951 2014/12/14 2044:00/951	,00001 4 3 1								
initalisetCounted contysEt 52 62 63 64 64 64 65 64 65 65 65 65 65 65	984, avertifiere 2014/12/14 2044:00-921 2014/12/14 2044:00-921 2014/12/14 2044:00-921 2014/12/14 2045:00-921 2014/12/14 2045:00-921 2014/12/14 2045:00-921	, 2000 4 3 1								
teristreetOeald sorty 53 sorty 81 52 aarty 91 aarty 12 62 aarty 91 53	1994, prest Tans 2514 (47) 274 4 2040 00 PST 2514 (47) 4 2040 00 PST 2514 (47) 274 4 2040 00 PST 2514 (47) 254 4 2040 00 PST	, 2000) 4 3 1								
linital wetOward locating 129 locating 181 locating 181 locating 181 locating 181 locating 181 locating 189 locating 189	1996, Joseff Time (1994) 1214 (2014) 00 (401) 2014 (121) 4 (2014) 00 (401)	,0000 4 1 1								
Inclust contOrmald Inclustry S29 Incompositi 652 Incompositi 852 Incompositi 852 Incompositi Incomposi	1000, 2000/1001 2014/12/14 (2040)09/11 2014/12/14 (2040)09/11									
lakali wellowald iscarby 529 sourby 681 52 53 54 54 54 55 55 55 55 55 55 55 55 55 55	1844, Joseff Tilles 1844, 1974 (2044) 00 (91) 2844, 1974 (2044) 00 (93) 2844, 1974 (2044) 00 (95) 2844, 1974 (2045) 00 (95)	١								

As you can see the system quickly created a chart by time for further interpretation.

However for better interpretation, click on "Chart Settings" and Choose "Line"





Now let's restore our save search by clicking on the icon. Choose the "Saved Search Tab"

Filter	Saved Search								
Name 🔺	or opening.	Туре		Start Date	Start Time	End Date	End Time	Local	
BJW-Micr Authentic	osoft ation Failures	Unified Quer	У	SNow - 10m		\$Now			
3JW-Micr	osoft ation Failures	🛐 Unified Quer	У	SNow - 10m		\$Now			
Configura Configura Ichart)	ition - ition Changes	Unified Quer	y	\$Now - 10m		SNow			
onfiguration - onfiguration Changes chart) [Import]		🛐 Unified Quer	У	SNow - 10m		\$Now			
Configura Product	ition Changes by	🛐 Unified Quer	v	\$Now-1h		\$Now		-	
Demo Ne	tFlow by port	Unified Quer	'Y	\$Now - 10m		SNow			
lame: B ype: U lescript	UW-Microsoft Au nified Query ion: /Authentica	thentication Fail tion/Verify AND	lures /Failure Al	ID deviceProc	luct CONTAIN	IS "Microsoft	Load + 0	Close C	lose

Click on "Load + Close", then click on "Go" to execute the query



Fields

Change the field display and set it back to "All Fields"

🅢 ArcSight Logg	NetFlow_Demo Security Webserver	boards
= H 4 0	System Fieldsets All Fields	All Fields
(/Authentication/Vei	Base Event Fields Categories	S "Microsoft
21 events (Scannec	EndPoint Protection Firewall HIDS Minimal Fields NetFlow	

Now scroll to the right to see the **destinationUserName** field.

Ensure the Start Time is set to "\$Now - 1h"

🍈 ArcSight Logger	Summary A	nalyze 🗸 🛛 Dashboard	s Reports Confi	guration System Admi	n (Take me to (Alt+o)		EPS In: 107 EPS Out:	CPU: 13%	2 1: 17 admin 🗸
₩ H 🧶 O 🗸 /	All Fields	\$ Custom time	range 0 Start \$Now-	1h 🕑 Dynamic	End SNow	🛃 Dynamic			
/Authentication/Verify	AND /Failure AND devi	iceProduct CONTAINS "Micr	osoft*			🗸 Go!	Advanced		
148 events (Scanned:	382,491 events, 00:0)2.37B) 🗘						1 bar	= 1 minute
20									
5									
20:20:39	20:2	28:39	20:36:39	20	44:39	20:52:39	21:00:39		
>> stegoryObject	categoryOutcome	categorySignificance	destinationAddress	destinationHostName	destinationNtDomain	destinationUserNam	e destinationZoneURI	deviceAddress	deviceCustom
lost/Operating System	/Failure	/informational/Warning	172.16.1.10	hrweb01.hr.east.arcnet.com		mario	/All Zones/ArcNet Zones/hr.east.arcnet.com - internal		3
lost/Operating System	/Failure	/informational/Warning	172.16.1.10	hrweb01.hr.east.arcnet.com		mario	/All Zones/ArcNet Zones/hr.east.arcnet.com - internal		
lost/Operating System	/Failure	/Informational/Warning	10.1.6.4			jimmyj	/All Zones/System Zones/Private Address Space	10.1.6.4	
lost/Operating System	/Failure	/Informational/Warning	10.1.0.3			jimmyj	/All Zones/System Zones/Private	10.1.0.3	

Now let's click on a user, in my case "jimmyj"

🇑 ArcSight Logger	Summary	Analyze 💙	Dashboards	Reports	Configuration 💙	System Admin	(Take me to (Alt+o)		EPS In:
	ields		Custom time range	🗘 Start	\$Now - 1h	🖓 Dynamic End	\$Now	🕑 Dynamic	
/Authentication/Verify ANI) /Failure AND	deviceProduct CO	NTAINS "Microsoft"	" AND dest	inationUserName CONT	AINS "jimmyj"		🐱 Go!	Advanced

Now I want to see all activity related to this user ID by deleting all criteria prior to destinationUserName. Your search should be *destinationUserName CONTAINS "jimmyj"*

🍈 ArcSight Logger	Summary	Analyze 🗸	Dashboards	Reports	Configuration 🗸	System Admin	(Take me to (Alt+o)	\supset	E
🗃 🖽 🍕 🔿 🗸 All	Fields	(a)	Custom time range	t 🗧 Start	\$Now - 1h	Oynamic End	\$Now	🕑 Dynamic	
destinationUserName CO	NTAINS "jimmyj	•						❤ Go!	Advanced

Minimize the "Radar" by clicking on the up-arrow in the following

1 bar = 1 minute 🔺 📖

Minimize the "Field Summary" by clicking on

🅼 Arc	Sight L	ogger Summary	Analyze V Dashboards	Reports (Configuration 🗸	System Admin Tak	e me to (Alt+o)	\supset	EPS In: 108	EPS Out: 0	CPU:	B% 2 ::23 → admin →
• B	. 0	 All Fields 	\$ Custom time rang	e \$ Start \$M	iow - 1h	Oynamic End \$No	w	Oynamic 201				
/Authen	tication/	Verify AND /Failure AND	deviceProduct CONTAINS "Microsoft	" AND destinat	ionUserName CONTA	INS "jimmyj"		🗸 Go! Adv	ranced			
15 even	ts (Scan	nned: 376,049 events, 0	0:01.189) 暮									-1
30	Time	e (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassid	name	agentAddress		agentHostName
⊟ 2	2014	V12/14 21:18:53 PST	10.0.0.11 [demo_events]	Local	Microsoft	Mindows		Security:533	Logon Failure	172.16.100.1		:gro2E65-f12287
н 3	2014	1/12/14 21:18:52 PST	10.0.0.12 [demo_events]	Local	Microsoft	Microsoff Windows		Security:533	Logon Failure	172.16.100.1		tgro2E65-f12287
9-4	2014	N/12/14 21:05:26 PST	10.0.0.11 [demo_events]	Local	Microsoft	Mindows		Security:533	Logon Failure	172.16.100.1		rgro2E65-f12287
9 S	2014	I/12/14 21:05:26 PST	10.0.0.11 [demo_events]	Local	Microsoft	Microsoft Windows		Security:533	Logon Failure	172,16.100.1		tgro2E65-f12287
a 6	2014	1/12/14 21:05:24 PST	10.0.0.12 [demo_events]	Local	Microsoft	Microsoft Windows		Security:533	Logon Failure	172.16.100.1		:gro2E65-f12287
3 7	2014	1/12/14 20:51:58 PST	10.0.0.11 [demo_events]	Local	Microsoft	Microsoli Windows		Security:533	Logon Failure	172.16.100.1		(gro2E65-f12287

Notice that "**jimmyj**" only appears in Microsoft events at this point so let's change the investigation to view activity based on an IP address instead. Click on an IP in the **deviceAddress** field.

🅼 Arc	Sight Logger Summary	Analyze V Dashboards R	eports Configuration 🗸	System Admin (Take me to, (Alt+o)	\Box		3 Out: 0 CPU: 25% 2 1:22 admin ~
= m -	🗧 O 🗸 🛛 All Fields	Custom time range	Start SNow - 1h	Opnamic End SNow	🕑 Dynamic		
/Authen	tication/Verify AND /Failure AND	deviceProduct CONTAINS "Microsoft" A	ND destinationUserName CONT	'AINS "Jimmyj"	Go! Advance	d	
15 even	ts (Scanned: 376,049 events, 01	0:01.189) 🐥					*1
39	categoryOutcome	categorySignificance	destinationAddress	destinationUserName	destinationZoneURI Address Space	deviceAddress	deviceEventCategory
n	(Failure)	/informational/Warning	10.1.0.3	jimmyj	/All Zones/System Zones/Private Address Space	10.1.0.3	Security Audit
n	(JELETE	/informational/Warning	10.1.1.5	jimmyj	/All Zones/System Zones/Private Address Space	10.1.1.5	Security Audit
n		/informational/Warning	10.1.6.4	jimmyj	/All Zones/System Zones/Private Address Space	10.1.6.4	Security Audit
n	Weiling	/informational/Warning	10.1.0.3	jimmyj	/All Zones/System Zones/Private Address Space	10.1.0.3	Security Audit
n	Fallero	/informational/Warning	10.1.1.5	jimmyj	/All Zones/System Zones/Private Address Space	10.1.1.5	Security Audit
	VEDUCTO	/informational/Warning	10.1.6.4	jimmyj	/All Zones/System Zones/Private	10.1.6.4	Security Audit

Then remove the search for jimmyj so it looks like this.

destinationAddress CONTAINS "10.1.1.5"

Now you can see activity from all of the feeds where the **deviceAddress** contains **10.1.1.5** for example Tripwire, Microsoft, Oracle and others. (depends of course on your event feeds)



🅼 Arcs	i <mark>ight Logg</mark> er	Summary Analyze 🗸 Da	shboards Report	s Configuration	 System Admin 	(Take me to (Alt+o))	EPS In: 109	EPS Out: CPU: 19	admin 🗸
🖮 🗎 🦊	🗧 O 🖌 All Fie	lds 🕴 🕴 Cu	stom time range 🕴 🗧 St	art SNow - 1h	Oynamic End	\$Now	🗹 Dynamic			
destinati	onAddress CONTAIN	S "10.1.1.5"					🐱 Go! Ar	Ivanced		
92 event	s (Scanned: 377,07 agentHostName	0 events, 00:01.079)	baseEventCount	categoryBehavlor	categoryDeviceGroup	categoryObject	category0	categorySignificance	destinationAddress	~ 11 destinationDnsDo
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Modify/Content	/Operating System	/Host/Resource/File	/Success	/Informational	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/Informational/Warning	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/Informational/Warning	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	ан 1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/informational/Warning	10.1.1.5	
100.1	cgro2E65-f12287	/All Zones/System Zones/Private Address Space	1	/Delete	/IDS/Host/File Integrity	/Host/Resource/File	/Success	/informational/Warning	10.1.1.5	

8.3. Viewing a Live Feed

Many individuals prefer to see events that are a constant scroll by like a "tail -f" command in UNIX. We have this capability thru the Live Event Viewer

Choose Analyze > Live Event Viewer

<i>þ</i> ArcSight Logger	Summary	Analyze 🗸	Dashboards
Security	~	Search	
All Failed Logins by User		Alerts Live Event Vie	ewer

Enter "Security:529" in the top "Search For" box

ii 192.168.2.235			
Search Composer Search Results	Help	iii 192.168.2.235	
What do you want to find? Build a new filter or load an existing filter		Search Composer Search Results	@ Help
FIJER 🎬 🛗 + - 🛤		► II ■ ♥ J	
Exclude/Include Terms Search Terms		Searching Sevents (3,654 scanned) Display Buffer 1000	14:39 O
Seech For: Seech For:		3: 2014/215154:631957100.0.11 (Berro, overts) 4: 2014/215154:631957100.0.11 (Berro, overts) 4: 28-bec: 1519:16:30192; 28:16:8019; 28:16:80	OMPOresoft Worksoft //Follure //Follure //Follure ter 11 1556 199638 ast across ter 11 confile //All Consection confile //All Consection and or backsoft confile Consection Zones/Private DMICross/TIMICrosoft //Follure //Follure ter 11 1556 1996082 ast across/Timicrosoft //Follure
Choose If a logical NOT should be applied to the search term and enter the text to search for		csSLabel=Authentication Package Name csSLabel=EventSource cn1Label=LogonType cs4Label=Reacce csSLabel=Object Name cs1Label=Accesses abost=oldsmobile agt=192.168.40.140 agentZoneURI=/All 2 Address Space av=2.9.3.0.0 atz=AmericaLos_Angeles aid=Lty2tcg8BABCAAY	n cs2Label=EventlogCategory Zones/System Zones/Private
Where do you want to look? Choose from device groups and storage groups.		5 - 2014/12/15 19-16-21 DST 10:0.0.11 [damo quents] <128x0ar 15 19:16-20 192 168 10 192 (55:0	NMicrosoft Microsoft
Device Groups 🥒	Windows[2]conity252[Loon Failure[Very-High eventid=9 external3e=windk21 category5gnilicance categoryBehavior "Authentication/Verify categoryDev/ceGroup"/Operating System categoryOutcome	I=/Normal -/Failure	
Storage Groups 🖋		categoryObject=/host/Operating System art=1165861898182 cateSecurity deviceSeverity-Addt_fall shost=desktop27.ny2.east_arcnet.com src=10.0.113.27 sourceZoneURI=/All Zones/ArcNet Zones/ny2.e suser=administrator sproc=NtLm5sp dhost=hnweb01.hr.east_arcnet.com dst=172.16.1.10 destination2	ure rt=1165861898182 east.arcnet.com - internal ZoneURI=/All Zones/ArcNet
Start		Zones/Inr.east.arcnet.com - internal duser-mijolinison cs2-Logon/Logoff cs3-Security cs4-Ukrknown us s5Labi-Anthentication Package Name cs3Labi-Raboti-EventSource nrl Labi-Lingon/Type cr4Labi-Raboto cs8Labi-Anthentication Package Name cs3Labi-Raboti-CentSource nrl Labi-Lingon/Type cr4Labi-Raboti-Raboti- Address Space avel 29:10. Data-rehenerical Disk Analesia AntheniorBBBB.	ser name or bad password cn1=3 n cs2Label=EventlogCategory Zones/System Zones/Private



8.4. Dashboards

8.4.1. Data Monitor: MS - Last Logon Failures

Now I want to create a Data Monitor that will show me the last 10 windows logon failures.

categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure" AND NOT (destinationUserName IS NULL) | top destinationUserName

Or we can also limit our analysis to Microsoft only failures by adding before the | top destinationUserName

"AND deviceProduct CONTAINS "Microsoft"

Example:

categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure" AND NOT (destinationUserName IS NULL) AND deviceProduct CONTAINS "Microsoft" | top destinationUserName

By viewing the Field Summary we can quickly see the percentages of each deviceEventClassId that is in the return data set.

(NOTE- when displaying the chart "| top destinationUserName" I do not get the Field Summary option

You can choose to chart the "Values by Time" or "Top Values" by clicking on the appropriate label.

Enter the search in the search box:

/Authentication/Verify AND /Failure AND deviceProduct CONTAINS Microsoft

?«	Time (Event Time)	Device	Logger					
Selected Fields (4)	1 2014/12/15 19:16:30 PST	10.0.0.12 [demo_events]	Local					
deviceEventClassId 3	deviceEventClassId (3)		×					
deviceProduct 1	Display events containing deviceEventClassId							
deviceVendor 1	Chart on: Values by time Top values							
name 2	Field Value	Count %						
Discovered Fields (0)	Security:529	10 66.666%						
No fields to display	Security:533	3 20%						
	Security:681	2 13.333%						

Click on "Top values"

Notice that a chart is automatically built for you



ArcSight Logger	Summary	Analyze 🗸	Dashbeares	Reports	Configuration	 System Adar 	in Take me to _ (W)	-1 D		EPS In:	105	EPS OUT: D	CPU: 20%	edmin -
	ALTields		Custom time ran	e s Set	12/15/2014	19:16:22 Dyn	mi 54 @ 8/16/292	23:12:55	Dynamic					
Authentication/Verity	NND /Fallure AND d	evicsProduct (2	NTANS Microsof	l whore dev	celiventClassid in	not null top device	EventClassid	l	64	Marcal				
levents (Scorood 24	680 events, 60:03	6001 🔶												
														Chart Settl
0						Search Re	sults							
•					-									
1				_					_					
								10						
	1	a.				devicetive	ntClassEd				1	¢		
out ventClassid	Jawa													
rity.529	18													
mys11														
102201	2													

Since this is my area of responsibility I want to place this in a dashboard so that I can quickly see the current results without having to execute a search this time.

Now I want to save this chart so I can use it in a dashboard. Click on

Notice that there is a new choice presented. Dashboard Panel. Click on Dashboard Panel

		Save Query	🕜 Help
		Panel Title	Microsoft Authentication Failures
		Save as	Filter Saved Search Obstact Search
		Saved Search	New saved search Saved search name
Save Query	🕜 Help	Dashboard	BJW-Microsoft Authentikation Failures Compared and the second and the se
Name Microsoft Authentication Failures Save as Filter Saved Search Dashboard panel Schedule it (You can change the schedule settings later) Type Scheduled Search Scheduled Alert		Panel type Chart type Chart limit	Microsoft Related Events Chart (*) or Ø Add both types Pie (*) 10
Save	Cancel		Save

Notice the choices made:

Select Saved search as "Microsoft Authentication Failures" reusing the query

Select "New dashboard" and enter "Microsoft Related Events"

Checkmark "Add both types"

Change Chart type to "Pie"

Click on Save

The following message will pop up:





Click on Dashboards

Change drop down to "Microsoft Related Events"

Your dashboard is now displayed.

🍈 ArcSight Logger	Summary	Analyze 🗸	Dashboards	Reports	Configuration 🗸	System A	Admin Take me to (Al	t+0)	EPS In: IDE	EPS Out:	CPU:	اھ»	admin
Microsoft Related Events	×	Tools •											
Microsoft Authentication	Failures						Microsoft Authenticatio	n Failures					øx
							deviceEventClassId	_count					
							Security:529	14					
							Security:681	5					
							Security:533	3					
	Security:529						IA5:2	1					
				ounty:533									
			L IAS:2				Displaying 1 - 4 of 4				14-4	Page 1	of 1 p
View on Search Page					Refreshed at 2014/12	/16 13:29:08	View on Search Page			Re	freshed at	2014/12	/16 13:29

Let's add another dashboard by building on what the system already created for us.

Click on "View on Search Page" The system jumps to the Analyze Tab and displays

/Authentication/Verify and /Failure AND deviceProduct CONTAINS Microsoft | where deviceEventClassId is not null | top deviceEventClassId

Change this to:

/Authentication/Verify and /Failure AND deviceProduct CONTAINS Microsoft | top destinationUserName

You have probably already noticed that the system has extensive context sensitive help prompting you and giving you examples every step of the way.

Click on GO







Change to a Pie Chart

	Chart Settings		×		
	Chart Title	Search Results			
Chart Cattings	Chart Type	Column	~	Δρηίν	Close
<u>chart Settings</u>	Display Limit	Column		whhra	CIUSE
	App	Bar			
	App	Pie			
		Area			
		Line			
		Stacked Column			
		Stacked Bar			

Choose SAVE



Save Query 🕜 Help 旜 ArcSight Logger Summary Panel Title Microsoft Failed Logon Attempts (± Security ¥ Save as Saved Search Obshboard panel Intrusion and Configuration Events Saved Search o New saved search Saved search name Login and Connection Activity Microsoft Failed Logon Attempts Monitor 1top_Malicious_IP by Product \$ Mail Dashboard O Mail 4 Microsoft Activity New dashboard Dashboard name **Microsoft Related Events** Microsoft Related Events Microsoft Related Events Panel type Chart 💠 or 🗆 Add both types Microsoft Related Events \$ Chart type Pie **Top Malicious Activity** Chart limit 10 Compliance Network Operations Security Save Cancel TippingPoint

Enter the selections as shown below and click SAVE

Select the "Dashboards" tab and "Microsoft Related Events" from the dropdown box on the right.

🅼 ArcSight Logger Summary Analyze 🛩 Dashboard	ds Reports Configuration 🗸 System	Admin (Take me to (Alt	+0)	EPS In: IOB	EPS Out: 0 CPU: 33%	19:38 admin 🗸
Microsoft Related Events Taols -						
Microsoft Authentication Failures	a x •	Microsoft Authentication	1 Failures			Ø 8 -
		deviceEventClassId	_count			
		Security:529	30			
		Security:681	12			
540 PN 529		Security:533	6			
		IAS:2	2			
	Security: 681					
2 DAS:2		Displaying 1 - 4 of 4			14 4 Page 1	of 1 > 1
	and the second second second second second second	and the second second second				

Change the format of the display

Click on Tools and choose Change Layout

ArcSight Logger Summary	Analyze 🗸 Dashboard	Charge Layout Drag panels to charge the layout	
Microsoft Related Events	Tools -	Hicroval't Authentication Hicroval't Authentication Failans Failans	
Microsoft Authentication Failures	Create Dashboard Delete Dashboard Edit Dashboard Set as Default		
Security:529	Add Panel Change Layout	See	col.

Choose Save



8.5. Reporting

Dashboard Viewer Dashboard Preferences Widget Designer Recent Reports Jobs Execution Status Classic Viewer Classic Designer Classic Preferences

When you choose "Reports from the menu or the "Take me to..." dialogue, you will be brought to the Dashboard Viewer. Dashboards display reporting data to provide a quick view of the latest information about network events. You can assemble various reports and external links onto a dashboard.

However, you must place each report or link into its own widget and then place the widget in the dashboard. A dashboard can contain multiple widgets.

Placing reports on a dashboard gives you access to the most recently published results for those reports. Keep in mind, reports must be run and published in order for the results to be accessible on a dashboard viewer. If you schedule a report to run, publish, and save for a reasonable retention period (for example, one month), then those results will always be available for dashboard views.

For example, you can add one or more reports to a dashboard, and configure reports to autorefresh on a specified interval (for example, every hour). The dashboard will access the latest published reports results, in this case, every hour.

If you have also scheduled the reports to run and publish every hour, your dashboard will show current results. This eliminates the need to manually run and view each report once per hour in order to retrieve the same information updates.

Example:

Dashboard Viewer Dashboard Preferences Widget De	signer Recent Reports Jobs Execution Status Classic Viewer Cl	assic Designer Classic Preferences	
Security Dashboard PCI Dashboard 👻			
top_10_IDS_alerts		(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	
		n 🖬 🖆 🕹 🕹 🕅	** 6 6 6
SANS Top 5 (5) Top	Alerts from IDS		
		09/26/2014 2:55 PM	-
	Top 10 Alerts		
(snort_decoder): Truncated Ipv4 Options	5460		
(spp_frag3) Short fragment, possible DoS att	empt 6220		
BAD-TRAFFIC Unassigned/Reserved IP prot	2680		
BAD-TRAFFIC ip reserved bit set	1470		
File Watch:Accessed	7	29150	
top_bandwidth			
	🗖 🔍 🌒 📾	🥩 🖂 🍖 💠 🗐 1/19	♦● 🗗 😭 🤮
Top Bandwidth Usag	ge by Source		
			09/26/2014 3:33 PM
Start Time:09/26/14 01:33 PM Scan Limit:100000	End Time:09/26/14 03:33 PM		
Con carre 100000			
Total Bytes (GB)			
143.32.193.236			
206.38.47.135			



8.6. Running a default report

Choose **Reports** from the Menu

Then under "Navigation" click on Report Explorer

In the Reports column choose "**Device Monitoring**" then "**Operating System**" Then choose "Login Errors by User" (Left Example below)

ArcSight Logger Sur	mmary Analyze 🗸 Dashboards	Reports Configuration 🗸 System	n Admin (Take me to (Alt+o)
Dashboard Scheduled Reports Navigation Category Explorer Report Explorer Query Explorer Parameter Explorer Favorites Explorer	✓ (Root) Default Reports Demo Reports ✓ Device Monitoring	 Login Errors by User User Administration 	Actions: Quick Run with default options Run in Background Run Report
Design New Report Queries Parameters Parameter Value Groups Template Styles Administration Deploy Report Bundle Report Administration	Anti-Virus CrossDevice Database Firewall Identity Management IDS-IPS Network		List Published Outputs Create Dashboard Widget Customize Report More - Properties: Name: Login Errors by User Type: Adhoc
Report Administration Report Category Filters Report Categories iPackager	Operating System VPN Foundation ISO 27002 IT Gov Demo Reports NetFlow NIST 800-53 Pf1 Demo Reports		Format: HTML Query Object: DM-OS-Login Errors by User Modified On: 09/23/2014 13:44 Category: Operating System Public: True Description: This report shows the details of fail ed logins for each username (time, event name, source, and destinatio

Click on "Quick Run with default options". Choose "Run Now"



ArcSight Logger	Summary	Analyze 👻	Dashboards	Reports	Configuration 🗸	System Admin	(Take me to (Alt+o
Dashboard Scheduled Reports Navigation Category Explorer	Report F Login En This repo	Parameters rors by User : ort shows the deta	ils of failed logins fo	er each usernan	he (time, event name, sour	ce, and destination).	Run Now 👻
Report Explorer							
Query Explorer	Additio	nal Filters					
Parameter Explorer Favorites Explorer	Start	\$Now - 2h		N	lynamic		
Design	End				lynamic		
New Report Queries Parameters Parameter Value Groups	Scan Lin	nit (100000 al Only	Use ctrl-	click to selec	t or deselect items		
Template Styles	Device	Groups		s	torage Groups		
Administration Deploy Report Bundle	flow_da PCI raw_sys SOX	ita slog		\$	Default Storage Group Flow data Internal Event Storage Grou PCI Storage Group	φ	\$
Report Administration	Devices			P	eers (To include peers	, uncheck Local Onl	y)
Report Category Filters Report Categories	10.0.0.1 10.0.0.1 10.0.0.1 10.0.0.1	11 (demo_events) 12 (demo_events) 13 (raw_syslog) 14 (raw_syslog)		\$	There are no Peers to displ	ay	
iPackager	10.0.0	a taw shardt					Des New Job

			l 🚾 🖷 🕼	r <u>(⇔ ⊠ ∢</u>) [🔮 💠 🔶 4/471 🔹 🔶 😩	ľľľ	
ogin Erro	rs by User				12/1	6/2014 12·28 PI	м
End Time	Error	Source Zone	Source Address	Source Host Name	Destination Zone	Destination Address	Destination Host Name
10/04/2009	badlogin	/All Zones/System Zones/RFC1700	127.0.0.1	localhost	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/Public Address Space/198.20.0.0- 222.255.255.255	213.144.137.66	sdsl-137-66. init7.net	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/RFC1700	127.0.0.1	localhost	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/Public Address Space/198.20.0.0- 222.255.255.255	213.144.137.66	sdsl-137-66. init7.net	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/RFC1700	127.0.0.1	localhost	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlogin	/All Zones/System Zones/Public Address Space/198.20.0.0- 222.255.255.255	213.144.137.66	sdsl-137-66. init7.net	/All Zones/System Zones/Private Address Space	10.0.0.27	
10/04/2009	badlocin	/All Zones/System	127.0.0.1	localhost	/All Zones/System Zones/Private	10.0.0.27	

Note that you can save the report in multiple formats such as .csv, .pdf, rtf. You can also email the document or publish it to the portal.



8.7. Creating a report, by customizing default report

Since Logger ships with a variety of useful, pre-built reports for common security scenarios, you can use these not only to run as-is but also as templates for building new reports. If you are just beginning with the Report Designer, a good way to learn fast is to start with an existing report that has some of the features you want in your new report, save the original report under a new name, and then modify it.



Modifications to reports and other ArcSight-defined content may be overwritten without warning when the content is upgraded. Do not modify ArcSight-defined content directly.

Make modifications to a copy of any ArcSight-defined content as a general practice, and subsequent upgrades will not affect the modifications.

First we want to make a new "Category" so that we can have a place to save our reports.

Choose **Reports** from the Menu Then under "**Navigation**" click on "**Category Explorer**" Suggestion is to enter your initials such as "**BW Reports**" Click on "**Save**" (In this case I choose to keep the folder Public)

ADD New Category		
		?
Category Name	BW Reports	
Category ID		System Generated
	Scope: Public Private Hidden	
	Save Cancel	

Now to customize the report

Rather than create a report from scratch, I am going to:

Copy the report Copy the query Change the query Change the report to use the new query Run the newly modified report.

It is always recommended that you create/copy a standard report into the new category group we just created before making changes. This insures no conflict as ArcSight Supplied updates are provided to you.

We are going to use "Login Errors by User" as the basis for our report.

Copy the Report

Choose **Reports** from the Menu



Then under "Navigation" click on "Report Explorer"

In the Reports column Expand **Device Monitoring** by clicking on the *icon* click "**Operating System**"

Select the report with a Left-Click on "Login Errors by User"

When selected it will turn BLUE

Navigation			
Category Explorer			
Report Explorer	a (Root)	 Login Errors by User 	Actions:
Query Explorer	BW Reports	 User Administration 	Quick Run with default options
Parameter Explorer	Default Reports		Run in Background
Favorites Explorer	Demo Reports		Run Report
Design	Device Monitoring		List Published Outputs
New Report	Anti-Virus		Create Dashboard Widget
Queries	GroceDevice		Customize Report
Parameters	CIOSSDEVICE		
Parameter Value Groups	Database		More 🗸

Click on "Customize Report"

Click on "Save As.." button



First Step is to refresh the menu by closing the root folder by clicking on the ⁴ icon in front of the Root Folder. Then click on it again ⁴ to refresh the directory



Click on the Folder so it shows that is selected by changing to BLUE



🖌 🗊 (Root)			
Device Monitoring			
🕨 📻 BW Reports			
🕨 🗊 Default Reports			
🕨 🗊 Demo Reports			
Report Name BW Windows Logon Failure	Save	Cancel	✤ Options

Add your initials in front of the new name you give the report and Click "Save"



Click "Close"

Copy the Query

Click on the data source icon

Ad hoc Report Design	er > BW Windows Logon Failure
8 🛃 🍃	💸 🟂 🛃 🗃 ᡝ 🗞 Expand All
Run	Preview Save Save As Open
Data Source	
Select Source —	
Query Object:	/Operating System/Login Errors by User
	Query Editor

Click on "Query Editor"

Query					
Query	Parameter	Parameter Value	Groups	Graph	
Add Ne	ew Open	Delete Save	Save As	Cancel	Advanced
Name Lo	gin Errors by Us	ser			



Now we are going to rename it and save it

Click on the Triangle in front of the root folder and click again to refresh the menu Click on your folder, in my case "**BW Reports**" to select the folder Set the Query Object to "**BW Windows Logon Failure**" then click "**Save**"

Name	
🔺 📻 (Root)	
▶ 😭 Device Monitoring	
▶ 🛱 BW Reports	
Image: Second	
🕨 💼 Demo Reports	
Equadation	•
ry Object BW Windows Logon Failure Save Cancel	¥ Options
Ouerv Obiect Editor	
Query Object Editor	ailura
Query Object Editor	ailure
Query Object Editor Successfully replaced query object: BW Windows Logon Factor Add New Open Delete Save Save As Cancer	ailure el Advanced
Query Object Editor Successfully replaced query object: BW Windows Logon Face Add New Open Delete Save Save As Cance	ailure el Advanced

Note the name change.

Change the Query

To edit the query we now click on the new "Data Source" icon



The query appears and we are going to change the where clause.

FIRST you must click on the	SQL Design SELECT events.arc_o	"Design	" Icon to expose the editor
FIRST you must click on the		Design	icon to expose the editor

WHERE events.arc_categoryDeviceGroup = '/Operating System' AND events.arc_categoryBehavior = '/Authentication/Verify' AND events.arc_categoryOutcome != '/Success' AND (events.arc_categorySignificance = '/Informational/Error' OR events.arc_categorySignificance = '/Informational/Warning'

To illustrate how we make a change to the SQL we will change the query to only show logon failures and only for device vendor Microsoft.

(In production: we would alter a Parameter to pass the Device Vendor instead of hard coding the device vendor. This was only to expose you to the query editor)

SELECT events.arc_destinationUserName "User Name", events.arc_endTime "End Time", events.arc_name "Error", events.arc_sourceZoneURI "Source Zone", events.arc_sourceAddress "Source Address", events.arc_sourceHostName "Source Host Name", events.arc_destinationZoneURI "Destination Zone", events.arc_destinationAddress "Destination Address", events.arc_destinationHostName "Destination Host Name", events.arc_deviceVendor FROM events

- WHERE events.arc_categoryDeviceGroup = '/Operating System' AND events.arc_categoryBehavior = '/Authentication/Verify' AND events.arc_categoryOutcome != '/Failure' AND events.arc_deviceVendor = 'Microsoft'
- ORDER BY events.arc_destinationUserName, events.arc_endTime

Click "<mark>Ok</mark>"

Click "Save" or you will lose your changes

Change the report to use the query

We now need to pair the query with the report by clicking on the "Data Source" icon

	λ 💥 Σ			9	Expand A
Run	Preview	Save	Save As	Open	
A. 1994 1993					
Data Source	e				
B Data Source	e				_

Change the Query Object by clicking on the "**Root**" folder to close it Then reopen it to see the BW Reports folder and choose the "**BW Windows Logon Failure**"

Ad hoc Report Designer	r > BW Windows Logon Failure
8 🛃 🕞	💸 🔽 🖞 🖫 📾 🏨 😵 🤶 Expand All
Data source miss	sing
Run	Preview Save Save As Open
🔒 Data Source	
Select Source	(Root) Ta-
Report Settings —	Name
Report Title:	/ 😰 (Root)
Template:	BW Reports
Report Format:	🔂 BW Windows Logon Failure
Report Contents:	
:	a

Double Click on "BW Windows Logon Failure" if the query object is not already set.

Click "Save" and "Close"



Ad hoc Report Designer > BW_Login Errors by User	🗃 🛍 😵 오 Expand All
Run Preview Save	Save As Open
Select Display Fields	
Available Fields 🔍 🕔 🕢	Selected Fields
User Name	A
End Time	>
Error	
Source Zone	
Source Address	
Source Host Name	*
Destination Zone	
Destination Address	~
-	Add New Fields At Runtime

Click on to select all the fields

Also move the ArcDevicvendor to the top by selecting it and clicking the up arrow till it is at the top.



Click on "Save"





Click "<mark>Close</mark>" Click "<mark>OK</mark>"

Click **Run** Click "<mark>Run Now</mark>"

BW_Login	BW_Login Errors by User											
Start Time:12/16/14 01 Scan Limit:100000	:02 PM	End	Time:12/16/14 03:02 PM			12/16/2014 3:02 PM						
Device Vendor	Device Vendor User Name End Time		Error	Source Zone	Source Address	Source Host Name						
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com						
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com						
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com						
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com						
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com						
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com						

To run the report:

Choose "Reports Tab" Choose "Report Explorer" Choose "BW Reports" Choose "BW Windows Logon Failure" from Reports Column Choose "Quick Run with default options" Choose "Run Now"

Ad hoc Report Designer > BW Windows Logon Fa	ilure	pand All						
		💿 🗉 획 👜 🖷 🕼 📔 🛃 🁌 🕸 🔷 1/53						
✓ (Root) BW Reports	O BW Windows Logon Failure	Actions: Quick Run with default options						





BW Windo	ws Logon	Failure				
Start Time:12/16/14 06 Scan Limit:100000	:40 PM	End	Time:12/16/14 08:40 PM			12/16/2014 8:40 PM
Device Vendor	User Name	End Time	Епог	Source Zone	Source Address	Source Host Name
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2. east.arcnet.com - internal	10.0.113.27	desktop27.ny2.east.arcnet.com
Microsoft		12/11/2006	Account logon failed.	/All Zones/ArcNet Zones/ny2.	10.0.113.27	desktop27.ny2.east.arcnet.com



9. Pipeline Operators:

Pipeline Operators are critical to refining searches to obtain the information that is sought after. The idea is to add clauses, which are made up of pipeline operators and event attributes, until the search yields the desired results. The order of the pipeline can matter, so think about what it is you want to search for, and how to search for it. Usually, the finished pipeline is a representation of the spoken search process.

Keys – Identifies keys in raw events based on specified delimiters The keys operator can only be used to determine keys; you cannot pipe those keys into other operators.

Extract – Displays key-value pairs from raw events

Fields - Includes or excludes specified fields

Regex - Selects events that match a specified regular expression

Rename – Renames a CEF or REX extracted field

Replace - Replaces a specified string in one or more specified fields with a new specified string

Rex - Extracts values based on a specified regular expression

Transaction – Group events that have same values in specified fields. For example, if host and portNum are specified and two events contain "hostA" and "8080", the events are grouped in a transaction. The transaction IDs created in this search are sorted in ascending order.

Duration - The time in milliseconds of the duration of a transaction, which is the difference between the event time of the last event in the transaction and the first event in the transaction.

Eventcount - Displays the number of events in transactions.

Where – displays events matching criteria specified in "where" expression Allows you to use our Field-based operators on Raw events (User-defined Fields extracted from raw events using Pipeline Operators such as rex or extract)



10. Selected Examples:

"What are the counts of destination ports in my Netflow traffic?" Netflow Chart by count of Events by Destination Port

netflow | cef dpt |chart _count by dpt | sort - _count

Change Chart type to "Line"



"What are the byte counts, in and out, for Netflow traffic, every 30 seconds?" Netflow| cef bytesIn bytesOut|chart avg(bytesIn),avg(bytesOut) span=30s

() ArtSight Lagger	Sannay Analyza 🗸	Resident Reports Cord	lguration 🐱 System A	dele Trice en 140	Hal	ars in	IDS prove D	01 28 at	45
	non a	(Coloring and Street CE 12)	15/2014 10:10:22 0	view ted [] N162123	2121215	own.			
Netflowi of bytesir byter	Outlichart anglbyteeln) suplay	Account space-blog			-	fait Advent			
Sileventa Diannel 162	302 eventa, 02/03/3871 3	0							
			Search	Results				Over13	tties
- reg. befalls	- ang interDut								
100,000 100,000 100,000 100 100 100 100	11	1 1	1	J.J.	11	11	11	11	
-	and hereits	an banks							
Charlot in the second	544 15254 19521	NAME OF TAXABLE PARTY							
1010010101010100	21210228.10383	21170776-02181							
199301015 1811100-957	10015195,04002	CONTROL MADE							
144/12/18 10:17:30-767	EM35714281714	835,33714385714							
111/12/15 15:16:00 /97	\$12,75714285794	812701420218							
14/12/15 10:16:00/57	AMA.INCIDATIVIZM	846.354248951230							
10101015-061800-007	1030-4714201714	1128-471-6281714							
HUTUPA REPAIRING	41279802103481	41279802951601							
194,1215 193846 957	James anapproved	2579.1019047019							
144/12/15 1928/30/97	821.54093236095	WIT SIRVEZIMENT							
	1040.0071420571	1040 9671-628571							
014112112 102100-001									



Top Talker:

"What Source Addresses are responsible for the Firewall traffic, and by how much?"

categoryDeviceGroup = "/Firewall" AND categoryBehavior = "/Access" and bytesIn IS NOT NULL | EVAL total_bytes=bytesIn + bytesOut | chart sum(total_bytes) as bytes by sourceAddress | sort - bytes





Here is a search string that will search Blue Coat events, and through using the pipe operator and rex command, will pull out the information after the "q=" in the Google search.

deviceVendor="Blue Coat" | rex "<u>http://www.google.com/search\?q\\=(?</u><term>[^\\&]+)" | top term

If you copy and paste the above expression in to logger, ensure that the double-quotes don't end up as slanty double-quotes in the logger search. This will cause an error in the search. Windows has a way of doing this at times.

Quick Overview of Device Vendors:

| top deviceVendor

Quick Overview of Device Products:



| top deviceProduct

What versions of Connectors are reporting into Logger?

agent:012 | top deviceVersion

How many TippingPoint events per hour?

deviceVendor=TippingPoint | chart sum(baseEventCount) span=1h

What's coming into Logger?

| top name

Failed Logins by User

categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure" AND NOT (destinationUserName IS NULL) | top destinationUserName

Top NetFlow destination ports

destinationPort > 0 AND deviceProduct = "Cisco NetFlow" | top destinationPort

What products have had changes to them recently?

categoryBehavior startswith "/Modify/Configuration" | top deviceProduct



Example of Regex:

| regex="CEF:0.*?Zara" 14,481 returned



Limit to Unix and username Zara

deviceProduct="Unix" | regex="CEF:0.*?Zara"

🍈 ArcSight Logger	Summary	Analyze 🗸 Dashbo	ards Reports Confi	guration 🗸	System Adr	min (Take me	to (Alt+o)		EPS In: 105 EF		30% 20:00
	ields	t) Custom	imerange 🔹 Start 🔛 12/	15/2014	19:16:22 Oyr	namic End 🔛 8/	16/2922 23:1	2:55 Dynamic			
deviceProduct= Unix Tregi	exª CEPU."	Zara						✓ Gol Advar	nced		
59 events (Scanned: 296,6	849 events,	00:03.007) 🐺									1 bar = 1 minute
2 0 19:18:29		19:26:29		19:34:29			19:42:29		19:50:29		
2.4		Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassid	name	agentAddress	agentHostName
Selected Fields (4) deviceEventClassid 4	H 1	2014/12/15 19:18:29 PST	10.0.0.15 [SOX_events]	Local	Unix	855		arcsight:10:30	Feiled pessword	172.16.20.45	cgrochowskiT61P
deviceProduct 1 deviceVendor 1 name 4	E E	2014/12/15 19:19:07 PST	10.0.0.15 (SOK_events)	Local	Unix	202		arcsight:10:30	Feiled password	172.16.20.45	cgrochowskiT61P
Discovered Fields (0) No fields to display	⊒ 3	2014/12/15 19:19:08 PST	10.0.0.16 [SOX_events]	Local	Unix	200		arcsight:10:23	Accepted password	172.16.20.45	cgrochowskiT61P



Top 20 Products by event count:

deviceProduct != "ArcSight" AND deviceProduct IS NOT NULL | top 20 deviceProduct (does not account for aggregation, see next query)

🍈 ArcSight Logger	Summary Analyze	Dashboards	Reports Configura	tion 🗸 System A	dmin Take me to	(Alt+o)	EPS I	105 EPS Out: 0	CPU: 28%	20:0 I admin 🗸
∎ th 🗧 o 🗸 i k	il Fields	a) Custom time rang	e'‡: Start ∰ 12/15/2	014 19:16:22 0	mamic End 😭 8/16/2	23:12:55	Oynamic			
deviceProduct != "ArcSig	ht" AND deviceProduct IS N	01 NULL top 20 device	Product				Gol Advanced			
20 events (Scanned: 28	3,948 events, 00:19.115)	+								
										hart Settin
25,000				Search	Results					
20,000										
15,000										
10,000										
5.000										
and the second second	Sta	11	1	Cash.	Sector	11	21	art	Sar.	
4				dev	iceProduct					
viceProduct	_count									
byApplicationArchive	21453									
0K	20064									
co NetFlaw	18402									
ruShield	14194									
cle	13274									
ntrol Manager	13183									
crosoft Windows	13139									
ford Friday Distant	70617									
DUR System Protection										
L Server	9667									
icital System Protection (CServer ort	9667 9394									
kolai sysiem Protection (C.Server Iort ItyOne	9667 9394 8713									

Top 20 products by event count, aggregation used:

deviceProduct != "ArcSight" AND deviceProduct IS NOT NULL | chart sum(baseEventCount) as Event_Count by deviceProduct | sort - Event_Count





How many events by each source from highest to lowest:

deviceProduct != "ArcSight" AND deviceProduct IS NOT NULL | chart sum(baseEventCount) as Event_Count by deviceProduct | sort - Event_Count



Blue Coat Bytes In and Bytes Out

deviceVendor="Blue Coat" and destinationHostName is not null AND NOT destinationHostName CONTAINS "windowsupdate" |chart sum(bytesIn) as TTLBytesIn, sum(bytesOut) by sourceAddress | sort – TTLBytesIn

deviceVendor="Blue Coat" and destinationHostName is not null AND NOT destinationHostName CONTAINS "windowsupdate" |chart sum(bytesIn) as TTLBytesIn, sum(bytesOut) by sourceAddress | sort - TTLBytesIn



Transaction

categoryBehavior = "/Authentication/Verify" AND categoryOutcome CONTAINS "/Success" AND destinationUserName IS NOT NULL| transaction deviceProduct, destinationUserName maxspan= 2h

🍈 ArcSight Logger	Summary	Analyze 🗸 Dashbo	ards Reports Confi	guration 🗸	System Admin	(Take me to (Alt+			EPS In: 🔲	EPS Out:	CPU: 20%	20:04 admin 🗸
CategoryBehavior = "/Auth destinationUserName max	Fields entication/Ve sspan= 2h	trify" AND categoryOutcome	time range 🔹 Start 🔛 12/ CONTAINS "/Success" AND d	15/2014 estinationU	19:16:22 Dynamic I serName IS NOT NULLI tr	Ind 腔 8/16/2922	23:12:55 duct,	Oynamic Gol Adv	anced			
4,345 events (Scanned: 3	10,409 event	s, 00:01.530)	Baulca	laner	dectinationIlcortiame	deviceProduct	duration	mastraast	transactionid	devicationder	douiraUersian	Asuicatus
Selected Fields (0) No fields to display	⊞ 1	2014/12/15 19:17:28 PST	10.0.0.16 [50X_events]	Local	Zaun	Unix	2433000	6	1	Unix		arcsight:1
No fields to display	⊕ z	2014/12/15 19:22:46 PST	10.0.0.16 [SOX_events]	Local	Zaun	Unix	2433000	6	1	Unix		arcsight:1
	⊞ 3	2014/12/15 19:36:46 PST	10.0.0.16 [SOX_events]	Local	Zaun	Unix	2433000	6	1	Unix		arcsight:1
	a 4	2014/12/15 19:42:07 PST	10.0.0.15 [50X_events]	Local	Zaun	Unix	2433000	6	1	Unix		arcsight:1
	∋ 5	2014/12/15 19:51:44 PST	10.0.0.15 [SOX_events]	Local	Zaun	Unix	2433000	6	1	Unix		arcsight:1

Transaction and De Duplication

categoryBehavior = "/Authentication/Verify" AND categoryOutcome CONTAINS "/Success" AND destinationUserName IS NOT NULL| transaction deviceProduct, destinationUserName maxspan= 2h | dedup deviceProduct, destinationUserName | sort deviceProduct destinationUserName

🍈 ArcSight Logger	Summary	Analyze 🗸 Dashbo	ards Reports Config	guration 🗸	System Admin	(Take me to (Alt+o)			EPS In: 106	EPS Out:	сри: 23%	20:05 admin 💙
🖴 🖹 🍕 O 🗸 14	l Fields	0 Custom	time range 🛊 Start 🔛 12/1	5/2014 1	9:16:22 Dynamic E	nd 🔛 8/16/2922	23:12:55	Dynamic				
categoryBehavior = "/Aut destinationUserName ma	thentication/Ve axspan= 2h i de	erify" AND categoryOutcome edup deviceProduct, destinat	CONTAINS "/Success" AND de ionUserName I sort devicePr	stinationUs oduct destin	erName IS NOT NULLI tra ationUserName	Insaction deviceProduc	ct, ~	Go! Adva	nced			
254 events (Scanned: 3	10,409 events,	00:01.725) 🐺										
7 (4)		Time (Event Time)	Device	Logger	destinationUserName	deviceProduct	duration	eventcount	transactionid	deviceVendor	deviceVersion	deviceEven
Selected Fields (0) No fields to display	3 I	2014/12/15 19:21:51 PST	10.0.0.17 [PCI_events]	Local	Yuan Fan	ACESERVER	2107000	4	263	RSA		ACESERVER
No fields to display	2 Z	2014/12/15 19:21:00 PST	10.0.0.11 [demo_events]	Local	daveshimp	BigIron	2503000	14	126	Foundry		TelnetSSHL
	H 3	2014/12/15 19:19:42 PST	10.0.0.12 [demo_events]	Local	John Appleseed	Bax.net	2424000	14	40	Вак		LOGIN
	9 4	2014/12/15 19:21:03 PST	10.0.0.12 (demo_events)	Local	SNMP	Cisco VPN	2423000	55	228	CISCO		AUTH/36
	8	2014/12/15 19:24:11 PST	10.0.0.12 [demo_events]	Local	admin	Cisco VPN	1823000	24	124	CISCO		AUTH/36
	. 6	2014/12/15 19:24:12 PST	10.0.0.12 [demo_events]	Local	pptpuser	Cisco VPN	1821000	12	89	CISCO		AUTH/4
	. 7	2014/12/15 19:17:51 PST	10.0.0.12 [demo_events]	Local	root	Cisco VPN	2448000	8	162	CISCO		AUTH/4



11. Reporting Example

If you have two loggers peered, how can you report on the Average EPS per day per Logger

Here is the query, and with Logger 6.0 we wrote this report. Each Line in the chart is a Logger in the peer group. And those lines in the chart are a little bit interactive, where you can scroll and Logger will change and show the values.

The query SELECT DATE(events.arc_deviceReceiptTime) as "Date", events.arc_deviceAddress as "Logger", AVG(events.arc_deviceCustomNumber1) as "Average EPS" FROM events WHERE events.arc_deviceEventClassId = "eps:100" AND events.arc_deviceAddress IS NOT NULL GROUP BY events.arc_deviceAddress, DATE(events.arc_deviceReceiptTime) ORDER BY

DATE(events.arc_deviceReceiptTime)



