Your Question

Article: 00107 Ouestion:

NET REPORT

How to Create a Double RDNS Net Area for Several Clients?

Net Report Answer

Introduction

This Article explains how to create a double RDNS (Reverse Domain Name Server) Net Area for several clients.

1.1 Creating a Double RDNS Net Area

To create a double RDNS Net Area for several clients, please follow the steps below:

Steps

1. Select **Start>All Programs>NetReport> Management Console**. The **Login** dialog box appears.

▲ ⁰ Login	1 [°]		
م ۵	Login :		ОК
	Password :	1	Cancel

- 2. Enter your Login and Password.
- 3. Click **OK**. Wait for the Net Report Management Console to load.
- 4. Select **Console root> NetReport> localhost> ULA> Settings> Initializations** in the left **Console root** pane. The **Initializations** screen appears in the central pane.

✿ netreport - [Console rootiNetReport\localhostWLA\Sett	ings\Initialisations]			
🚯 File Action View Favorites Window Help				_ 8
🧰 Console root 🛛 🗸				
🚊 🚸 NetReport 🔤	2 67)		Initializ	zations
🖻 🧌 localhost				
📲 Packages Server				
🖻 🚸 ULA			>NetReport/localhost/ULA/Settings/ir	itialisations<
E Settings	Initialization	s		
Action Source	Name	Enable	Comment	
Attack Source	Action Source			
Correlation Space	Action Source	M		
Events by Source	Attack Source			83
WMT Alasta	Allack Source	le la		1927
Mail Oddresses	Correlation Space			EE
Database Connection	Conclation Opace			
IP to Country	Events by Source			
an co coana y		1.		120
SMTP Server Name	Port Accepted			
Performance Counters For NetReport Filters				
RDNS	😑 WMI Alerts			
RDNS net area				
Sessions	📃 😇 Mail Addresses		Sets Mail Adresses for all Mail Actions	
	📮 📴 Database Connection			
- 🔐 SQLVulnerability	😅 IP to Country		Convert an IP adress to a Country	
🕂 🔷 Filters				
	📕 🔤 Log Storage	¥		



5. Click the turquoise bullet to the left of the **RDNS net area** initialization. The row will be grayed.

NET REPORT



- 6. Click the 🗎 Copy icon in the tool bar at the base of the Initializations screen.
- 7. Click the E Paste icon in the tool bar at the base of the Initialization screen. The Copy of RDNS net area row appears in the Initializations table.

∲ netreport - [Console root\NetReport\localhost\ULA*\Sett	ings\Initialisations]				×
🚯 Eile Action <u>V</u> iew Favorites <u>W</u> indow <u>H</u> elp				_8	×
Console root				-	
🖻 🚸 NetReport	Log Storage	\checkmark		ബ	
🖻 👊 localhost		_		-	
Packages Server	SMIP Server Name	V	SMTP Address used to send a mail		
	Porformanco Countore For NotPoport Filtore		Conoral Parformance Counters for NotPoport Filters	25	
	enormance counters i or iverkeport i inters		General Penormance Counters for Netweport Filters		
Action Source	Copy of RDNS net area	V		2	
- 😽 Attack Source				135.134.2.49	
- 🤴 Correlation Space	S RDNS	V	General RDNS	2	
- 🤯 Events by Source				135.134.2.49	
- Port Accepted	🤤 RDNS net area	~			
WMI Alerts		_	Operation 1.20 Beacher	135.139.2.99	
Mail Addresses	Sessions	V	Session initialisation		
IP to Country	Sessions (10 minutes)		Session definition for 10 minutes		
and Log Storage		I.	Session demition for to minutes	9	
SMTP Server Name	SQL Firewall Alert	V	Correlation using SQL sample		
😽 Performance Counters For NetReport Filters			5 1		
RDNS	SQLCache	$\overline{\checkmark}$	SQL definition to get data from an SQL database		
🤮 RDNS net area					
	SQLVulnerability	✓	SQL definition to get data from an SQL database		
Sessions (10 minutes)	O Oslavka d Ishkali a Kana			÷ -9	
SQL Firewall Alert	U Selected Initialisations		Connection to another ULA	▥ 📑	
SOLVulperability					
Copy of RDNS net area					
<]				-
				_	



8. Modify the name of the new initialization to **RDNS net area Client 1**.

Metreport - [Console root\NetReport\localhost\ULA*\Settin	ngs\Initialisations]				×
🚯 Eile Action View Favorites Window Help				_ 8	×
🔁 Console root 🔼				~	
E VetReport	Log Storage	◄		GI	
⊡ localhost		_			
Packages Server	SMIP Server Name	V	SMIP Address used to send a mail		
E V ULA"	Derformance Counters For NotPenert Filters		Conoral Parformance Counters for NotPoport Filters	<u>1</u>	
	· Fenomance Counters For NetReport Filters	I.	General Periormance Counters for NetReport Filters		
Action Source	RDNS net area Client 1		RDNS net area Client 1	2	
Attack Source				135.139.2.95	
- \iint Correlation Space	RDNS		General RDNS	2	
- By Events by Source				135.184.2.49	
- 🤴 Port Accepted	💭 RDNS net area	☑		2	
- 🤴 WMI Alerts				135.134.2.49	
Mail Addresses	Sessions		Session Initialisation		
Database Connection		_			
IP to Country	Sessions (10 minutes)	V	Session definition for 10 minutes		
SMTD Server Name	SOL Eirowall Alart		Correlation using SQL comple		
Berformance Counters For NetPeport Filters	SGET Newall Alen	I.	Correlation using SQL sample		
RDNS	SQI Cache		SQL definition to get data from an SQL database		
RDNS net area					
Sessions	SQLVulnerability	•	SQL definition to get data from an SQL database		
				43	
	0 Selected Initialisations		Connection to another ULA 📃 🖻 🛱 🗋	🗓 💕 📗	
😥 SQLCache					
RDNS net area Client 1					-
		_			-

- 9. Repeat steps 5 7 to create a second RDNS net area initialization.
- 10. Rename the second new initialization to **RDNS net area Client 2**.

File Action View Favorites Window Help	tingsvinitiausationsj				×
Console root	IP to Country	~	Convert an IP adress to a Country		
E VetReport		_			
E- No localhost	U Log Storage	V			
Packages Server	SMTP Server Name		SMTP Address used to send a mail	NZ	
	Jiviti Delver Name		Jiviti Address dsed to seria a main		
	Performance Counters For NetReport Filters	V	General Performance Counters for NetReport Filters	NS I	
- 🤯 Action Source				ENZ	
- 🤴 Attack Source	S RDNS	☑	General RDNS	2	
- 🤯 Correlation Space				135.134.2.49	
Events by Source	RDNS net area	◄			
Port Accepted	DDNO ant serve Olivet 1	-	DDNO and area Olicet 1	135.137.2.15	
WMI Alerts	BUNS het area Client I	M	RDINS het area Client I	135.135.249	
Mail Addresses	PDNS net area Client 2		PDNS net area Client 2	2	
IB to Country		1.		135.151.2.19	
Log Storage	Sessions	☑	Session Initialisation		
M SMTP Server Name					
😽 Performance Counters For NetReport Filters	Sessions (10 minutes)		Session definition for 10 minutes		
RDNS					
RDNS net area	SQL Firewall Alert	◄	Correlation using SQL sample		
- 👂 Sessions		_			
Sessions (10 minutes)	SQLCache	V	SQL definition to get data from an SQL database		
SQL Firewall Alert	SOLVulnorshility		SOL definition to get data from an SOL database		
SQLCache	- SGEY Unerability	I.	Soc deminion to get data nom an Soc database		
RDNS pet area Client 1	0 Selected Initialisations		Connection to another LILA 📃 🖻 🛱 🗂	1 2	
					-



11. Select Console root> NetReport> localhost> ULA> Filters> [Filter Name]> Dictionary in the left Console root pane. The Dictionary screen appears in the central pane.

netreport - [Console root/NetReport/localhost/ULA*/Filte	ers\Fortinet FortiGate\Diction	ary]	
🚯 File Action View Favorites Window Help			X
Console root	E Dictionary		Dictionary
Database Management - Firewall and Proxy	action_group	Values	
		😑 pass	Accepted
Fortinet FortiGate H K Actions		e block	Blocked
Eields		accept	Accepted
Dictionary		e deny	Blocked
🖃 🌍 Agents 🕀 📑 Log Vault		e detected	Accepted
🗄 🖏 Backups		dropped	Blocked
		😊 reset	Blocked
		🙁 reset_client	Blocked
		reset_server	Blocked
		🔵 drop_session	Blocked
		ອ pass_session	Accepted
)		

12. Click the **New** icon from the **Selected Entries** tool bar at the base of the **Dictionary** screen. A **New Entry** dictionary entry appears.

🚯 netreport - [Console root\NetReport\localhost\ULA*\Filt	ters\Fortinet FortiGate\Dic	tionary]		
🚯 Eile Action View Favorites Window Help				_ [2] ×
← → 🗈 🖬 😫				
Console root NetReport Icaliost Packages Server ULA* Settings Filters Database Management - Firewall and Proxy Database Management - IPS Database Management - IPS Database Management - IPS Attions Fields Dictionary Agents Log Vault Backups	New Entry O Selected Entries	 notice information debug 0 1 2 3 4 5 6 7 0 Selected Values 0 Selected Values 	5 6 7 0 1 2 3 3 4 5 6 7 7 s	
	,			

13. Rename the new dictionary entry **RDNS_Client**.

NET REPORT

netreport - [Console root/NetReport/localhost/ULA*/Fil	Iters\Fortinet FortiGate\Dict	ionary]		
🚯 Eile Action View Favorites Window Help				X
 Console root Console root NetReport Iocalhost Settings Filters Database Management - Firewall and Proxy Database Management - IPS EngineEvent Fields Dictionary Agents Log Vault Ends 	RDNS_Client	 notice information debug 0 1 2 3 4 5 6 7 0 Selected Value 0 Selected Value 	5 6 7 0 1 2 3 4 5 6 6 7 5 6 6 7 5	
	TotWelkeportVocalhost/ULA*VFilters/Fortinet FortiGate/Dictionary] wgrites Window Help r se Management - Firewall and Proxy se Management - IPS Event t FortiGate ions es ds tionary			
				•

14. Click the **Decision** In the **Selected Values** tool bar at the base of the **RDNS_Client** dictionary entry. A **NewKey** row appears.

netreport - [Console root\NetReport\localhost\ULA*\Filt	ters\Fortinet FortiGate\Dict	ionary]		
💽 Eile Action View Favorites Window Help				<u>_ 문 ×</u>
Console root NetReport Icalhost I	RDNS_Client	 notice information debug 0 1 2 3 4 5 6 7 0 Selected Value NewKey 0 Selected Value 	5 6 7 0 1 2 3 4 5 6 6 7 2 8 8 8 8 8 8	
	0 Selected Entries			ħ Ē 1 i ⅔ -
	console rootVietReportVacathostVULA*VFilters/Fortinet FortiGateUticitionary] dew Favarites Window Help ages Server ettings ettings ters © Database Management - Firewall and Proxy © Database Management - JS Fringthe Fortificate © Database Management - JS e fields Database Management - JS e fields © Delected Values e fields © Delected Entries			



15. Modify the NewKey value to the name of the client firewall, in this example, FW00025 with the value of the RDNS net area initialization, in this example, RDNS net area Client 1.

NET REPORT

netreport - [Console root\NetReport\localhost\ULA*\Fil File Action View Favorites Window Help	lters\Fortinet FortiGate\Dic	tionary]			
→ Ē 📧 😫					
Console root NetReport		😅 notice	5		
E- Calhost		information	6		
		😊 debug	7		
Eltings Image: Settings Image: Settings Image: Settings		0	0		
P Database Management - Firewall and Proxy Database Management - IPS P M EngineEvent		e 1	1		
		2	2		
Fortinet FortiGate Actions		3	3		
E-A Rules		9 4	4		
Dictionary		9 5	5		
Agents		e 6	6		
🗄 🛫 🌍 Backups			9 7	7	
		0 Selected Value	s	🔁 🗂 🏛 🔧	
	RDNS_Client	Values			
		FW00025	RDNS net area Client 1		
		0 Selected Value	S	🖧 🗂 💼 🔮	
	0 Selected Entries			Þa 🔁 🖞 🗊 💡	
	,				

- 16. Click the **New** icon in the **Selected Values** tool bar at the base of the **RDNS_Client** dictionary entry. A **NewKey** row appears.
- Modify the NewKey value to the name of the client firewall, in this example, FW00026 with the value of the RDNS net area initialization, in this example, RDNS net area Client
 2.

netreport - [Console root\NetReport\localhost\ULA*\Fil	ters\Fortinet FortiGate\Dic	tionary]		
🚯 Eile Action View Favorites Window Help				<u>_8×</u>
Console root		😑 notice	5	
localhost		🤤 information	6	
		😑 debug	7	
		0	0	
Database Management - Firewall and Proxy Database Management - IPS		e 1	1	
EngineEvent		2	2	
Fortinet FortiGate Actions		3	3	
Eields		a	4	
Dictionary		9 5	5	
E S Log Vault		e 6	6	
E - 🖏 Backups		9 7	7	
		0 Selected Value:	s	😂 🗋 💼 🧝
	RDNS_Client	Values		
		FW00025	RDNS net area Client 1	
		FW00026	RDNS net area Client 2	
		0 Selected Value	s	& 1 i 🖇 🗸
	<i>y</i>			



18. Select **Console root> NetReport> localhost> ULA> Filters> [Filter Name]> Fields** in the left **Console root** pane. The **Fields** screen appears in the central pane.

NET REPORT

netreport - [Console root\NetReport\localhost\ULA*\Fi File Action View Eavorites Window Heln	lters\Fortinet FortiGate\Fields]				- 17
Console root Co					Fields
Je Packages Server E			>NetReport/localhost/U	LA/Filters/Fortinet Fort	:iGate/Fields<
E General Settings	∥ Fields				
Database Management - Firewall and Proxy	Name 🔺	Туре	Expression	Comment	
Database Management - IPS Database Management - IPS Former Fortinate Fortinate Fortigate Fortigate	😅 _rcvd	Integer	➡ iff(IsNullOrEmpty(Record		/ Edit
	🤤 _sent	Integer	➡ iff(IsNullOrEmpty(Record	:	/ Edit
	😅 _type	String	➡ iff(Record("type")="traffic	;	/ Edit
Dictionary	😅 _vpn	String	Record("vpn")		/ Edit
🗉 💎 Agents 🗉 🛃 Log Vault	e action	String	 Record("status") 		/ Edit
⊞👹 Backups	Action_group	String	 DictLookup("action_group 	1	/ Edit
	Action_Src	String	➡ field("action")&field("src'	1	/ Edit
	😅 attack	String	📕 "FGT" & Record("attack		/ Edit
	Bad_Record	String	Record("BadRecord")		/ Edit
	😅 bytes	Integer	➡ field("_rcvd")+field("_sen	•	/ Edit
	🙍 cat	String	Record("cat")	ips: Attack catedory	/ Edit

19. Click the **New** icon in the tool bar. The **_New Field** row appears in the **Fields** table.

netreport - [Console root\NetReport\localhost\ULA*\Filt	ers\Fortinet FortiGate\Field	5]				×	
🔮 File Action Yiew Favgrites Window Help						×	
Console root				l	Fields		
□ · · · · · · · · · · · · · · · · · · ·			>NetReport/localhost/U	A/Filters/Fortinet FortiG	ate/Fields<		
Settings	∥ Fields						
Database Management - Firewall and Proxy	Name 🔺	Туре	Expression	Comment			
	New Field	String	Record("afield")		/ Edit		
Fortinet FortiGate Actions	😑 _rcvd	Integer	iff(IsNullOrEmpty(Record		/ Edit		
Rules Fields	🤤 _sent	Integer	iff(IsNullOrEmpty(Record		/ Edit		
Dictionary	🛢 _type	String	iff(Record("type")="traffic		/ Edit		
General Log Vault	😑 _vpn	String	Record("vpn")		/ Edit		
	ອ action	String	Record("status")		/ Edit		
	Action_group	String	DictLookup("action_grou		/ Edit		
	Action_Src	String	field("action")&field("src"		/ Edit		
	😊 attack	String	FGT" & Record("attack		/ Edit		
	Bad_Record	String	 Record("BadRecord") 		/ Edit		
	🗖 bvtes	Integer	field(" rcvd")+field(" sen		/ Edit	-	



20. Click the **Edit** button to the right of the **New Field** row. The **Field Edition** dialog box appears.

🕘 Field Editio	n Web Page Dialog	
∥Edit	Field	
Name :	_New Field	
Type :	String	•
Value :	Record("afield")	
Comment :		
	OK Cancel SVbScript	
		-

21. Enter the Name **RDNS_Client** in the **Name** text box.

22. Enter the following Value: DictLookup("RDNS_Client", Record | ("device_id"))

🕘 Field Editio	n Web Page Dialog	
		· · · ·
₿ E d i t	Field	
Name :	RDNS_Client	
Type :	String	•
Value :	DictLookup("RDNS_Client",Record ("device_id"))	
Comment :		
	OK Cancel SVbScript	
		-

23. Click **OK**.

NET REPORT

Note: this article uses the following device as an example: Fortinet Fortigate. Please note that the Value may differ according to the device you select.



24. Click the Zedit

Edit button to the right of the **Src_net_area** row.

File Action View Favorites Window Help				_82
← → 🗈 📧 😫				
 Image: Second state of the secon	 rule search_engine search_string service SessionUserIP SessionUserIPDomain SessionUserIPDomainObj SessionUserIPObj 	String String String Float Float Object Object	Record("policyid") iff(field("search_string")< GetSearchString(field("D iff(IsNullOrEmpty(Recorc Field("SessionUserIPOb Field("SessionUserIPDo Server.GetEnvObj("/Initia Server.GetEnvObj("/Initia	/ Edit / Edit / Edit / Edit / Edit / Edit / Edit / Edit / Edit
🔁 🙀 Log Vault 😥 😵 Backups	 Src_country Src_name Src_net_area src_port status subtype 	String String String String String String String	Record('stc') iff(field("Src_net_area")= ExecRDNS("RDNS",field ExecRDNS("RDNS net { Record("src_port") Record("status") Record("subtype")	/ Edit / Edit / Edit / Edit / Edit / Edit / Edit

25. Modify the Value from: ExecRDNS("RDNS net area", field("src"))

0	Field Editio	n Web Page Dialog	
	∥Edit	Field	
	Name :	Src_net_area	
	Туре :	String	•
	Value :	ExecRDNS("RDNS net area",field("src"))	
	Comment :		
		OK Cancel &VbScript	
			-

To:

```
ExecRDNS(field("RDNS_Client"), field("src"))
```

🕘 Field Ed	ition Web Page Dialog	
_		
₿ E d	it Field	
Name :	Src_net_area	
Type :	String	•
Value :	ExecRDNS(field("RDNS_Client"),field("src"))	
Comme	nt :	
	OK Cancel BVbScript	
		•



26. Click **OK**. The **Fields** screen appears.

27. Click **Edit** to the right of the **Dst_net_area** row. The **Field Edition** dialog box appears.

<u>File Action View Favorites Window Help</u>				_8
→ E E 2				
Console root	😇 attack	String	FGT" & Record("attack	/ Edit
Pretkeport	Bad_Record	String	Record("BadRecord")	/ Edit
📜 Packages Server	😅 bytes	Integer	field("_rcvd")+field("_sen	/ Edit
Ellers	🛢 cat	String	Record("cat") ips: Attack category	/ Edit
Database Management - Firewall and Proxy	😊 Date	Time	■ IFF(IsNullOrEmpty(Reco	/ Edit
	DateStr	String	■ IFF(IsNullOrEmpty(Reco	/ Edit
	😅 dst	IP Address	▼ Record("dst")	/ Edit
	dst_category	String	▼ Record("cat")& " - "ℜ(/ Edit
	Dst_country	String	✓ iff(field("Dst_net_area")=	/ Edit
	Dst_name	String	ExecRDNS("RDNS",field	/ Edit
E 😝 Eddaps	Dst_net_area	String	ExecRDNS("RDNS net a	/ Edit
	Dst_www	String	Split(Record("hostname"	/ Edit
	elapsed	Float	Record("duration")	/ Edit
	EmptyString	String	•	/ Edit
	File_type	String	■ IFF(InStrRev(Record("file	/ Edit
	- TOA	loc:		7 - 414

28. Modify the Value from: ExecRDNS ("RDNS net area", Field ("dst"))

🖹 Field Editio	n Web Page Dialog	
₿ E d i t	Field	
Name :	Dst_net_area	
Type :	String	•
Value :	ExecRDNS("RDNS <mark>net area</mark> ",Field("dst"))	
Comment :		
	OK Cancel &VbScript	
		-

To: ExecRDNS(field("RDNS_Client"),Field("dst"))

🕙 Field Editio	m Web Page Dialog	
₿Edit	t Field	
Name :	Dst_net_area	
Type :	String	•
Value :	ExecRDNS(field("RDNS_Client"),Field("dst"))	
Comment	:	
	OK Cancel &VbScript	



29. Click **OK**. The **Fields** screen appears in the central pane.

30. Select **Console root> NetReport> localhost> ULA** in the left **Console root** pane.

Note: the asterisk to the right of the ULA branch indicating that you must apply all the changes you have made.



31. Click the Apply Changes button.