ISE ىلع لجسلا تاليلحت ةمزح مەف

تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>ةىساسأ تامولعم</u> <u>كاتس كل</u> <u>لجس تاليلحتك ELK ةمزح</u> <u>لجسلا تالىلحت نىكمت</u> <u>لقنتلا ةمئاق</u> <u>ةجمدم تامولعم تاحول</u> <u>ةدىدج تامولعم تاحول ءاشنا</u> <u>(تانايب ردصم) سرهف طامناً ءاشنا 1. ةوطخلا</u> <u>تايئرم ءاشنا .2 ةوطخلا</u> <u>تامولعم ةحول ءاشنا .3 ةوطخاا</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>ةلص تاذ تامولعم</u>

ةمدقملا

يف ةنمضملا ELK سدكم تانوكم دنتسملا اذه فصي Cisco Identity Services Engine (ISE) 3.3 ماظنلا لجس تاليلحت لالخ نم 360.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- Cisco ISE
- كاتس كلإ •

ةمدختسملا تانوكملا

.Cisco ISE 3.3 ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

لجسلا تاليلحتو ةبقارملا System 360 نمضتي.

ماظنلاو تاقيبطتلا تايئاصحإ نم ةريبك ةعومجم ةبقارم ةيناكمإ ةبقارملا ةزيم كل حيتت دعت .ةيزكرم مكحت ةدحو نم رشن ةيلمع يف دقعلاا عيمجل (KPI) ةيسيئرلاا ءادألاا تارشؤمو ةئيبل ةماعلا ةحصلا لوح ةقمعتم ةيؤر ىلع لوصحلل ةديفم (KPI) يساسألاا ءادألاا تارشؤم ةصاخلا تانايبلاو ماظنلا تانيوكتل اطسبم اليثمت تايئاصحإلاا رفوت .ةدقعلا مادختسالاب

ةياەنلا ةطقن ةقداصمل قمعتملا ليلحتلل نرم تاليلحت ماظن لجسلا تاليلحت رفوت صخلم ليلحت اضيأ كنكمي .فينصتلل syslog تانايبو (AAA) ةبساحملاو ضيوفتلاو ريرقتو Cisco ISE Counters ل ةلثامم ريراقت ءاشنإ كنكمي .ةجلاعملا تالاحو Cisco ISE قحص .قحصلا صخلم

كاتس كلإ

ةجلاعمو عمجل مدختست ردصملا ةحوتفم جماربلا نم ةعﺉاش ةعومجم نع ةرابع ELK سدكم نإ و Kibana. و Kibana، دانا الالالالال الالالال الالالال الالال

- Elasticsearch: Elasticsearch تايمك نيزختل ممصم وهو .عزوم ثحبو تاليلحت كرحم وه وهو .ابيرقت يلعفلا تقولا يفو ةعرسب اهليلحتو اهنع ثحبلاو تانايبلا نم ةريبك .قريبك ةجردب ريوطتلل لباق وهو JSON يلإ دنتست راسفتسإ ةغل مدختسي
- Logstash: Logstash اەتجلاعم راسم وه Logstash: Logstash اەتجلاعم راسم وه Logstash: Logstash رثكأ اەلعجو ،تانايبلا ءارثإو ليلحت ىلع رداق وهف .ةددعتم رداصم نم اەليوحتو تاهجو لاخدالا رداصم نم ةعساو ةعومجم Logstash معدي .ليلحتلل ةبسانمو اميظنت جارخإلا
- حمسي وهو Elasticsearch عم لمعت تانايبلل ضرع ةصنم يه انابيك :
 انابيك تاموسرو تاطخمو تامولعم تاجول ءاشنإب نيمدختسملل
 لهسلان م انابيك قهجاو لعجت اهمهفو Elasticsearch يف قنزخملا تانايبلا فاشكتسال

نم ةفلتخم عاوناً ليلحتو ةرادإل ايوق اسدكم لكشت اهنإف ،تانوكملا هذه نيب عمجلا دنعو ةاكاحملا تاناكمإ ريفوت عم ،كلذ ريغو تاسايقلا ىلا لجسلا تافلم نم ،تانايبلا تامولعملا صالختسال ةيضارتفالا.



ELK سدكم قڧدت

لجس تاليلحتك ELK ةمزح

- دقع ىلع ليغشتلا ديق FlexibleSearch+LogStash+Kibana سدكمل لصفنم ليثم دجوي MnT طقف.
 - · ال Context-Visibility ل Elasticsearch ب طابترإ يأ ىلع اذه يوتحي ال
 - ELK 7.17 راج ∘
- عونلاا اذه نم اهب ةصاخ ةلصفنم تالاح ةيوناثلاو ةطسوتملا تاكبشللو.
 - ∍ تانايبلا ضرعي امم ،ارفوتم ناك اذإ يوناثلا MNT ىلع الإ Kibana نيكمت متي ال طقف ةدقعلا هذه نم.
- يضارتفا لكشب لجسلا تاليلحت ليطعت مت.
- دراوم كلەتسى Oracle.
- ماياً 7 ىصقاً دحب تانايب نيزخت.
- العالي المجال المعالي المجال المعالي المجال ا المحالي المحالي المحالي المحالي المحال المحال المحال المحال المحال المحال المحال المحالي المحالي المحالي المحال

. تانايبلا ةلازاب FlexibleSearch موقي ،دودحلا نم يأ ىلإ لوصولا درجمب



لجس تاليلحتك ELK قفدت



ISE يف ELK ل يبايسنا ططخم

لجسلا تاليلحت نيكمت

مت الي الحت الي مت الكشب لجسلا المنيكمتال . System 360 > Settings من ايف حضوم وہ امك (Operations - System 360 - Settings).

	Identity Services Engine Operations / System 360
щ	Settings Monitoring Log Analytics
10	Monitoring and Log Analytics Settings
*	Monitoring enables you to monitor a wide range of applications, system statistics, and key performance indicators (KPI) of all deployment nodes from a centralized console.
0	Monitoring
a 0	Go to Monitoring 🖸 View
n	Log Analytics provides a flexible analytics system for in-depth analysis of syslog data generated from different endpoints.
?	Go to Log Analytics 🖄 View
	Reset Save

لجسلا تاليلحت نيكمت

AD Connector running 41413

M&T Session Database running 26017

مادختساب ةلاحلا نم ققحتلا كنكمي ،ELK سدكم ةئيەتل ةقيقد يلاوح ISE قرغتسي app stat ise.

رذجلا نم ةيواحلا ةلاح نم ققحتلا كنكمي ،كلذ ىلإ ةفاضإلاب.

M&T Log Processor running 33547 Certificate Authority Service running 41230 EST Service running 659568 SXP Engine Service disabled TC-NAC Service disabled PassiveID WMI Service disabled PassiveID Syslog Service disabled PassiveID API Service disabled PassiveID Agent Service disabled PassiveID Endpoint Service disabled PassiveID SPAN Service disabled DHCP Server (dhcpd) disabled DNS Server (named) disabled ISE Messaging Service running 10937 ISE API Gateway Database Service running 13294 ISE API Gateway Service running 586762 ISE pxGrid Direct Service running 637606 Segmentation Policy Service disabled REST Auth Service disabled SSE Connector disabled Hermes (pxGrid Cloud Agent) disabled McTrust (Meraki Sync Service) disabled ISE Node Exporter running 44422 ISE Prometheus Service running 47890 ISE Grafana Service running 51094

ISE MNT LogAnalytics Elasticsearch running 611684

ISE Logstash Service running 614339

ISE Kibana Service running 616064

ISE Native IPSec Service running 75883 MFC Profiler running 651910

لقنتلا ةمئاق

ةنرملا لقنتلا ةمئاق ىلإ لوصولا كنكمي ،ELK تامدخ ليغشت ءدب درجمب.



لقنتلا ةمئاق

ةجمدم تامولعم تاحول

- نم تانايب ىلع يوتحت ةجمدم تامولعم تاحول ىلع ISE يوتحي ،يضارتفا لكشب RADIUS قظحالم ةيناكمإو ماظنلا عادأو TACACS و ISE.
- د Operations > Log Analytics كال القتنال اللخ نم هذه تامولعملاتا تاحول ىل الوصول انكمي Operations > Log Analytics . • Sandwich Menu > Analytics > Dashboards .



ةجمدم تامولعم تاحول

• اىل اتاجول تامولعمل اتاجول ISE 3.3.

Title	Description	Tags Action:
ISE Observability Dashboard		Ø
ISE Overview Dashboard		Ø
ISE Processes Summary		Ø
ISE Troubleshooting Dashboard		Ø
Profiler Performance		Ø
Profiler Summary		Ø
RADIUS Accounting Summary		Ø
RADIUS Authentication Summary		Ø
RADIUS Performance		Ø
RADIUS Step Latency		Ø
TACACS Accounting Summary		Ø
TACACS Authentication Summary		Ø

ISE 3.3 لجس تاليلحت تامولعم تاحول

ةديدج تامولعم تاحول ءاشنإ

(تانايب ردصم) سرهف طامناً ءاشنإ .1 ةوطخلا

عم انابيك لعافت ةيفيك ديدحت كل حيتت لاكشأ يه "ةسرەفلا طامنأ" نإف ،انابيك يفو تارشۇم نم رثكأ وأ رشۇم Elasticsearch.

يف حضوم وه امك Create Index Pattern رقنا مث ، Management > Stack Management > Kibana > Index Patterns رقنا مث ، Create Index Pattern كار وصلاً.

Settings	Monitoring	Log Analytics	
🤣 e	lastic	Q Search Elastic	0
≡	Stack Management	t Index patterns	
() Inges	Management	The second secon	Create index pattern
Alert	s and Insights © and Connectors	Q Search	
Kibar Index Saved	na ⊙ x Patterns d Objects	Pattern 1 mnt_analytics_tacacs_authentication* Default	
Tags Advar	nced Settings	mnt_analytics_sggregate_steplatency* 	

سرەف شقن ءاشنإ

. ISE ىلع ةرفوتملا سراەڧلا ةڧاكب ةمئاق يلاتلا راطإلا رەظي

- .* مادختساب لدب فرح وأ مات قباطت نوكي نأ نكميو ،هب متهت يذلا سرهفلا مسا بتكا •
- لماع مادختسإ ديرأ ال" وأ logging_at_timezone وأ logging_at وأ ينمزلا عباطلا لقح ددح

."تقولا ةيفصت

• رقنامث Create index pattern.

Create index pattern Your index pattern matches 1 source. Name mnt_analytics_radius_authentication Alias mnt_analytics_radius_authentication Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed. Rows per page: 50 $\,\,\smallsetminus\,\,$ Timestamp field logged_at \sim Select a timestamp field for use with the global time filter. Show advanced settings Create index pattern \times Close

سرەف ديدحت

اقحال اەمادختسإ نكمي يتلا ةطبترملا تاريغتملا لك سرەڧلا درسي ،اەئاشنإ درجمب تايئرملا ءاشنإل.

E Stack Management Index	patterns mnt_analytics_radius_authentication											
Management Ingest © Ingest Pipelines	mnt_analytics_radius_ Time field: logged_at	authentication		t *								
Alerts and Insights © Rules and Connectors	View and edit fields in mnt_analytics_radius_authentication. Field attributes, such as type and searchability, are based on field mappings @ in Elasticsearch.											
Index Patterns Saved Objects	Name 个	Type Format	Searchable Aggregatable	Excluded								
Tags Advanced Settings	_id _index	_id _index	• •	0								
	_score source	_source		0								
	_type	_type	• •	0								
	access_service access_service.keyword	text keyword	• •	0								

سرەڧلا تاريغتم



تانايبلا ذخأ كل حيتت اهنإ .كتانايبل ايموسر اليثمت "تايئرملا" لثمت ،انابيك يفو ىنعم تاذ تاططخمو ةينايب موسرو تاططخم ىلإ اهليوحتو Elasticsearch يف ةنزخملا اهئاشنإ كنكمي يتلا تايئرملا نم ةعئاشلا عاونألا ضعب هذه .ليلحتلاو مەفلا ليەستل

- المب يصوم .تالفإو بحس ررحم مادختساب تايئرم ءاشنإ :ةسدعلا.
- ةنراقم لەسي امم ،ةيسأر ةطرشأ يف تانايبلا ەذە ضرعت :ةيطيرشلا تاططخملا ةينمزلا لصاوفلا وأ تائفلا ربع ميقلا.
- تانايبلا طاقن نم ةلسلسك تانايبلا ةيطخلا تاططخملا ضرعت :ةيطخلا تاططخملا تقولا رورمب تاهاجتالا روصتل ةديفم يهو .طوطخلاب ةلصتملا
- ثيح ،يرئاد ينايب مسر يف تانايبلا ةيرئادلا تاططخملا لُثمت :ةيرىًادلا تاططخملا مبسانت يلإ ريشي يذلا عطقملا مجو ةئف يرئادلا ططخملا نم عطقم لك لثمي.
- اضيأ ةيحاسملا تاططخملا رەظت ،ةيطخلا تاططخملا رارغ ىلع :ةيحاسملا تاططخملا رادقم ةيؤر لەسي امم ،رطسألا تحت ةحاسملا ألمت اەنكلو ،تقولا رورمب تاەاجتالا .تارييغتلا
- وأ ةفوفصم يف تانايبلا ميق ليثمتل ناولألا ةرارحلا طئارخ مدختست :ةرارحلا طئارخ تانايبلا يف تانيابتلا وأ تازيكرتلا راهظإل ةديفم يهو .ةكبش.
- وأ ماقرألاا دادعأ لثم ،ةدرفم ةيمقر اميق تايئرملا هذه ضرعت :ةيُرتملاً تايئرملاً .ةيسيئرلا ءادألا تارشؤم راهظإل تارشؤملا هذه مدختست ام ابلاغو .تاطسوتملا
- كل حيتي امم ،يلودج لكش يف ةيلوأ تانايب تانايب لوادج مدقت :تانايبلا لوادج اهتيفصت وأ تانايبلا بيترتو ةيليصفت تامولعم ةدهاشم.
- ضرعتو لصاوف وأ تادادس ىلإ تانايبلا ةينايبلا موسرلا مسقت :ةينايبلا موسرلا تانايبلا عيزوت تايلمع مەفل ةديفم يەو .ةيواح لك يف تانايبلا طاقن ددع وأ ددرت.
- ضرع كل حيتي امم ،ةيئاضفويجلا تانايبلا ضرعب هذه موقت :تايثادحإلاا طئارخ صئاصخ ليثمتل ةفلتخم ماجحاً وأ ،ناولاً ،تامالع مادختساو ةطيرخ ىلع تانايبلا .تانايبلا
- Tag Cloud: لك مجح ريشي ثيح ،تاملكلا تاددرت زييمتلا تامالع تاذ بحسلا ضرعت تانايب ةعومجم يف اهددرت وأ اهتيمهأ ىلإ ةملك.

. قروصلا يف حضوم وه امك Create Visualization قوف رقنا مث ، Analytics > Visualize Library ، قروصلا يف

😔 elastic			ର Se	arch Elastic		
Visualize Library						
△ Home		sualize Library				Create visualization
Recently viewed	\sim	,				
ISE Processes Summary		Building a dashboard? Create and ad				
📕 Analytics	\sim	Search				Tags 🗸
Overview						
Discover		Title	Туре	Description	Tags	Actions
Dashboard		AD Connector	Dens			Ø
Visualize Library		App Server	Lens			Ø
Management Stack Management	~	Authentication Success Rate -markdown	1 Markdown			Ø
oraor management		Authentication latency Per ID	1 Markdown			Ø

تايئرم ءاشنإ

ةيعقاولا ىلع ةسدعلا لضفي ،لاثملا اذه يف ،كتاليضفت تايئرم ددح.



تايئرملا عون ديدحت

:نم لڨنتلا رصانع فلأتت ،Kibana Lens

- شقن وأ تانايبلا ردصم ديدحت كنكمي ،ىرسيلا ةحوللا يف :تانايبلا ردصم ديدحت كتدەاشمل ەمادختسإ ديرت يذلا Elasticsearch سرەف.
- Visual Canvas: بحس لالخ نم كروصت هيف ينبت يذلا ناكملا يه ةيزكرملا ةقطنملا. ططخملا تادادعا نيوكتو ،تاططخملا عاوناً ديدجتو ،اهطاقساو لوقحلا.
- كل حيتي ،ةحوللاا ىلعأ يف تاودأ طيرش نع ثحبلاا كنكمي :ضرعلا تاودأ طيرش نيوكتو تاحشرم ةفاضإو ططخملا عاونأ رييغتل تارايخ كلذ يف امب ،كروصت صيصخت .ططخملا تادادعإ
- حيتت يتلاو ،"تانايبلا" ةحول ىلإ لوصولا كنكمي ،نميألا بناجلا يف :تانايبلا ةحول لقحلا تادادعإو ،عيمجتلاو ،تانايبلا ليوحت ةرادإ كل.
- ،لااثملا ليبس ىلع) اەئاشناب موقت يتلا تايئرملا عونل اقبط :ةقبطلا ةرادا، تاقبط نيوكتل ةقبط ةرادا ةقطنم ىلع لوصحلا كنكمي ،(تاقبطلا تاذ تاططخملا كتآرم يف ةددعتم.
- يقيقحلا تقولا يف ةنياعم ريفوت متي ،تايئرملا يلع تارييغت ءارجإ دنع :ةنياعم •

.ةيلاحلا تادادعإلاا عم كب صاخلا ططخملا ودبي فيك ةيؤر كنكمي ثيحب يجذومن لكشب

- ةنيعم تادادعإ ىلإ لوصولا كنكمي ،ددحملا ططخملا عون بسح ىلع :تايئرملا تادادعإ تايمستلاو ،نوللا ةمظناً ،روحملا نيوكت لثم ،اذه تايئرملا عونل.
- امم ،كب ةصاخلا تايئرملا ىل تاءارج و تالعافت ةفاض كنكمي : قيل عافتلا تادادع المم ،كب قصاخلات العائمي المراجع ا المراجع المراج المراجع مراجع المراجع ا مراجع المراجع الم مراجع المراجع ال مراجع المراجع الم مراجع المراجع المراجع المراجع المراجع المراجع المراجع المراج مراجع المراجع المراجع المراجع المراجع المراجع المراجع المراجمع المراجع المراجع المراجع المراجع المراع المراجع المراجع الم
- ىلإ اەتڧاضإ وأ كتيآرم ظڧحل تارايخ ةداع دجوت ،ةسدعلا ةەجاو ىلعأ يڧ :ةكراشمو ظڧح نيرخآلا عم اەتكراشم وأ تامولعم ةحول.



تاسدعلا تايئرم

لوقحلا ىرسىلا ةحوللا رەظت ال ، Cisco <u>CSCwh48057</u> نم ءاطخألا حىحصت فرعم ببسب ةبولطملا لوقحلا دىدحت كنكمي ،نمىألا بناجلا نم ،لاح يأ ىلع .مادختسالل ةحاتملا وه ةقداصملا لوصو نمز نأل ارظن ،لاثملا اذه يف .يطيطختلا مسرلا طمن ىلإ ةفاضإلاب لوصو نمز ضرعل ينايبلا مسرلا ميمصت مت دقف ،كرتشم مامتهاب ىظحي عوضوم المال الم



لوصولاا نمز لباقم ةياەنلا ةطقن فرعم

.ةروصلا يف حضوم وه امك ىنميلا ةيوازلا يف رز save قوف رقنلا كنكمي ،ءاهتنالا درجمب

		Inspect Download as CSV 🛛 🔀 Save
	KQL Last 1 hour	Show dates C Refresh
Save Lens visualization		×
Title	Add to dashboard	mnt_analytics_radius_authenticati V
EPvsLatency Description	Existing Search dashboards	Vertical axis
Joncasil ep vs latency lens visualization.	New None	Endpoint ID ×
	Add to library ③	Horizontal axis
		Ø Median of totalauthenlatency →
	Cancel Save and go to Dashboard	Add or drag-and-drop a field
		Break down by
0 100 200 300 400 50	0 600 700 800 900 1,000 1,100 1,200	
Median d	of totalauthenlatency	

تايئرملا ظفح

تامولعم ةحول ءاشنإ .3 ةوطخلا

تاحول نأ رابتعالاا يف عض .ةديدج تامولعم ةحول ىلإ ةديدجلا تايئرملا ايئاقلت فيضي وهو تايئرملا ةكراشمو صيصختو ءاشنإ نم نيمدختسملا نكمت انابيك يف تامولعملا Elasticsearch. تارشؤم يف ةنزخملا تانايبلا ىلإ ةدنتسملا ةيلعافتلا ريراقتلاو

💮 elastic								ର Sear	rch Elastic	:							0		
≡	Dashboard	Editing	New Da:	shboard)										Unsaved changes	Options	Share	Switch to view mode	Save
•	Search												KQL	*	Last 1 hour			Show dates	් Refresh
.	+ Add filter																		
ø	Create visualiza	tion	(Ŧ)	All type	s v	Ð	Add fro	m libra	ry										
EPvs	Latency ①											\$							
	2E:E6:89:30:81:A6										1,200920820								
Endpoint ID	4D:EF:00:C9:0D:C4																		
	2E:01:57:46:8C:FD	0 100	0 200	300 40	00 500	600	700 80	0 900	1,000 1,1	100 1,200									
				Me	dian of t	totalaut	henlaten	icy											

ةديدج تامولعم ةحول

اهحالصإو ءاطخألا فاشكتسا

- المدخ ليغشت نم قوقحت MNT. يلع ELK المدخ ليغشت نم ق
- تالجسلا ىلع رثع دقف ،تايواحلا ىلع لمعت Elasticsearch و ،Kibana و ،Kibana تأ امبو يف

```
admin#show logging application ise-kibana/kibana.log
admin#show logging application ise-logstash/logstash.log
admin#show logging application mnt-la-elasticsearch/mnt-la-elasticsearch.log
```

ةلص تاذ تامولعم

- <u>ISE 3.3 لوؤسم ليلد</u>
- <u>انابيك قئاثو</u> •
- <u>انم تاليزنتلاو ينقتلا معدلا</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما