ArcSight Status Monitoring について

2023 年 3 月 16 日

ArcSight Support

Contents

opentext™

１．はじめに

本資料は、ArcSight Status Monitoring について説明したものです。ArcSight Status Monitoring は、ESM のパフォーマンスの問題発生時、解析のため使用することがあります。また、問題が発生していなくとも定期的に確認されると問題発生を事前に回避できる可能性があるかと思います。

なお、このツールはサポートされているものではないためドキュメントなどはありませんが、今後も継続して提供されると聞いています。

（通称 manage.jsp と呼ばれています。）

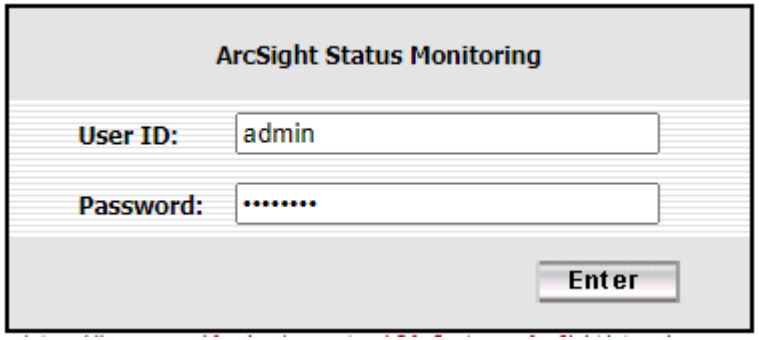
2. ArcSight Status Monitoring　へのアクセス

通常のブラウザから 次の URL にアクセスしてください。

https://<hostname>:8443/arcsight/web/manage.jsp

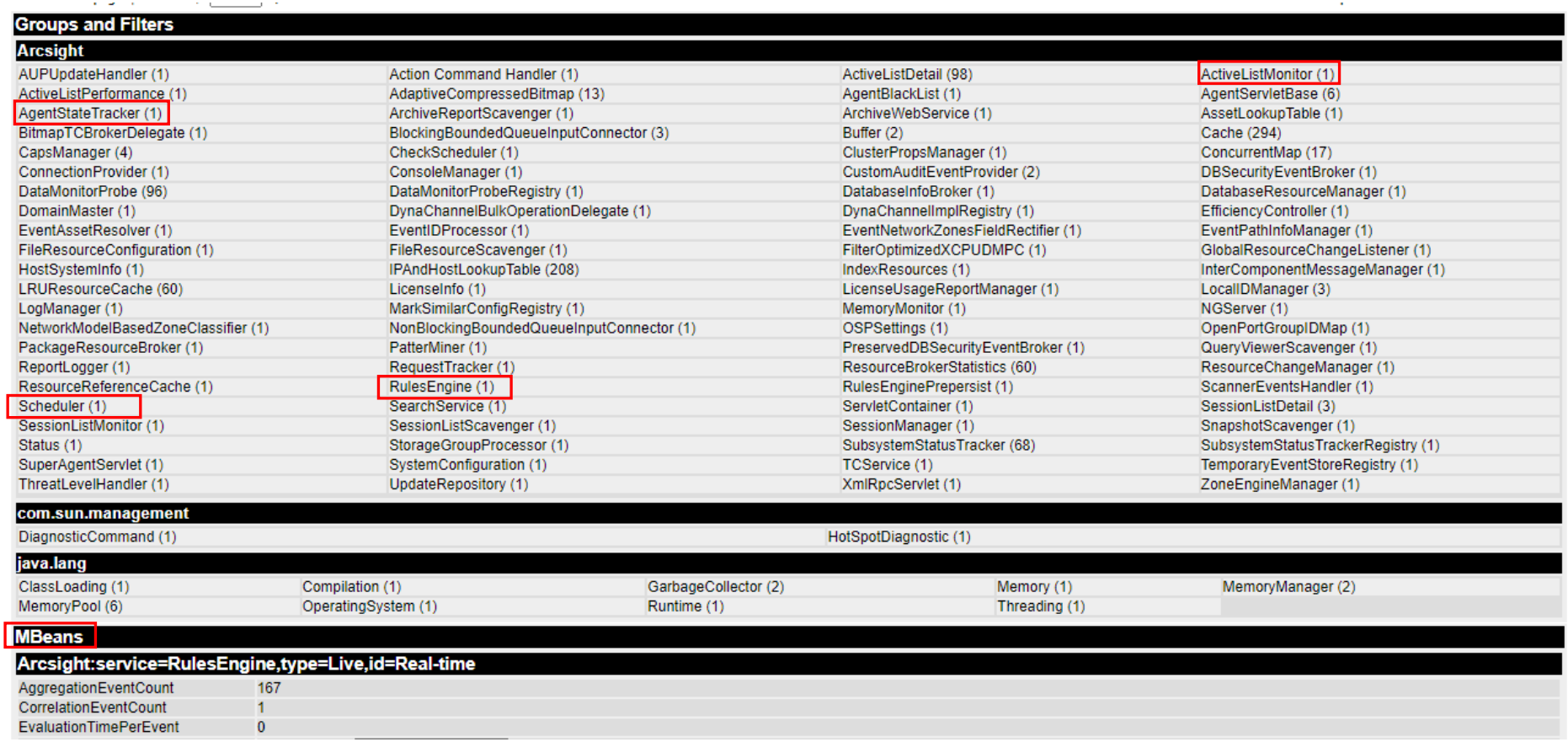
（ここで、<hostname>は ESM Manager Server のホスト名または IP アドレスです。 Certificate error が出るかもしれませんが、問題ありませんのでアクセスしてください。）

表示された画面でログイン（コンソールと同じユーザ ID とパスワード）していただくと 次ページのような画面が開きます。



3. 初期画面

本資料では次に表示されている項目の内、ActiveListMonitor, AgentStateTracker, RuleEngine および Scheduler をご説明します。それぞれの項目をクリックしていただくと、画面下の MBeans 以降にそれぞれの情報が表示されます。



Groups and Filters

Arcsight

AUPUpdateHandler (1)	Action Command Handler (1)	ActiveListDetail (98)	ActiveListMonitor (1)
ActiveListPerformance (1)	AdaptiveCompressedBitmap (13)	AgentBlackList (1)	AgentServletBase (6)
AgentStateTracker (1)	ArchiveReportScavenger (1)	ArchiveWebService (1)	AssetLookupTable (1)
BitmapTCBrokerDelegate (1)	BlockingBoundedQueueInputConnector (3)	Buffer (2)	Cache (294)
CapsManager (4)	CheckScheduler (1)	ClusterPropsManager (1)	ConcurrentMap (17)
ConnectionProvider (1)	ConsoleManager (1)	CustomAuditEventProvider (2)	DBSecurityEventBroker (1)
DataMonitorProbe (96)	DataMonitorProbeRegistry (1)	DatabaseInfoBroker (1)	DatabaseResourceManager (1)
DomainMaster (1)	DynaChannelBulkOperationDelegate (1)	DynaChannelImplRegistry (1)	EfficiencyController (1)
EventAssetResolver (1)	EventIDProcessor (1)	EventNetworkZonesFieldRectifier (1)	EventPathInfoManager (1)
FileResourceConfiguration (1)	FileResourceScavenger (1)	FilterOptimizedXCPUDMPC (1)	GlobalResourceChangeListener (1)
HostSystemInfo (1)	IPAndHostLookupTable (208)	IndexResources (1)	InterComponentMessageManager (1)
LRUResourceCache (60)	LicenseInfo (1)	LicenseUsageReportManager (1)	LocalIDManager (3)
LogManager (1)	MarkSimilarConfigRegistry (1)	MemoryMonitor (1)	NGServer (1)
NetworkModelBasedZoneClassifier (1)	NonBlockingBoundedQueueInputConnector (1)	OSPSettings (1)	OpenPortGroupIDMap (1)
PackageResourceBroker (1)	PatterMiner (1)	PreservedDBSecurityEventBroker (1)	QueryViewerScavenger (1)
ReportLogger (1)	RequestTracker (1)	ResourceBrokerStatistics (60)	ResourceChangeManager (1)
ResourceReferenceCache (1)	RulesEngine (1)	RulesEnginePrepersist (1)	ScannerEventsHandler (1)
Scheduler (1)	SearchService (1)	ServletContainer (1)	SessionListDetail (3)
SessionListMonitor (1)	SessionListScavenger (1)	SessionManager (1)	SnapshotScavenger (1)
Status (1)	StorageGroupProcessor (1)	SubsystemStatusTracker (68)	SubsystemStatusTrackerRegistry (1)
SuperAgentServlet (1)	SystemConfiguration (1)	TCService (1)	TemporaryEventStoreRegistry (1)
ThreatLevelHandler (1)	UpdateRepository (1)	XmlRpcServlet (1)	ZoneEngineManager (1)

com.sun.management

DiagnosticCommand (1)	HotSpotDiagnostic (1)

java.lang

ClassLoading (1)	Compilation (1)	GarbageCollector (2)	Memory (1)	MemoryManager (2)
MemoryPool (6)	OperatingSystem (1)	Runtime (1)	Threading (1)	

MBeans

Arcsight:service=RulesEngine,type=Live,id=Real-time

AggregationEventCount	167
CorrelationEventCount	1
EvaluationTimePerEvent	0

4. ActiveListMonitor

ActiveListMonitor は Active List の状態をモニターするものです。Active List のエントリはメモリに常駐し、ルールなどで参照されたり、エントリが追加/更新/削除されます。特に“Percent Used” が 100 % になると頻繁にエントリの入れ替えが発生し、ESM のパフォーマンスに影響があるため、該当の ActiveList の Capacity を増やす、 TTL を短くする、エントリを追加しているルールを見直していただくなどを推奨しています。

MBeans

Arcsight:service=ActiveListMonitor,type=MysqlActiveListBroker

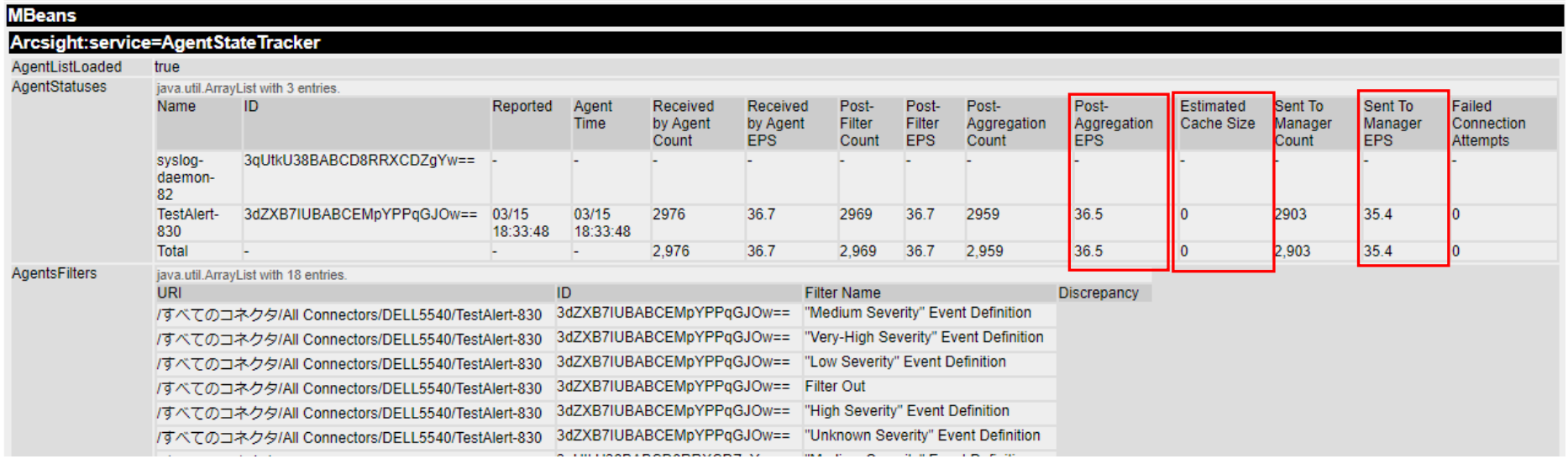
ActiveCacheInformation — java.util.ArrayList with 97 entries.

Name	ID	Capacity	Main Entry Count	Percent Used	Context Count	Query Rate - Last 5 Mins	Query Rate - Last Hour	Query Rate - Total	Change Rate - Last 5 Mins	Change Rate - Last Hour	Change Rate - Total	DB Queue % Used	Context Count	Temp Entry Count	Max Temp ID	Temp Entry Capacity
AL1	H5stHFoYBABCCDue3I0VQlw==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL2	HPTObFoYBABCITZmqSays8g==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL3	HXC4gMYYBABCAoCRHVWbVUg==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL4	H6uo5MYYBABCBExMCWDvbJg==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL5	H0tlQNIYBABCAj7aiarEDHA==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL6	HE+pbNIYBABCAwxp79jpQLw==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL7	H9gWcNIYBABCBpZ79VfEPMA==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
AL8	HqirpNIYBABCCr+PH8-fD1Q==	10000	1	0.01%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
APT TMP Tracking	HeoHePHkBABCk5D31fpKOrg==	1000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
APT Tracking	HYBSQp3gBABDSMwNGTTc-hQ==	1000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Additional Suspicious Addresses	Ha0saTmsBABDgWcA3NbEAJg==	500000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Additional Suspicious Domain	H45UlcWsBABCiJEzYkfbAOw==	500000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Additional Suspicious Email	HIIIpcWsBABCiNI4WGcEqhg==	500000	0	0.00%	1	0.0067/s	0.0006/s	0.0298/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Additional Suspicious Hash	HVuQpcWsBABCiNQQwp8kYww==	500000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Additional Suspicious URL	HVTMqcWsBABCiNvT-MsOvxQ==	500000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
All Monitored Devices	HycbNbEUBABCBKGt8PZShUw==	100000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Application List	H+Ircfm4BABD239ty-mSKog==	1000	18	1.80%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Archive Task Failures	Hiz1vlDABABCCZh-AzO0hdw==	10000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Attacker Based Suppression	Ht7rzJGsBABChgsJrHmTmPQ==	100000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Attacker and Target Based Suppression	H7hmfJGsBABCb1Q8yV0WVaA==	100000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Attacker and Target and Username Based Suppression	HnZ3-JGsBABCjeF6nuhEyvg==	100000	0	0.00%	1	0.0000/s	0.0000/s	0.0000/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0
Black List - Connectors	HNsSQZB0BABCBD37GCqa7qw==	1000	0	0.00%	1	0.0200/s	0.0017/s	0.0205/s	0.0000/s	0.0026/s	0.0026/s	0.00%	1	0		0

5. AgentStateTracker

AgentStateTracker はコネクタの状態をトラックするものです。（ここでは “Agent”と“Connector”は同義です）

まず、”Estimated Cache Size”でコネクタ側でイベントがキャッシュされていないかご確認ください。（キャッシュされていると、ESM へのイベントの到着の遅延などの問題が発生します。）また、ESM のパフォーマンスに問題がなければ、“Post-Aggregation EPS” と “Sent To Manager EPS” は同じような値になります。（“Post-Aggregation EPS”は、コネクタ側でイベントが Aggregation 処理された後のイベントの EPS になります。また、“Sent To Manager EPS”は、ESM へ送られたイベントの EPS になります。）



MBeans

Arcsight:service=AgentStateTracker

AgentListLoaded: true

AgentStatuses: java.util.ArrayList with 3 entries.

Name	ID	Reported	Agent Time	Received by Agent Count	Received by Agent EPS	Post-Filter Count	Post-Filter EPS	Post-Aggregation Count	Post-Aggregation EPS	Estimated Cache Size	Sent To Manager Count	Sent To Manager EPS	Failed Connection Attempts
syslog-daemon-82	3qUtkU38BABCD8RRXCDZgYw==	-	-	-	-	-	-	-	-	-	-	-	-
TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	03/15 18:33:48	03/15 18:33:48	2976	36.7	2969	36.7	2959	36.5	0	2903	35.4	0
Total	-	-	-	2,976	36.7	2,969	36.7	2,959	36.5	0	2,903	35.4	0

AgentsFilters: java.util.ArrayList with 18 entries.

URI	ID	Filter Name	Discrepancy
/すべてのコネクタ/All Connectors/DELL5540/TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	"Medium Severity" Event Definition	
/すべてのコネクタ/All Connectors/DELL5540/TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	"Very-High Severity" Event Definition	
/すべてのコネクタ/All Connectors/DELL5540/TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	"Low Severity" Event Definition	
/すべてのコネクタ/All Connectors/DELL5540/TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	Filter Out	
/すべてのコネクタ/All Connectors/DELL5540/TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	"High Severity" Event Definition	
/すべてのコネクタ/All Connectors/DELL5540/TestAlert-830	3dZXB7IUBABCEMpYPPqGJOw==	"Unknown Severity" Event Definition	

もし、“Post-Aggregation EPS” ＞ “Sent To Manager EPS” となっている場合、ESM 側で送られたイベントの処理容量を越えていることを意味し、（ESM のパフォーマンスやネットワークの問題など）、コネクタでイベントをキャッシュし始めますので、原因によってコネクタ側でイベントの量を少なくする（イベントのフィルターアウトや Aggregation の設定など）をお勧めしています。

6. RulesEngine

RulesEngine は ESM のルール エンジンの情報になります。ここでは “Partial Matches”（ルールの Aggregation で一部的にマッチしている数）の数が 100,000 を超えると ESM のパフォーマンスに影響があると言われています。次の KB をご参照され対応をお勧めしています。

Best practices on reducing partial Rule matches
https://support.microfocus.com/kb/kmdoc.php?id=KM1271148

MBeans

Arcsight:service=RulesEngine,type=Live,id=Real-time

AggregationEventCount	628
CorrelationEventCount	1
EvaluationTimePerEvent	0
FractionalRuleCpuThreshold	50 New value: Set
GarbageCollectorEventCount	0
GeneratedM1Count	275
InputBufferLength	0
InputBufferStatus	Accumulating elements ... for 50633
LastCheckPointSize	3729852
ListCacheMissDebugEnabled	false
LoadedRules	java.util.ArrayList with 431 entries.

Rule Id	Rule Name	Active ?	Matching Events	Correlation Events	Aggregation Sets	Partial Matches	Total Time (nsec)	Time(%)	Memory(Bytes)
5f0SJ2ysBABCHkhpGWm6O3Q==	Connector Discovered or Updated	true	733	733	8	686	35402	20.84	11386
5A6wNdjABABCARnBvpPlizQ==	Archive Events	true	0	0	0	0	10581	6.23	318
5psdB9G0BABCYgmzJtgDU1g==	Detected Directory Traversal	true	1679	1714	35	1575	8898	5.24	36774
50F18E3EBABCfrwTnfwtraw==	Track Rules with MITRE ID	true	0	0	0	0	8051	4.74	318
5k09UV2sBABCLy0RYG9o-Xw==	Track Rules triggered	true	0	0	0	0	7749	4.56	318
5YL3LuWsBABDCHbq7mQlLmg==	Dangerous Browsing to a Suspicious Domain	true	0	0	0	0	5464	3.22	250
50BdTp3gBABD862y0bM5Jyw==	File Hash is related to Sophisticated APT malware or 0-day Activity	true	0	0	0	0	5242	3.09	250
5kPRqp3gBABD9yTVBdKfplg==	URL is related to APT Malware Activity	true	0	0	0	0	5102	3	250
5DD+9ikUBABDRnk1TsrsCqA==	Critical Monitored Devices	true	0	0	0	0	4848	2.85	318
5MMZP8+8AABCASu1RhdKCOQ==	Compromise - Attempt	true	0	0	0	0	4847	2.85	250
5GUMhR2sBABCPjV2Qkn8wqw==	Detected Cross Site Scripting	true	0	0	0	0	4770	2.81	250
5nW2h9yYBABCjZGUNYI0egQ==	Query Running Time	true	0	0	0	0	4509	2.65	318
5c6MeR2sBABCPc8EH34Wtgw==	Exploit Attempt Detected by IDS	true	0	0	0	0	4348	2.56	250
5gT4hR2sBABCPipuwQzabMg==	Detected SQL Injection	true	0	0	0	0	3695	2.18	250
5VNNB9G0BABCYhYR08GBtmw==	Detected Format String Attack	true	0	0	0	0	3240	1.91	250
5jKbmjQsBABCBHvf4bstZ2A==	ArcSight User Login	true	0	0	0	1	2938	1.73	250

なお、不要なルールは無効化していただくことをお勧めします。

7. Scheduler

Scheduler は ESM でスケジュールされているジョブの情報となります。こちらは複数のレポートなどが同時に実行されていないかご確認ください。

MBeans

Arcsight:service=Scheduler

CurrentlyExecutingTasks: java.util.ArrayList with 0 entries.

ID	Name	Type	User

CurrentlyQueuedTasks: java.util.ArrayList with 0 entries.

ID	Name	Type	User

SchedulerThreadPoolSize: 7

TaskQueue: java.util.ArrayList with 18 entries.

ID	Name	Next Run	Type	User	Type	Priority
;mKrEUn8BABCDAAXRAQBJkw==	Resource Search Index Updater	Wed Mar 15 14:45:00 JST 2023	Other	RootUser	ScheduledTask	High
;X63EUn8BABCDAQAJE6gbpw==	AUP Updater	Wed Mar 15 14:50:00 JST 2023	Other	RootUser	ScheduledTask	High
;6U6444YBABCD9LAlfQbjcQ==	Table Stats Updator	Wed Mar 15 15:00:00 JST 2023	Hourly	RootUser	ScheduledTask	High
;Za7EUn8BABCDBFteRLHRDA==	PurgeStaleMarkSimilarConfigs	Wed Mar 15 15:00:00 JST 2023	Hourly	RootUser	ScheduledTask	High
;s5nWv2EBABCAIngs5RTKIQ==	Hourly EPS in Persistor	Wed Mar 15 15:05:00 JST 2023	Hourly	admin	Trend	Normal
;Ba-EUn8BABCDBdOJo9CrtQ==	Sortable Fields Updater	Wed Mar 15 15:10:00 JST 2023	Hourly	RootUser	ScheduledTask	High
;QhM-IEEBABCAM18Cs4iD8g==	Events Count	Wed Mar 15 15:30:00 JST 2023	Hourly	admin	Trend	Normal
;pOOQszMBABCATW2kzVxz-Q==	Trend Queries	Wed Mar 15 18:03:58 JST 2023	Daily	admin	Trend	Normal
;XS9SOEwBABCAGmlzINsRQQ==	Connector Daily Average EPS	Wed Mar 15 20:40:04 JST 2023	Daily	admin	Trend	Normal
;x-NROEwBABCAGMPNhLorDg==	Connector Average EPS - Last 7 days	Wed Mar 15 20:42:19 JST 2023	Daily	admin	Trend	Normal
;JSCyDSwBABCCda9txYM2TQ==	Connector Total Events - Hourly	Wed Mar 15 20:42:45 JST 2023	Daily	admin	Trend	Normal
;ThBPRzMBABCwxNBR2Cj2Fg==	Report Queries	Wed Mar 15 21:14:10 JST 2023	Daily	admin	Trend	Normal
;ep9SOEwBABCAHBNtz2FPSA==	QueryViewer Queries	Wed Mar 15 21:22:23 JST 2023	Daily	admin	Trend	Normal
;dYVefSoBABCCdgfExdAnCA==	Failed Queries	Wed Mar 15 21:45:51 JST 2023	Daily	admin	Trend	Normal
;TtRtnRABABCADIWUVBa7Bg==	ArcSight User Login Trends - Hourly	Wed Mar 15 22:00:00 JST 2023	Daily	admin	Trend	Normal
;Nk+444YBABCD9Xv-sezaaA==	Dependent Resource Validator	Thu Mar 16 01:55:00 JST 2023	Daily	RootUser	ScheduledTask	High
;SEdvpT8BABCBEF5TK9GS2w==	Storage Licensing Data	Thu Mar 16 02:52:22 JST 2023	Daily	admin	Trend	Normal
;7nq5eiUBABCIByWCTw1mIQ==	ASM Database Free Space	Thu Mar 16 07:34:00 JST 2023	Daily	admin	Trend	Normal

特に月次処理などで負荷の高い、また時間のかかる複数のレポート作成を同時実行された場合、ESM のパフォーマンスに影響を与えることがあり、それらの実行時刻を分散していただくなどお勧めすることがあります。

以上