

Site Reliability Engineering with Phantom

Tanuj Arcot, Victor Menezes, Tim Pacl

Dell Technologies



Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved

Tim Pacl

Splunk Architect | Dell Technologies



Victor Menezes

Splunk Admin | Dell Technologies

A vibrant collage of global landmarks and activities. In the center is a large, multi-colored rainbow. To the left, a man in a grey jacket and black shirt is skydiving. Below him is a small car. To the right, a woman in a black shirt and jeans is also skydiving. The collage includes various world landmarks: the Eiffel Tower, the Golden Gate Bridge, the Taj Mahal, the Sphinx, the Leaning Tower of Pisa, and the Sydney Opera House. There are also hot air balloons, a satellite, and a city skyline on the far left. The background is a mix of orange and pink hues.

Victor Menezes

Splunk Admin | Dell Technologies

A vibrant collage of global landmarks and activities. In the center is a large, multi-colored rainbow. To the left, a man in a grey jacket and black shirt is skydiving. Below him is a small car. To the right, a woman in a black shirt and jeans is also skydiving. The collage includes various world landmarks: the Eiffel Tower, the Golden Gate Bridge, the Taj Mahal, the Sphinx, the Leaning Tower of Pisa, and the Sydney Opera House. There are also hot air balloons, a satellite, and a city skyline on the far left. The entire scene is set against a white background with a grey horizon line at the bottom.

Tanuj Arcot

SRE Architect | Dell Technologies



Agenda

SRE with Phantom

Phantom.

It's not just for security anymore!

1) What is SRE?

What is Site Reliability Engineering?

2) Why Phantom for SRE?

What Phantom delivers for SRE

3) Walkthrough: Investigate

Fraud Investigations, DB Investigations

4) Walkthrough: Remediate

IIS Remediations, Forwarder Remediation

5) Walkthrough: Extending Phantom Playbooks

Integrating with ServiceNow, Teams, Twilio, and more

6) Call to Action

How can you get started

What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”.

What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”. Primary objectives are:

1. Improve Observability

What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”. Primary objectives are:

1. Improve Observability
2. Reduce MTTF
 - Mean Time to Find Issues

What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”. Primary objectives are:

1. Improve Observability
2. Reduce MTTF
 - Mean Time to Find Issues
3. Reduce MTTR
 - Mean Time to Resolve Issues

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Splunk Users

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk

- Scheduled / Interval Pull of Splunk Data into Phantom

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk

- Scheduled / Interval Pull of Splunk Data into Phantom
- Interval Push Splunk Data into Phantom

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk

- Scheduled / Interval Pull of Splunk Data into Phantom
- Interval Push Splunk Data into Phantom
- Trigger Push of Splunk Data into Phantom with Splunk Alert

Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk

- Scheduled / Interval Pull of Splunk Data into Phantom
- Interval Push Splunk Data into Phantom
- Trigger Push of Splunk Data into Phantom with Splunk Alert
- Trigger Phantom Playbook Execution from Splunk Alert

Why Phantom for SRE?

Data-driven Orchestration

Why Phantom for SRE?

Data-driven Orchestration

- Key Differentiator Compared to other Orchestration Tools

Why Phantom for SRE?

Data-driven Orchestration

- Key Differentiator Compared to other Orchestration Tools
- Making Our Data Truly Actionable!

Why Phantom for SRE?

Data-driven Orchestration

- Key Differentiator Compared to other Orchestration Tools
- Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation

Why Phantom for SRE?

Data-driven Orchestration

- Key Differentiator Compared to other Orchestration Tools
- Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation

- Doing More with What We Have

Why Phantom for SRE?

Data-driven Orchestration

- Key Differentiator Compared to other Orchestration Tools
- Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation

- Doing More with What We Have
- Reacting Quicker to What is Happening

Why Phantom for SRE?

Data-driven Orchestration

- Key Differentiator Compared to other Orchestration Tools
- Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation

- Doing More with What We Have
- Reacting Quicker to What is Happening
- Reducing the Cost of What We do

Why Phantom for SRE?

Keep the lights on for legacy platforms

Why Phantom for SRE?

Keep the lights on for legacy platforms

- Broad Compatibility with Both Container and Legacy Platforms

Why Phantom for SRE?

Keep the lights on for legacy platforms

- Broad Compatibility with Both Container and Legacy Platforms

Agentless Action

Why Phantom for SRE?

Keep the lights on for legacy platforms

- Broad Compatibility with Both Container and Legacy Platforms

Agentless Action

- No Agent Software to Install 😊

Why Phantom for SRE?

Keep the lights on for legacy platforms

- Broad Compatibility with Both Container and Legacy Platforms

Agentless Action

- No Agent Software to Install 😊
- Using APIs and Existing Tools to Take Action

Why Phantom for SRE?

Keep the lights on for legacy platforms

- Broad Compatibility with Both Container and Legacy Platforms

Agentless Action

- No Agent Software to Install 😊
- Using APIs and Existing Tools to Take Action

Native Extensibility



Walkthrough: Fraud Use Case

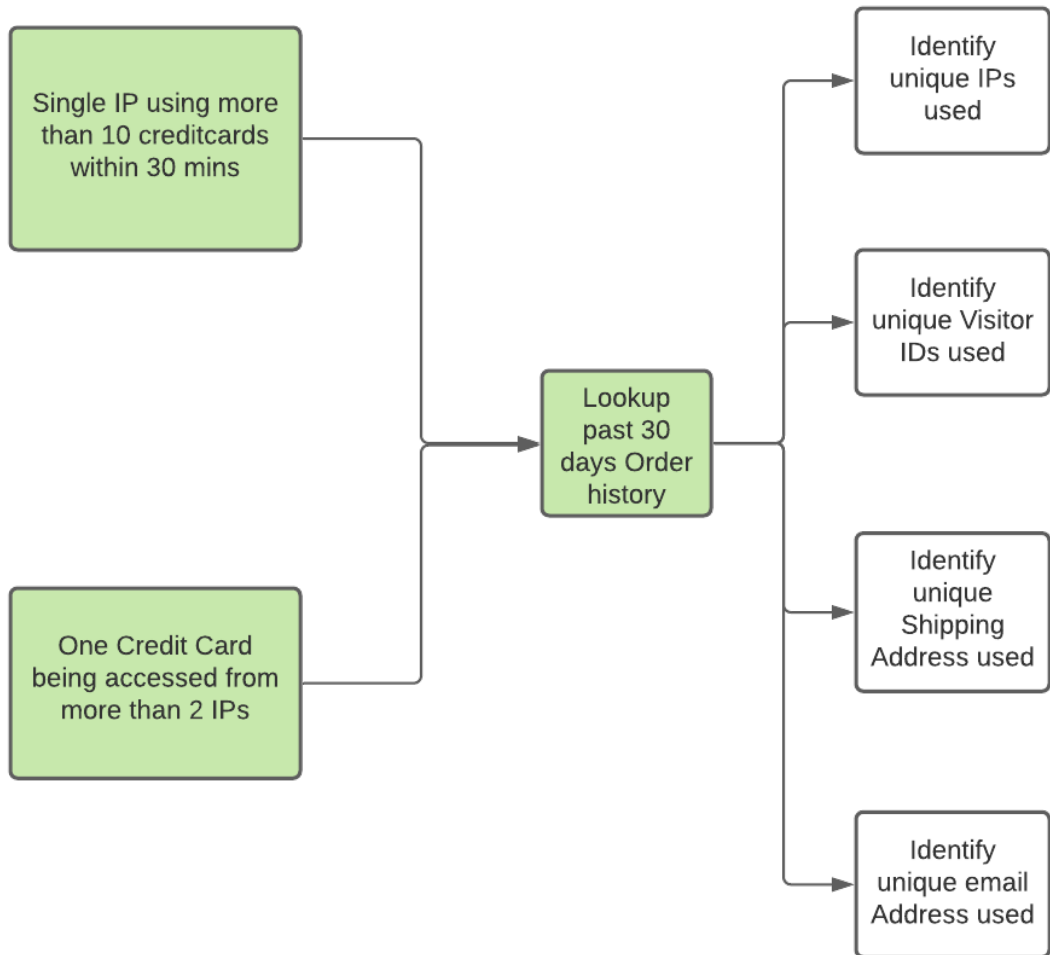


Credit Card Fraud Investigations

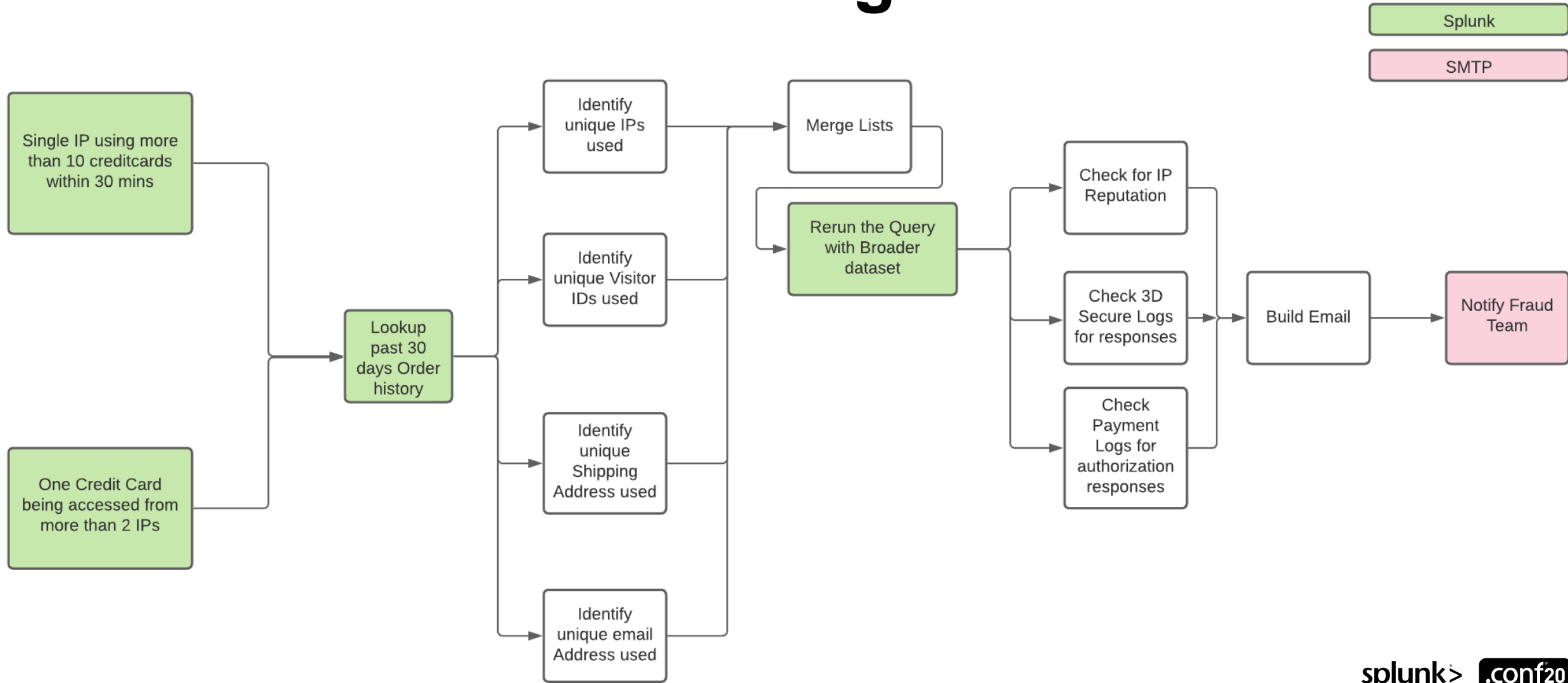
Single IP using more
than 10 creditcards
within 30 mins

One Credit Card
being accessed from
more than 2 IPs

Credit Card Fraud Investigations



Credit Card Fraud Investigations



Results

Splunk Alert - Last 4 hours Activity										
IP Address	IP Country	Country	Earliest Time	Latest Time	Visitor IDs used	Cart IDs used	Credit Cards used	Avg time per IPAddress	Total Time Spent	
11.14.137.145	South Korea,United States	United States	08/26/20 06:32:06	08/26/20 08:18:05	3	5	1	35 minutes	106 minutes	
Credit Card Salted Hash										
5E2E86AAABF1CCF11F1E2A63CE39A807ACA2B06DF7CAAF3F34AF09C1985EE066E74F3494DC65032E7F30F23BE35F0DB6DA5B11C783D7F68EDEE6F78E344B188D										

Activity Overview for the last 30 days															
Order Submissions	IP Address used			Email Addresses used			MCMID used			Shipping Street Address used			Products purchased		
Total Orders 6		Order Count	Revenue		Order Count	Revenue		Order Count	Revenue		Order Count	Revenue		Order Count	Revenue
Order Value 636,495.95	138.14.137	1	799.19	vsgf742@naver.com	5	3,995.95	82392589500463381893533350636562709904	3	2,397.57	5515 NE 148TH AVE STE 302 BB 63	4	3,196.76	Inspiron 15 5000	5	3,995.95
	117.14.145	2	1,598.38	wlsqndy2@gmail.com	1	632,500.00	61252739729676864324017796155658197479	1	799.19	2 28 703	1	632,500.00	Dell 27 Gaming Monitor - S2721DGF	1	632,500.00
	14.14.145	3	634,098.38				651769595685852941381937539700080306	1	632,500.00	5515 NE 148TH AVE STE 302 #B 63	1	799.19			
							30005350285230246733325671746533334499	1	799.19						

Results

ThreeDSecure Overview for the last 30 days						
IP Address	Total Hits	Authentication Successful (Y)	Authentication Attempted (A)	Authentication Failed (N)	Authentication Unavailable (U)	Empty
117.111.15.14	2	2	0	0	0	0
138.6.8.137	1	1	0	0	0	0
14.4.4.145	2	2	0	0	0	0

Transactions for the last 30 days								
Time	Dpid	MCMID	IP Address	Email	Payment Info	Shipping Address	Product	Order Total
08/26/2020, 08:18	2006-1320612	82392589500463381893533350636562709904 Logged In?:True	138.6.8.137	vsg6742@naver.com	PaymentType: CreditCardMasterCard GPID: 9f5a0829-9071-4185-8999-8f8801640775 isCCVerified: true	5515 NE 148TH AVE STE 302 Bldg 8 Portland, OR 97221, us	Product ID: nn5505efpps Product Name: Inspiron 15 5000	799.1
08/26/2020, 07:50	2006-11249053	82392589500463381893533350636562709904 Logged In?:True	117.111.15.14	vsg6742@naver.com	PaymentType: CreditCardMasterCard GPID: dc330ff9-b7cd-4517-835d-ab09c0a7e867 Status: FAILURE isCCVerified: true bepResponseCode: 530 bepResponseMessage: Do Not Honor AuthDescription: Generic decline - No other information is being provided by the issuer. AuthReason: 2 - REFUSED - REFUSED	5515 NE 148TH AVE STE 302 Bldg 8 Portland, OR 97221, us	Product ID: nn5505efpps Product Name: Inspiron 15 5000	799.1
08/26/2020, 07:16	2006-1087194	82392589500463381893533350636562709904 Logged In?:True	117.111.15.14	vsg6742@naver.com	PaymentType: CreditCardMasterCard GPID: 09295672-8485-4a77-b874-c8543fb0697c Status: SUCCESS isCCVerified: true bepResponseCode: 100 bepResponseMessage: No reason to Decline AuthDescription: Approved AuthReason: OK	5515 NE 148TH AVE STE 302 Bldg 8 Portland, OR 97221, us	Product ID: nn5505efpps Product Name: Inspiron 15 5000	799.1

Results

Splunk Alert - Last 4 hours Activity									
IP Address	IP Country	Country	Earliest Time	Latest Time	Visitor IDs used	Cart IDs used	Credit Cards used	Avg time per Credit Card	Total Time Spent
177.110	Brazil	Brazil	08/26/20 08:57:11	08/26/20 10:43:48	1	1	34	3 minutes	107 minutes
Credit Card Salted Hash									
00D4782193482D7FB1D1918E80C237703D89DE154E6C5E407EF00660189FC93A666FF3D4EDE97C6F79D96582E2EFC439EBE2AA7C723168D20F356185BF509F02 01004491D201470630916A6C1F4877EA0DE7713D46EA60044BD53A4D80960B0998DF0A84A464C8CAE3B6BB12266780EF2FD226FF83F173D57FCB4F490C1FA1CE 20146480674047DE1201664C86BB45FFDE9408A6524F1DC839C351B4DD52BE00899CAE40769392654D697FB00594CE1A09A92A93BBF070D773ED3089E3509ED8 2157209F76B461660EEB38890F192274D39E72D75F2603AD79142F7AEEA51EC5583811E9DBAD8E6B2968B7CD89D3AE724BC789746078EF63C9FF913B335702EC 225C3B03773A135B17B793627F2127DE27C79A5276AF0E6A7C3DBEE011A9F28A73039B72A707811FFD6275169549A786ECA1DAEFF16683EA59C647F4A3205A8A 22695D6030F41D7E656B31D88873AAB82743EAB942CC4FD340489DB33F39443D70802A1EA70726EA3985A3B6F91D5C2A023B6D3F65416D5081FD57AC5E354FC9 2AA63319FEF24C1388E324EDB2D3940E5EC7F471A50148434C7948B1A907831411622AAE44150B1F3963476183687EEF00202DC83EE561C56E48DFB12A10BCED 2B912DAE511CC32E728F3AE55BB950959B91BA7DF28A9D11783F828B9395AA0ECF39E9291727F7D69534C8C055BB382CAE18C624BDE6F2EEDD36E6F16845D1AA 3F325032ACA7B753B8997AE9D4E35243079F30F92D7BA60EDB33087DA5F42A58BD81FBC6C82A3577299AF5CC11FFB3154DEF21B4F1C1B8A8ECF6D76BE1AADE5A 40AAA95E30398C051E9CEE66C926BAD9223B9357AD947E0CA45AA3F522A3C4F248503547D194680BCF307ACD6E546EC391D82653F98B14A743012B6F0279B57D 5114D0EFA970CEB50841433ADAE650E28AA40336534C8D776E4517D4D9CF70FB00D79F75194CED7016B0ED41EC201B76F1DCA1B81E91E32F925D98F76891C1 6A2FADC8982F69EDCF6447E15F8284CE7DF0CE119CB23A7A14442598107A47254C79562E53A2C1DBC7ADAF25B4C1288CD3C72640104345EA945F81781901E136 742E58BD9A0AC200693E58A5BE8E6E3A1B3A86A2BDFD932363E1F377A9DA86AD7355F2B58AC02575893930723A9F2AE381A2FB2EE54D4F435DE68A7C1AC1B9BB 918B282135690D6C8D9E54389517A30B81E4B6F920AB9A0A19FE78A8584B525E57E9E18BC93E5AE7E20D59EA3458C95DE2019123887B8DA4295DADE59043B196 94CAC7B08E1769173FA42D3A562D4BDAE9E814239C7F9B0AAB220F2F2B7B5340F4605DBF500FF3C3706E862D88D6B863DDAD8B679DFCA0B05C8DE2C66C4DCB3A 95F3E5D66E6F93F206CAE06BCE5B22E519DFAA62D31E0BC94C155303884F658B073DD33ACA4E1732240020082A928F5EC8182380E978E4A888E7F2217D4B78FB A5CAEC14F7F4A76FB69679E0B23366B75E751F8E56D30B8AA6C817505C62ECOD258CA6A10FFD2DCBF8A503F3A5969E1862DB7373D320767BA9F17CE472C1CA76 A8F5A8A4844054E6565512E048821A116631E71E83399A0C0BD832673F26026FA347238545E27A65D9E626B4C98D4F79DF355A1DCE5B725560A0D3388A24318A A9A18D3F7F64BF7E617C9727C7EB17E1BE890B5FD6B113688543A474CFE5FB934A605D85071B561B615AFB2B15420B18F09154598464607B7DB2FA5187116ED AF62FE8BF487823083BC27B40598D00EE70D3F5528C511B1EF0D2C8969C33A62DD18FBCDFA70CD644308669652A601DC16317981201032587885F6C8318D1E10 BCDB689F337761D52C23320658541805AB509B6E15D054DAD5F0A476C381865A6F4E6685E89003094A55B477AC81ED0A58BFAC3478C7E0B040D70A8BD0DE07D6 BE5DC6CC00851AD24530A19297CE04F7DE7D1A7185FCCF8EDE632FC38760D3F30F595727A17D5B7C0721DAB54CDB0C18BD8F30D4B85468369BF478D639EA295C BFD0CA37EBDAE4C5F761C27C207081B63766D6C936EB62F8B5C9AD82706AC6D3712C028CD2E1C9286A902F08764388CE9D3629DD6A0B5F426E49C5EC97846812 C88DB17683B4E5D0A7A2E2267C5C96C61E88B044B8845A6398825EB8355A62888C14A9F607084A80DE0E28E86AC929FB5D9593A9D003BDA94F044A5835772758 CBCDAF6B39A5DFC93184D45F2A88BC22D1C391206F92DB6E50B0F9C8F4CAAA4C6F4238573D6AB85D03DAB43AD16350A044A26FEE9941E2DDCA6F00625924D63A D046D45C0685DCE43B962EB9C779CFE0D96119BE098B9EFAB27CE260598D20EE6949232DC829B0A37242C35A526594805BFCE688C2D9528EB8EFB9BF3D855A7 D5ED7DEB2DEFBF7A8FE96527F68765D5D802C6F6315D8C5D8019E49D0352D6D81D852110E1AEA55C2E392E3C9A7CA6ED7510BDFE816C2A95F3DA88A80EE01C69 D6C2CC4750BD560AAB53AA328CB409BF8975D5138D0E6EDDC6BC35C8513D684820320916D0FB51745EAD3760D3F3E16753AE6DF1748FF8C7B4E9277CD632774 D74048147D54672889FF19424E5653572FD0E9E7015E60FB2C90701776F683C297B08DB9CF6F2F1355CCFF21A417E62E94C05153D1987792AC9748966E985F0 E36621FCFF690695659B80FE7C776BEB3FCEE7959F18FD7EFC20E6EB1E6CA1F6646A7CC6AC25EE7AE271467BDD45F41F4A3B3E444462155FB112AA53D5AA513 E836A86A7FB2AA9C5875E9C3179FFF1979BA7414194FF25A8AED4956CDBA01DB3258E6E520558755E86AA8A07ED0A7B96AA574FD4BAA3E9C4F369982CFFE1630 F99002DBA67211E4AEE9F6FB85D80AC01591086172486A9409B1ED38614460051AA485426EB0478F2BF9E6BA1BA2BAFDE331F1EBC35EB31D645F8D251E0CD535 FA56808FD1854DC2A08BD8C482300BF8CD10E1179EE3E39948A3778DA96CA4DB126569E8A8AF85E9A0C254B958DE16234B86426B9B3AFF49D45FB6F1AC8FB209 FC0613388CBA9F6395882D1A6B100CD5D88682833E919C537F5CAF82A4DFA25410219926BF4641C7B1052E725D4DC1921F000B5ABC152D063E636B7F04E91704									



Walkthrough: DB Investigation



Database Investigations

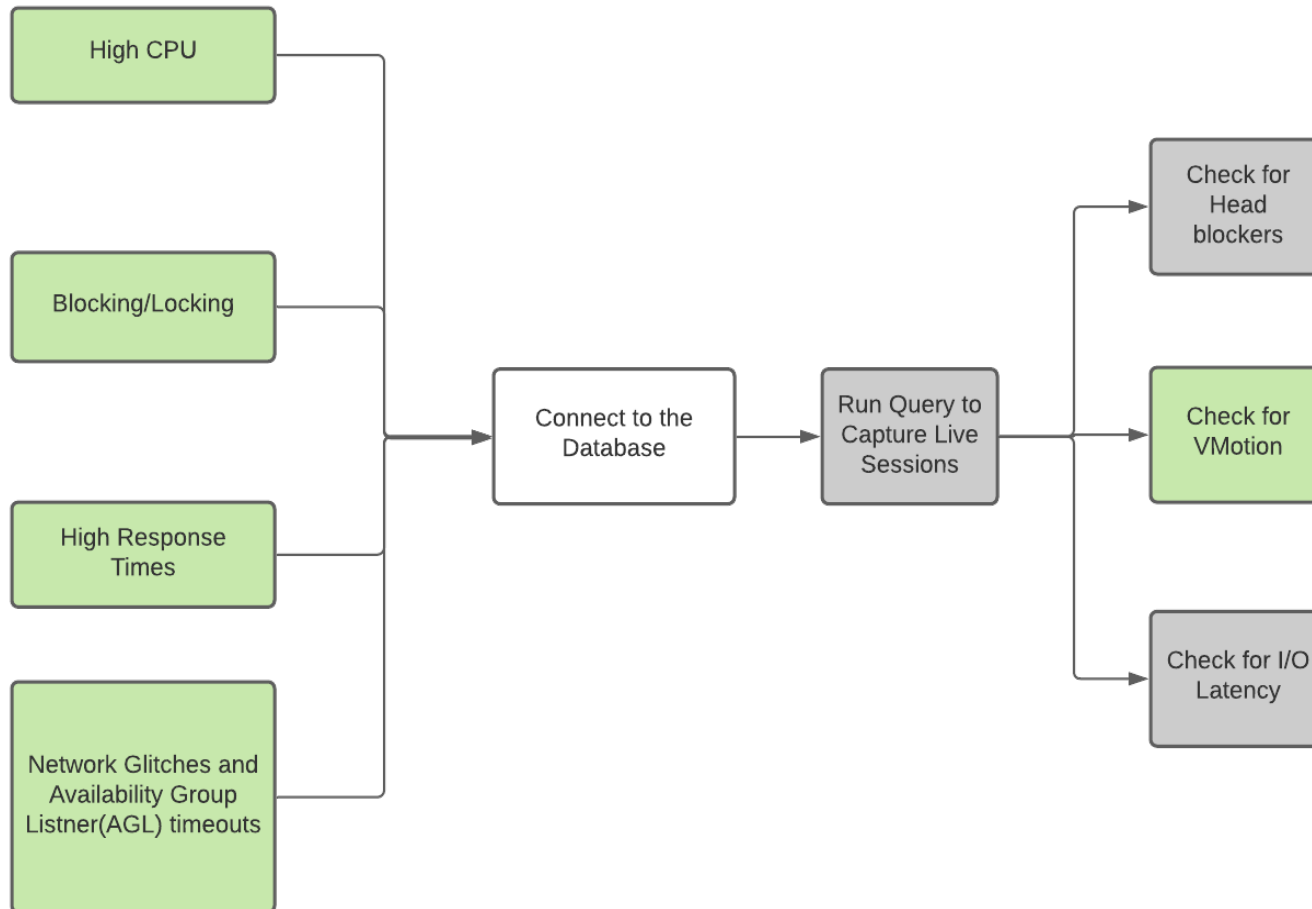
High CPU

Blocking/Locking

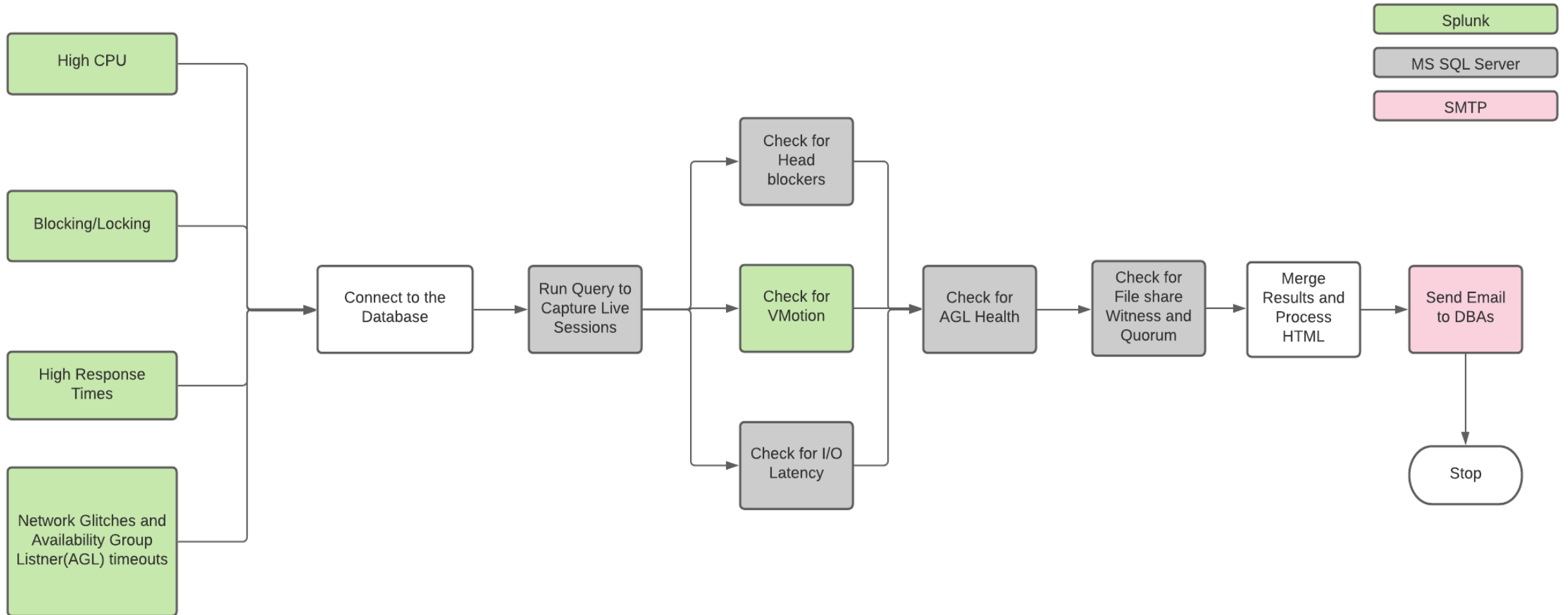
High Response
Times

Network Glitches and
Availability Group
Listener(AGL) timeouts

Database Investigations



Database Investigations



Results

AG Quorum Details

Member_Name	Member_State_Desc	Member_Type_Desc	Number_of_Quorum_Votes
AUSPWB2BDB01	DOWN	CLUSTER_NODE	1
AUSPWB2BDB02	UP	CLUSTER_NODE	1
File Share Witness	UP	FILE_SHARE_WITNESS	1

AppDB	Host	Message
B2B	AUSPWB2BDB02	2020-07-22 08:55:17.00 spid266 The availability group GLOBALB2BAG01 is not healthy. Current primary: AUSPWB2BDB02

AGL Health Status

AG Name	AG Replica Node	AG Replica Role	DBName	AG Sync State	AG Sync Health State	AG Summary State	AG Availability Mode	AG Failover Mode	Redo Queue Size MB	Log Send Queue Size MB	Is Failover Ready?	Suspend Reason	DB Tlog Reuse Wait	DB State	AG Sync Time	AGL
GLOBALB2BAG01	AUSPWB2BDB02	PRIMARY	B2B_Log	SYNCHRONIZED	HEALTHY	ConnectedState: CONNECTED OpState: ONLINE RecoveryState: ONLINE	SYNCHRONOUS_COMMIT	AUTOMATIC	None	None	True	None	AVAILABILITY_REPLICA	ONLINE	LastHardenedTime: None LastCommitTime: 2020-07-22 09:16:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB02	PRIMARY	B2B_Staging_Log	SYNCHRONIZED	HEALTHY	ConnectedState: CONNECTED OpState: ONLINE RecoveryState: ONLINE	SYNCHRONOUS_COMMIT	AUTOMATIC	None	None	True	None	NOTHING	ONLINE	LastHardenedTime: None LastCommitTime: 2020-07-22 09:16:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB02	PRIMARY	b2b_Tools	SYNCHRONIZED	HEALTHY	ConnectedState: CONNECTED OpState: ONLINE RecoveryState: ONLINE	SYNCHRONOUS_COMMIT	AUTOMATIC	None	None	True	None	NOTHING	ONLINE	LastHardenedTime: None LastCommitTime: 2020-07-22 09:15:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB02	PRIMARY	QAToolsGlobal	SYNCHRONIZED	HEALTHY	ConnectedState: CONNECTED OpState: ONLINE RecoveryState: ONLINE	SYNCHRONOUS_COMMIT	AUTOMATIC	None	None	True	None	LOG_BACKUP	ONLINE	LastHardenedTime: None LastCommitTime: 2020-07-22 09:02:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB01	SECONDARY	B2B_Log	NOT SYNCHRONIZING	NOT_HEALTHY	ConnectedState: DISCONNECTED OpState: None RecoveryState: None	SYNCHRONOUS_COMMIT	AUTOMATIC	0	None	False	None	AVAILABILITY_REPLICA	None	LastHardenedTime: 2020-07-22 08:54:00 LastCommitTime: 2020-07-22 08:54:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB01	SECONDARY	B2B_Staging_Log	NOT SYNCHRONIZING	NOT_HEALTHY	ConnectedState: DISCONNECTED OpState: None RecoveryState: None	SYNCHRONOUS_COMMIT	AUTOMATIC	0	None	False	None	NOTHING	None	LastHardenedTime: 2020-07-22 08:54:00 LastCommitTime: 2020-07-22 08:54:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB01	SECONDARY	b2b_Tools	NOT SYNCHRONIZING	NOT_HEALTHY	ConnectedState: DISCONNECTED OpState: None RecoveryState: None	SYNCHRONOUS_COMMIT	AUTOMATIC	0	None	False	None	NOTHING	None	LastHardenedTime: 2020-07-22 08:33:00 LastCommitTime: 2020-07-22 08:32:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')
GLOBALB2BAG01	AUSPWB2BDB01	SECONDARY	QAToolsGlobal	NOT SYNCHRONIZING	NOT_HEALTHY	ConnectedState: DISCONNECTED OpState: None RecoveryState: None	SYNCHRONOUS_COMMIT	AUTOMATIC	0	None	False	None	LOG_BACKUP	None	LastHardenedTime: 2020-07-22 08:33:00 LastCommitTime: 2020-07-22 08:32:00	AGL: GLOBALB2BAGL01 AGL IPs: ('IP Address: 10.191.13.17' or 'IP Address: 10.191.15.17')

[illegible]



Walkthrough: Windows Webserver Auto Remediation



Windows Webserver Auto Remediation

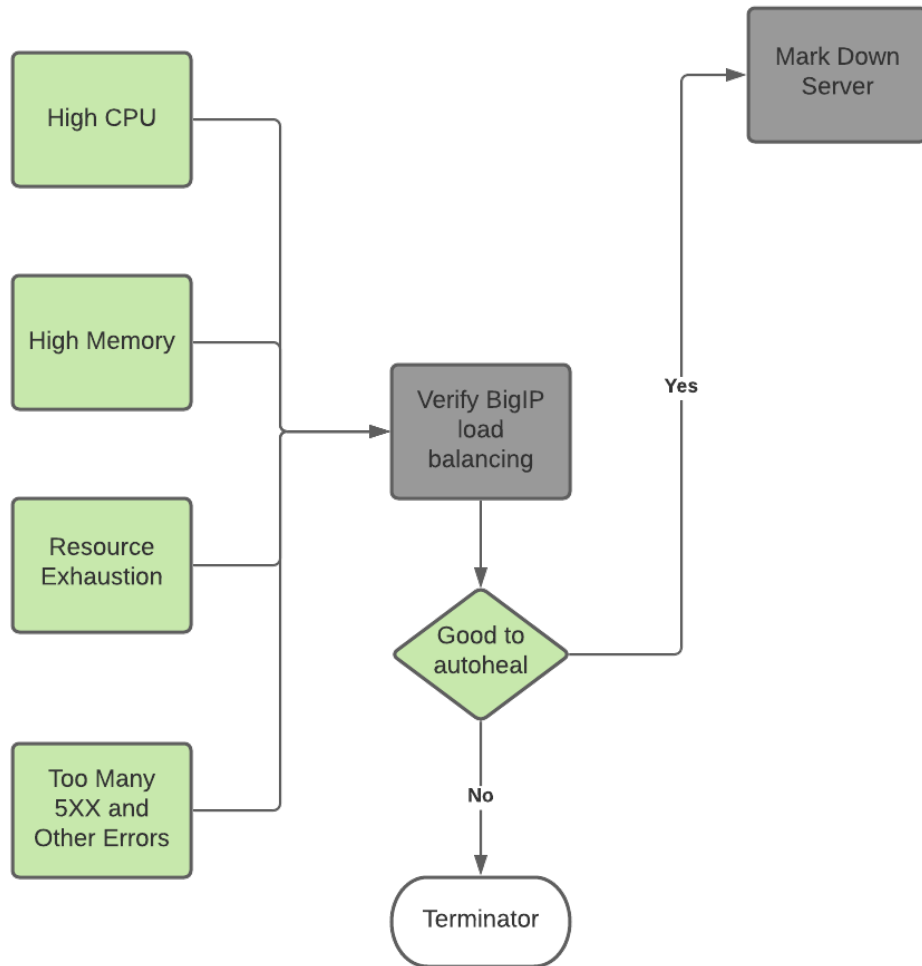
High CPU

High Memory

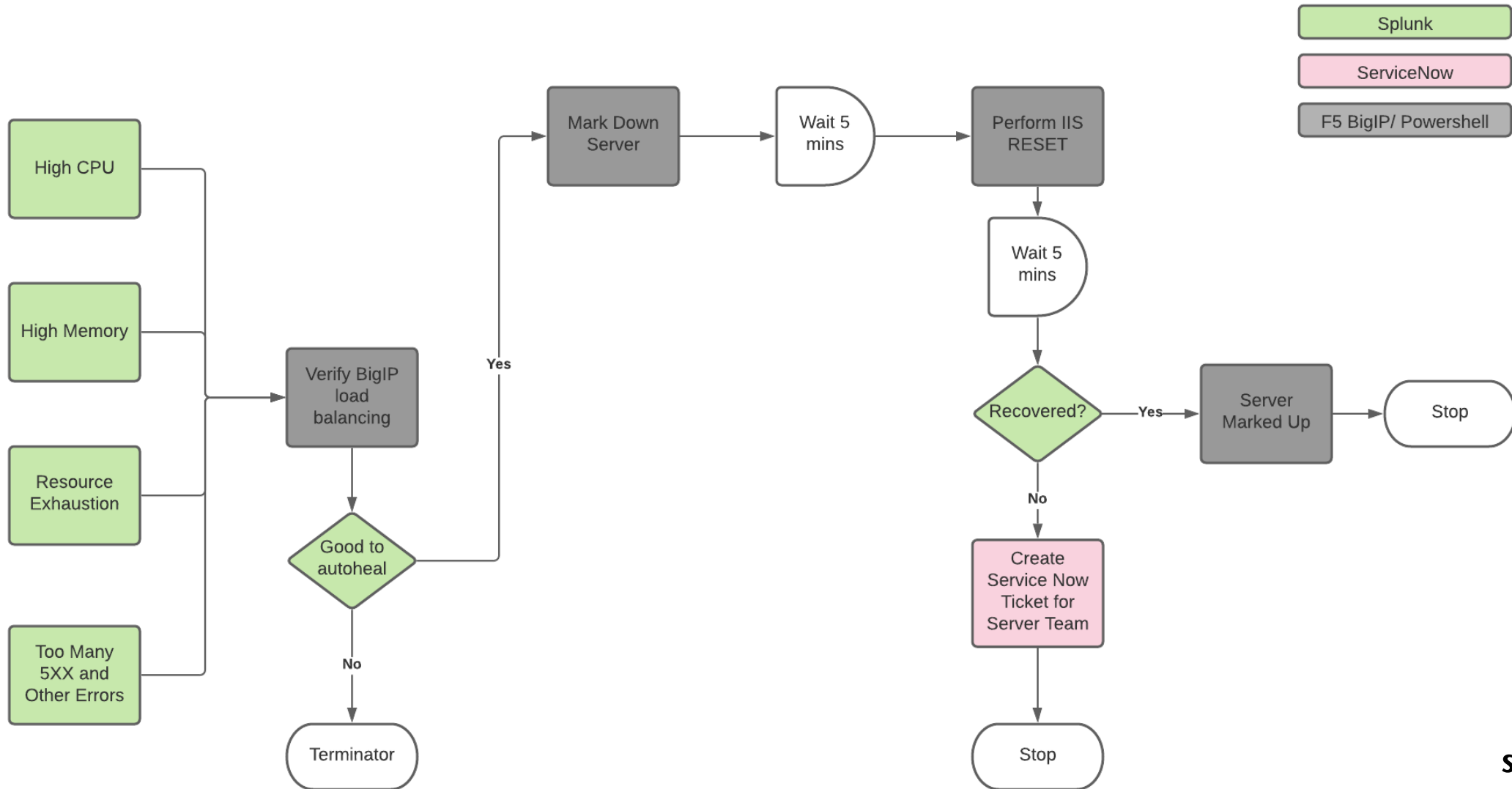
Resource
Exhaustion

Too Many
5XX and
Other Errors

Windows Webserver Auto Remediation



Windows Webserver Auto Remediation



Results

Splunk Alert	
Server	P60 [REDACTED] 4.aus.amer.dell.com
IP Address	No Data
Load Balanced?	Yes
Troux ID	1000236
Application Name	DCQO Gii Quote Gateway
Segment	PEO
Symptom/Issue	Resource Exhaustion

Script Results				
Action	Status	Message	Pool Name	Controller IP
Mark Down	Success	Mark Down performed successfully!	/Common/giiopenbasket-svc-p60	10.177.12.4
Mark Down	Success	Mark Down performed successfully!	/Common/giiopenbasket-svc-p60-1010	10.177.12.4
Mark Down	Success	Mark Down performed successfully!	/Common/giiopenbasket-svc-p60-1210	10.177.12.4
Mark Down	Success	Mark Down performed successfully!	/Common/giiopenbasket-svc-p60-443	10.177.12.4
IIS RESET	Success	IIS Reset Completed Successfully		
Mark Up	Success	Mark Up performed successfully!	/Common/giiopenbasket-svc-p60	10.177.12.4
Mark Up	Success	Mark Up performed successfully!	/Common/giiopenbasket-svc-p60-1010	10.177.12.4
Mark Up	Success	Mark Up performed successfully!	/Common/giiopenbasket-svc-p60-1210	10.177.12.4
Mark Up	Success	Mark Up performed successfully!	/Common/giiopenbasket-svc-p60-443	10.177.12.4

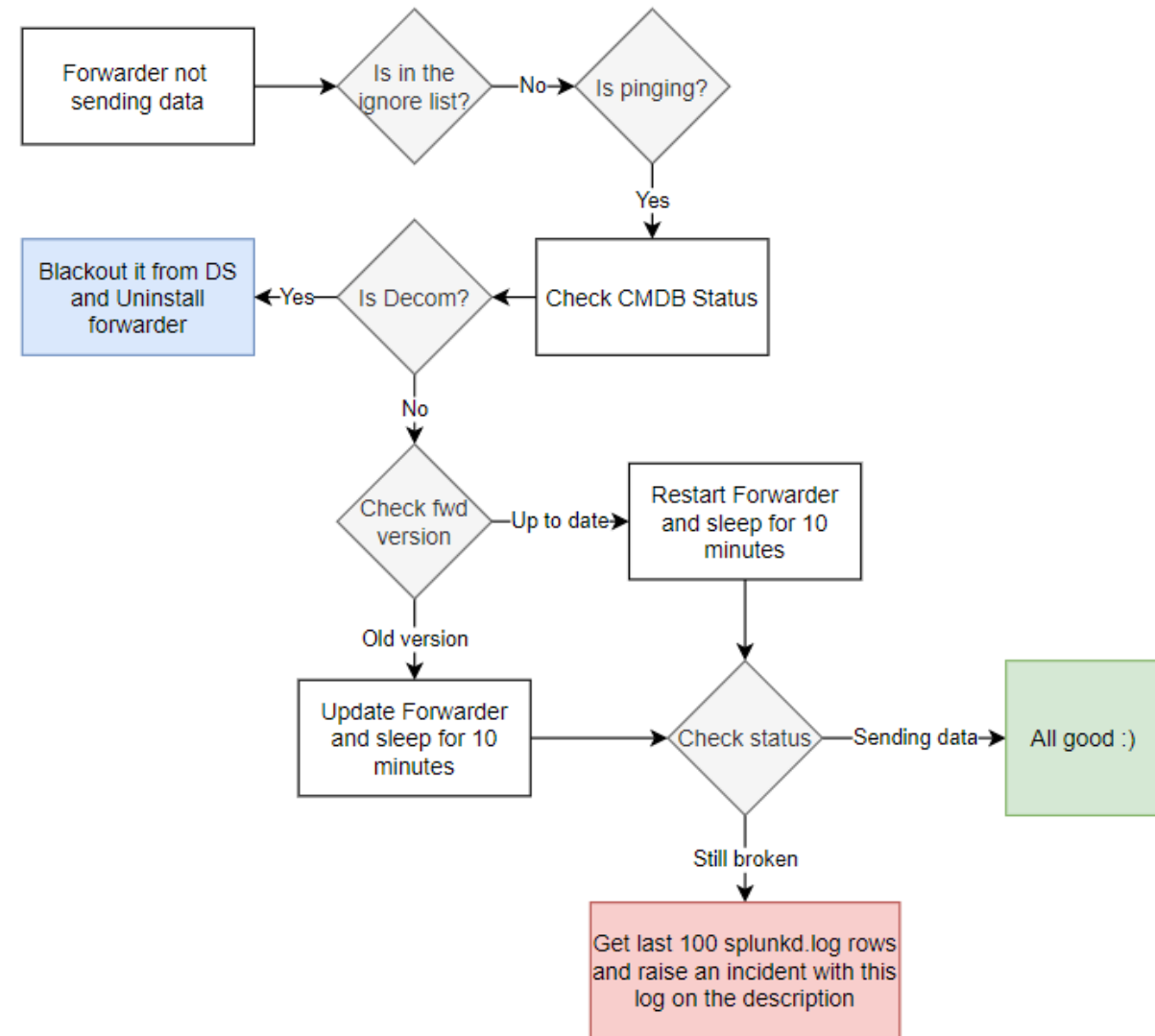


Walkthrough: Forwarder Remediation



Walkthrough

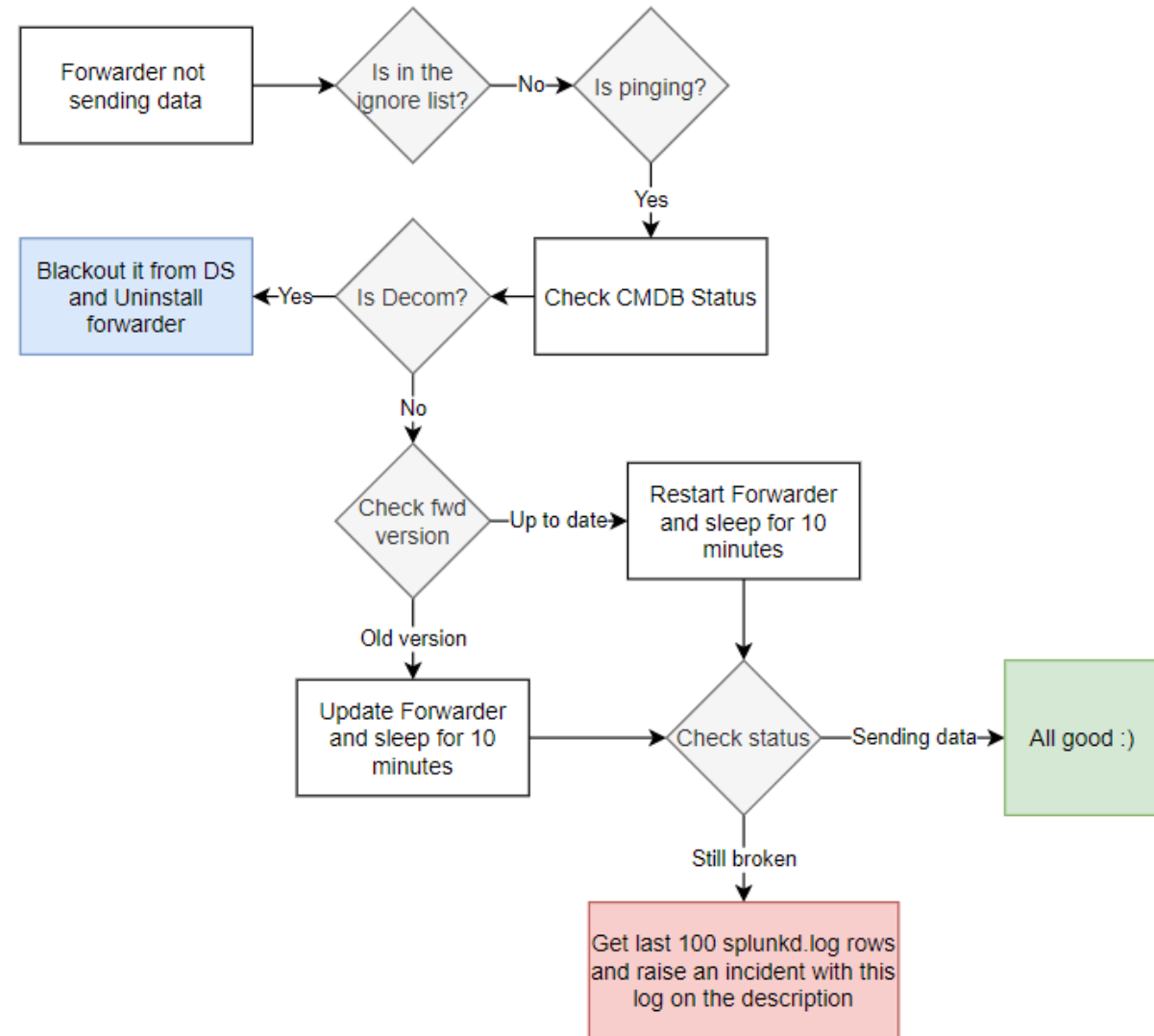
Splunk forwarder remediation – is pinging



Walkthrough

Splunk forwarder remediation – is pinging

Manipulate filesystem files

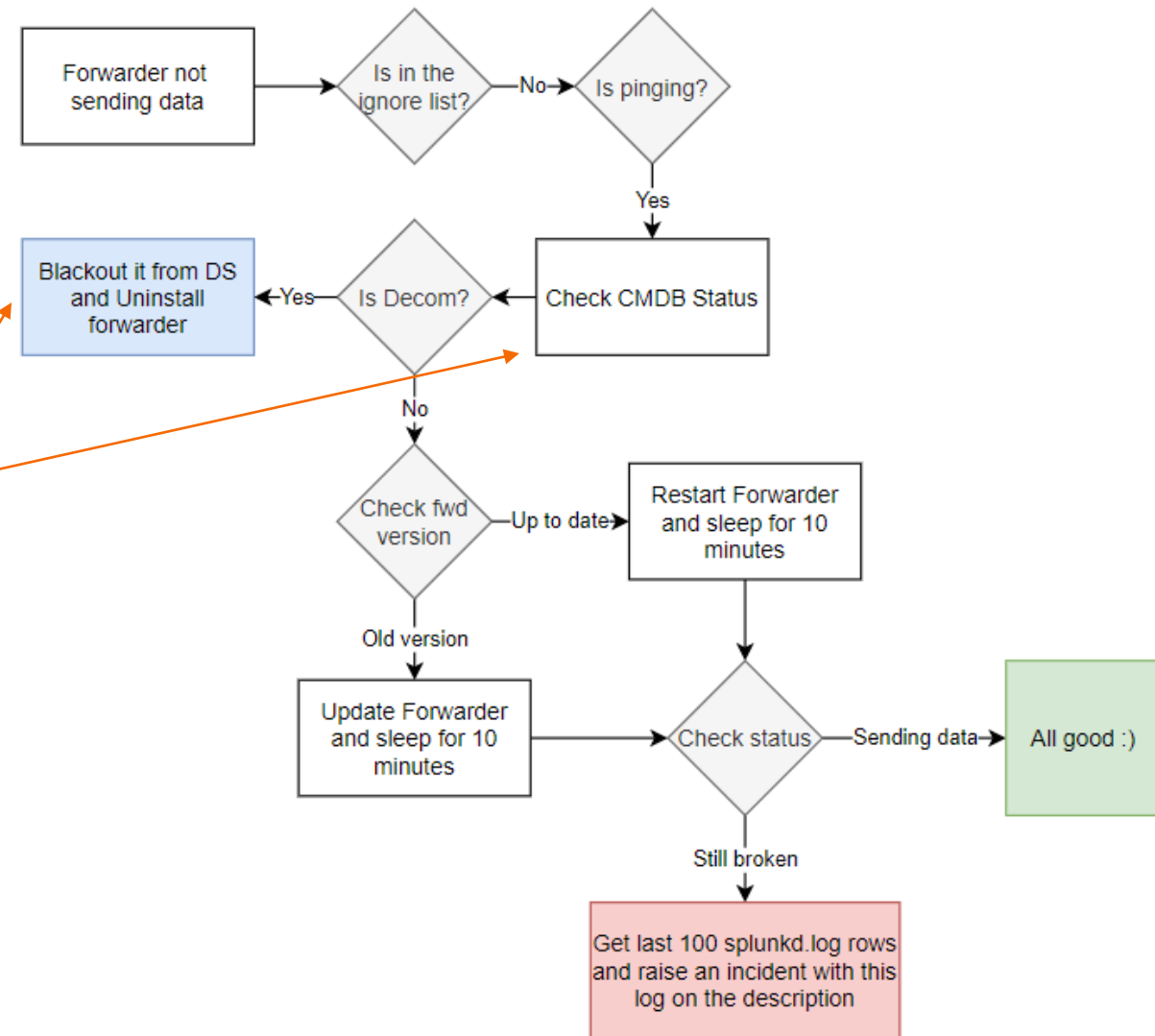


Walkthrough

Splunk forwarder remediation – is pinging

Manipulate filesystem files

Call API endpoints



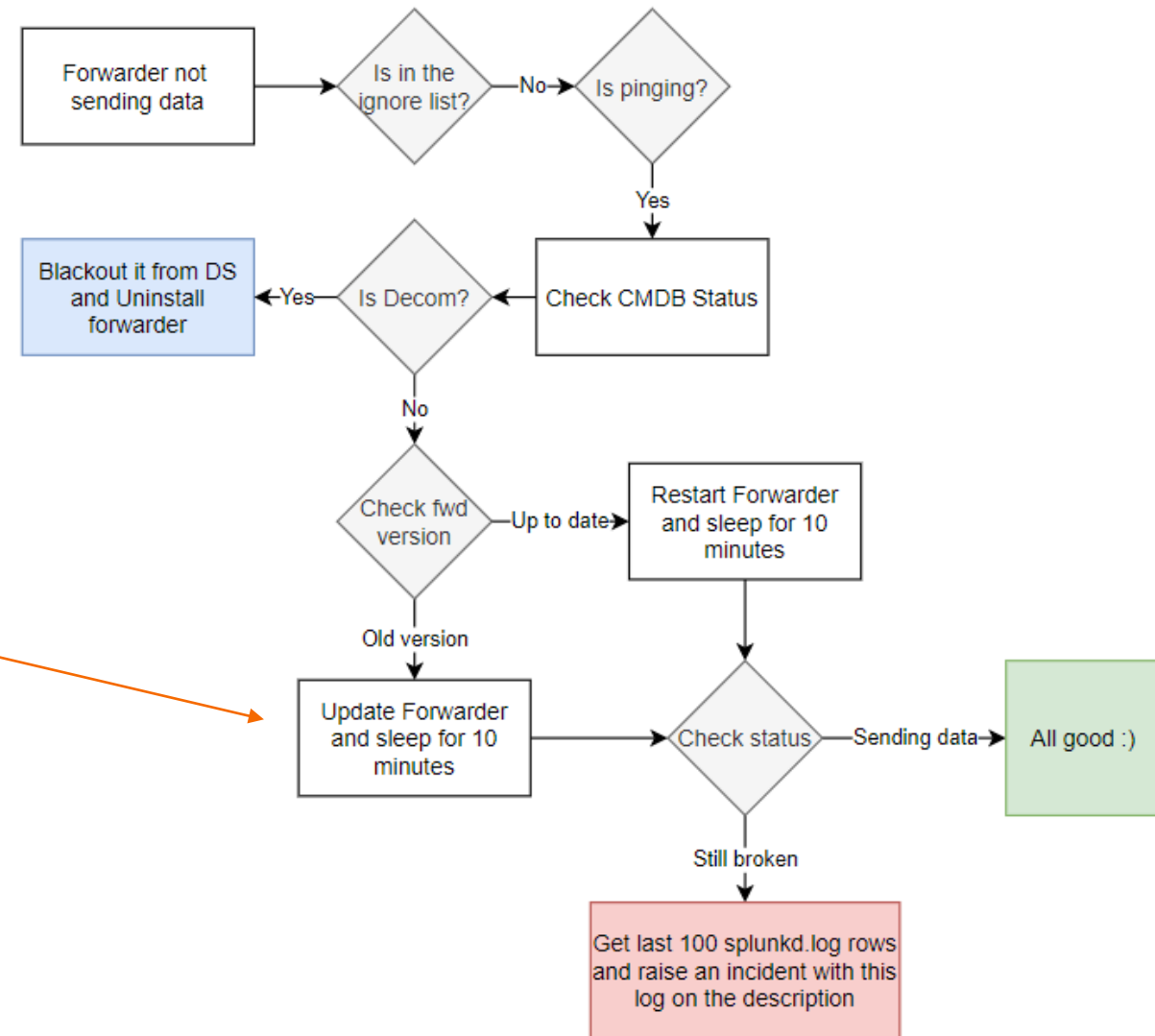
Walkthrough

Splunk forwarder remediation – is pinging

Manipulate filesystem files

Call API endpoints

Keeps the forwarders up-to-date



Walkthrough

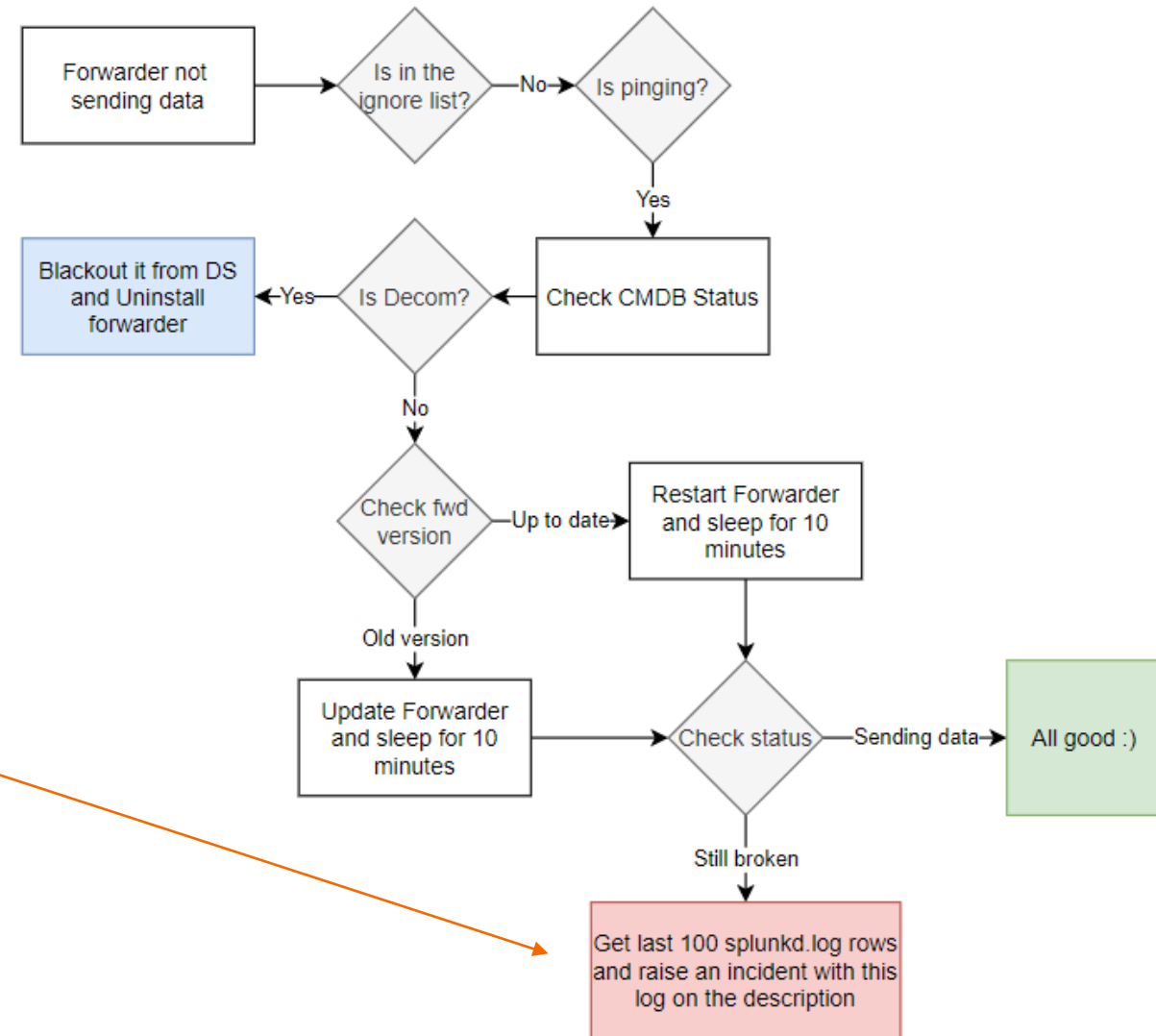
Splunk forwarder remediation – is pinging

Manipulate filesystem files

Call API endpoints

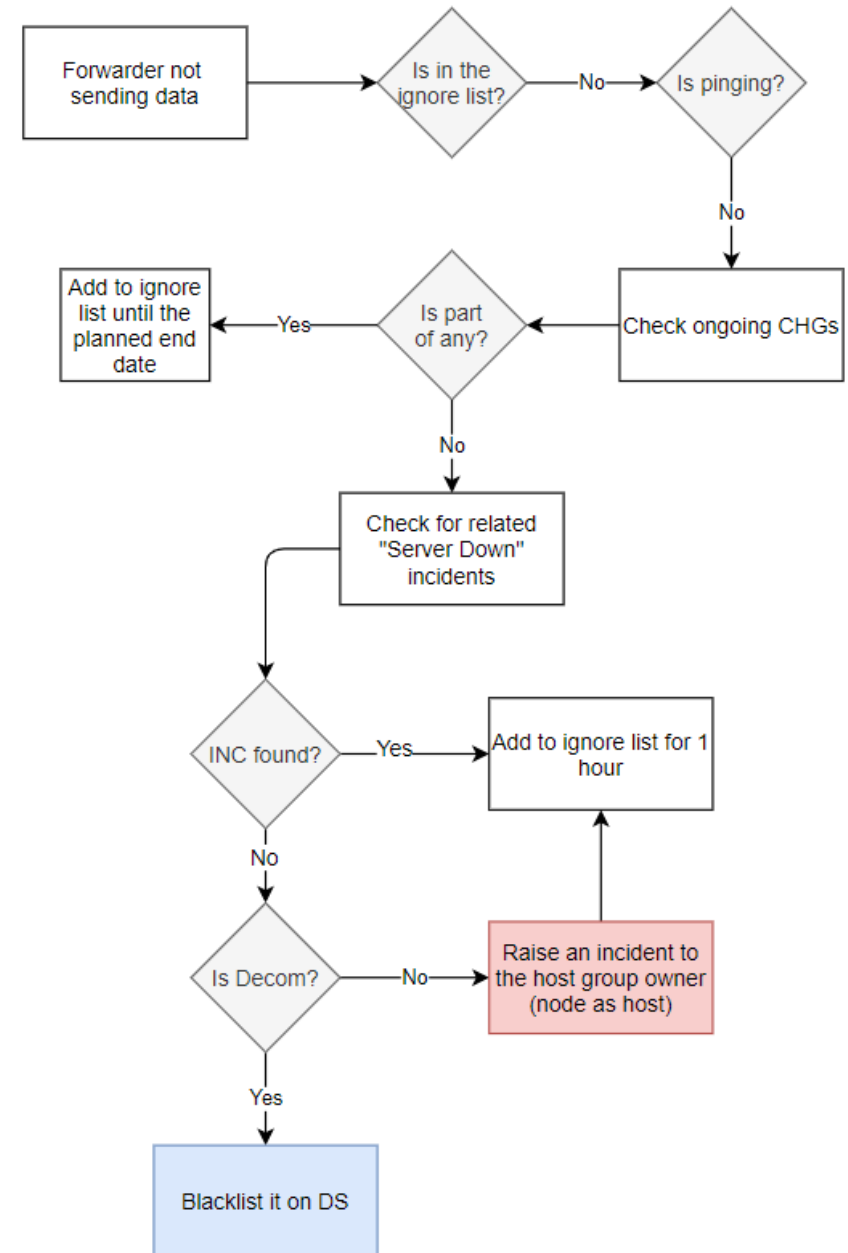
Keeps the forwarders up-to-date

Trigger an incident with enriched data



Walkthrough

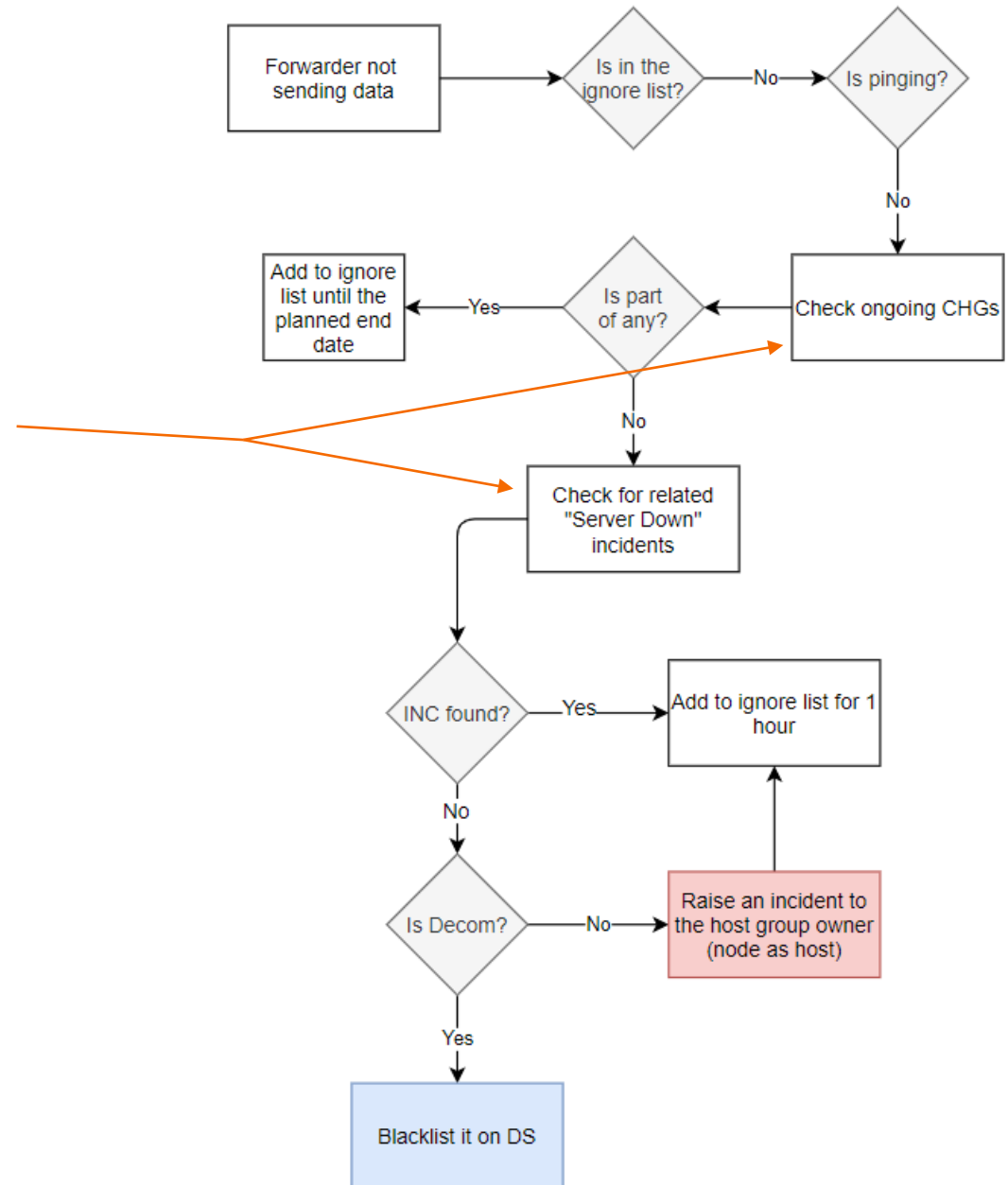
Splunk forwarder remediation – not pinging



Walkthrough

Splunk forwarder remediation – not pinging

Investigate reasons of unavailability

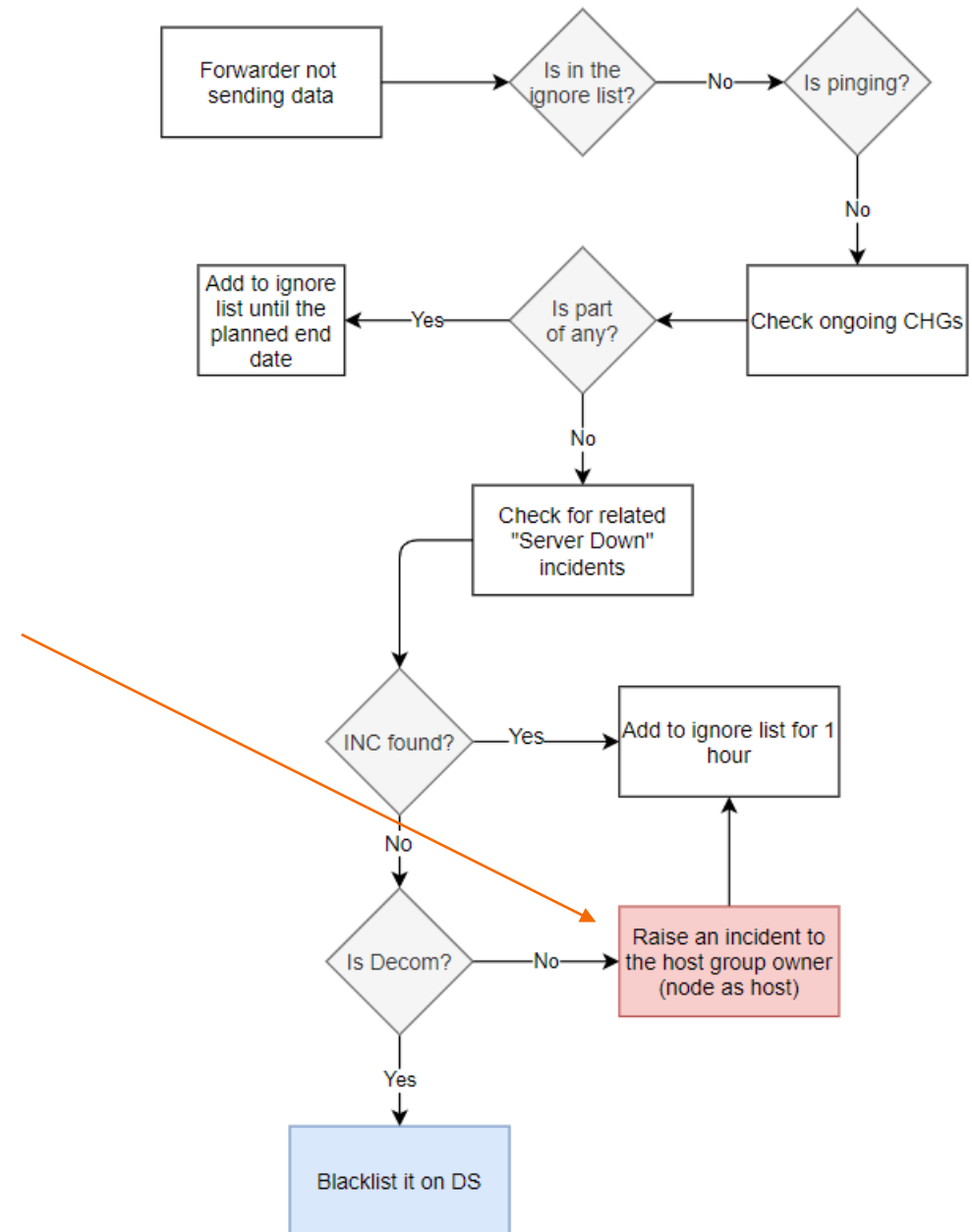


Walkthrough

Splunk forwarder remediation – not pinging

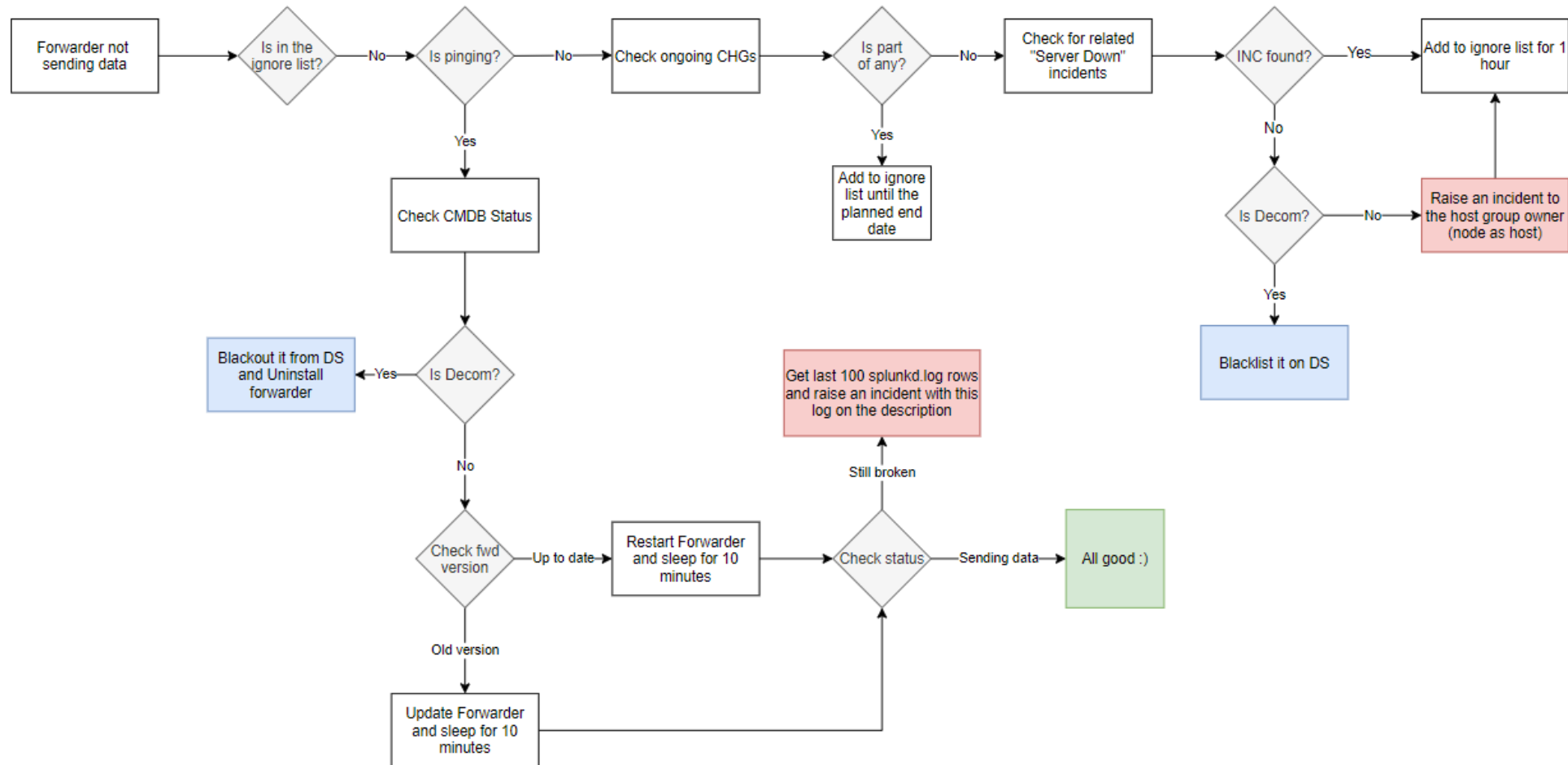
Investigate reasons of unavailability

Report server down to the responsible team



Walkthrough

Splunk forwarder remediation – full diagram





Walkthrough: Extending Phantom Playbooks



Integrations

Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Integrations

Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Install/update apps via UI

Integrations

Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Install/update apps via UI

Create your own apps via UI

Integrations

Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Install/update apps via UI


Create your own apps via UI

Configure multiple assets per app

Walkthrough

Phantom integrations - teams

HTTP post



HTTP
Publisher: Phantom
App version: 2.1.15
Python version: 2.7
Product vendor: Generic
[Documentation](#)

Description
This App facilitates making HTTP requests as actions

ASSET CONFIGURATION CONFIGURE NEW ASSET

Asset (22)

ms teams - dce sre

Asset Info

Asset Settings

Approval Settings

Access Control

Base URL for making queries. (e.g. https://myservice/)

https://outlook.office.com

Phantom Auth token (for use with Phantom servers)

Password (for HTTP basic auth)

Optional

Base URL endpoint for test connectivity. (e.g. /some/specific/endpoint)

Username (for HTTP basic auth)

Optional

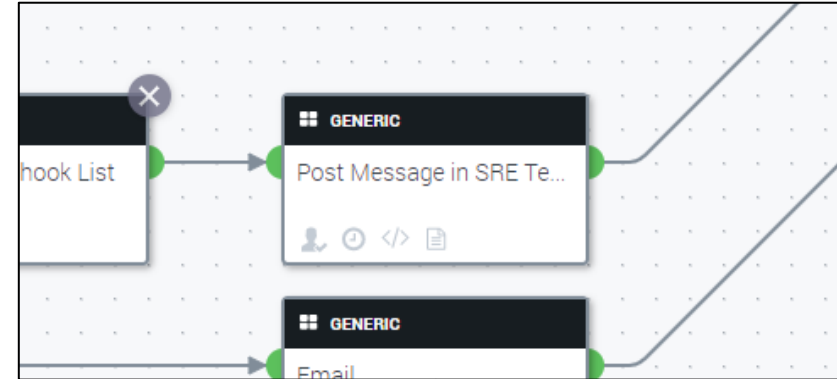
Timeout for HTTP calls

Optional

► Advanced


EDIT

TEST CONNECTIVITY



Walkthrough

Phantom integrations - teams



HTTP
Publisher: Phantom
App version: 2.1.15
Python version: 2.7
Product vendor: Generic
[Documentation](#)

Description
This App facilitates making HTTP requests as actions

ASSET CONFIGURATION CONFIGURE NEW ASSET

Asset (22)

ms teams - dce sre

Asset Info

Asset Settings

Approval Settings

Access Control

Base URL for making queries. (e.g. https://myservice/)

Base URL endpoint for test connectivity. (e.g. /some/specific/endpoint)

Phantom Auth token (for use with Phantom servers)

Username (for HTTP basic auth)

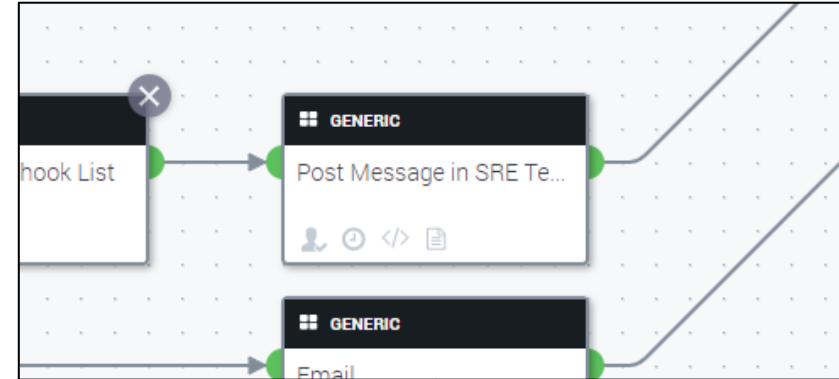
Password (for HTTP basic auth)

Timeout for HTTP calls

► Advanced

EDIT

TEST CONNECTIVITY



HTTP post

Walkthrough

Phantom integrations - teams

Fully customized message card

The screenshot displays the Splunk Teams interface. On the left, a sidebar lists various teams, including 'SRE DCE - SRE', 'iDRAC9 Telemetry / Splunk Core Team', 'Splunk DB Alerts', 'SRE Phantom Automation', 'SRE-DBA', 'Online Fraud Defense', 'Phantom Playbook - DCQO', 'Phantom Project', '3rd party performance', and 'Major Incident Management'. The 'SRE DCE - SRE' team is selected, and its 'General' channel is active. The main content area shows a message from 'SRE Automations' dated Monday 1:47 PM. The message card is titled 'SRE Automation' and contains a yellow alert banner stating 'The Dell.com ACC dashboard is alerting. Cart Services[96], Delivery Promise[1534], PCF Configurator[261], Responsive Cart[570], Server-Network[321]'. Below the banner, a list of team members is shown, followed by a summary of activity and a suppression notice. A table titled 'Error by Error Type' lists various error codes and their descriptions. At the bottom, there are four buttons: 'Join the SRE Bridge Now', 'Dell.com SMCC Dashboard', 'ARR Dashboard', and 'Dell.com NGINX Dashboard'. Yellow arrows point from the team list to the message card, highlighting the integration.

Walkthrough

Phantom integrations – Twilio & Slack



Slack

Publisher: Phantom

App version: 1.2.21

Python version: 2.7

Product vendor: Slack Technologies

[Documentation](#)

Description

Integrate with Slack to post messages and attachments to channels

ASSET CONFIGURATION

[CONFIGURE NEW ASSET](#)

Asset (2)

sreslack

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Bot User OAuth Access Token

Verification Token

IP of host making the REST calls (or "any")

any

Automation User Auth Token

Optional

Question timeout (in minutes)

30

How often to poll for a response (in seconds)

30

POST incoming for Slack to this location

https://ausdlphantomap1.us.dell.com/rest/handler/slack_3ac26c7f6baa4-4583-86ff-5aac62778a86/sreslack

► Advanced


EDIT

TEST CONNECTIVITY

Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset

**Slack**
Publisher: Phantom
App version: 1.2.21
Python version: 2.7
Product vendor: Slack Technologies
[Documentation](#)

Description
Integrate with Slack to post messages and attachments to channels

ASSET CONFIGURATIONCONFIGURE NEW ASSET

Asset (2)
sreslack

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Bot User OAuth Access Token

Verification Token

IP of host making the REST calls (or "any")
any

Automation User Auth Token
Optional

Question timeout (in minutes)
30

How often to poll for a response (in seconds)
30

POST incoming for Slack to this location
`https://ausdlphantomap1.us.dell.com/rest/handler/slack_3ac29c7f6baa4-4583-86f7-5aac62778a86/sreslack`

▸ Advanced

EDIT


TEST CONNECTIVITY

Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity



Slack
Publisher: Phantom
App version: 1.2.21
Python version: 2.7
Product vendor: Slack Technologies
[Documentation](#)

Description
Integrate with Slack to post messages and attachments to channels

ASSET CONFIGURATION CONFIGURE NEW ASSET

Asset (2)

sreslack

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Bot User OAuth Access Token

Verification Token

IP of host making the REST calls (or "any")

any

Automation User Auth Token

Optional

Question timeout (in minutes)

30

How often to poll for a response (in seconds)

30

POST incoming for Slack to this location

https://ausdlphantomap1.us.dell.com/rest/handler/slack_3ac25c7f6baa4-4583-86f7-5aac62778a86/sreslack

▸ Advanced

EDIT

TEST CONNECTIVITY

splunk> .conf20


Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity

Add the action call in the
playbook

**Slack**
Publisher: Phantom
App version: 1.2.21
Python version: 2.7
Product vendor: Slack Technologies
[Documentation](#)

Description
Integrate with Slack to post messages and attachments to channels

ASSET CONFIGURATIONCONFIGURE NEW ASSET

Asset (2)
sreslack

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Bot User OAuth Access Token

Verification Token

IP of host making the REST calls (or "any")
any

Automation User Auth Token
Optional

Question timeout (in minutes)
30

How often to poll for a response (in seconds)
30

POST incoming for Slack to this location
`https://ausdlphantomap1.us.dell.com/rest/handler/slack_3ac25c7f6baa4-4583-86f7-5aac82778a86/sreslack`

▸ Advanced

EDITTEST CONNECTIVITY

Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity

Add the action call in the
playbook

Slack
Publisher: Phantom
App version: 1.2.21
Python version: 2.7
Product vendor: Slack Technologies
[Documentation](#)

Description
Integrate with Slack to post messages and attachments to channels

ASSET CONFIGURATION

Asset (2)
sreslack

Asset Info
Bot User OAuth Access

IP of host making the REST calls (or any)
any

Question timeout (in minutes)
30

How often to poll for a response (in seconds)
30

POST incoming for Slack to this location
https://ausdlphantomap1.us.dell.com/rest/handler/slack_3ac25c7f8baa8-4583-869f-5aac62778ba8/sreslack

Advanced

[EDIT](#) [TEST CONNECTIVITY](#)

Walkthrough


Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity

Add the action call in the
playbook

Twilio configuration follows
the same standard



Twilio
Publisher: Phantom
App version: 1.0.9
Python version: 2.7
Product vendor: Twilio
[Documentation](#)

Description

This app integrates with Twilio to send messages

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (1)

twilio us

Asset Info

Asset Settings

Approval Settings

Access Control

Twilio Base URL (e.g. <https://api.twilio.com/2010-04-01>)

<https://api.twilio.com/2010-04-01>

Auth Token

To Phone Number (Used only for test connectivity)

Optional

Account SID

From Phone Number (Twilio Assigned, e.g. +15101281337)

► Advanced

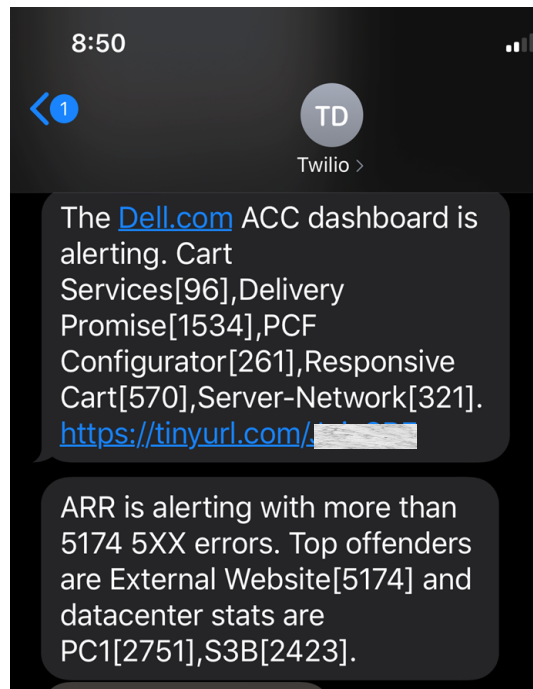
EDIT

TEST CONNECTIVITY

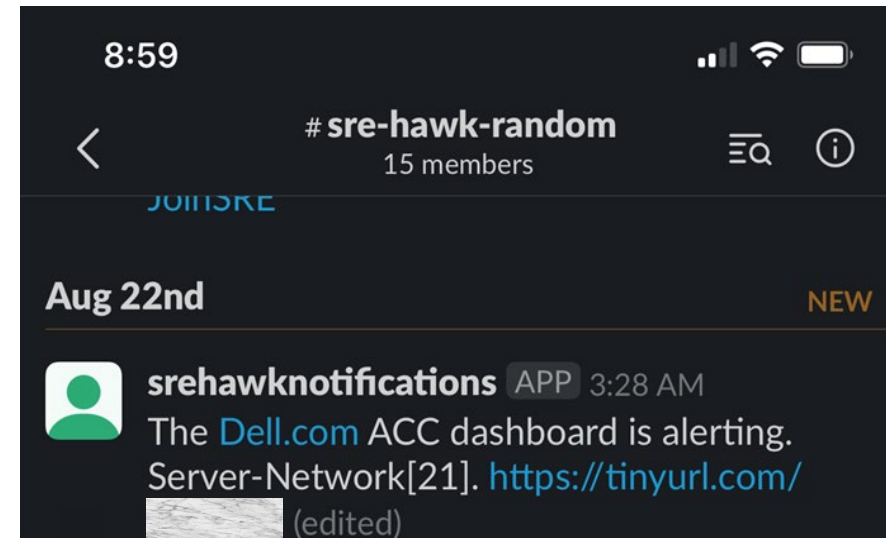
Walkthrough

Phantom integrations – Twilio & Slack

Twilio



Slack



Walkthrough

Phantom integrations - ServiceNow



ServiceNow

Publisher: Splunk
App version: 1.2.59
Python version: 2.7
Product vendor: ServiceNow
[Documentation](#)

Description

This app integrates with ServiceNow to perform investigative and generic actions

ASSET CONFIGURATION

[CONFIGURE NEW ASSET](#)

Asset (1)

servicenow - uat

[Asset Info](#)[Asset Settings](#)[Ingest Settings](#)[Approval Settings](#)[Access Control](#)

Device URL including the port, e.g. https://myservicenow.enterprise.com:8080

https://delltechuat.service-now.com

Password

Client Secret. Required with Client ID

Optional

Filter to use with On Poll separated by '^' (e.g. description=This is a test^assigned_to=test.name)

Optional

Max container (For other runs of schedule polling)

100

Username

Optional

Client ID. OAuth will be preferred if provided

Optional

Table to ingest issues from

Optional

Max container (For first run of schedule polling)

10000


► Advanced

[EDIT](#)[TEST CONNECTIVITY](#)

Walkthrough

Phantom integrations - ServiceNow

Manage incidents



ServiceNow
Publisher: Splunk
App version: 1.2.59
Python version: 2.7
Product vendor: ServiceNow
[Documentation](#)

Description
This app integrates with ServiceNow to perform investigative and generic actions

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (1)

servicenow - uat

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Device URL including the port, e.g. https://myservicenow.enterprise.com:8080

Password

Client Secret. Required with Client ID

Filter to use with On Poll separated by '*' (e.g. description=This is a test^assigned_to=test.name)

Max container (For other runs of schedule polling)

Username

Client ID. OAuth will be preferred if provided

Table to ingest issues from

Max container (For first run of schedule polling)

Advanced

EDIT


TEST CONNECTIVITY

Walkthrough

Phantom integrations - ServiceNow

Manage incidents

Run queries over API



ServiceNow
Publisher: Splunk
App version: 1.2.59
Python version: 2.7
Product vendor: ServiceNow
[Documentation](#)

Description
This app integrates with ServiceNow to perform investigative and generic actions

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (1)

servicenow - uat

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Device URL including the port, e.g. https://myservicenow.enterprise.com:8080

Username

Password

Client ID. OAuth will be preferred if provided

Client Secret. Required with Client ID

Table to ingest issues from

Filter to use with On Poll separated by '*' (e.g. description=This is a test^assigned_to=test.name)

Max container (For first run of schedule polling)

Max container (For other runs of schedule polling)

► Advanced

EDIT

TEST CONNECTIVITY


Walkthrough

Phantom integrations - ServiceNow

Manage incidents

Run queries over API

List tickets



ServiceNow
Publisher: Splunk
App version: 1.2.59
Python version: 2.7
Product vendor: ServiceNow
[Documentation](#)

Description
This app integrates with ServiceNow to perform investigative and generic actions

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (1)

servicenow - uat

Asset Info

Asset Settings

Ingest Settings

Approval Settings

Access Control

Device URL including the port, e.g. https://myservicenow.enterprise.com:8080

Username

Password

Client ID. OAuth will be preferred if provided

Client Secret. Required with Client ID

Table to ingest issues from

Filter to use with On Poll separated by '*' (e.g. description=This is a test^assigned_to=test.name)

Max container (For first run of schedule polling)

Max container (For other runs of schedule polling)

► Advanced

EDIT

TEST CONNECTIVITY

Walkthrough

Phantom integrations - ServiceNow

Manage incidents

Run queries over API

List tickets

Simple as adding a new action
to your playbook

servicenow

Available Actions (14)

Search actions

add comment

add work note

create ticket

describe catalog item

describe service catalog

get ticket

get variables

list categories



Walkthrough

Phantom integrations - ServiceNow

The screenshot displays the ServiceNow Incident form for Incident - INC12578935. The form is titled "Incident - INC12578935" and includes a sidebar with navigation icons. The form fields are organized into two columns. The left column contains fields for Number, Caller, Location, Product, Category, Subcategory, Impact, Urgency, Priority, Response Level, Short Description, and Description. The right column contains fields for Opened, Opened by, Source, Support Method, Incident State, Assignment group, Assigned to, Event, Event Source, Customer Escalation, and MIM. The form is titled "Incident - INC12578935" and includes a sidebar with navigation icons. The form fields are organized into two columns. The left column contains fields for Number, Caller, Location, Product, Category, Subcategory, Impact, Urgency, Priority, Response Level, Short Description, and Description. The right column contains fields for Opened, Opened by, Source, Support Method, Incident State, Assignment group, Assigned to, Event, Event Source, Customer Escalation, and MIM.

Field	Value
Number	INC12578935
Opened	2020-09-01 14:07:58
* Caller	Event Integration
* Location	Round Rock, TX
* Product	Splunk Dell (779889)
* Category	EVENT GENERATED
* Subcategory	PROD
Impact	2 - High
Urgency	3 - Medium
Priority	3 - Medium
Response Level	Normal
Opened by	
Source	Event
Support Method	-- None --
Incident State	New
Assignment group	DAO-OBSERVABILITY-LOGGING
Assigned to	
Event	<input checked="" type="checkbox"/>
Event Source	SPLUNK DELL
Customer Escalation	<input type="checkbox"/>
MIM	<input type="checkbox"/>
* Short Description	Phantom_-_Integration_-_Splunk Dell (779889)
* Description	The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:

Walkthrough

Phantom integrations - ServiceNow

Add attachments

The screenshot shows the ServiceNow Incident form for INC12578935. The form is titled "Incident - INC12578935" and includes buttons for "Create Child Incident", "Resolve Incident", "Run Routing Rules", "Search knowledge", and "Update". The form fields are as follows:

Field	Value
Number	INC12578935
Opened	2020-09-01 14:07:58
* Caller	Event Integration
* Location	Round Rock, TX
* Product	Splunk Dell (779889)
* Category	EVENT GENERATED
* Subcategory	PROD
Impact	2 - High
Urgency	3 - Medium
Priority	3 - Medium
Response Level	Normal
Opened by	
Source	Event
Support Method	-- None --
Incident State	New
Assignment group	DAO-OBSERVABILITY-LOGGING
Assigned to	
Event	<input checked="" type="checkbox"/>
Event Source	SPLUNK DELL
Customer Escalation	<input type="checkbox"/>
MIM	<input type="checkbox"/>
* Short Description	Phantom_-_Integration_-_Splunk Dell (779889)
* Description	The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:

Walkthrough

Phantom integrations - ServiceNow

Add attachments

Update assignment

The screenshot displays the ServiceNow Incident form for Incident INC12578935. The form is titled "Incident - INC12578935" and includes a sidebar with navigation icons. The main form area contains the following fields:

- Number: INC12578935
- Caller: Event Integration
- Location: Round Rock, TX
- Product: Splunk Dell (779889)
- Category: EVENT GENERATED
- Subcategory: PROD
- Impact: 2 - High
- Urgency: 3 - Medium
- Priority: 3 - Medium
- Response Level: Normal
- Opened: 2020-09-01 14:07:58
- Opened by: [User]
- Source: Event
- Support Method: -- None --
- Incident State: New
- Assignment group: DAO-OBSERVABILITY-LOGGING
- Assigned to: [User]
- Event: ☒
- Event Source: SPLUNK DELL
- Customer Escalation: ☐
- MIM: ☐
- Short Description: Phantom_-_Integration_-_Splunk Dell (779889)
- Description: The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:

Walkthrough

Phantom integrations - ServiceNow

Add attachments

Update assignment

Change priority

The screenshot shows the ServiceNow Incident form for Incident INC12578935. The form is titled "Incident - INC12578935" and includes a navigation bar with icons for home, incident, knowledge, and other functions. The form fields are organized into two columns. The left column contains fields for Number (INC12578935), Caller (Event Integration), Location (Round Rock, TX), Product (Splunk Dell (779889)), Category (EVENT GENERATED), Subcategory (PROD), Impact (2 - High), Urgency (3 - Medium), Priority (3 - Medium), and Response Level (Normal). The right column contains fields for Opened (2020-09-01 14:07:58), Opened by, Source (Event), Support Method (-- None --), Incident State (New), Assignment group (DAO-OBSERVABILITY-LOGGING), Assigned to, Event (checked), Event Source (SPLUNK DELL), Customer Escalation, and MIM. The Short Description field contains "Phantom_-_Integration_-_Splunk Dell (779889)". The Description field contains "The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:". The form also includes buttons for "Create Child Incident", "Resolve Incident", "Run Routing Rules", "Search knowledge", and "Update".

Field	Value
Number	INC12578935
Caller	Event Integration
Location	Round Rock, TX
Product	Splunk Dell (779889)
Category	EVENT GENERATED
Subcategory	PROD
Impact	2 - High
Urgency	3 - Medium
Priority	3 - Medium
Response Level	Normal
Opened	2020-09-01 14:07:58
Opened by	
Source	Event
Support Method	-- None --
Incident State	New
Assignment group	DAO-OBSERVABILITY-LOGGING
Assigned to	
Event	<input checked="" type="checkbox"/>
Event Source	SPLUNK DELL
Customer Escalation	<input type="checkbox"/>
MIM	<input type="checkbox"/>
Short Description	Phantom_-_Integration_-_Splunk Dell (779889)
Description	The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:

Walkthrough

Phantom integrations - ServiceNow

Add attachments

Update assignment

Change priority

Manage Incident state

The screenshot shows the ServiceNow Incident form for Incident INC12578935. The form is titled "Incident - INC12578935" and includes a navigation bar with icons for home, incident, and other functions. The form fields are organized into two columns. The left column contains fields for Number (INC12578935), Caller (Event Integration), Location (Round Rock, TX), Product (Splunk Dell (779889)), Category (EVENT GENERATED), Subcategory (PROD), Impact (2 - High), Urgency (3 - Medium), Priority (3 - Medium), and Response Level (Normal). The right column contains fields for Opened (2020-09-01 14:07:58), Opened by, Source (Event), Support Method (-- None --), Incident State (New), Assignment group (DAO-OBSERVABILITY-LOGGING), Assigned to, Event (checked), Event Source (SPLUNK DELL), Customer Escalation, and MIM. The Short Description field contains "Phantom_-_Integration_-_Splunk Dell (779889)". The Description field contains "The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:". The form also includes buttons for "Create Child Incident", "Resolve Incident", "Run Routing Rules", "Search knowledge", and "Update".

serviceNow Dell Service Management Suite

Victor Menezes

Incident - INC12578935

Create Child Incident Resolve Incident Run Routing Rules Search knowledge Update

Number INC12578935

Opened 2020-09-01 14:07:58

* Caller Event Integration

* Location Round Rock, TX

* Product Splunk Dell (779889)

* Category EVENT GENERATED

* Subcategory PROD

Impact 2 - High

Urgency 3 - Medium

Priority 3 - Medium

Response Level Normal

Opened by

Source Event

Support Method -- None --

Incident State New

Assignment group DAO-OBSERVABILITY-LOGGING

Assigned to

Event ☒

Event Source SPLUNK DELL

Customer Escalation ☐

MIM ☐

* Short Description Phantom_-_Integration_-_Splunk Dell (779889)

* Description The below host list could not be remediated by Phantom Playbook. Please check the servers according to their related error status:

Walkthrough

Phantom integrations - Others

Ticketing

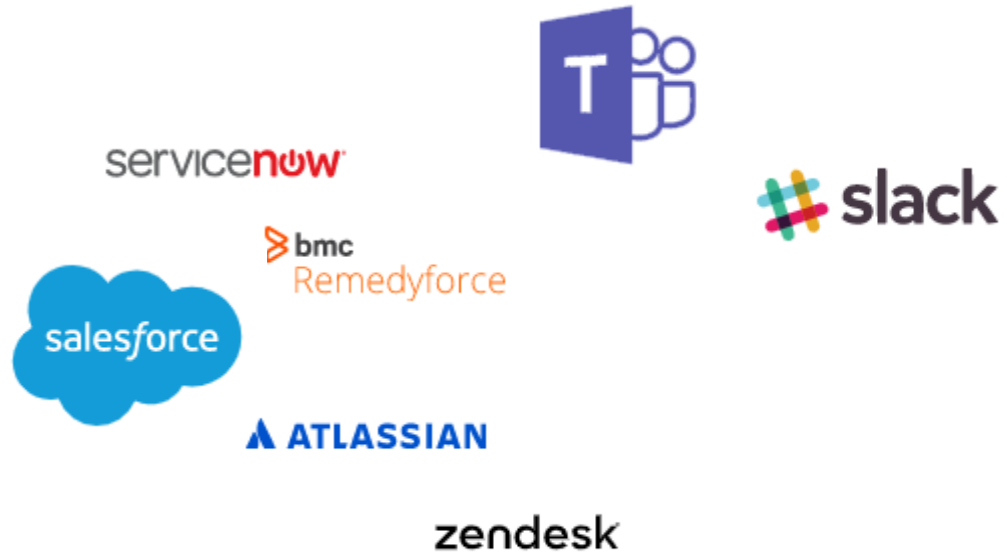


Walkthrough

Phantom integrations - Others

Ticketing

Information



Walkthrough

Phantom integrations - Others

Ticketing

Information

Virtualization



Walkthrough

Phantom integrations - Others

Ticketing

Information

Virtualization

Database



Walkthrough

Phantom integrations - Others

Ticketing

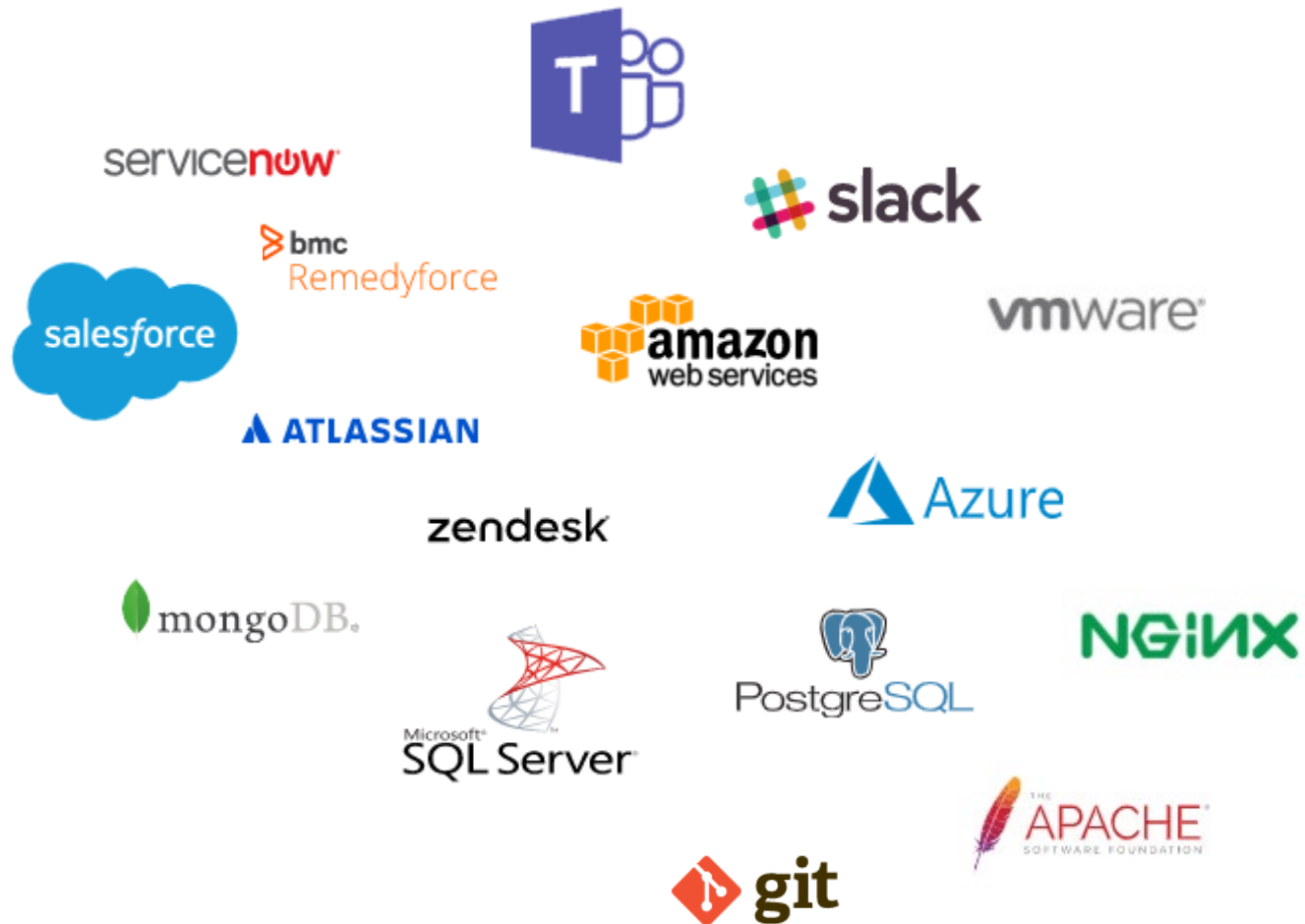
Information

Virtualization

Database

Devops

More...



Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
- 300 + Apps at my.phantom.us

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
- 300 + Apps at my.phantom.us
- Custom Functions

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
- 300 + Apps at my.phantom.us
- Custom Functions
- Build Your Own Apps

Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
- 300 + Apps at my.phantom.us
- Custom Functions
- Build Your Own Apps
- Only Limited by Your Imagination

Call to Action

How you can get started with Phantom

Get an Account on my.phantom.us

- Account is free
- Access to documentation, product downloads, and more

Call to Action

How you can get started with Phantom

Get an Account on my.phantom.us

- Account is free
- Access to documentation, product downloads, and more

Get the Free Community Edition

- Limited Functionality After 100 Actions in a Day
- Easy, Single-Server Install

Call to Action

How you can get started with Phantom

Get an Account on my.phantom.us

- Account is free
- Access to documentation, product downloads, and more

Get the Free Community Edition

- Limited Functionality After 100 Actions in a Day
- Easy, Single-Server Install

Get Trained

- A Training Investment Will Kickstart Your Productivity!
- Check Out the Splunk [Training Portal](#)



Thank You

Please provide feedback via the
SESSION SURVEY

