



# **Table of Contents**

1	Key New	Peatures and Enhancements	8
2	Automat	ion Data Table (ADT)	10
	2.1 Comp	ponents of Automation Data Table	13
	2.1.1	Table Data	15
	2.1.2	Automation Data Table Builder	16
	2.2 Creat	e ADT Automatically	19
	2.2.1	Define Base Table Data	23
	2.2.2	Enrich Basic Table Data with Column Groups	24
	2.3 Other	r ADT Functions	
	2.3.1	Lock/Unlock ADT and ADT Editing Rights Control	
	2.3.2	Editing Rights Control for ADT	
	2.3.3	View ADT Execution Log	
	2.3.4	ADT Audit Log	
	2.3.5	User Privilege for ADT	35
3	ADT Base	ed PDAS	
	3.1 Instal	I ADT Intents for TAF	
	3.1.1	Trigger Diagnosis Using ADT Intents	
	3.1.2	Trigger Diagnosis Using Intent Template	
	3.2 Instal	I ADT Intents to Preventive Automation	40
	3.2.1	ADT- Based Looking Glass Probe	41
	3.2.2	Use Primary Probe to Trigger Intents of ADT	47
	3.2.3	Use Intent Timer to Trigger Intents of ADT	
	3.2.4	View Triggered Automation from PA Dashboard	50
	3.2.5	Probe Instance Enhancement	52
	3.2.6	Auto Probe	57
	3.2.7	Other New Features and Enhancements for PAF	58

	3.3 Insta	ll ADT to Auto Intent	60
	3.3.1	Auto Intent Tab in IBA Center	61
	3.3.2	Use Auto Intent to Create Intent for Map Devices	63
	3.3.3	Use Intent Template Not Included in Auto Intent	64
	3.3.4	Filter Intent Template/ADT in Auto Intent	64
	3.3.5	Use ADT Automation Asset Via Auto Intent	65
	3.4 Use	ADT to Replicate Path Intent	66
	3.4.1	Batch Path Intent Replication from ADT	67
	3.4.2	On-demand Path Intent Replication from Path Browser/Auto Intent	70
	3.4.3	Delete/Unlock Path Intents in Batch	71
4	Networ	k Intent Enhancements	74
	4.1 Crea	te Intent Data View and Intent Map	75
	4.1.1	Build Intent Data View	78
	4.1.2	Build Intent Map	78
	4.2 Emb	edded Incident	79
	4.2.1	Document Critical Findings in Embedded Incident	80
	4.2.2	Create New or Reuse an Incident to Organize Results Reasonably	81
	4.2.3	Manage Historical Results	
	4.2.3 4.3 Follo	Manage Historical Results	
	4.2.3 4.3 Follo 4.3.1	Manage Historical Results w-up Diagnosis Follow-up Intent Template	
	4.2.3 4.3 Follo 4.3.1 4.3.2	Manage Historical Results w-up Diagnosis Follow-up Intent Template Follow-up Self	
	4.2.3 4.3 Follo 4.3.1 4.3.2 4.3.3	Manage Historical Results w-up Diagnosis Follow-up Intent Template Follow-up Self Follow-up ADT Intents	
	4.2.3 4.3 Follo 4.3.1 4.3.2 4.3.3 4.3.4	Manage Historical Results w-up Diagnosis Follow-up Intent Template Follow-up Self Follow-up ADT Intents Call Qapp	
	4.2.3 4.3 Follo 4.3.1 4.3.2 4.3.3 4.3.4 4.4 New	Manage Historical Results	
	4.2.3 4.3 Follo 4.3.1 4.3.2 4.3.3 4.3.4 4.4 New 4.4.1	Manage Historical Results	
	<ul> <li>4.2.3</li> <li>4.3 Follo</li> <li>4.3.1</li> <li>4.3.2</li> <li>4.3.3</li> <li>4.3.4</li> <li>4.4 New</li> <li>4.4.1</li> <li>4.4.2</li> </ul>	Manage Historical Results	
	<ul> <li>4.2.3</li> <li>4.3 Follo</li> <li>4.3.1</li> <li>4.3.2</li> <li>4.3.3</li> <li>4.3.4</li> <li>4.4 New</li> <li>4.4.1</li> <li>4.4.2</li> <li>4.4.3</li> </ul>	Manage Historical Results	

4.4	.5	Support Built-in Table and ADT	110				
4.5	Cont	ntrol the Update of Intent Baseline by Logic					
4.6	Inten	t Variable and Intent Diagnosis Block	114				
4.6	.6.1 Intent Variable						
4.6	5.2	Intent Diagnosis Block	118				
4.7	Prog	rammable Notification to 3 <sup>rd</sup> -party system	120				
4.7	'.1	Send Email	121				
4.7	.2	Call Webhook	122				
4.8	Sche	dule Intent	124				
4.9	API D	iagnosis in Intent Definition	126				
4.10	Simp	lified Intent debug	129				
4.11	Othe	r Intent's Improvements	131				
4.1	.1.1	Intent View	131				
4.1	.1.2	View Diagnosis Message	132				
4.1	.1.3	Export CSV Report to Files	133				
4.12	Inten	t Replication Improvements	134				
4.1	.2.1	Device Scope Configuration	136				
4.1	.2.2	Set Macro Variable	136				
4.1	.2.3	Intent Replication for Path	139				
4.1	.2.4	Intent Map Setting Configuration	141				
4.1	.2.5	Configuration of Critical Variables	141				
4.1	.2.6	Intent Parser Qualification:	142				
4.1	.2.7	Cloned Intent Name Rule	143				
4.13	Inten	t Decode and Baseline Improvements	144				
4.1	.3.1	Intent Decode / Baseline Settings Adjustment	145				
4.1	.3.2	Intent Decode Displaying Status	146				
4.1	.3.3	Intent Decode Results Improvements	147				
4.1	.3.4	Show Decode Results for API Parser	148				

5	ļ	Automat	tion Bot	150
	5.1	Use C	Chat Bot (End User)	150
	5.2	Chatk	oot Creation Flow	153
	5.2	2.1	Intent (NI) Node	154
	5.2	2.2	Intent Template (NIT) Node	155
	5.2	2.3	Automation Data Table (ADT) Node	155
	5.2	2.4	Condition Node to Control Flow	156
	5.2	2.5	Selection Node	157
	5.3	Addit	ional Features	158
6	F	Report a	nd Dashboard	160
	6.1	Key C	Components to View Report and Dashboard	162
	6.3	1.1	Key Components to View Report	162
	6.:	1.2	Key Components to View Dashboard	163
	6.2	Key C	Components to Create the Report and Dashboard	163
	6.2	2.1	Key Components to Create a Report	164
	6.2	2.2	Key Components to Create a Dashboard	167
	6.3	Creat	e Report	168
	6.3	3.1	Define Report Properties	168
	6.3	3.2	Define Report Input	175
	6.3	3.3	Define Report Columns	177
	6.3	3.4	Pivot Table	180
	6.3	3.5	Drill-down Actions	184
	6.3	3.6	Report Filter	186
	6.3	3.7	Run Report	188
	6.4	Creat	e Dashboard	189
	6.4	4.1	Chart	189
	6.4	4.2	Call-Out	192
	6.4	4.3	Refresh Dashboard	195

6.5 Repo	ort and Dashboard Examples	195
6.5.1	Monitor Failover Failure for Outage Prevention	195
6.5.2	Automate Diagnosis of Transient Problems	196
6.5.3	Perform Security Assessment for Network Security	198
6.5.4	Perform Continuous Monitoring of Application Performance	198
7 Other E	nhancements	200
7.1 Dom	nain Setup and Data Accuracy Improvements	200
7.1.1	Discovery and Fine Tune Improvements	200
7.1.2	Benchmark Improvements	206
7.2 Торо	ology Accuracy Improvements	206
7.2.1	Open Topology Improvements	206
7.2.2	One IP Table Improvement	207
7.2.3	Remove Zone Selection from Add Topology Link	208
7.3 Circu	uit Break in Server Benchmark	208
7.3.1	Circuit Break Global Settings	209
7.3.2	Execute Circuit Break Check in Server Benchmark	
7.3.3	Manage Circuit Break Data	
7.3.4	Run Circuit Break Benchmark	
7.4 Syst	em-wide Intent Execution Workload Control	215
7.5 Lock	and Single Editing Control	216
7.5.1	Lock Function	217
7.5.2	Single-editing Control	218
7.5.3	Related Features	218
7.6 Supp	port Plus	219
7.7 Auto	o Update Improvements	222
7.8 New	/ Vendor Support	223
7.8.1	Support NSX-T	223
7.8.2	Other Device Type Support	225

7.9	)	Security Improvement	225
8	Cas	ses Resolved in R11.1	28

# **1** Key New Features and Enhancements

NetBrain release R11.1 greatly enhances the Intent-based **Problem Diagnosis Automation System (PDAS)**, which automates the Diagnosis of repetitive problems and enforces preventive measures across the entire network. Especially, R11.1 strengthens NetBrain as a scalable platform to build, update and execute thousands to millions of intents across your whole network with the following new features and enhancements:



• <u>Automation Data Table (ADT)</u><sup>New</sup>

An **Automation Data Table** (ADT) is an extended global data table for managing the critical network assets and network intents associated with those network assets. ADT is a database for intents, supporting intent creation and replication, and can be used as the base of the PDAS system.

#### ADT-based PDAS Automation Flow

ADT serves as a data reservoir in NetBrain and can be used across functions to provide data for the proper operations, including TAF (Triggered Automation Framework), PAF (Preventive Automation Framework), Auto Intent, Chat Bot, and follow-up Intent Diagnosis:

- <u>TAF Enhancements</u>: R11.1 supports ADT intents in TAF Triggered Diagnosis and assigning ADT values to Macro Variables in the intent template.
- <u>PAF Enhancements</u>: R11.1 adds a new probe, Looking Glass Probe <sup>New</sup>, and enhances PAF functions to ensure the critical assets defined within ADTs function properly by triggering the corresponding intents through the PAF probes. Users can also batch-create probes with a new feature Auto Probe <sup>New</sup>.

- <u>Auto Intent Enhancements</u>: R11.1 incorporates ADT assets into Auto Intent to support interactive troubleshooting and create the map's embedded intents and path intents.
- <u>Path Intent Enhancements</u>: R11.1 supports batch path intent replication from ADT, using ADT data sources as macro variables of the path intent, and path intent replication from the path browser and Auto Intent.

#### Network Intent Enhancements

R11.1 adds many new features to enhance the no-code programmability of Network Intent (NI), including:

- Major enhancement of Intent's no-code programmability, such as <u>follow-up diagnosis</u>, <u>intent</u> <u>dataview</u>, and <u>intent map</u>.
- <u>Use Intent to drive programable notifications to 3<sup>rd</sup> party solutions</u>.
- Support intent across API-based networks such as SDN or Cloud.
- On-Demand replication of Intent.

<u>Automation Bot</u> New

Use an Automation Bot to build an interactive, multi-step automation chatbot and execute multiple intent-based automations to solve real-world challenges without using NetBrain IE system UI. A chatbot provides self-service to a large audience without knowing the NetBrain system.

#### • <u>Report and Dashboard</u> New

Report and Dashboard provides a single interface to organize, analyze, and share data from different NetBrain automation assets, such as ADT Intent results, and a visual display of multiple automation results from PDAs.

#### • Other Enhancements

R11.1 enhances the foundations and many features, such as **Circuit Break**<sup>New,</sup> to solve the benchmark performance issues due to the large data table, improving the data accuracy and open topology.

# 2 Automation Data Table (ADT)

An **Automation Data Table (ADT)** is an extended global data table for managing the critical network assets and network intents associated with those network assets. ADT provides users with two capabilities:

- Use ADT to build, organize and share the critical assets, such as critical Application and Path, WAN Link, Device Failover, Subnet, and Route, then associate intents and diagnosis results for troubleshooting network problems.
- ADT is a database for intents, supporting intent creation and replication. The system provides methods (Base Table and Column Group) in Automation Data Table Builder to ensure that users can build the basic table data and create and bind the intent for each automation asset.

The following diagram illustrates what an ADT looks like:

						5 A (U 1 Tags: Monitor	utomation Tag of I sed to filter intents in TAI <sup>1 Tags</sup> Interface	ntent Column F/PAF/Auto Intent)	4 Intent Output
	(defi	ned as base table)	bject			2 Path Intents (Pre-replicated wi	ith specified intent templa	3 Path	Мар
No.	Application Name S	Path 🤷 🗭	Path Devices 🔗	Path Interfaces 🔏	Path Status S	Path Intent	Path Intent 2	Path Map 💦	Intent Output 🛛 🚍
1	Salesforce Server	BOS-to-TOR-https	BJ-3750-2 BJ-Arista-1 BJ-Arista-2	ASA-AA/context2/act - inside ASA37_38-server - Network ASA@Switch - Ethernet1/3 ASAV41NEW-PBR-SERVER	Success	Monitor Path Health	Check Interface CRC Error	BOS-to-TOR-https	Ethernet0/0's dupl  Ethernet0/1's dupl Ethernet0/1's dupl Bj-3750-2 - Interfac
2	QOS Path	NYC-to-BOS	Bj-Avaya-1 Bj-Avaya-2 BJ-Cat-5000 BJ-L2-Core-A	BJ*POP - FastEthernet0/0/0 BJ-Arista-1 - Ethernet4 BJ-Avaya-2 - Avaya Ethernet BJ-Avaya-2 - Avaya Ethernet	Success	Monitor Path Health	Check Interface CRC Error	NYC-to-BOS	Ethernet0/0's dupl Ethernet0/1's dupl Ethernet0/1's dupl Bj-Cat-5000 - Interf
3	Traditional Data Center	TOR-to-BOS	BJ-Avaya-2 BJ-Cat-5000 BJ-L2-Core-A BJ-L2-coreB	BJ-Arista-2 - Ethernet2/3 BJ-Cat-5000 - 3/6 BJ-L2-coreB - FastEthernet0/ BJ-L2-Core-A - FastEthernet0	Failed	Monitor Path Health	Check Interface CRC Error	TOR-to-BOS	Ethernet0/0's dupl Ethernet0/1's dupl Ethernet0/1's dupl BJ-L2-Core-A - Inter
4	QOS Path	DB Backup	ASA-AA/admin/act ASA-AA/admin/stby BJ_L2_Core_3 LA.DIS,1	ASA-AA/act - Ethernet0/1.4 ASA-AA/admin/stby - outside ASA.Switch - Ethernet1/0	Success	Monitor Path Health	Check Interface CRC Error	DB Backup	Ethernet0/0's dupl Ethernet0/1's dupl Ethernet0/1's dupl BJ_L2_Core_3- Inter
5	POC	MPLS_DMVPN_PA	BJ-R2 BJ-R3 BST,POP1 qapp-c3560-1	BJ-R2 - Loopback2 BJ-R2 - FastEthernet0/1 BJ-R3 - FastEthernet0/1.10 BJ-R3 - FastEthernet0/1		Monitor Path Health	Check Interface CRC Error	MPLS_DMVPN_PA1	Ethernet0/0's dupl Ethernet0/1's dupl Ethernet0/1's dupl qapp-c3560-1 - Inte
6	Traditional Data Center	Two-HSRP	ASA-AA/context1/stby BJ*POP BJ_L2_Core_3 BJ_core_3550	BJ*POP - FastEthernet0/0/0 BJ*POP - FastEthernet0/0/1 BJ*POP - FastEthernet0/0/2 BJ_L2_Core_3 - FastEthernet	Failed	Monitor Path Health	Check Interface CRC Error	Two-HSRP	Ethernet0/0's dupl Ethernet0/1's dupl Ethernet0/1's dupl BJ_core_3550 - Inter
7	QOS Path	NYC-to-SMF	Emu_NB_NYC_MGMT F5-MGMT	F5-MGMT - Ethernet0/2 F5-MGMT - Ethernet1/0	Success	Monitor Path Health	Check Interface CRC Error	NYC-to-SMF	Ethernet0/0's dupl Ethernet0/1's dupl

The following diagram illustrates how to create Automation Data Table:



After ADTs are created, users can use ADT for NetBrain Problem Diagnosis Automation System (PDAS), called ADT-based PDAS, which provides the following key values:

- Trigger ADT intents and deliver ADT maps in Triggered Automation Framework (TAF)
- Next-gen ADT-based Preventive Automation (PAF)
- Intent replication for application path (Path Intent)
- Troubleshoot network problems in NetBrain Bot based on ADT

The following diagram illustrates how ADT works in the PDAS system:



#### **PDAS Overview**

The ADT-based PDAS differs from the previous PDAS in the following two respects:

- The intents in ADT are pre-replicated, and the intents cloned from the intent template are on-demand replicated.
- The intents in ADT are referenced to automation assets.

As the ADT-based PDAS system shows its main value in TAF and PAF, we provide two diagrams to illustrate how ADT-based PDAS works in TAF and PAF, respectively.

The following diagram illustrates how ADT-based PDAS works in TAF:



The following diagram illustrates how ADT-based PDAS works in PAF:



# 2.1 Components of Automation Data Table

**Automation Data Table Manager** is a centralized management interface of ADTs where end users can create, edit, and delete ADT. It consists of the following components:



1. A Folder Tree structure to organize shared tables and my tables.



2. Table Operating Area to edit, clear and export data.

- **Table Data** for displaying the ADT data.
- Automation Data Table Builder for creating ADT.
- Add Data Manually menu for manually editing data.

#### 2.1.1 Table Data

Table data, the final table data of an ADT, is shown in the diagram below and includes:

1 Table	Header 🛛 🕘 ADT E	Base Ta	able		🌀 Manua	lly Added Row				Automation Tag	3 ADT Column Group	🕘 Manua	ally Added Colum
No.	Application Name	S	Path	•* 🐢	Path Devices	Source	S Destination	S Path Sta	atus S	Path Intent	Intent Output	E P	rority
1	Salesforce Server		App1		BJ-3750-2 BJ-Arista-1 BJ-Arista-2	10.10.10.1	192.168.1.1			Monitor Pa PAT	tuals to baselin aph1 of BJ_L2_0 TH guals to baselin Paragraph1 of GW2La	ie H Core_3 h ie ab has	-
2	QOS Path		NYC-to-BOS		BJ-Avaya-1 BJ-Avaya-2 BJ-Cat-5000 BJ-L2-Core-A	10.8.8.162	10.8.1.26			Monitor Path Health	h para equals to baselin Paragraph1 of BJ_L2_C para equals to baselin Paragraph1 of GW2La	ie N Core_3 h ie ab has	
3	Traditional Data Center	r	Арр1		BJ-Avaya-2 BJ-Cat-5000 BJ-L2-Core-A BJ-L2-coreB	10.8.1.4	10.8.3.140	Failed		Monitor Path Health	h para equals to baselin Paragraph1 of BJ_L2_ para equals to baselin Paragraph1 of GW2La	ie H Core_3 h ie ab has	+
4	QOS Path		DB Backup		ASA-AA/admin/act ASA-AA/admin/stby BJ_L2_Core_3 LA.DIS,1	10.8.1.4	10.8.3.130			Monitor Path Health	h para equals to baselin Paragraph1 of BJ_L2_( para equals to baselin Paragraph1 of GW2La	ie N Core_3 h ie ab has	
5	POC		MPLS_DMVPN_PATH		BJ-R2 BJ-R3 BST,POP1 qapp-c3560-1	10.8.2.19	10.8.5.11			Monitor Path Health	h para equals to baselin Paragraph1 of BJ_L2_( para equals to baselin Paragraph1 of GW2La	ie H Core_3 h ie ab has	ŀ
6	Traditional Data Center	r	App2		ASA-AA/context1/stby BJ*POP BJ_L2_Core_3 BJ_core_3550	10.8.1.4	10.8.3.196	Failed		Monitor Path Health	h para equals to baselin Paragraph1 of BJ_L2_ para equals to baselin Paragraph1 of GW2La	ie H Core_3 h ie ab has	
7	QOS Path		NYC-to-SMF		Emu_NB_NYC_MGMT F5-MGMT	10.8.8.162	10.8.2.14			Monitor Path Health	h para equals to baselin Paragraph1 of BJ_L2_0	ie L Core_3 h	

- **Table Header**: Display all the defined columns in the current ADT. Several operations on the column can be performed here (**Edit/Delete/Set as Table Key**). The basic column information, such as the display name, column name and data type, is displayed as a tip window.
- **ADT Base Table**: The base table contains basic source data for building automation assets in ADT. A base table is a way of building basic data. We provide 7 methods to create and populate the base table.
- **ADT Column Group**: The columns added to ADT by Automation Data Table Builder to enrich the ADT data of automation columns. Column groups depend on base table data and use the base table data as inputs. There are 6 methods to add a column group.

### 2.1.2 Automation Data Table Builder

An integrated UI with capabilities for dynamically creating table data and dynamic columns. **Base Table Builder** and **Column Group Builder** are included here to ensure users can build the table data and create/bind the intent for each automation asset.

• **Base Table Builder:** Creating a basic network table.

	🕘 Colum Group Area	5 Filter Row
	Automation Data Table Builder_Security Zones of network	×
1 Column Header —	Column Header:	Reset All
	Operation         Operation <t< th=""><th>Failover Config-let</th></t<>	Failover Config-let
	Base Group 1 Group + Column Group (Base); Description:	Select Column ~
	Use Intern Template update dev1e data table Device VRF Interface	
2 Methods to	Select Method To Build Base Table: To be defined To be defined To be defined	
Build Base Table	Intent Template: Check Device and Neighbor	
Pre-Replicated Intent Template	Built-in Fields:	
Intent Cluster	Replicated Intent	
Path and Intent	Intent Macro Variable:	
Device Group	interface 💩 (Drag and drop column header from the upper area or available data field from the left here)	
Site	Device Status Code S Filter Row	•
Import CSV	Intent Output: Filter Devices by Device Groups/Sites: Select ~	
	Device Status Code 3	
3 Available Fields	intent Map 💈	
	Last Updated Time O	
6 Auto Update	Auto-Update No Scheduled Update	Cancel Apply
	🔕 Base Table Builder	

The system supports 7 methods to populate automation (intent/probe/map) columns, facilitating enriching/updating the ADT contents:

Method	Populated Columns	Populated Rows
Pre-replicated Intent Template	<ul> <li>Replicated Intent</li> <li>Replicated Device</li> </ul>	1 device and 1 replicated intent per row. Furthermore, the network attributes corresponding to the device can be extended by macro variables.

	<ul> <li>Macro Variable (Dynamic)</li> <li>Intent Output *</li> </ul>	
Intent Cluster	<ul> <li>Member Intent Name</li> <li>Member Intent Devices</li> <li>Signature Variables (Dynamic)</li> <li>Intent Output *</li> </ul>	1 member intent per row. Furthermore, the attributes corresponding to the automation asset can be added as row data.
Application Path	<ul> <li>Application Name</li> <li>Path</li> <li>Path Name</li> <li>Path Devices</li> <li>Path hops (device interfaces)</li> <li>Path Map</li> <li>Source</li> <li>Destination</li> <li>Path Status</li> </ul>	1 path per row. Furthermore, the path properties can be added as row data.
Map Folder	<ul> <li>Map</li> <li>Map Name</li> <li>Map Devices</li> <li>Map Device Interfaces</li> <li>Map Intent</li> <li>Intent Output *</li> </ul>	1 map and 1 map intent per row. Furthermore, the map can be added as row data.
Site	<ul><li>Site Name</li><li>Devices in Site</li><li>Site Map</li></ul>	1 site device and 1 site map intent per row. Furthermore, the site properties can be added as row data.

	<ul> <li>Site Map Intent</li> <li>Intent Output *</li> </ul>	
Devices of Device Group	<ul> <li>Device Name</li> <li>Device Group Name</li> <li>Device Properties (Dynamic)</li> </ul>	1 device per row. Furthermore, the device group name and properties can be added as row data.
Imported CSV	CSV Columns (Dynamic)	1 CSV row per row.

**Note**: The Intent Output column includes the following data: Intent Status Code, Intent Message, Intent Status Code, Device Status Code, Intent Devices, Intent Map, Intent CLI Commands, and Last Execution Time.

• **Column Group Builder:** Creating dynamic automation columns or property columns for each automation asset.

		Olum Group Area	5 Logic to Populate New Column
	Automation Data Table Builder_Security Zor	ies of network	×
1 Column Header —	olumn Header:		Reset All
	A         S         B           Name         HSRP VIP	C     C     D     C     C     D     C     C     C     D     C     C     C     D     C	B         H         S         I         I           Failover Config-let         Failover Configuration I
	Base Group 1 Group +	Column Group (Group 1) :	Select Column ~
	Description: Use Intent Template update dev1e data table Select Method to Build Group Table:	A S B C S Name HSRP VIP Group ID Mamber Intern Name To be defined	
2 Methods to Build Column Group	Intent Template	members mente verne	
ntent Template	Built-in Fields:	(Drag and drop column header from the upper area or available data field from the left here)	
tent Cluster	Replicated Intent	Define Logic to Populate New Columns for Each Row:	
fonitoring Probe	Intent Output:	Replicate Current Intent on Device: bgp_nbr	~
unction Call	Intent Message	Set Macro Variables of Seed Intent Template:	
ook up imported CSV	Device Status Code 5	A Seed Device Macro Variable Type Set Variable from Automation Data Table Field	
	Intent Map	4 😋 R1	
	Last Undated Time	target_subnet string route (LP Device Route Failover ~	
	cost opouted time	Mgmt_IP string Please Select V	
		4 🥶 SW1	
Available Fields		target_subnet string US-BOS-SW1.subnet ~	
Available Fields —		Maximum number of command sections included in the cloned intent: 20	
6 Auto Update	Auto-Update No Scheduled Update		Cancel Apply
-		Column Group Builder	

The system provides 5 column group builders:

Method	Populate Column Data	Logic
Intent Template	Cloned Intent for each Row	Clone intent for each valid row based on the defined device column. Add an intent column, then add the intent outputs to additional columns.
lntent Cluster	Member Intent	Select a NIC, then match and filter a member intent for each valid row and add the intent outputs to additional columns.
Monitoring Probe	Probe	Filter probes by the probe name using the current ADT data.
Imported CSV	CSV Column	Use selected key columns to match the rows in CSV files and append specified columns from CSV files to the ADT for new columns in the matched rows.
Function Call	Column's properties Covert source column by function	Specify a column with the type of device and use device properties and functions (e.g., transferring an IP address to a hostname) to fill in additional columns.

# 2.2 Create ADT Automatically

ADT table can be created automatically with the following steps:

1. Go to **Automation Data Table Builder>Base** to build a base table containing data fields to include automation asset data to be used.

120	or		
lag			Automation Data Table Builder X
«	Œ	Automation Data Table Builder	
	lter	ns: 19 Rows 9 Columns	Column Header: Reset All
			g a ig a or a or g a ig a ig a i
	No.	Application Name	Application Name Path Path Devices Source Destination Path Status Path Intent Output
	1	Salesforce Server	d I Pranty
			Base         New Group         +         Column Group (Base):         Select Column v
	2	QOS Path N	Description: ct 10 c2 c2 c4 10 c6 10
			Select Method to Build Base Table: Path Path Source Destination Path Status
			Application Path 🗸
	3	Traditional Data Center Ap	Application Path: 4 Items
			Bullein Fields:
	4	QOS Path DE	Application Name
			8 Path of P
			Path Name (5
	5	POC	Path Devices 🧠
	Ĩ		Path hops (device interfac 🔌
			Path Map 🚓
		T IN ID C	§ Source 1
	0	Traditional Data Center Ap	Destination     (1)     (7)     (
	7	005 Bath	Auto-Update No Scheduled Update     Apply     Save and Update     Cancel     Apply     Save and Update
	·	Q05F801	

 Go to Automation Data Table Builder > Column Group tab to create column groups to enrich the base table data.

er		Automation Data Table Builder	
æ	Automation Data Table Builder	Column Header:	Reset All
lten	Application Name	8         c1         5         c2         4 <sup>3</sup> 6         6         5         5         5         6         1         7         10         5         66         5         6         5         6         5         6         5         6         5         6         5         6         5         10         7         10         5         66         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         6         5         7         10         5         7         10         5         7         10         5         7         10         5         7         10<	5
1	Salesforce Server	Proprior     Four Verrie     Second read     Four Verrie     Four Verrie     Four Verrie       Image: Second read     Promity     Four Verrie     Four Verrie     Four Verrie	
2	QOS Path	Base Group1 + Column Group (Group1): Select Colum	umn 🗸
		Select Method to Build Group Table:	
3	Traditional Data Center	Column Type:	
4	QOS Path	Convert Column Value by Function Select One Column of ADT as the Source Column: Exercise Column of ADT as the Source Column of ADT	
	POC	Bullein Fields:	
	Traditional Data Center	Intent Status Code  Device Status Code I Intent Devices	
		(Brag and drop column header from the upper area or available data field from the left here)	
7	QOS Path	O Auto-Update No Scheduled Update Cancel Apply Save and U     Save and U	Jpdate

3. Go to Automation Data Table Builder (Schedule Update) to schedule updating ADT data periodically.



4. Go to **Automation Data Table Manager** (**Add Data Manually**), and manually add or adjust the table data.

		1	Add Data Manually 🗸 😑	<b>a</b>
		Sear	Add Table Column	G
Path Intent	🚺 🟷 Int	ent Ou	Add Table Row	≡

 Go to Automation Data Table Manager, then create tags for the automation column/map column from the Tag Current Column of the drop-down menu. The tags can filter the intents used for TAF, PAF, Bot, Auto Intent or Follow-up Intent.



For example, users can organize all critical application paths and their automation intents into an ADT, including the key path data (such as the source and destination), then use the ADT to monitor the critical applications (PAF) and trouble any application-related issue (TAF/Chatbot/Auto Intent). The system can find the related paths for different types of events (e.g., *a device interface has errors, the device configuration changes*) by matching the ADT column data and the event information and execute the associated path intents for the problem diagnosis and change verification.



### 2.2.1 Define Base Table Data

Users can use the data from the Path Browser to build the base ADT table by the method **Application Path**. Users can select paths from the Path Browser.

=	E NotBrain Search for device, configura	tion Q, 🔶 Path	Search incident 🔍 🚆 🗔 🚅 🌐 BOS I	lab Domain 1 👔 🕘
-	Automation Data Table Ma	nager		
r.	Search	C     C	C Update Now     Add Det     Search  Path Status Path Intent Path Intent Status	a Manually $\checkmark \equiv 0$ Q O E Automation Map PathMap1
t	Column Header: Path Name Path Device Case Group 1 Group +	Cource Destination Path Status Path Inter	G I & H I     Path Intent Status Failover Configuration I	PathMap2
<ol> <li>Methods to</li> </ol>	Description: Use Intent Template update dev1e data table Select Method To Build Base Table: Path and Intent	Path Name Path Name C Group ID Group ID Member Intent Devices		
Build Base Table	Path and Intent: 3 Selected Applications Built-In Fields: Application Name Path P Path P Path Name Path Devices Path hops (device interf.			
2 Available Fields —	Path Map Ref Path hope devi Source 3 Destination 5 Path Status 5	e interfaces) (Drag and drap column header from the upper area or available data field from the left bere		
3 Auto Update	Auto-Update No Scheduled Update		Cancel Apply	4

🙆 Base Table Builder

**Mapping Available Fields to Column Group:** Drag and drop the available fields to the column group definition area to create ADT columns automatically. Select fields from the following field categories in this area:

a) Built-in Fields: The built-in fields available for this base table are listed in this area. Applicable fields included application, path (the link to this path), path name, other path properties, and path intent (see the table below for details).

Field Type	Fields	Description
Built-in Field	Application Name	The built-in fields are created from path properties.

Path
Path Name
Path Devices
Path hops (device interfaces)
Path Map
Source
Destination
Path Status

b) Intent Outputs: Intent information of path intent can be displayed in the intent output columns of the ADT, such as intent message, intent status code, intent devices, intent map, intent CLI commands, and last execution time.

After ADT is created in Automation Data Table Builder, users can enable the Auto-Update for this ADT to update the data periodically.

# 2.2.2 Enrich Basic Table Data with Column Groups

For a base table created via the application path, column groups can be added to cover more data. The system supports several methods to populate dynamic columns for a path-based table. The table below describes each of the methods.

Method	When do I need to use this method?	Use Case
Use Intent Template	Add some additional intent columns for an ADT.	Intent Template (on-demand replication and Auto- Replicated) is selected and used. Users add an intent column (mandatory), then the intent outputs to additional columns.
Use Intent Cluster	Add some additional intent columns for an ADT.	Match and filter a member intent for each valid row and add the intent outputs to additional columns.
Use Auto-Probe	Add some additional probe columns for an ADT.	Filter a probe by the name using the current ADT data.

Use CSV File	Have a pre-generated CSV file and want to enrich table data with it.	Use selected key columns to match the rows in CSV files and append specified columns from CSV files to the ADT for new columns in the matched rows.
Use Function	Enrich ADT with some key column properties.	Specify a column with the type of device and use device properties and functions to fill in additional columns.
Intent Replication for Path	Want to generate some suitable path intent for application paths.	See training documentation of Intent Replication for Path for more information.

#### 2.2.2.1 Add Automation Column from Intent Template

Based on the base data of ADT, the intent template in the automation column can be used to replicate one intent for each ADT row. This cloned intent includes the automation data in this ADT and the detailed information of the cloned intent, shown in intent output columns. Users can select a base table column containing device information for replicating intents.

The following diagram illustrates how the intent template works in Column Group Builder:



The following diagram illustrates what the Column Group Builder looks like when the **Intent Template** method is selected:

	He     Automation Data Table Manager      Sourch     Q	a Manually ~ = a Q O Configuration Issues
	Automation Data Table Builder, Security Zones of network  Column Header:  Column Header: Column Header:  Column Header: Column Header:  Column Header: Column Header: Column H	
	Base     Group 1     Group (Group 1):     Select Column >       Description:     Image: Column Group (Group 1):     Image: Column Group (Group 1):     Select Column >       Use Intent Template update dev1e data table     Image: Column Group (Group 1):     Image: Column Group (Group 1):     Image: Column Group (Group 1):       Select Method to Build Group Table:     Image: Column Group (Group 1):     Image: Column Group (Group 1):     Image: Column Group (Group 1):	
Methods to	Intent Template   Intent In	
	Intent Output:     Replicate Current Intent on Device:     bgg.nbr       Intent Message     Set Macro Variables of Seed Intent Template:       Device Status Code     Seed Device:   Set Variable from Automation Data Table Field	
	Interit Map     →     ● R1       Last Updated Time     ●     Mgmt_IP     string     route (LP Device Route Failover ~       Mgmt_IP     string     Please Select ~       ✓     ●	
2 Available Fields —	target_subnet string US-BOS-SW1 subnet ~ Maximum number of command sections included in the cloned intent: 20	
4 Auto Update	Auto-Update No Scheduled Update Column Cancel Apply	

The following table describes available fields for building a group table if the intent template is the data source:

Field Type	Fields	Description
Built-in Field	Replicated Intent	The built-in fields are created from the replicated intent from the intent template.
Intent Output Field	Intent Message Intent Status Code Device Status Code Intent Devices Intent Map Intent CLI Commands	The intent output fields are created from intent details of the intents generated from the intent template.

Last Execution	
Time	
CSV Columns	

#### 2.2.2.2 Add Probe into ADT for Prevention Automation

Probe installed for ADT can trigger the automation process associated with the ADT automation assets. The corresponding PDAS flow is shown in the following diagram:



A probe column can be defined for using the primary and secondary probes to trigger automation with assets in the ADT. The probe properties are used as the built-in data for the probe column. The Flash alerts generated by the probes can also be the available data source. The following diagram illustrates how Monitoring Probe works in Column Group Builder:



The following diagram illustrates what the Column Group Builder looks like when the **Monitoring Probe** method is selected:

	E NETBrain Search for device, confi	guration Q, 🔶 Path	Search incident 🗨 🛄 🗔 📫 805 I	ab Domain 1 🛞 🔞
	+ Automation Data Table	Manager		
	SearchQ	C      C     C	Update Now Add Date Search  rce 1 Device Interface Status	A Manually ~ = 6 Q O Interface Config-let S Kace ethermet 0/0
	Column Header: Column Header: A 1 B Name HSRP VIP Base Group 1 Group +	C      D      C      D      C      C      D      Device List      Source 1     Automatic     Column Group (Group 1):	Reset All an 1 Fallover Config-let Select Collumn  Select Column	utdown dress 10.10.10.10 255.255.0 face ethernet 0/0 tutdown drage 11.10.10.10
1 Methods to Build Column Group 2 Probe Type	Use Intent Template update dev1e data table Select Method to Build Group Table: Monitoring Probe	A      B     A     B     A     B     A     B     A     B     A     B     A     B     A     B     A     B     A     B     A     B     A     B     A     B     A     B		255.255.1 face ethernet 0/0 hutdown dress 12.10.10.10 255.255.2
3 Create Probe by Name Search	Treate Probe by Name Search: 3 Probe Groups Built-in Fields Probe      Probe      Probe      Probe Output:	Populate Column Logic for Probe: Matching Probe by Device: Failover Devices  Define Conditions to Match Probe for Each Row of ADT:		face ethernet 0/0 hutdown dress 13.10.10.10 255.255.3 face ethernet 0/0
	Flash Alert	Probe Men/ger         Operator         Data Field of Automation Data Table           A         Probe Name         Matches         Failover Devices(\$string)           B         Probe Name         Failover Devices(\$string)	~	hutdown dress 14.10.10.10 255.255.4 face ethernet 0/0
Available Fields —-		Boolean Expression: A and B		nutdown dress 15.10.10.10 255.255.5
6 Auto Update	Auto-Update No Scheduled Update	5 Logic to Populat 	e New Column Cancel Apply	h.

The following table describes the data fields for building group columns via a monitoring probe:

Field Type	Fields	Description
Built-in Field	Probe	The built-in field is the probe selected.
Output Field	Flash Alert	The Output Field is created by flash alerts generated by the probes.

### 2.2.2.3 Add ADT Column from Imported CSV

If users have local CSV files containing data, the CSV file can be imported to create an ADT group table. By default, all columns in the CSV are added as available fields in ADT. To successfully merge the CSV columns to the base table, users can select fields from the CSV and fields in ADT as the table keys to be paired.

The following diagram illustrates how Imported CSV works in Column Group Builder:



The following diagram illustrates what the Column Group Builder looks like when the **Imported CSV** method is selected:



# 2.3 Other ADT Functions

## 2.3.1 Lock/Unlock ADT and ADT Editing Rights Control

To avoid mis-operations on the ADT data, ADT can be locked/unlocked by its creator or other users with the privilege. Moreover, editing rights are introduced to the ADT feature to prevent data loss due to editing conflicts.

For each ADT table, the creator of ADT can switch on the Locking function and set a locking mode (With Password or Without Password). A locked ADT is in View-Only mode and can be edited after entering the password. Lock annotation can be added to provide detailed lock information.

Lock Settings	<
C Lock Locked by James Green on 9/2/2023	
○ Without Password	
With Password:     Confirm Password:	
Lock Annotation:	
This file is currently locked by James Green whom you can contact to get more details.	
	ļ
Cancel OK	

### 2.3.2 Editing Rights Control for ADT

An ADT may be edited by two or more users simultaneously; in this case, one of the edited ADT cannot be saved, causing data loss. To prevent such a problem, the user editing the ADT first owns the editing rights, and only the user with editing rights can edit the ADT.

If a user without editing rights attempts to edit the ADT, a message will notify the user that the editing right is required.

### 2.3.3 View ADT Execution Log

The execution log is provided for an ADT to record the operations such as replicating intents, matching intent and the intent execution errors. Users can check and export the ADT execution log. Users can specify a time range to check the execution log for the period.



#### 2.3.4 ADT Audit Log

The audit log is provided to record and track the changes made to ADT to protect essential ADT assets. The ADT audit log records the following operations:

- Create ADT: Record relevant information when a new ADT is created.
- Delete ADT: Record relevant information when an ADT is deleted.
- Edit ADT: Record relevant information each time the ADT is edited.

## 2.3.5 User Privilege for ADT

ADTs are organized in folders. Two privileges (Shared Resource and File Management and Private Resource Management privilege) are associated with ADT.

- Open ADT Manager: a user having the Shared Resource and File Management privilege or Private Resource Management privilege can open the ADT manager.
- Edit private ADT: Require Private Resource Management privilege to edit a private ADT.
- Select ADT: No privilege is required for selecting an ADT.
- Use Intent-based ADT: Require the privilege to edit intent to edit the ADT.

# **3 ADT Based PDAS**

ADT serves as a data reservoir in NetBrain. It can be used across functions (TAF, PAF, Auto Intent, Chat Bot, and follow-up Intent Diagnosis) to provide data for the proper operations.



## 3.1 Install ADT Intents for TAF

To analyze and solve the network issues of automation assets, we can install Intents of ADT to TAF and trigger these intents by the 3<sup>rd</sup> party events. For this purpose, R11.1 improved TAF Triggered Diagnosis to support ADT intents, a set of Intents associated with specific assets (e.g., application paths, critical failover links) in ADT. Another TAF enhancement is to support assigning values to Macro Variables in the intent template.


# 3.1.1 Trigger Diagnosis Using ADT Intents

For issues related to Automation Assets, it is preferred to trigger ADT intents to troubleshoot issues related to automation assets, e.g., **checking failover links** and **checking Critical Routes**. To conveniently address and analyze the network issues of automation assets, users can install Intents of ADT to TAF and trigger these intents by events (tickets from a third party).



The following diagram illustrates an example of how ADT-based PDAS works in TAF:

		Network Assets 1: Fa	ailover links	🖏 Auto	mation Da	ata Tables				
		Failover Link Name	Primary Devices	Primary	nk	Secondary Device	Intent			
		Internet 1	R1	R1.E0/0		R2	Check Failover-Internet1	1		
Ticket		AT&WAN	BOS-R1	BOS-R1.e	1/0	BOS-R2	Check Failover-AT&T WAN	1		
		P&G WAN	Tot-R1	Tot-R1.e	0	Tot-R2	Check Fallover-P&G WAN			
ServiceNow Ticket								÷	Notify	
Interface error: R1.E0/0	1	🔍 Find related ne	etwork assets			2 .	Execute matched Intents			NetBrain
		Network Assets 2: Cr	ritical application paths	;						Incident
		Failover Link Name	Path Name	Path De	ice Pa	ath Interface	Intent			
		Salesforce_Flow	Webserver	Webser	er R1	I.E0/0	Check QOS Config-Salesforce Flow	1		
				R1	R1	I.E0/1	0			
		Web Browser Flow	Data Engine	Data En	ine BC	DS-R1.e0/0	Check QOS Config-Web Browse Flow			
				R2						
		Core_datebase	DataBase_Sever1	DataBa	e_Server1 To	ot-R1.e0/0	Check WOS Config-Core Database			
				R3	R1	1.E0/0				

The key logic of triggering ADT intent is illustrated in the following diagram:

		Find Automation Assets by Incident Fields:
Configure Triggered Automation	×	Find Automation Assets by Incident Fields
Name: Z Enabled	Description:	A Failover Devices V Contains V Application_Devices V
Incoming Incident	Select Intent from Automation Data Table Automation Data Table: FailoverLinks	Failover Anne     Application, Name     Application, Dark     Bo     Failover Description     Dat.UP     Hadress     Select Intents of Automation Assets:     Select Intents     Select Intents     Column 1, Column 2     w     Interts     Match any     Match any     GSPF Checking     Match any     Cligner Checking
Execution Setting: Seconte Network Intent Deliver Intent Map	Maximum number of Network Intent(s) matched for one trigger task:           Deliver Automation Maps:         All Maps           Ø Advance Settings           G         Cancel	Solution Maps: Select     QOS     L2 Device     ce Settings      Select Map     Selected Maps: Column1, Column 2
		Maps with Tags: match any v select togs v Cancel OK etr

1. Find related Automation Assets. Find matching row data based on whether the corresponding incident field exists in the ADT column.

- Trigger associated intents of Automation Assets. All the intents of the matched ADT rows will be triggered by default, and the user can filter the intents to be executed with automation tags or manually choose intents by selecting columns.
- 3. Deliver automation Maps of Automation Assets to the Incident pane. All the maps of the matched ADT rows will be delivered to the incident pane by default. Users can filter the delivered maps with automation tags or manually choose maps by selecting columns.

The logic for matching ADT intents in ADT-based TAF is shown in the following diagram below:



#### 3.1.2 Trigger Diagnosis Using Intent Template

The Intents can be replicated from the intent template for troubleshooting. In the process of installing the intent template to TAF, in some cases, some macro variables of the intent template need to be set to a certain specific value, e.g., the target subnet for **show ip route <subnet**> command. To support TAF in these cases, users can enter values for macro variables of the intent template during the TAF installation. Data fields of incoming incident type can be used as the data source to set the value for macro variables.

figure Triggered Automation for Intent Template		×
Name: check MTU and Duplex 🗹 Enable	Description:	
Incoming Incident: O Incoming Incident Type	Intent:	
Select Incident Type: Interface Error Check	Name: Check MTU and Duplex Mismatching Browne	
A OSPE_Area v Matches v 1	Replicate Current Intent on: IssueDevice_Name	
B Select Criteria v	Set Macro Variables of Seed Intent Template:           Seed Device         Macro Variable         Type         Sec Variables from Incoming Incide           CA-TO         Interface_Name         V           OSPF_Area         string         Interface_Name         V	Set Value for macro variable
Boolean Expression: A	Use pre-decode values if the device variable is null Maximum number of command sections included in the cloned intent: 99	
Execution Setting: O Execute Intent O Deliver Intent Map	Both     O Advance Setting	5
Test	Cancel	K.

# 3.2 Install ADT Intents to Preventive Automation

ADT can be installed in the Intent Based Automation Center (IBA) for preventive automation. R11.1 updates the PAF function based on ADT in many ways, including:

- ADT-based PAF configuration: To ensure the critical assets defined within ADTs are functioning properly, the system executes the intents of ADT by preventive automation through one of the following ways:
  - **Looking Glass Probe**: Get the monitor status of a device via SNMP/CLI. Then based on the alert data, the intents defined within ADT intents can be matched and executed.
  - **Primary Probe**: Trigger the intents defined in the same row based on the probe column defined in the ADT table.
  - **Intent Timer**: Trigger the intent execution based on the intent timer pre-defined.



- Probe Instance enhancements: Improve the monitoring probe to support ADT-based PAF function.
- Auto Probe: Provide a quick way for power users to batch-create probes on a set of qualified devices or interfaces.

#### 3.2.1 ADT- Based Looking Glass Probe

#### 3.2.1.1 Looking Glass Probe

A probe performs diagnosis at the device level to determine its health status for a single device. Running a probe for the entire network requires the deployment of this probe on all devices, which leads to inefficiencies and increased traffic for both network devices and the NetBrain system. Alternatively, users can run the probe on a small set of devices (**looking glass probes**), which can detect any anomaly for the whole network. Then, these probes will parse alert information to identify problematic entries and trigger intent diagnosis for a larger group of devices. Typical looking glass probes include:

• **Route Table Check**: Filter critical route from the *show ip route* and compare the data with the baseline to verify the routes remain the same. Any changed routes can be exported to the error code to trigger the corresponding intent diagnosis stored in ADT.

• Neighbor Table Check: Using the command *show ip bgp neighbor*, compare the BGP neighbor status with baseline data to verify these neighbors are healthy. In case of any neighbor with issues, the neighbor information can be exported to the error code to trigger the intent diagnosis stored in ADT.

Users can choose the appropriate looking glass probes to monitor the network health status while utilizing minimal resources on both network devices and NetBrain System. If the looking glass probe generates an alert and the error code matches the corresponding intents in the ADT table, the configured intents will be triggered.

For example, a looking glass monitors the critical route status on a device. If there is any change in the routing entry for the looking glass probe, the changed entry (added, removed, and modified entries) will be exported into the error code. Then, the error code can be used to match the intents of ADT. The following table is an example ADT for the critical WAN link asset:

Failover Link Name	Primary Device	Critical Route	Secondary Device	Primary Link	Intent1	Intent2
Internet 1	R1	10.8.1.0/28	R2	R2.E0/0	Monitor Failover Link Health - Internet1	Verify QOS Config - Internet1
AT&T WAN	BOS-R1	192.168.10.0/24	BOS-R2	BOS- R2.e0/0	Monitor Failover Link - AT&T WAN	Verify QOS Config - AT&T WAN
P&G WAN	Tot-R1	172.16.16.0/24	Tot-R2	Tot- R2.e0/0	Monitor Failover Link Health - P&G WAN	Verify QOS Config - P&G WAN

Based on the error code table contents, we use the subnet contents to look up if there is any entry match.

Looking Glass Probe         Image: Second S								
Export changed entries with columns subnet/next-hop IP			Network Assets Failover Link Name	1: Failover links Critical Route	Primary Devices	Primary Link R1.E0/0	Secondary Device	Intent Check Failover-Internet1
Furger Code Table 1 @	1		AT&WAN P&G WAN	192.168.10.0/24 172.16.16.0/24	BOS-R1 Tot-R1	BOS-R1.e0/0 Tot-R1.e0/0	BOS-R2 Tot-R2	Check Failover-AT&T WAN Check Failover-P&G WAN
		(1	Find critical r	oute affected by	subnet informati	on	2	Execute matched Intents
Subnet Next-hop IP	Trigger		Network Assets	2. Critical applicat	ion naths			
10.8.1.0/28 10.8.1.49			Failover Link Name	Critical Route	Path Name	Path Device	Path Interface	Intent
10.8.1.32/29 10.8.1.49	Subnet Match Critical Route		Salesforce_Flow	→ 10.8.1.0/28	Webserver	Webserver	R1.E0/0	Check QOS Config-Salesforce Flow
						R1	R1.E0/1	
	-		Web Browser Flow	192.168.10.0/24	Data Engine	Data Engine	BOS-R1.e0/0	Check QOS Config-Web Browse Flow
						R2		
			Core_datebase	172.16.16.0/24	DataBase_Sever1	DataBase_Server1	Tot-R1.e0/0	Check WOS Config-Core Database
						R3	R1.E0/0	

The above diagram shows the error code generated by looking glass probe for several subnets and the changed subnet information exported from the routing table. Then, the system matches these subnets with the ADT Table column "critical route" to check if any WAN link is affected and find the first Failover link that contains the affected critical route. Further, the system will trigger the intent execution (*Monitor Failover Link Health-Internet1* and *Verify QOS config – Internet1*).

#### 3.2.1.2 ADT Creation Flow Based on Looking Glass Probe

The process of configuring looking glass probes to trigger ADT involves the following steps:

Installing intents of ADT to be triggered by looking	glass p	probe i	requir	es the i	following	steps:		1		Primary Flash Probe Details of	device R1				- · ·	
					-					Name: Interface Issue		Description				
										Display Name		Land II Date	atom Operations			
												United to Device		1		
1 Configure Looking Class										variables + Add	Define Abert Ru	es Roma 🗰 instructed	a v Table Key and V	10100	s to wontor: seed O	
1. Configure Looking Glass										<ul> <li>Interface (Clack Hota)</li> <li>Intfs.(table (Filter: Disabled)</li> </ul>						
Probe (Alert rule and Error											A (3 m	Γ.	✓ Does Not Equal	v Baseline v	View 🖀	
( )											<ul> <li>Select</li> </ul>		v			
Code)		Device		Looking Glass I	Probe	Error Co	de		Freque	ency	Boolean D	pression: A				
		VUS-BOS-F	R1 (	Check Route		2 Data Fi	eld		Every	1 Day	Then					
											Aiert Mess	age: Enter the messa	ige you want to display when the	Allert Rule is true.		
		Define th	e criteria to	find matching	rows in the autom	ation data table	e using error cod	ie			C Export	Error Code: Defined D	ata Fields			
2. Configure Match Condition																
for error code of LG probe with		ADT	Data Fields			Error Co	de Data Fields								ancel OK	
IOI CITOL COLO DI LO PIODE WITH		A Sut	bnet	~	Matches	~ Device		~	Û							
AD1 row		D No	ut have		Matches				÷			\				
		B INE	xt nop	Ŷ	Matches	* IP		×								
		C Sele	ect	~				Automatio	on Data Table	Trigger Method	Active	Probe Loc	ation	Preventive Coverage	Last Modified by	Last Modified Ti
								Wan Link I	Fallover	Looking Glass Pr	obe 0	9hi	ered Tables/WAN Link Fallover	Unknown	xxx/xx/xxxxx htcmmsss	xxx/m/xxxxx Mrze
		Boole	an A and i	в					Prevent	tive Coverage						×
																_
3. Calculate LG Probe Coverage									Set	lect Probe to calculate	Coverage	Results of All Probe	5	**	w: Show Not Covered Only	~
										All probes	20/100 its	ens are not being co	vered	-		
						_				Check Route (US-BOS-R1)	Coverage	Device	Config Check Route	g check intent1	mornz	
								-		Check Route (US-TOR-R1)	2 probes 2 probes	Probe 1: Config	Congreek Route Change	R2 Golden Config C	Neck R1 Config Drift Check	
										Config Check (US-805-R2)	2 probes	Error Code Row	Matched:	R3 Golden Config C	heck R3 Config Drift Check	x
4. (optional) Configure											1 probes	10.10.10.1/2	Next Hop	R4 Golden Config C	heck R4 Config Drift Check	k Cakula
cocondary probe for		Looking Glas	is Probe		Intent Execution I	tules	Data Table: WAN Li	ink Fallover	6		2 probes	Probe 2: Routing	g Check	R5 Golden Config C	heck RS Config Drift Check	x
secondary probe for							Remy 100			Calculate Coverage		Error Code Row	Matched:			intent
verification	Run se	condary probe befor	re executing intents	O Select Secondar	y Probe 🗸		Device Confi	fig Check	Ð			10.10.10.1/2	192.168.1.2			R1 Co
	Intent Opt	tions		To trigger the intent, in addition to matchi	the secondary probe needs i ng the criteria of the looking	o generate an alert glass probe.									Oose	R2 Co
	Execut	te All Intents					R1 R1.00	onfig Check	C R Part	et v BG# Dagnos			84	Config Check Route	Neck R3 Golden Con	fig Check R3 Co
and the second se	O Execut	te intents with Tags					R2 R2.00	oring Check					85	Config Check Route	heck R4 Golden Con	rfg Check R4 Co
5 (ontional) Configure Intent to							R5 R5.C0	orfig Check	0 #							
	Last Resor	rt Timer					R6 R6.C0	orfig Check	() N						0	
Trigger		a intent if intent has	not been triggered	by the probe or other	methods within										$\sim$	
IIIBBEI	Enforce	A HIGHLI HIGHLIGH		-,,												
IIIBBEI	2	Days N	Weeks Months											-D.	•	- 2
Inggen	2	Days	Weeks Months										N	et3r	ain	5

R11.1 enhances the probe with the following functionalities to support the looking glass probe:

#### 1. Compare with Baseline Data and Filter Rows/Columns if needed.

- Probe diagnosis results can be compared with baseline data that is initially stored when the probe is executed, and the data can be used as the baseline to check against further data.
- Table columns can be filtered by ADT table to keep critical ones or exclude non-important items.
- Certain table columns can be filtered so that only critical columns will be considered.
- 2. Export Error contents to error code.

Specified contents can be exported to the Error Code and can be used to match ADT columns.

Primary Flash Pr	obe Details of device US-E	005-R2						×	
Name:	Critical_route	Description:	Check critical rou	ute					
Display Name:	Critical_route	Level:	Device Level	O Interface	Level			Help	
Variables(1) +	Add 🗸	Define Alert Rules:		-1		S	elect Monitor Var	iables(0)	
▲ ► Critical Ro	ute s (Filter: Enabled )	Loop Table Row	s ows/columns	Co	mpare with baseline				
_		A 🖩 cisco	ios_routes	~	Does not equal	∽ Baseline	0	Ē	
		B Select V	ariable	~	_				
		Boolean Expre	ssion: A		Export Data to Error Cod	e ping from single varial	ole to Error Code:		
		Then			Export data from table:	mcisco_ios_routes	~		
		Alert Message	route entry	changed	route entry	device	+Add		
		Export Erro	r Code: Defined	define e	∎ subnet v	B this_device ∨			
view Sample				define e	rror code			Cancel	ЭК

#### 3.2.1.3 Looking Glass Probe Use Cases

Use looking glass probe to monitor critical parameters that can be used to drive the diagnosis of related network devices, such as critical routes, topology neighbor check and routing neighbor check.

- **Routing Table Check**: You can use the command *show ip route* and filter critical route to compare the data with the baseline to verify the routes remain the same. Any changed route can be exported to the error code to trigger the corresponding intent diagnosis stored in ADT.
- **Topology Neighbor Check**: You can use the command **show cpd neighbor** or **show lldp neighbor** to figure out the neighbor change for a core device, and from the changed entries, you can trigger the diagnosis of neighboring devices.
- **Routing Neighbor Check**: You can use the command *show ip bgp neighbor* and compare the BGP neighbor status with baseline data to verify whether these neighbors are healthy. If any neighbor has issues, the neighbor information can be exported to the error code, further triggering the intent diagnosis stored in ADT.

The following example shows a looking glass probe installed on **US-BOS-R2** for critical route check, where the border device can identify critical route changes and trigger the intent diagnosis for each critical route.



The creation of an ADT table triggered by Looking glass probe involves the following steps:

- Create looking glass probe: Create looking glass probes to create alerts.
- Create an ADT table: Create an ADT table for critical assets.
- Install ADT to be triggered by looking glass probes: install the ADT table to be triggered by looking glass probes.



# 3.2.2 Use Primary Probe to Trigger Intents of ADT

Looking glass probes may not be able to trigger all ADTs since some Intents may not find looking glass probes. In this case, use the probes defined in the ADT column to trigger the intent execution.

Users can add the primary probe column in the ADT tables, and the probe with its polling frequency can be executed periodically. The probe will trigger the configured intents within the same row it creates any alert.

No.	Name(Primary Probe)	VRF(String)	Interface(String)	IP(String)	I Source 1	Device Interface Status	Interface Config-let
1	CA-TOR-R1.CPU Check 🕚	RED Blue	e0/0 e0/1	10.10.10.10/24	Check Interface Status1	There aren't any issues for this interface	Interface ethernet 0/0 no shutdown ip address 10.10.10.10 255.255.255.0
2	CA-TOR-R1.CPU Check	Blue Green	e0/1 e0/2	12.10.10.10/24	Check Interface Status2	There aren't any issues for this interface	Interface ethernet 0/0 no shutdown ip address 11.10.10.10 255.255.255.1
3	CA-TOR-R1.CPU Check	Green RED	e0/2 e0/3	13.10.10.10/24	Check Interface Status3	There aren't any issues for this interface	Interface ethernet 0/0 no shutdown ip address 12.10.10.10 255.255.255.2
4	CA-TOR-R1.CPU Check	RED	e0/3	14.10.10.10/24	Check Interface Status4	There aren't any issues for this interface	Interface ethernet 0/0 no shutdown ip address 13.10.10.10 255.255.255.3

# 3.2.3 Use Intent Timer to Trigger Intents of ADT

Some ADTs may not be triggered by looking glass probes or primary probes. Instead, users can use the intent timer to run the intents of the ADT table periodically.

Items: 1	+ Install Automation Table	<sup>1</sup> Sort (alphabetically)		🛕 10 L	ooking Glass Probe	Search Q
Enable	Automation Data Table	Trigger Method	Location	Preventive Coverage	Last Modified by	Last Modified Time
	Wan Link Failover	Looking Glass Probe 3/3	Shared Tables/WAN Link Failover	80%	xx/xx/xxxx hh:mm:ss	xx/xx/xxxx hh:mm:ss
	Config Drift Check	Primary Probe 200/200	Shared Tables/Config Drift Check	100%	xx/xx/xxxx hh:mm:ss	xx/xx/xxxx hh:mm:ss
	Config Compliance Check	Intent Timer N/A	Shared Tables/Config Compliance Cheo	k Unknown	xx/xx/xxxx hh:mm:ss	xx/xx/xxxx hh:mm:ss
Intent Timer			Data Table: WAN L	ink Failover 🖸		
						Search Q =
Execution Sc	hedule Weekly on Monday	~				
	Every Monday from 2022-	-08-02 09:00 AM to 2022-10-30 9:00AM	Device Conf	ig Check Routing Cl	neck Intent1	Intent2
	Time zone. (orc- os.oo) e	Eastern nime	R1 R1.C	onfig Check 🕑 R1.Route (	Check 🕒 R1 Golden	Config Check R1 Config Drift Check
Intent Option	s		R2 R2.C	onfig Check 🕚 R2.Route (	Check 🕒 R2 Golden	Config Check R2 Config Drift Check
Execute A	ll Intents		R4 R4.C	onfig Check 🕑 R4.Route (	Check 🕒 R3 Golden	Config Check R3 Config Drift Check
C Execute S	elected Intents		R5 R5.C	onfig Check 🕑 R5.Route (	Check 🕒 R4 Golden	Config Check R4 Config Drift Check
Execute In	ntents with Tags		R6 R6.C	onfig Check 🕚 R6.Route (	Check 🕒 R5 Golden	Config Check R5 Config Drift Check

To configure the ADT executed by the Intent timer, users can install the ADT with the trigger method via Intent Timer. From the configuration window, select the intent timer to trigger the selected intents.

	its Netbrain Downioa	10	Published Intents	Preventive Autor	nation via ADT								
ltems: 1 🕂	Install Automation Table							🛕 10 Loo	king Glass P	Probe C	Search		٩
Enable A	Automation Data Table	≑ Tri	ger Method	Active Probe	Location		Preventive Co	verage	Last Modifi	ed by	Last Mo	dified Time	
. v	Wan Link Failover	Lo	oking Glass Probe	3/3	Shared Table	s/WAN Link Failover		80%	xx/xx/xxxx	hh:mm:ss	xx/xx/xx	xx hh:mm:ss	
	Config Drift Check	Pri	mary Probe	200/200	Shared Table	s/Config Drift Check		100%	xx/xx/xxxx	hh:mm:ss	χαλούλα	oox hh:mm:ss	
	Config Compliance Check	Int	ant Timer	N/A	Shared Table	s/Config Compliance Che	ck Unknown		xx/xx/xxxx	hh:mm:ss	xx/xx/xx	xxx hhommoss	
ntent Timer						Data Table: WAN I	.ink Failover [						
ntent Timer	: Select schedule	~	]			Data Table: WAN I	.ink Failover [				Search	۹	] :
ntent Timer xecute intent	Select schedule Weekly on Friday	0	]			Data Table: WAN I	ink Failover 🖸	Routing Chec	k	Intent1	Search	Q Intent2	] :
ntent Timer Execute intent	Select schedule Weekly on Friday Weekly on Sunday	0				Data Table: WAN I	ink Failover 📑	Routing Chec	k	Intent1	Search	Q Intent2	] :
ntent Timer ixecute intent ntent Options	Select schedule Weekly on Friday Weekly on Sunday Inte	0	Executes Every Moo	nday		Data Table: WAN I Device Cont R1 R1.C	ink Failover 🖸 fig Check	Routing Chee	k eck (3)	Intent1 R1 Golden	Search Config Check	Q Intent2 R1 Config Dr	) :
ntent Timer Execute intent Intent Options Execute All Execute Sel	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Every day	0	Executes Every Mor From: 2022-08-02 0 To: 2022-10-30	nday 9:00 AM		Data Table: WAN L Device Cont R1 R1.C R2 R2.C	ink Failover C	Routing Chee R1.Route Che R2.Route Che	k eck (S) eck (S)	Intent1 R1 Golden R2 Golden	Search Config Check Config Check	Q Intent2 R1 Config Dri R2 Config Dri	ift C
ntent Timer xecute intent ntent Options Execute All Execute Sel Execute Into	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Every day ent: Custom schedule	0 0 0 0	Executes Every Moo From: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 19:00 AM 15:00) Eastern Time		Data Table: WAN I Device Cont R1 R1.C R2 R2.C R4 R4.C	ink Failover C	Routing Chec R1.Route Che R2.Route Che R4.Route Che	k eck ③ eck ③	Intent1 R1 Golden 1 R2 Golden 1 R3 Golden 1	Search Config Check Config Check	Q Intent2 R1 Config Dri R2 Config Dri R3 Config Dri	ift C ift C
ntent Timer xecute intent itent Options Execute All Execute Sel Execute Inte	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Every day ent: Custom schedule Remove schedule	0	Executes Every Moo From: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 19:00 AM 15:00) Eastern Time		Data Table: WAN I Device Cont R1 R1.C R2 R2.C R4 R4.C R5 R5.C	ink Failover fig Check onfig Check onfig Check onfig Check onfig Check onfig Check onfig Check onfig Check	Routing Chec R1.Route Che R2.Route Che R4.Route Che R5.Route Che	k eck O eck O eck O	Intent1 R1 Golden I R2 Golden I R3 Golden I R4 Golden I	Search Config Check Config Check Config Check Config Check	Q Intent2 R1 Config Dri R2 Config Dri R3 Config Dri R4 Config Dri	ift C ift C
tent Timer recute intent tent Options Execute All Execute All Execute Inte	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Exery day ent Custom schedule Remove schedule	0	Executes Every Moo From: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 19:00 AM 15:00) Eastern Time		Data Table: WAN I Device Cont R1 R1.C R2 R2.C R4 R4.C R5 R5.C R6 R6.C	ink Failover ing Check onfig Check onf	Routing Chec R1.Route Che R2.Route Che R4.Route Che R5.Route Che R6.Route Che	k (*) sck (*) sck (*) sck (*) sck (*)	Intent1 R1 Golden I R2 Golden I R3 Golden I R4 Golden I R5 Golden I	Search Config Check Config Check Config Check Config Check Config Check	Q Intent2 R1 Config Dri R2 Config Dri R3 Config Dri R4 Config Dri R5 Config Dri	ift C ift C ift C
tent Timer ecute intent ent Options Execute All Execute Sel Execute Inti	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Inte Every day ents Custom schedule Remove schedule	0	Executes Every Moo Fram: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 19:00 AM 15:00) Eastern Time		Data Table: WAN I           Device         Cont           R1         R1.0           R2         R2.0           R4         R4.0           R5         R5.0           R6         R6.0	ink Failover ing Check onfig Check Onf	Routing Chec R1.Route Che R2.Route Che R4.Route Che R5.Route Che R6.Route Che	k () sck () sck () sck () sck ()	Intent1 R1 Golden I R3 Golden I R4 Golden I R5 Golden I	Search Config Check Config Check Config Check Config Check Config Check	R1 Config Dri R2 Config Dri R3 Config Dri R4 Config Dri R5 Config Dri	ift C ift C ift C
tent Timer secute intent tent Options Execute All Execute Sel Execute Intr	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Inte Every day ents Custom schedule Remove schedule	0	Executes Every Moo From: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 99:00 AM 95:00) Eastern Time		Data Table: WAN I           Device         Cont           R1         R1.C           R2         R2.C           R4         R4.C           R5         R5.C           R6         R6.C	ink Failover ing Check onfig Check Onf	Routing Chec R1.Route Chi R2.Route Chi R4.Route Chi R5.Route Chi R6.Route Chi	k (S) sck (S) sck (S) sck (S) sck (S)	Intent1 R1 Golden I R2 Golden I R3 Golden I R4 Golden I R5 Golden I	Search Config Check Config Check Config Check Config Check Config Check	R1 Config Dr R2 Config Dr R3 Config Dr R4 Config Dr R5 Config Dr	ift ( ift ( ift (
tent Timer kecute intent tent Options Execute All Execute Sel Execute Intr	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Inte Weekly on Monday ext: Every day ents Custom schedule Remove schedule	0	Executes Every Mon From: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 19:00 AM 15:00) Eastern Time		Data Table: WAN I           Device         Cont           R1         R1.C           R2         R2.C           R4         R4.C           R5         R5.C           R6         R6.C	ink Failover ing Check onfig Check Onf	Routing Chec R1.Route Chi R2.Route Chi R4.Route Chi R5.Route Chi R6.Route Chi	k Rek © Rek © Rek © Rek ©	Intent1 R1 Golden I R2 Golden I R3 Golden I R4 Golden I R5 Golden I	Search Config Check Config Check Config Check Config Check Config Check	R1 Config Dr R2 Config Dr R3 Config Dr R4 Config Dr R5 Config Dr	ift ( ift ( ift (
etent Timer kecute intent tent Options Execute All Execute All Execute Sel	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday iett Every day ents Custom schedule Remove schedule	0	Executes Every Moo From: 2022-08-02 0 To: 2022-10-30 Time Zone: (UTC- 0	nday 9:00 AM 15:00) Eastern Time		Data Table: WAN I Device Con R1 R1.C R2 R2.C R4 R4.C R5 R5.C	ink Failover ing Check onfig Check Onf	Routing Chec R1.Route Chi R2.Route Chi R4.Route Chi R5.Route Chi R6.Route Chi	k Rek (S) Rek (S) Rek (S) Rek (S)	Intent1 R1 Golden I R2 Golden I R3 Golden I R4 Golden I R5 Golden I	Search Config Check Config Check Config Check Config Check Config Check	Q Intent2 R1 Config Dri R3 Config Dri R4 Config Dri R5 Config Dri	ift ( ift ( ift (
tent Timer lecute intent ent Options Execute All Execute Sel Execute Intr	Select schedule Weekly on Friday Weekly on Sunday Inte Weekly on Monday Inte Weekly on Monday etct Every day ent: Custom schedule Remove schedule	000000000000000000000000000000000000000	Executes Every Mo From: 2022-08-02 Tro: 2022-10-30 Time Zone: (UTC- 0	nday 9:00 AM 95:00) Eastern Time		Data Table: WAN I Device Cont R1 R1.C R2 R2.C R4 R4.C R5 R5.C R6 R6.C	ink Failover fig Check onfig Check Onf	Routing Chec R1.Route Chi R2.Route Chi R4.Route Chi R5.Route Chi R6.Route Chi	k () ktk () ktk () ktk () ktk ()	Intent1 R1 Golden I R2 Golden I R3 Golden I R4 Golden I R5 Golden I	Search Config Check Config Check Config Check Config Check Config Check	R1 Config Dri R2 Config Dri R3 Config Dri R5 Config Dri	ift ( ift ( ift C

# 3.2.4 View Triggered Automation from PA Dashboard

PAF-based ADT results can be viewed from the PA dashboard or the **report and dashboard** new in R11.1. The following shows how the probe execution and intent trigger results can be viewed.

eventive Automation Dashboard	d	€Help S ¥ ×					
Network: 🚫 All Devices 🗸		1H 6H 24H 7D Custom @	Execution Tree			<b>0</b> H	elp G 🕴 X
		03/22/23 02:00 PM - 03/23/23 02:50 PM 🕚	ar BJ-L2-coreB ∽	Incident: Se	lect	03/22/23 02:00 PM - 03/	23/23 02:50 PM
406	1 991	1	All				
Devices	A Brober	Natural Intents				Show: 🗌 A	Hert Only Q
G Dentes			— Triggered by Current	Device			
Devic	ces with Alerts	Tag Distribution Across Intent with Alerts					
			vesion	DM set		nit_all_qif_BJ-L2-co	reB1 🔳
	Intent Alerts		09/29/23 02/21	PM			
	Procevience		CLI Unreacha	ble			
	64						
		No Intent Alerts	- A SNMP Onread	nable			
	341		High Erecuter				
7			03/23/23 02:21	PM ~			
No Alerts							
				-7			
64 Devices A 64	Probes with Alerts	Search Q					
Device	Probes with Alert	Intents with Alert	Legend				
All server-48,187	A 1	<b>1</b> 0	Alert History - All Automatio	ins			~ ~
apic1	A 1	10.0	49 Items Show: All	~		Search	Q 1
apic2	Δ 1	10 0	Execution Time	Probe Name	Alert Message	Executed NI	
apic3	A 1	10	3/23/2023, 2:21:03 PM	🖄 vesion	15.0(2)SE	nit_all_qlf_B)-	L2-coreB 1
BJ_Acc_SW1	A 1	10	3/23/2023, 1:51:04 PM	🖄 vesion	15.0(2)SE	nit_all_qlf_8]-	L2-coreB 1
BJ-Cat-5000	A 1	10 0	3/23/2023, 1:21:03 PM	🖄 vesion	15.0(2)SE	nit_all_qlf_BJ-	L2-coreB 1
@ BJ-R1	A 1	10	3/23/2023, 12:51:04 PM	🖄 vesion	15.0(2)SE	nit_all_q)f_B}-	L2-coreB 1
Bjta002443-SW12	A 1	10 0	3/23/2023, 12:21:03 PM	🖄 vesion	15.0(2)SE	11. citalloff.Bi-	L2-coreB1
BST	A 1	10.0	3/23/2023, 11:51:03 AM	X vesion	15.0(2)5E	nit_all_qif_Bj-	L2-coreB 1
EVE-L30UT-48,132	Δ 1	10	3/23/2023, 11:21:03 AM	X vesion	15.0(2)SE	nit_all_qlf_8}-	L2-coreB 1
			3/23/2023, 10:51:03 AM	X vesion	15.0(2)SE	nit all olf BI-	12-coreB1

The intent results for the current device triggered by the intent timer can be found in Triggered by Related

#### Device or Intent Timer.



## 3.2.5 Probe Instance Enhancement

Monitoring Probe has been improved with the following functions in R11.1 to support the looking glass probe use case:

	Primary Flash Probe Details of de	evice R1	×
	Name: Interface Issue	Description:	
	Display Name:	Level:   Device Level  Interface Level	
	Variables + Add	Define Alert Rules Variables to Mon	itor: Select 🕕
	<ul> <li>Interface [Cisco IOS]</li> <li>intfs_table (Filter: Disabled)</li> </ul>	✓ Loop Table Rows ⊞ intfs_table ✓ Table Key: intf ✓ ← 2 NEW If	NEW
Define Table Row/Column Filter		A I mtu ~ Does Not Equal ~ Baseline ~ View	Define Comparison with Baseline
		Boolean Expression: A	
		Then	
		Alert Message: Enter the message you want to display when the Alert Rule is true.	
		Export Error Code: Defined Data Fields	
	View Sample	Cancel	ок
		Define Error Code	

- 1. **Define Table row/column filter** to keep only critical contents.
  - Filter by column: Select the columns you want to keep so the probe will diagnose only certain columns.
  - Filter by row: Use the ADT table as the source for filtering the parser table. Users can keep or filter certain rows to match with ADT table contents.

Enable Filters for "intfs_table"			X
Filter by Column (3) C	ted columns		Unselect All
<ul> <li>\$crc</li> <li>\$deferred</li> <li>\$\$dly</li> <li>\$\$stuplex</li> <li>\$\$intf \$P\$</li> <li>\$\$intf_reset</li> <li>\$\$ip_addr</li> <li>\$\$mt</li> </ul>			
Filter by Row     Image: Construction of the second s	interface v Column Mappping	exist in below list	
interface	hosting_device	description	
f0/0	US-BOS-R2	This route is to PE1	
f0/1	US-BOS-R2	This route is to PE2	
f0/2	US-BOS-R2	This route is to PE3	
		Cancel	ОК

2. **Define Table key**: The table key can be defined directly within the probe. (In the earlier version, the table key comes from the parser definition).

The table key compares the table rows against baseline/last values to identify unique rows. When looping table rows, you cannot compare the table with the baseline/last value without the table key.

✔ Loop Table Rows 🛛 🌐	intf_vrf ∽ Table Key:	<u>intf name</u> ∨	
A Select Variable	~	✓ intf_name ○ vrf_name	
Boolean Expression:	eg. A AND B		
Then	-		

3. **Define Comparison with Baseline Logic**: use the baseline to define the comparison logic against baseline data.

When the data is retrieved for the first time, the data will be saved and used as baseline data. The baseline data remains the same and doesn't change. If the baseline data doesn't match the current network status, you can use the Clear Baseline function to clear the existing baseline. The system will further retrieve the data and use it as baseline data.

	International Action	Table Keys intf N			variables to ivio	nitor: Select 🕕	
If	H Intis_table •	Table Key. Intr					
A S mtu	~	Does Not Equal	~	Baseline	✓ View	<b></b>	
B Select Variable	~						
Boolean Expressio	in: A	'iew Baseline					
Then							
		\$route_source p	\$Nework	\$subnets	\$replicates	\$overhead	
Alert Message:	inter the messag	connected	0	9	0	612	
🗹 Export Error Co	ode: Defined Da	static	1	1	0	136	
		application	0	0	0	0	
		ospf 1	0	32	0	2380	
		nhrp	0	0	0	0	
 		bg65001	0	3	0	204	
							~

4. **Export Error Code**: Define the error code to export the error contents to trigger Intent execution within the ADT table. The error code column can be defined from the table or a single value used in the **if** condition.

Primary Flash Probe Details of device	Export Data to Error Code	×	×
Name:         Display Name:         Variables(3) + Add ∨         ▲ Image: BGP Interface Config Propert         ⊞ Intf_vrf (Filter: Undefined )         ▲ Image: BGP Neighbors [Cisco 105]         ③ BGP Neighbors [Cisco 105]         ⑤ bgp_rr         冊 bgp_nbrs (Filter: Undefined )         View Sample	Define the column mapping from single variable to Error Code: Export data from table:  Bbgp_nbrs   bgp neighbor +Add  max.nlri_update max.nlri_update min_incoming_ttl min_incoming_ttl mini_nlri_update mint: multisession_ca nbr_id nbr_type nbr_version Alert Message: Export Error Code: Undefined	:eline	e
Sample			×

The table column can be used as an error code column besides the single value. The error code column can be further expanded with the following data types:

 Built-in data > *this device*: this device can be exported if an alert is generated, which is very useful when there are multiple looking glass devices, and you want to define match conditions based on looking glass devices.

Export Data to Error Code		$\times$
Define the column mapping from Export data from table:bgp_	nsingle variable to Error Code:	
bgp neighbor +Add		
📔 nbr_id 🗸 🗸		
<ul> <li>Built-in Data</li> <li>this_device</li> <li>BGP Neighbors [Cisco</li> <li>Bgp_nbrs</li> </ul>	Cancel OK	
i ack_hold addr_family_ipv4	Does not equal	Ba
<pre>[] connection_ecn ]] connection_state</pre>	В	
<pre>[] connection_tabl [] connections_dro</pre>	-	
Alert Message:		

• Append column via ADT table: ADT column can be appended to the error code to expand the column.

port	data from table:	mbgp_nb	rs 🗸						
	aighbor	+Add						- 84	
1	O New Column	<ul> <li>Apper</li> </ul>	nd Column						Select Mor
	Column Display	Name				Cancel	OK		
	C 1 N					Cancer	UK	eline	
L	Column Name			~	Does not	equal	~	Baseline	
	Append From			~					
	ADT Table	O Function							
	Select ADT Table	to Append C	olumn						
	New Table1		~						
	Lookup Assess Column								
	device								
			v						
	Error Code Colu	nn							Cancel
	bgp neighbo	r	~						
	Lookup Column								
	device		~						
		Cancel	ОК						

#### 3.2.6 Auto Probe

Auto Probe provides a quick way for power users to create probes from the seed probe(s) in batches on a set of qualified devices or interfaces. Once completed, power users can use these device/interface probes to set up the ADT-based PAF.

Search Anything and Create Map	Search Path		Support Search Incident	rwang
⚠️ Preventive Automation Manager		8	(1%) devices have monitoring probe enabled	1 (0%) devices have preventive automation enabled (2) Help
Monitoring Probe Auto Probe Probe Triggered	Intent Probe Triggered Intent Cluster	Schedule CLI Commands Po	olling Control	
Type to search     Q     S     ≪       ▲ ≦     Shared Auto Probes (2)     ∠     ≦       ▲ ≦     Cisco (2)     ▲     Critical WAN Link Status Check	OSPF Neighbor Check  Description:	Author: chris	Probe-	Save
OSPF Neighbor Check	Level:  Device  Interface	Type:      Primary      Secondary	Probe Timer: Every 4 weeks	
Auto Probe Manager	Seed Probes	+ Ad	d Select critical variables	
Auto Probe Manager	🟠 OSPF Neighbor Check		The Variable	Critical Variable
			<ul> <li>OSPF Neighbors [Cisco IOS]</li> </ul>	
			▲	
			s \$dead	
			s \$intf	
			s \$nbr_addr	
	2. Instantiate Probes	arget Devices/Interface	es to Create Probes	
	Probe Name: OSPF Neighbor Check		Description:	
	Target Devices: 1 Device Groups + S	elect From Automation Data Table		Create Probe
	Probe Created(31) Failed(101)	Execution Log		Search Devices Q
	Device		Probe Status	
	BJ*POP		Disabled	
	BJ-3750-1		Disabled	
	BJ-L2-coreB		Disabled	
	BLL2_Core_5		Disabled	

Besides selecting the seed probes and target devices or interfaces, users can specify critical variables to identify whether the probe is qualified on the target device. With the critical variables, the system can test the critical variables against the live network and find the correct seed probe for a target device.

🛕 OSPF Neighbor Check ∠	Auth	Author: chris Save							
Description:									
1. Define Probe Information									
Level:      Device      Interface	Type: 💿 Primary 🔿 Secondary	Pr	robe Timer: Every 4 weeks						
Seed Probes	+ Add	Select	critical variables						
A OSPF Neighbor Check [Cisco]	≡	4	Variable	Critical Variable					
OSPF Neighbor Check [Juniper]	=	4	SPF Neighbors [Cisco IOS]						
OSPF Neighbor Check [Extreme]	Ξ	4	<pre>m ospf_nbrs</pre>						
			§ \$dead						
			s \$intf						
			s \$nbr_addr						

## 3.2.7 Other New Features and Enhancements for PAF

#### 3.2.7.1 Last Resort Timer

For intents triggered by looking glass probe or primary probe, there is a chance that the probe status is healthy and probes generate no alerts for some time. To ensure that these intents are executed even if no alert is generated, enable **Last Resort Timer** and configure the condition. So if certain intents are not triggered within the defined time frame, the system will further trigger the intents to execute.

Looking Glass Probe	Intent Execution Rules	Data Table	e: WAN Link Failover	2	
Run secondary probe before executing intent	s ● Select Secondary Probe ~	Items: 100			
Intent Options	To trigger the intent, the secondary probe needs to generate an alert	Device	Config Check	Routing Check	
Execute All Intents	in addition to matching the criteria of the looking glass probe.	R1	R1.Config Check (	R1.Route Check	٩
Execute Selected Intents		R2	R2.Config Check (	R2.Route Check	•
Execute Intents with Tags	Execute Intents with Tags				٩
		R5	R5.Config Check (	R5.Route Check	٩
Last Resort Timer		R6	R6.Config Check (	R6.Route Check	٩
Enforce intent if intent has not been triggered	d by the probe or other methods within				
2 Days Weeks Months	5				
Trigger Suppression Settings					

#### 3.2.7.2 Trigger Suppression

For intents triggered by looking glass probe or primary probe, if the probe generates alerts consecutively and you don't want the intent to be triggered each time, configure the trigger suppression to specify the intents to be triggered once within the defined time frame.



## 3.3 Install ADT to Auto Intent

Auto Intent allows users to create and run intents on Map, which can be enabled from the Auto Intent Tab in Intent-Based Automation Center (IBA Center, Intent Library in the early releases). R11.1 makes the following enhancements for the Auto Intent:



- 1. **Pre-qualified Automation Assets:** A folder structure to display and organize ADT's network intent templates and automation assets (intent/map/path). Users can view and use the items by category.
  - **Intent Template:** The intent templates enabled for Auto Intent are listed in the left pane.
  - **ADT Assets:** Intents/Maps/Paths of the enabled ADT are listed in the left pane.
- 2. **Selected Device/Intents:** Show the items selected from the left pane.
- 3. Intent Preview & Input for Macro Variables: Preview items highlighted or selected in the left pane and the items highlighted in the Selected Device/Intents area to facilitate network intent selection; input values for macro variables of the target device to create proper intent.
- 4. **Save & Run Intent:** Run intent and view the execution results, then add the created intent as map/path/common intent for further troubleshooting.

#### 3.3.1 Auto Intent Tab in IBA Center

Generally, power users will operate on the Auto Intent tab in IBA Center.

• Enable intent template for Auto Intent so that end users can replicate intent templates and customize the macro variables if necessary to create appropriate intent for map devices.



耳 Intent Based Automation Center

• Enable ADT (Automation Data Table) Intents/Maps/Paths for Auto Intent so that end users can find related automation assets (Intent/Map/Path) for map devices from pre-defined ADT to understand and troubleshoot network problems.

Installed Intents	Published Intents	Prevent	ive Automat	on via ADT	Auto	Intent NetBrain	Download			
Add Folder		Auton	nation Data	Table: Failove	er Links De	escription: Description for	r Diagnosis Code1			Sav
🛅 Cisco IOS Regular	Check	Displa	y Name in A	uto Intent:	Failover Links					
🔺 🚞 Design Check										
L3 - Route Ch	neck	Find a	utomation a	ssets by devic	ce properties o	or visible interfaces:				
1 L3 OSPF Che	ck	А	HSRP VIP		✓ Mat	tches ~ Mgmt	IP ~ 🕇	i i i		
L2 Switch VT	P Check		6-1	•						
Error Detect	back	5	Select Criter	Id	Ť					
Eailover Link	s									
Path Related Inte	nts	Boo	lean Expres	sion: A						
I QoS		Select	intents/map	s/paths to be	listed in Auto	Ena	Enable ADT for Auto Intent			
<ol> <li>Security Rule</li> </ol>		List	List in Auto Intent Intent Column Display Name							
🌐 Data Center1 F	aths			<b>1</b> So	urce1					
						60 4 (61)CDD 1//	n 1			
			<b>4</b>	II AU	itomation i	\$Source1 (\$HSRP_VI	P) 🗲			
				🚠 Au	itomation Map	\$Automation_Map		-		
				Pa	th					
		ADT P	review:							
		No.	Name	HSRP VIP	Group ID	Source 1	I Automation1	Failover Config-let	💑 Automation Map	Path
		1	Group1	10.8.1.1	1	Check HSRP	Check HSRP1	interface Vlan400	HSRP Design	Core HSRP Path
								ip address 10.8.3.194		
		2	Group2	10.8.2.2	2	Check HSRP Nbr	Check HSRP Nbr1	interface Vlan400	HSRP Nbr Map	HSRP Change
								in address 10.8.3.194		0
		2	C2	10.9.10.5	11	Chack UCDD	Chack HCDD1	interface Vian 400	CALUSED Design	USDD Desire
		3	Group3	10.6.10.5		CHECK HORP	CHECK HORP I	interface vian400	CA MSKP Design	HSKP Design
								ip address 10.8.3.194		

• Build a folder structure to display assets in Auto Intent Pane with a clear and meaningful organization so that end users can understand and operate on the automation assets.

In the second	D		<b>C</b>
1ntent	Based	Automatio	n Center

Installed Intents	Published Intents	Preventive Automation via AD	Auto Intent	NetBrain Download
+ Add Folder		Intent: conf-ACL-extended	Description: Description for	or Diagnosis Code1
Search Q  Cisco IOS Regular Check  Design Check  L3 - Route Check  L3 OSPF Check  L3 OSPF Check  L2 Switch VTP Check		Intent Decoding Schedule: R Replication Settings for Auto On-demand Not use l Pre-replicated 0 devices	Recurring - 6 PM Friday Weekly o Intent: baseline data s replicated for this intent.	Last Decoded at: 06:53 /
<ul> <li>Error Detect</li> <li>SNMP ACL Che</li> </ul>	eck	2 Macro Variables:	Macro Variable	Command
Hailover Links	-c	VPE-DE1	Waci o valiable	Command
I QoS			VRF Name	show ip route vrf
💶 Security Rule 🌐 Data Center1 Pa	ths		VRF Name	show ip route vrf

#### 3.3.2 Use Auto Intent to Create Intent for Map Devices

Auto intent supports replicating the intent template with customizable macro variables. With this functionality, end users can replicate desired intent from an intent template by simply setting the macro variables.



- Users can preview the data of the intent template via the following two operations:
  - Click (unselect is OK) an item in the Pre-qualified Automation Assets pane to preview its macro variables and command data.
  - o Click an item in the Selected Device/Intent area to preview its macro variables and command data.
- If the intent template has macro variables defined, users can change the value, which will affect the replication results.

#### 3.3.3 Use Intent Template Not Included in Auto Intent

Apart from the intent templates already listed in Auto Intent, users can use additional ones not installed and decoded in IBA Center, giving users more flexibility to use intents in Auto Intent.

Select one or more devices (Devices not included in the device list can also be added and selected) and one intent template to pair and add to the Selected Device/Intent Entries area.

ed Inten	ts E	Embedded II	ntent	Add Intent			×
~~	Creatio	n of Intent					
0 ≡	Last Cre	pated: 6/15/2	022, 8:55:25 A	Select Devices:	🗹 🤭 ВЈ*РОР		
A	dd Intent	e/Inte	ent Entries		🛃 🔤 BJ-L2-Core-A		
Vi	iew by Inte	ent	ent Entres		🕑 🥗 BJ-R3		
Se	elect All		L3 OSF		✓		r
D	eselect All	:-SW1	1-Weel		ST_POP2		
vitch	🥔 C	A-TOR-SW1	其 L3 OSF		STX.Core 😂		L
	🙆 В	J*POP	I Switch		STX.Core2		
: •	🤭 В	J_R1	I Switch		+ Add Devices		0
	🤭 R	2	1 Design	Select Intent as	Template: Select		2  -
k	🤭 R	3	I BGP N	Select intent as	Template. Select		4
:hec	🤭 R	4	I BGP N			Cancel	ОК
	🤭 R	5	I Design				I

#### 3.3.4 Filter Intent Template/ADT in Auto Intent

In R11.1, the filter function of Auto Intent is improved to be more intuitive and functional. When there are too many items, users can find the ones needed by filtering the items. An independent pane will appear to the left after clicking  $\Upsilon$  Filter (0), making it easier to define the filter conditions centrally. The improved filter function leads users to pay more attention to the automation assets and network objects enabled for Auto Intent.



#### 3.3.5 Use ADT Automation Asset Via Auto Intent

To fully understand and troubleshoot an issue, users normally need to analyze the related maps and paths besides intents. By enabling ADT assets (Intent/Map/Path) to be used in Auto Intent, users can find automation assets for map devices, e.g., device-related failover links and the map, device-related path, and the path intents.

With the available ADT assets in Auto Intent, users can complete the following tasks:

	Auto Intent	Publish	ed Intent					
Pre-qualified Automation Assets								
8 D	evices 🕂		⊜ ≡					
T	Filter (0)	Search	Q					
A	II BGP (1)	IOS (3)	»					
4	💋 🧉 BJ*POP (8)							
	🖌 🗾 Command	d Check for S	witch					
	🛃 🖳 L3 Route	e Check - Ciso	to IOS					
	🗾 I Design I	Neighbor Che	ec					
	🔺 🛃 🔚 Failover	Links						
	🗸 I Swite	ch VLAN Cheo	ck					
	🗹 I Desi	gn Neighbor	Chec					
	💦 HSRF	P Design						
	💦 OSPI	- Nbr Map						
	<mark>ջ</mark> ያ App2	2/DC-HQ	-					
	<mark>ջ</mark> ያ App1	l/QoS Trainin	g					

- Use intents from ADT to create an intent for troubleshooting.
- View a map and use the map for troubleshooting.
- View a path and use the path for troubleshooting.

## 3.4 Use ADT to Replicate Path Intent

R11.1 made the following improvements on path intent:

• Path intent replication settings in the intent template (NIT): The system allows defining path macro variables or selecting ADT data sources as macro variables for an intent template to prepare for creating

path intents. Specifically, path variables and path device variables are used as the values of the macro variables of the intent template.



- Batch Path Intent Replication from ADT New: With the method "Intent Replication for Path" provided for building column groups in ADT, multiple path intents can be delivered from ADT with the data in ADT for running troubleshooting diagnosis.
- On-demand Path intent replication from path browser/Auto Intent <sup>New</sup>: Users can set to replicate path intents by selecting the intent template from an open path or Auto Intent. With the new improvements made on path intent replication, one path can have multiple path intents.

# 3.4.1 Batch Path Intent Replication from ADT

In R11.1, the system supports creating path intents with the new intent replication for path service in ADT.

The following diagram shows the logic of cloning path intents in batch via intent template with the data source in ADT.

	Automation I	Data Table ·	- Intent Replicat	tion For Path			
Application Name	Path Name	Path Status	Path Map	Path Intent		Path1	
Salesforce_FI ow	Web_Server	Success	Web_Server	??	Select Application Paths as Base Table	Path2	
Salesforce_FI ow	Data_Engine	Failed	Data_Engine	??			
Core_databas e	DataBase_Sever 1	Success	DataBase_Sever1	??	Set Cloned Intents	Path3	- 3
		• Application	Path ADT as Base Tab	le	As Path Intent	Path4	th Brow
Annual Information Allow Standy Lines of the Annual Standards		And				Path5	ser
				_		Path6	
Marine Mari Marine Marine Mari			Set cloned intents a	s Path Intent	1		
	******						

In the Intent Replication for Path Service, ADT serves as a tool to provide data to replicate path intents as scheduled. Specifically, users can add a group column to ADT via the "**Intent Replication for Path**" method. The available data fields include path intent and data fields of the path intent details. With the data in ADT, users can further set the variables for path intent replication. The created intents can be saved as path intents for future use.

olumr	n Header:													-		
B	c1 S	C	c2	0°	c3	<b>4</b> E	c4	5 ()	c5	s Đ	c6 Dath Ctatur	5 8	c7	I ()	c8	5
Aþ	c9 S	1	Patri		Path Device:		Source				Path Status		Path Intent		Intent Output	
	Prority															
	New Group															
126	New Group	Ŧ			Column Group (N	lew Group):									Select Co	olumn 🗸
escrip	ition:															
ASSOCI	lated intent for pat	n			c8	Outout		c7								
elect N	Method to Build Gro	oup Tabl	e:		Intent 1	Message	S P	ath Intent								
ntent	Replication for Pat	th	,	~												
tent T	Template: Select															
Correct 1	emplace. Select				(Drag and drop	column heade	from the upp	er area or avi	ailable data fi	ld from the le	eft here)					
uilt-in	Fields:															
£	Path Intent		p	C	efine Logic to Po	pulate New Ci	plumns for Ea	ch Row								
0					Clone Intent by	Path Varia	bles 🗸	on Path C	olumn: P	ath		~				
tent (	Dutput:															
C	Intent Message	5			Set cloned int	ent as path in	tent									
	Intent Status Code	S														
	Device Status Code				If path i	ntent with the	same name a	already creat	ed , what do	ou want to	do? 🕦					
	Device Status Code	: 0			<ul> <li>Over</li> </ul>	write Existing	Unlocked Pat	h Intents (	) Keep All th	e Existing Pa	th Intents					
	Intent Devices	્ય														
	Intent Map					~										
	test CI I Common				Lock Path Intent	0										
Ir	itent CLI Command	as 🖻														

The path parameters can be passed to the Macro Variables of the seed NIT to clone a path NI.

No.	Application Name S	Path 🙎 📑	Path Devices	ą	Source	5	Destination	S	Path Status	Path Intent			Intent Output	S	Prority	=
1	Salesforce Server	App1	BJ-3750-2 BJ-Arista-1 BJ-Arista-2		10.10.10.1		192.168.1.1			Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_ para equals to baseline Paragraph1 of GW2Lab has	_3 h s	н	Î
2	QOS Path	NYC-to-BOS	BJ-Avaya-1 BJ-Avaya-2 BJ-Cat-5000 BJ-L2-Core-A		10.8.8.162		10.8.1.26			Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_ para equals to baseline Paragraph1 of GW2Lab has	,3 h s	м	
3	Traditional Data Center	App1	BJ-Avaya-2 BJ-Cat-5000 BJ-L2-Core-A BJ-L2-coreB		10.8.1.4		10.8.3.140		Failed	Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_ para equals to baseline Paragraph1 of GW2Lab has	_3 h s	H+	
4	QOS Path	DB Backup	ASA-AA/admin/act ASA-AA/admin/stby BJ_L2_Core_3 LA.DIS,1		10.8.1.4		10.8.3.130			Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_ para equals to baseline Paragraph1 of GW2Lab has	_3 h s	м	ł
5	POC	MPLS_DMVPN_PATH	BJ-R2 BJ-R3 BST,POP1 qapp-c3560-1		10.8.2.19		10.8.5.11			Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_ para equals to baseline Paragraph1 of GW2Lab has	,3 h 5	H-	
6	Traditional Data Center	App2	ASA-AA/context1/stby BJ*POP BJ_L2_Core_3 BJ_core_3550		10.8.1.4		10.8.3.196		Failed	Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_ para equals to baseline Paragraph1 of GW2Lab has	_3 h 5	н	
7	QOS Path	NYC-to-SMF	Emu_NB_NYC_MGMT F5-MGMT		10.8.8.162		10.8.2.14			Monitor Pa	h Healt	h	para equals to baseline Paragraph1 of BJ_L2_Core_	_3 h	L	

## 3.4.2 On-demand Path Intent Replication from Path Browser/Auto Intent

In the previous versions, a path is associated with only one path intent. In R11.1, multiple path intents can be created and associated with one path, which enhances the capability of executing path intents for troubleshooting network issues from a path. All the path intents of a path are included in a "**View**" list in the Path Intent Pane. There are two ways to create a path intent:

• Replicate the path intent via Intent Template from the **Path Detail Pane**:



• Open **Auto Intent** to create path intent for a path: After a path intent is created with the automation assets in Auto Intent, the created intent can be associated with a path and saved as its path intent.



# 3.4.3 Delete/Unlock Path Intents in Batch

The system offers several options for deleting/unlocking path intents in batch.

Batch Remove/Unlock Path Intents from Network Intent Manager: In Network Intent Manager > Path Intent, each path forms a folder to include all the associated path intents. Users can delete/unlock multiple path intents at one time in the pop-up Dialog opened from the drop-down menu.

≣	NotBrain Search Anything and Create Map	Q Search	📀 Path	Search incident 🔍 🚊 🚍	📫 🌐 BOS lab Domain 1 🔮 🔞
+	Network Intent Manager > Path Intent	Help 🖸 🕴 🗙			
1	Path Intent	v			
Files	Search	Q			
&	2022 application		Delete Intents	Sea	
Site	training 2022		Intent Name	Lock Status	
() Network	i test 2		App 1     at-lab	🔒 with Password	
<u>9</u> 2	Auto test app     Auto test     Auto test app     Auto test a	v itents	App 2	🔒 with Password	
Path	App1     Delete In     at-lab	tents			
Runbook Template	▲ 🔮 App2 ■ App2				
<b>(</b>	I at-lab-2				
Network Change					
	I intent path -1		If you want to delete a locked inter	nt, please unlock it first.	Cancel Delete
Desktop	NYC-to-BOS				
Мар					
Desktop					

• Batch Remove/Unlock Path Intents from ADT Manager: for an ADT containing Path Intent Column, users can delete/unlock multiple path intents at a time in the pop-up dialog from the drop-down
#### menu of the Path Column.

Failover Link	S	1	Auto APP	CA-1	TOR-R1		10.10.10.1		192.16	58.1.1	Succe	Edit		
y Tables				CA-1	TOR-R2							Delete	Column	
Delete Ir	ntents								×	3.1.13	Succe	Delete I	ntents	
Itom: E						Canroh		0		~		Unlock	Intents	K
item: 5						Seurch.		~				Set as T	able Key	
۰	Intent Name			l	ock Status.							Tag Cur	rent Column	
	Auto App				🔒 with Pass	word				0.13	Success		Con-ACL-Stand	lard
	NY to BOS Tes				🔒 without P	asswore	i							
	BOS Test 1				🔒 with Pass	word				2	Success		BOS path test	
	💶 BJ-Lab													
	BOS Test 2													
										.1.1	Success		BOS path test 2	2
<li>If yo</li>	u want to delete a locked i	intent	t, please unlock it first.											
								a luc						
							Cancel	Delete						
				_										

# **4** Network Intent Enhancements

R11.1 has updated no-code intent capture, replication, and execution in many ways, including:

All Logic Block in the Diagnosis	Embedded Incident New	
Dagnosis Message: Save to Embedded  Save to Embedded  Hig Set Status Code for Device:  Hig Set Status Code for Intent:	ncident = Send Email: Include Intent Link S Include Link to Embedded I To: Select user or Input email Subject: [NetBrain] Intent Execution Issues.	addent ℤ = ♥ ii ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
Export to CSV Report: Define     CSV Name: BOS Lab CSV 12/12 - 1	E Intert Variable:     gVar1	
Collow Up Intent:      Network Intent     Current Intent (Self)     Stop Intent: Check Interface Status     Intent: Cluster: Single Device Sample     Intent: Template: BGP Check	Dydate Table Row: Define     Table Name: Incident Table     Update Column: column 1     R. Delete Table Row: Define	Operation on Intent Table
Intent Data View: Define  C device data unit, 3 interface data unit, 1 device note	Table Name: Indident Table Condition: Status contains changed	=
& Webhook API Call: Select Webhook: ServiceNow-1 v Json Body Sample	Call Qapp: Define Qapp:AA,Show interface [Cisco IOS]	5 Follow-up Qapp New
budy variatives Variative Value msg Select One status Select One	Set Intent Baseline      Set Baseline of All Commands v of This Device v with Current	Vpdate Intent Baseline
	All Logic Block in the Diagnosis	All Logic Block in the Diagnosis

- On-demand Replication of Intent (NIT)
  - Support replication intent on-demand for auto-intent, TAF, PAF, Bot, and follow-up diagnosis.
- Enhancements on Intent's No-code Programmability
  - Use intent to build map and data view <sup>2</sup> (this number refers to the number in the picture)
  - Embedded Incident <sup>9</sup>
  - Follow-up diagnosis with intent template <sup>1</sup>
  - Follow-up diagnosis with self<sup>1</sup>
  - Follow-up diagnosis with ADT (automation data table)<sup>1</sup>
  - Use ADT as the database for intent <sup>6</sup>
  - New operation on intent table <sup>6</sup>
  - Control the update of intent baseline by logic <sup>4</sup>
  - Intent Variable and Intent diagnoses <sup>7</sup>

#### • Enhancements on Intent's Notification

- Send an email with payload from within intent <sup>8</sup>
- Send data to 3<sup>rd</sup> party solution via webhook API <sup>3</sup>
- Use Qapp as a follow-up action <sup>5</sup>
- Other enhancements on intent:
  - Scheduled execution of intent directly
  - o Build intent on API-based network including cloud and SDN
  - Simplified intent debug
  - Export CSV report to Files
  - View diagnosis messages
  - Intent View UI enhancements

R11.1 introduces a new concept called '**Diagnosis Logic Block**' or '**Logic**'. The previous diagnosis logic is separated into 3 types of Logic: **diagnosis note & status code, export CSV,** and **follow-up intent**. R11.1 adds new logic: **Intent Data View** and **Webhook API Call**.

## 4.1 Create Intent Data View and Intent Map

Map and data view is the foundation for troubleshooting network problems. R11.1 improves the automatic creation ability of the intent map and adds a new concept, **intent data view**, to display the results of intent on the map, such as the network design and the intent status.

• View Intent Map and Intent Data View (End User)

Under the Intent pane of a map, end users can open an intent map and the data view for the published, embedded, or auto intent.



Users can also open an Intent from the Intent Manager and then Intent Map or Intent Data View from within the Intent.



- Open Intent Map: if the intent map does not exist, the system will create one based on the Intent Map Settings.
- Apply Intent Data View: Click the eye icon to apply the intent data view to the current context map. If any device used by Intent Data View is not on the map, the system will draw it on the map.

• Build Intent Data View: Users can add a new logic, '**Intent Data View**', in the intent diagnosis and define the intent data view.

	Create Intent Data View
2. Define Diagnosis     Add Note @ Add Diagnosis Can also click a variable on the left to add automation.      E Select Variable     Boolean Expression: A or B or C or D	Crate Interface Mater Phighlight Device Note Profestor Note
Set Intent Baseline     C       Advanced     C	Add Prefix interface:
Add Logic 🗸	+ Add Hypertix

• Create Intent Map: If the intent map doesn't exist, users can define the Intent Map Settings for the system to create one and then manually optimize the map layout and annotation.

Diagnosis Intent Template Settings	Network Intent (Edit Mode)	
Add Intent Diagnosis Block Switch Devices	🚺 route change monitoring (Published) 🚠 Diagnosis Tree Run 👻	with Live Network Save
	Check route table	👶 Intent Ma
	😕 + Add Device	Select Ma
	V 🕙 US-BOS-R2 Type Description here	dd Config Diagnosis 🛛 🖬 + 🖊 Create M
×	show ip route     Type Description here	Edit D
Data Source Settings Incident CSV Report Files Follow-up Intent	Protocol         Address         Age (min)         Hardware         Type           2         Internet         3.3.3         -         0003.0003         ARPA           12         Internet         172.24.10.250         192         00d3.58ac.fef2         ARPA	CSPF Nbr Down
Map:	13         Internet         172.24.10.249         -         000e.d7a7.1900         AMPA           22         Internet         172.24.10.225         136         022.5589.1900         AMPA           26         Internet         172.24.10.225         136         021.5589.1500         AMPA           28         Internet         172.24.30.1         -         000e.d7a7.1500         AMPA           29         Internet         172.24.36.2         9         001e.0fe2.5582         AMPA	
h IPv4 L3 Topology ~	✓	dd Config Diagnosis 🛛 🗖 + Add CLI Diag
t 3 neighbor devices for the devices	Show ip ospf interface Type Description here	Edit Di
	1 Topology-MTID Cost Disabled Shutdown Topology Mame 2 0 1 no no Base 3 Fohlod by indefine geneficiencies (and discovery in addresses)	CSPF Neighbor Dia
atus Code in Intent datavlew. o home intent when current intent is used as follow up intent.	<ul> <li>Limited of interime Contrary including decommany is soluces and</li> <li>Loopback interfaces is treated as a stub Boat</li> <li>Tunnel0 is up, line protocol is up</li> <li>Internet Address 10.8.1.65/30, Area 0, Attached via Network Statement</li> <li>Process ID 1. Router ID 10.11.11.1</li> <li>Network Type NOINT_COst 55</li> <li>Topology-MTLD Cost Disabled Shutdown Topology Name</li> </ul>	

### 4.1.1 Build Intent Data View

The Intent Data View is designed to display the diagnosis data and results on an intent map or any map, so users can view the network design or monitor the network status on the map.

Users can add a new logic, '**Intent Data View'**, in intent diagnosis and define the intent data view with the diagnosis data. Besides defining the device and interface data units, users can define the highlight and notes and draw a relationship arrow between devices.

Note	9	•	)	1 Interface Notes
A a Davisa	IPv4 Interface 🗸 🌖 1	intf(string)	👔 h_sequence(int)	
Highlight Highlight	ationship Arrow	q cnt(int)	) 📔 seq.nr(int)	🖕 1 Interface
Hostname	0		)	Highlights
🤍 📜 eigrp_neighbors(table)		i		
<b>?</b>	▶ Defin	e More		
<b></b>				
3				
Define More  Arrow for Neighbor Device				Re
Define More  Arrow for Neighbor Device  Source Destination of Arrow:		Visual Sty	1e:	Re
Define More  Arrow for Neighbor Device  Source Destination of Arrow:  Source Device:	Sthis device	Visual Sty Col	le: Random Color	Re
Define More  Arrow for Neighbor Device  Source Destination of Arrow:  Source Device:  Annotation for Source Device:	Sthis device Sthis_device	Visual Sty Col	le: or: Random Color s	R(
Define More  Arrow for Neighbor Device  Source Destination of Arrow:  Source Device:  Annotation for Source Device:  Destination Device:	sthis device Sthis_device	Visual Sty Col Line Sty Wid	He: Randam Color Mer	Ri
Define More  Arrow for Neighbor Device  Source Destination of Arrow.  Source Device:  Amoutation for Source Device:  Destination Device:  Amoutation for Destination Device:	Sthis device Schis_device II fiGRP_nbr_devicename SEISRP_nbr_devicename	Visual Sty Col Line Sty Wid Arre	Ne: Random Color Ite Mere Rendom Color	₩ 

### 4.1.2 Build Intent Map

An Intent Map is a map embedded in an Intent to show the network relationship between devices of this Intent. It can be created in two ways:

- Manually create a map first, then associate this map with an intent.
- Create an Intent Map automatically by the Intent Map Settings

route	change monitoring	Published	🛔 Diagnosis Tree			Run - with Live Network	Save 🕜 Help
eck rou	te table						Intent Map: Select
+ Add	Device						Select Map
<b>(</b>	US-BOS-R2	Туре	Description here			• Add Config Diagnosis	+ A Create Map
4 P	show ip route	Туре	Description here				Edit Diagnosis
1	Protocol	Address	Age (min)	Hardware	Туре		OSPF Nbr Down
1	Internet	3.3.3.3	-	0003.0003.0003	ARPA		Message Data View
12	1 Internet	172.24.10.250	192	00d0.58ac.f6f2	ARPA		
13	Internet	172.24.10.249	-	000e.d7a7.b900	ARPA		
22	Internet	172.24.32.225	136	0021.5589.b900	ARPA		
26	Internet	172.24.32.226	-	0021.5589.b520	ARPA		
28	Internet	172.24.36.1	-	000e.d7a7.b900	ARPA		
	US-BOS-SW1		Type Descript	ion here.		- + Add Config Diagnosis	+ Add CLI Diagnosis
⊿ <b>Þ</b> =	show ip ospf interf	ace	Type Descript	ion here			Edit Diagnosis
1	Topology-MTID	Cost Disabl	ed Shutdown	Topology Name			OSPF Neighbor Diagnosis
2	0	1 n	o no	Base			SV 🛢 Function Call
3	Enabled by i	nterface config,	including second	dary ip addresses			
4	Loopback int	erface is treated	as a stub Host				
5	Tunnel0 is up,	line protocol is	up				
7	Internet Add	ress 10.8.1.65/30	, Area U, Attack	ned via Network State	ment		
8	Topology_MT	D Cost Dies	hled Shutdown	Topology Name	COSC: 65		
0	Topotogy-MI1	D COSC DISG	Silucdowi	i iopoiogy name			

## 4.2 Embedded Incident

The embedded incident in intent supports:

- Transient problem diagnosis findings across multiple executions of the same intent are documented inside the Intent Incident.
- Long-term intent executions compliance intent or published intents may be executed after the network change, and the critical findings are documented inside the intent's incident so that users can review this from within intent.
- Send an email or webhook API call to the 3<sup>rd</sup> party with a link to point back to the incident /portal with more data for the execution results.

Interes Settings X	Output
Create Incident Settings	Network Intent (View Mode) - All Network Intents/Training/OSPF Route Table Check
Create incident diapat     Reset Incident If Last One Created      within Past     Deps     Add Interet Map to Incident	OSPF Route Table Check (Published)         Check OSPF Status for 2 devices
When current intent is used as follow-up intent:     Creater     Hours     Band data to incident of home intent only     Creater     Last Updated     Days	Result: 01/19/2022 09:15PM V Embedded Incident V A Solution of the Solution of
Servi dada la Riceri e li kua intereti dny     Beth (Servi data la Incident of Iscal Intert and home interet)     Intert Used as Follow-up Intert	2 Devices         3 Diagnoses         100122 1/1/2022 01:12 PM         as increased.         3
Diagnosis Message Settings in Intent	∨ O US-BOS-R2         1001BF 1/1/2022 02:12 PM         ple
D Diagnosis Message:	· · · · · · · · · · · · · · · · · · ·
OSPF Neighbor \$neighbor_id(US-BOS-R1.ospf_nbr_table) Status Change.	
-IS Set Status Code for Device:	
5 Set Status Code for Intent:	

Use the embedded incident as follows:



## 4.2.1 Document Critical Findings in Embedded Incident

Users can send messages and add a map to the incident, enabling users to track all execution history of a NI(T) from Interactive/Triggered/Preventive automation.

• Send a Message to Incident

Diagnosis Message Settings in Intent		Finding Message in Incident	
Diagnosis Message:		Finding from Intent	
✓ OSPF Neighbor \$neighbor_id(US-BOS-R1.ospf_nbr_table) Status Change.		Dean T 11:30 AM	
Set Status Code for Device:	1. Send MSG to Incident	OSPF Neighbor 10.11.11.11 Status Change.	
Set Status Code for Intent:		I OSPF Nbr Check	

• Add Map to Incident

Intent Map S	Settings in Intent			Map in	Incident	
Intent Settings	×		10006F abc		0	S ≡
Inclent Map and Data View Inclent Create Incident Output Reuse Incident if Last One Created Add Intent Map to Incident	CSV Report Files Follow-up Intent	2. Add Map to incident	Messages (2)	Maps (3)	Diagnosis (7)	Portal (O
Answer Hener (Ed) Moley El DEPArake Carrie	X Run v @ See @vn(r) = 		S Owner: zhaoxi			

# 4.2.2 Create New or Reuse an Incident to Organize Results Reasonably

ntent Settings					×					
Intent Map	and Data View	Data Source Settings	Incident	CSV Report Files	Follow-up Intent					
	Create Incid	lent Settings (Local	Settings)							
	Create Incident Output									
	🗹 Reuse	Incident if Last One Created	✓ within	Past 1 Days	~					
	🗹 Add Ir	ntent Map to Incident								
		-		×						
	When current	intent is used as follow-up int	ent: 🕦	Created	Hours					
	Send	data to incident of home intent	only	Last Updated	Days					
Send data to incident of local intent only										
	O Both	(Send data to Incident of local in	ntent and home in	tent)						
	Intent Use	d as Follow-up Inten	t							

Users can define the incident creation settings as follow:

• Create Incident Output



- If the Create Incident Output check box is selected, an incident will be generated when executing this NI for the first time; If this check box is not selected, the NI will not create an incident.
- Reuse incident check box indicates whether to use an existing incident from the second execution of NI. When the condition is not met, a new incident will be created. If it is not checked, a new incident is always created.

• Intent Used as Follow-up Intent



- The setting here is based on the assumption that the home incident exists. If the home incident is not generated, the follow-up intent (local intent) always generates an incident or sends messages according to its local settings.
- $\circ$  If the home incident is generated, users can set whether to use the home incident.
  - Send to home only: no local incident is created. Messages are sent to the home incident, and the intent map is added to the home incident.
  - Send to local only: local intent will create/reuse the local incident and send messages and intent map to the local incident.
  - Both: Indicates that the above two will work at the same time. It will send data to the home incident, and it will also create/reuse the local incident and send data to the local incident.

### 4.2.3 Manage Historical Results

Manage the embedded incidents in the following ways:

• For Single Intent: In the NI View mode, incidents generated by this intent can be displayed.

Network Intent (View Mode) - All Network Intents/Training/OSPF Route Table Check									
OSPF Route Table Check (Published)	heck OSPF Status for 2 devices								
Result: 01/19/2022 09:15PM 🗸 🖸 Embedded Incident 🗸	₼								
This intent execution is finished in a dura 100112 1/2/2022 02:12 PM	View Execution Log								
2 Devices 3 Diagnoses 100122 1/1/2022 11:12 PM 1001A1 1/1/2022 10:12 PM	as increased. 3								
✓         ✓         ●         1001BF 1/1/2022 02:12 PM	please focus this device`s chan								
show ip ospf interface	1 Diagnosis check OSPF hello time of interf								
<ol> <li>Loopback0 is up, line portocol is up</li> <li>Ethernet0/1 is up,line portocol is up</li> </ol>									

• For Entire Domain: Add the management of Intent Incidents in Incident Manager.

Incident Manager											C ł X		
Search	Q	7 Incidents (C	7 Incidents (Only those directly included under "Intent Incidents" are displayed)							Search Incident ID, Subject and Creator Q 🗅 Export			
🔺 🥅 All Incidents		Incident ID	Subject	Maps	Devices	Members	Status	Creation Time	Source	Creator	Attachment Size		
Triggered Network Change		1013SS	aa	1	1	1	Open	01/11/2022 11:10:12 PM	Intent1	John	ов		
Intent Incidents		100W3I	test by joey	1	0	1	Open	01/11/2022 11:10:12 PM	Intent2	John	0B		
		100UQK	test44	1	1	1	Open	01/11/2022 11:10:12 PM	Intent2	John	ОВ		
		100UQJ	test33	1	3	1	Open	01/11/2022 11:10:12 PM	Intent2	John	OB		
		100UOI	test2	1	1	1	Open	01/11/2022 11:10:12 PM	Intent2	John	OB		
		100UOA	test1	1	2	1	Open	01/11/2022 11:10:12 PM	Intent2	John	OB		
		100UNV	test	1	0	1	Open	01/11/2022 11:10:12 PM	Intent3	John	0B		

## 4.3 Follow-up Diagnosis

The previous version supports NI and NIC as the follow-up diagnosis. R11.1 adds NIT, Qapp, and the intents from ADT as the follow-up logic. Compared with NIC, NIT and Qapp do not replicate member Intents in advance, and the definition is simpler. Follow-up diagnosis enables multi-stage reasoning so that a follow-up intent can be taken as a home intent to do further follow-up diagnosis.



### 4.3.1 Follow-up Intent Template

An intent (home intent) can call a specified intent template to run the follow-up diagnosis, under which the diagnosis logic in the template can be applied to downstream devices calculated from the home intent. The home intent can also transfer other variables to the macro variables of the follow-up intent templates.



The follow-up intent supports the following setting:

		Follow-up Intents				×	
		1 Follow-up Intents:	+ Follow-up~				
Entry		→ I BGP check (inte	ent Template)			<b></b>	
Create Diagsnosis Message		* Description: Wh	ien				
Intent Data View		Replication Set	tings:				
Send Email		On-demand	Not use baseline data	this integet		- +	Replication Mode
Follow-up Intent	7	• Pre-replicate	eu o devices repricateu jor t	nis meni.			Replicate Device Scope
Set Intent Baseline		Replicate Curren	nt Intent to: This Device	's Neighbor V IPv4	L3 Neighbor	~ _	Boundary Settings
Advanced >	/	Set Macro Varia	bles of Seed Intent Templa	ate.			
Add Logic 🗸		Seed Devi	ce Macro Variable	Туре	Set Variable		
		🔺 🤭 R1	target_subnet	string	route (LP Device Route Failover Table)	~	Variable Mapping
v Then			vrf_name	string	Please Select	~	
Follow-up Intent:      Add Network Intent     Current I	ntent (Self) 🔿 Stop 📃	🔺 <sub></sub> 🖄 SW1					
	/		target_subnet	string	US-BOS-SW1.subnet	~	
Follow-up Intents		Merge multi	ple replicated intents into	one	1/2 Device Key Set for Selec	cted Table	Other Settings
		🗹 Draw Arrow	from This Device to Next	Arrow Settings			Arrow Relationship
0 Follow-up Intents: + Follow-up		Annotation for	Diagnosis Tree:				
Select Inte	nt (Standalone)	* Dra Evention	Mada Dasauta				
Select Inte	nt Template	- Pre-Execution	mode. because				Diamagia Tara Amagtatian
Select Inte	nts from ADT	Post-Execution	Mode			• •	Diagnosis Tree Annotation
Advanced	>	* If Follow	-up Intent is Executed:	Because			
		Prune other follow-u	up intents		Cancel	Save	

#### • Replication Mode

- On-demand: Retrieve the data from the live network.
- Pre-replicated: Use pre-decoded data (cached data).
- Replicate Current Intent to:
  - This Device's Neighbor, IPv4 L3 Neighbor, IPv6 L3 Neighbor, and L2 Neighbor can be selected.
  - Device by Variable, the range of variables that can be selected includes:
    - ✓ \$this\_device
    - ✓ Device Variables under Calling Intent
    - ✓ Device Macro Variables under Calling Intent
    - ✓ Global Variables under Calling Intent
- Set Macro Variables of Follow-up Intent Template: The range of variables that can be selected is the same as the Device by Variable in Replicate Device Scope.

4	Seed Device	Macro Variable	Туре	Set Variable		
4	管 R1					
		target_subnet	string	route (LP Device Route Failover Table)	~	
		vrf_name	string	US-BOS-R1.vrf	~	
4	沓 SW1					
		target_subnet	string	US-BOS-SW1.subnet	$\sim$	

- **Merge multiple replicated intents into one**: This check box is not selected by default, which indicates each device generates an intent.
- Set Device Key for Selected Table: Set the device key to match table variable values precisely.

Device Key Settings for Selected Table	×
<ol> <li>Define the device key. If None is selected, t</li> </ol>	able column value will be used for all devices.
Selected Table	Device Key Column
Critical ACL Entry	device 🗸
Device Route Failover Table	None ~
	None
	🖾 device
	🖾 acl_number
	🖾 entry
	description

• **Draw Arrow from This Device to Next**: Draw an arrow directly from the current device to the next device whose intent is to be replicated.

🗹 Draw Arrow f	rom This Device to Next Arrow Se	ttings				⊠ ≡
Annotation for D	Diagnosis Tree:			GRP-R1.eigrp in ×	ft)	=
	Annotation of This Device:	\$state	<b>B</b>			_
Post-Execution	Color:	Random Color				
* If Follow	Line Style:	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	]			
_	Width:					<b>,</b>
'rune other follo	Direction:					
_	Draw arrow through interface	\$intf ~	of topology	IPv4 L3 Neighbor 🗸 🗸	Cancel	Apply
_				Cancel OK	-	

An arrow example on a map:



• **Annotation for Diagnosis Tree:** Annotations are displayed on the line of Diagnosis Tree. The diagnosis tree of the follow-up intent template is as follows:

• **Pre-Execution Mode**: The basic information of the intent template is displayed on the left, and the information defined in the intent is displayed on the right.

Diagnosis Tree	
Pre-Execution   Post-Execution	Show ospt details
Intent Template Details - OSPF Interface MTU Mismatch Check	<u></u>
Avame: OSPF Interface MTU Mismatch Check     Edit Intent     Description: Una this Manager Chatter to check the OCPF mainteen face MTU	Description: When
Description: Use this Network intent Cluster to check the USPF neighbor interface MTU mismatch.	Replicate Follow-up intent to: bgp_nbr
E Location: All Network Intents\ABC Folder\OSPF Interface MTU Mismatch Check	Set macro variables of seed intent template:
	▲ Seed Device Macro Variable Type Set Variable
	4 🙆 R1
	target_subnet string route (LP Device
	vrf_name string US-BOS-R1.vrf
	4 😵 SW1
	target_subnet string US-BOS-SW1.subnet
	Annotation for Diagnosis Tree: Pre-Execution Mode: None Post-Execution Mode: If Follow-up Intent is Executed: There are some OSPF interface MTU mismatched issues to be fixed.

• **Post-Execution Mode**: The detailed results are displayed below. Besides the diagnosis details and comparison details, the follow-up intents/Qapps/ADT will be displayed.



### 4.3.2 Follow-up Self

An Intent (home intent) can call itself to be the follow-up intent template, under which the same logic will be applied to downstream devices calculated from the home intent. The logic is recursively called upon until it hits a boundary defined by logic or maximum depth.



The Follow-up Self settings are like follow-up NIT:

	Follow-up Self	
Entry	Repeat current intent's logic in neighbor or next-hop device recursively.  * Description: When	
Create Diagsnosis Message Intent Data View	Replication Settings:         On-demand       Not use baseline data         @ reverselicated       D dwines mellicated for this intere.	Replication Mode
Send Email Follow-up Intent	Replicate Current Intent to: This Device's Neighbor V IPv4 L3 Neighbor V	Replicate Device Scope
Set Intent Baseline	Limit Device Propagation and Follow-up Execution: Setting Set Macro Variables of Seed Intent Template:  Set Macro Variable Type Set Variable  Macro Variable Type Set Variable  Macro Variable Type Set Variable	
Then	target_subnet     string     route (LP Device Route Failover Table)       vrf_name     string     Please Select       string     SW1	Variable Mapping
	Merge multiple replicated intents into one  1/2 Device Key Set for Selected Table  C Draw Arrow from This Device to Next Arrow Settings	Other Settings Arrow Relationship
	Annotation for Diagnosis Tree: * Pre-Execution Mode: Because	Diagnosis Tree Annotation
	Post-Execution Mode: + If Follow-up Intent is Executed: Because	
	Prune other follow-up intents Cancel Save	

Users can control when to hit the boundary by defining max depths and device scope:

t Macro variables of Seed Intent	ntent Settings			×
Seed Device Macro Variabl				
🚱 R1	Intent Map and Data View Data Source Settings	Incident CSV Report Fi	les Follow-up Intent	
target_subnet				
vrf_name	The following settings are available only when the c	urrent intent is used as home intent.		
3 SW1				
target_subnet	1 Max Depth of Follow-up Intents' Execu	ition: 5		
Merge multiple replicated intent				
Draw Arrow from This Device to	2 Max number of command sections includ	ded in a cloned following-up intent: 99	)	site
otation for Diagnosis Tree:	Network Scope for Follow-up NIT and Sel	f Diagnosis:		My Network   NetbrainDC
re-Execution Mode: Because	Only Run on Network Devices;	Select Device Group, Site	~ — — <del>)</del>	🗌 🛞 Unassigned
	Stop Running at Border Device:	Select Device Group, Site	~ — →	In Excluded from site     In Excluded from site
t-Execution Mode:		Run on Border Device		📄 🛅 My Device Groups
* If Follow-up Intent is Execut				Image: Shared Device Groups
				Policy Device Groups

Users can set the max depths and follow-up intent count in **Area 1**. They can also set the max command sections in one cloned intent in **Area 2**.



Define network scope in **area 3**:

- Limit the range of devices. The devices beyond this range will not be replicated.
- When entering a border device, it will not continue to find its neighbors, but whether to clone the intent and continue the diagnosis on the current border device can be set.
- Device groups and sites can be selected for both selections, and multi-selection is supported.

Examples of Follow-up Self:

- Execute recursive diagnosis from the current Device towards a Target IP Self.
- Draw a path with the arrow.
- Execute recursive diagnosis across Multi-level Neighbors.
- Draw the multicasting tree and execute recursive diagnosis across the multicasting tree.



• Create a Technology Map and Highlight the Interface Area.

## 4.3.3 Follow-up ADT Intents

In R11.1, Automation Data Table (ADT) can reference multiple automation intent columns for each automation asset, and users can use intents (e.g., path intents) in ADT as follow-up diagnosis. The definition of follow-up

ADT	includes	the	following:
Follow-up ADT Intents	×	Follow-up ADT Intents	×
1 Follow up Nodes: • Follow Up • 0 • • • • ADT: FailoverLinks • Description: When Find Critical Automation Assets (ADT Rows) by Int Find Critical Automation Assets by device, or properties of Critical A Failover Device • C B Select Criteria • C B Select Criteria • C	tent Variables (Device or Device variables): •	1 Follow up Nodes: Follow Up V V Contains Follow Up Nodes: When Find Critical Automation Assets (ADT Rows) by Intent Variables (Device or Device variables) : Find Critical Assets by device, or properties of Critical Asset. A Failover Device V Contains V this, device B Select Criteria V Boolean Expression: A	
Select Intents of Found Critical Automation Asset  All Intents Selected Intents: Column 1, Column 2 Intents with Tags: Match any  Maximum number of Network Intent(s) matched	ts to Execute:	Select intents of Found Critical Automation Assets to Execute:         All Intents         Selected Intents:       Column1, Column 2         Intents with Tags:       Match any         Maximum number of       Stift Tags.         Maximum number of       Stift Tags.         Define Diagnosis Tree Annotation       QOS	
Prune other follow-up intents	Cancel Save	Prune other follow-up intents	Cancel Save

- 1. Find Automation Assets by Intent Variables (Context Device or other Device Variables)
- 2. Select the Intent of Automation Assets to be Executed.

Use the follow-up ADT intent to analyze the network problems of related automation assets. For example, check the OSPF and EIGRP state of the failover device when the HSRP state is changed.

### 4.3.4 Call Qapp

A new block, **Call Qapp**, can be added to the NI diagnosis. Users can select a Qapp and execute it by defining the matching relationship of input variables. The Qapp output link can be saved in NI if this Qapp is executed. Calling Qapp can execute Python scripts for advanced functions, e.g., making an API call to a 3<sup>rd</sup> party system to send the notification.

Intent Variables can be passed to follow-up Qapp. Users can execute the Qapp with a Qapp output link saved in NI.

	Entr	у	- 15	Call	Qapp					×
Create Diagsnosis Messag	ge			1	Qapp: + Add ~ O Multicasting check				Ū	
Intent Data View		A and B		•	*Description: When					
Send Email		Export CSV Report				r				Device Scope
Set Intent Baseline		Operate on Table			Set Value for Input Devices:	this_device, bgp_nbr			~	Device Scope
Advanced	>	Set Intent Variable			Set Value for input variables	of the follow-up Qapp:				
					Qapp Input Variable	Input Variable Type	Set Variable		0	
Add Logic 🗸		Call Qapp			Mgmt_IP	IP	suc_ip	~		
		Call Webhook API			target_subnet	string	route (Device Route Failover Table)	~	]	Variable Mapping
					process_id	number	Please Select	~		
					CPU Utilization	number	90	~		
					table1	table	summary_table	~	0	
					Annotation for Diagnosi * Pre-Execution Mode:	is Tree: Because				Diagnosis Tree Annotation
					Post-Execution Mode: * If Qapp is Execut	ed: Because				
							Can	cel	Save	

Use Qapp to Run Advanced Functions like Making API Calls to Outside Resources. For example, users can create an intent to get the device vendor, model, and serial number, then pass these parameters to a Qapp to call *Cisco Diagnosis API* to get *End of Life (EOL)*.

# 4.4 New Operation in Intent Table

Many network data are tables. R11.1 supports more operations of tables without coding:

Table Operation	Description
Merged Table <sup>Updated</sup>	Merge two tables using DB-style programming: full/inner/outer/left/right join
	two tables to extract matching data rows to improve the loop table efficiency
	in the diagnosis.
Appended Table <sup>New</sup>	Append the data from two tables with different sources.
Sub Table (Filtered by Condition) New	Filter table rows by a condition to create a sub table, reducing the noise in the
	diagnosis.

Add/Delete/Update/Query Table New	Support the "add/delete/update/query" table operation on the intent table
	and ADT to ensure the accuracy and completeness of table data.
Built-in Device Table Diagnosis New	Reference built-in device data, e.g., NAT table, and loop the built-in table rows
	to check the data accuracy and the live status for the table key metric.
Automation Assets Diagnosis New	Reference ADT, e.g., critical failover links, and loop the ADT rows to get the
	key assets as input for the follow-up diagnosis.

## 4.4.1 Merged Table

In the previous version, the system supports two Merging Rules: **Full Join** and **Inner Join**. R11.1 enhances Merged Table to perform DB-style merging rules (**outer/left/right join**) on table data.



The key logic of Merged Table:

Table Name	e: ospf_nbr_compar	e													
Input Table	es:				⇐										
	BJ*POP		(	Current 🗸		9	BJ_core_3550	- 1	Settings		Current	,			
Table 1:	ospf_nbr_intfs			~	Tabl	e 2:	ospf_nbr_intfs	- 6	Select colu	imns in merg	ed table				
Paired Keys	5:								Table 1:				Table 2	2	
Key 1:	this (BJ*POP)			~	Ke	y 1:	nbr (Bj_core_3550	.ospf_nl	c	olumns				Columns	
K 2		- 6 1 - + 0			Ka		a har last (D) and a		<b>S</b>	interface (BJ*	POP. ospf_intf	)		\$interface (BJ_core_3	550. ospf_intf)
Key 2:	interface (BJ*POP.os	pf_intf)		~	Ke	y 2:	nbr_intf (BJ_core_	3550.osj	S \$	cost (BJ*POP.	ospf_intf)			\$cost (B]_core_3550.	spf_intf)
Key 3:	nbr (BJ*POP.ospf_nb	or)		~	Ke	y 3:	this (BJ_core_3550	)	✓ 3	local_intf (B)*	POP. ospf_nbr			\$local_intf (B]_core_3	550. ospf_nbr)
Key 4:	nbr_intf (B]*POP.osp	of_nbr)		~	Ke	y 4:	interface (B]_core	3550.0	S 1	nbr (BJ*POP.	ospf_nbr)			<b>\$nbr</b> (BJ_core_3550. d	spf_nbr)
+ Add Pai	ired Keys								<b>S</b>	nbr_intf (BJ+P	OP. ospf_nbr)			<pre>\$nbr_intf(BJ_core_35</pre>	50. ospf_nbr)
Table 1(BJ	*POP. ospf_nbr_intfs)		Table 2(8	3J_core_355	Calculate	ද් _intfs)	සූ Output(	ospf_nb	Table Merş	ging Rule: Fi	ull Join (Keep Full Join (Keep nner Join (Only Duter Join (Only	all rows in bot all rows in bot y keep the row	h tables) th tables) /s with mai	v tching key) matching key)	ocel O
Device: BJ*P	OP			BJ*POP			Device: BJ_core	_3550		I	eft Join (Only	keep the rows	with value	in the left table)	
Table: ospf_i	ntfs( show ip ospf inte	erface )		ospf_nbrs(	show ip os	pf nei.	Table: ospf_int	fs( show i	p ospf in	terface ;	Right Join (Only	/ keep the row	ws with val	lue in the right table)	
\$this 😨 (Key	1) \$interface 🐺 (Key 2	) \$cost	\$area_id	\$local_intf	\$nbr \$nb	br_intf	\$this (Key 1)	\$interfac	e <b>III</b> (Key	2) \$cost	\$area_				
BJ*POP	Fasthernet1/1	64	0	Fasthern	BJ_c Fas	ther	BJ_core_3550	Fasthern	et2/2	64	0				
BJ*POP	Fasthernet1/2	64	0	Fasthern	BJ_c Fas	ther	BJ_core_3550	Fasthern	et2/3	64	0				
									Cano	el	ОК				

- 1. The output table name must follow variable naming rules.
- 2. Select the table variables for Table 1 and Table 2 and specify the data source (Current, Baseline, Last) for the table variable. The table variable includes the parser table, intent table, built-in table, ADT, and compound table.
- 3. **Add Paired Keys** to define the Paired Keys for Tables 1 and 2. The Paired Keys define the column pairs to be merged, and users can have multiple Paired Keys.
- 4. Select the columns and select the table merge rule in **Settings**.

Use the merged table to merge table data from two tables. For example, find the missing BGP prefixes between primary and secondary wan routers.

			÷						
Table Name:	weifing jeffe husje								
Input Tables	ULBOL#1		4	0530542			100	nad Sellerga R columna in mingar) tablic	
Table 1	hep prink	-	Table ;	5 142 profile		*	144	et:	Takin 2
Faired Keys:								Coloren	Columnia
says:	weathing the property will	h liveni) -	hay	Persent (US-205-	COURS Energy)			00,6eAs1.5305.P1	E 04,899(105105-10)
Rey 2.	nex_hop115-015-015	w (v?vq.08	Key i	2 rest_http://doi.org	Althory profile	~ B		tersevent diff. 205-21 have mediat	President (J.A. 805-81. http://www.ivi
+ A57 Fa	orned Margili							must have too mits, while a number	and her on any other and of
Table 1 (hgs.)	grafici Della 2 de	gr (ineffic) : Outpu	conterged lago pre	083					
Datas 1 (hgh.)	prefici table 2 de	grjoshi Outpu	timerged, ego, pre	a US-205	ku tege, prvtik				
talae 1 (hga,	prefix bitre 2 de	grjoshi Outpu ujetki v tetjivostrogi	<ul> <li>ant'avortari</li> </ul>	<ul> <li>uses</li> <li>uses</li> <li>uses</li> <li>uses</li> </ul>	NG Telep.prvtix 1. v. newt_toop pr	mg -			
Talar 1 (hgs. 10, 54/44 (http: 5-805-81 5-805-81 5-805-81	prefix bole 1 de 0.05 205 41 0.05 205 41 0.05 205 41 0.05 205 41 0.05 205 41 10.05 205 10.05	grupertie Outpu upertie v Next /septiming 15,961,133 15,961,133 15,961,131	<ul> <li>Bit, Bives cert.</li> <li>US-BOS-R2</li> <li>US-BOS-R2</li> <li>US-BOS-R2</li> </ul>	<ul> <li>US-BOS</li> <li>Intervision (Intervision)</li> <li>Intervision (Intervision)</li> </ul>	ký typ.polo i v restjoppi	me		Weiging Rule: Over Jos (Cril) kery the	men sett se militing vijs 🔹 🛛
Tativ 1 (kg), 64, 5405-81 5-805-81 5-805-81 5-805-81	perfor both 246 = U5 205 81 = 105 205 81 = entropy Engl = entropy Engl = 105 A009 105 A009	grijavitaj Outgo grijavita v notrjiva cerregi 10.961.53 10.961.53 10.961.53 10.961.53	<ul> <li>Bit, Bivita (B1), I</li> <li>Bit, Bivita (B1), I&lt;</li></ul>	Book of the sector of the	kg hyp.pintix 1 = v. newt,inip.pi	me -		Negang Rules Over Just (Only Resp. Pr	mere soft for multilling log( v)
Table 1 (hg), 54 (1644) (165) 54 (154) 54 (154)	perfor bone (e) = US 2005-81 = into e) tipe [] tipe = into e) tipe	grijevite Outpu uprite v not, tvo cerrigi 10.961.53 10.961.53 10.961.53 5.80.01	<ul> <li>Intergree lago pre</li> <li>Intergree lago pr</li></ul>	<ul> <li>US-BOS</li> <li>there is type (1)</li> <li>in the output (1)</li> </ul>	ng tep.prets 1 v. reetjenpte	me		Werging Rule: Over the 40-by keep the	rmes with its multi-leg legs v V
1 Julie 1 (hgs. 5405-81 5405-81 5405-81 5405-81 5405-81 5405-81	perfect betweet day = US-2005-R1 = Inter-spinger Einige <ul> <li>retrievelt getringer IDEA-00244</li></ul>	gr.govite Ov2pu c.grothe v next_trip.com/gr 15.961.131 15.961.131 5.861.131 5.861.131 5.861.131	<ul> <li>#st, #wis (tri), V5405-92 U5405-92 U5405-92 U5405-92 U5405-92         U5405-92         U5405-9          U5405-9         U5405-9         U5405-9          U5405-9</li></ul>	<ul> <li>a US-BOS</li> <li>a show is type 11</li> <li>a shown carried</li> </ul>	ng parta 1 – v mengangan	mg -	6	Megging Rate: Dutor Set (Dirly Very Pr	mens with its yaduling keys v
5 Julie 1 (hgs. 54 juli	perfici Done (d)	gr.junki) Outgu zantik 1994-199 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19 1994-19	<ul> <li>B1(Bx00101)</li> <li>US40542</li> <li>US40542</li> <li>US40542</li> <li>US40542</li> <li>US40542</li> <li>US40542</li> </ul>	n US-200 n US-200 nove tapp 11 v holoson (atting	ku hyp.prvhx 1 – v revet, hop.pr	me	E	Megging Rater Duttr (and sChild Kerp Pr	rmen with ne youthing wy. • • • • • • • • • • • • • • • • • • •
5 bite 1 (kgs. 54 bite 1 (kgs. 5405-81 5405-81 5405-81 5-805-81 5-805-81 5-805-81 5-805-81	petio biox 24 = US 20141 = US 20141 = US 20141 = US 2014 = US	(jinth) Output (jinth) Output (jinth) (398.138 (398.131 (398.131 (398.131 (398.131 (398.131 (398.131 (398.131 (398.131 (398.131) (398.131) (398.131)	<ul> <li>Bit, Biological (Bit), Second (Bit), US 402-402</li> <li>US 4</li></ul>	en US-905 en US-905 en US-905 v nutseon (enreg	ku hyp.prvhx 1 – v nevr,hop.pr	mg -	E	Herging Rate: Duty bery the	mers with the multi-line y larger v
1 Jahr 1 (Age, 3-805-81 3-805-81 3-805-81 3-805-81 3-805-81 3-805-81 3-805-81 3-805-81	perio         Doin 2.0           m US 2015***         0	(p) (whi) Output (p) (whi) Output (p) (whi) (p) (p) (p) (p) (p) (p) (p) (p) (p) (p	<ul> <li>Bit, Book (B), Jo</li> <li>Bit, Book (B), US (C), US</li></ul>	er US-905 er noven stang v noven stang	kg Ingelsenter Kg	mg -	E	Mengang Rules Octor (see 20-19 kenya tha	rmers soft for sublining top: v 0

## 4.4.2 Appended Table

Appended Table is added in R11.1, which appends one table row into the other. Users must define how to map the columns of two tables.

Idi	ble 1: USPF routes			Table 2: Cor	nected routes	
BJ_core_3550	23	show ip route ospf		∠ _ B]_core_3550	show ip ro	ute connected
ospf_routes				▲ ,		
flag (string)	subnet (string)	next_hop (string)	out_intf (string)	flag (string)	subnet (string)	intf (string)
O E2	192.168.29.0/24	172.24.10.33	Vlan10	C	172.24.10.224/27	FastEthernet0/3
0	172.25.52.0	172.24.100.2	Port-channel10	- C	172 24 32 224/28	FastEthernet0/1
0	172.25.54.0	172.24.100.2	Port-channel10	с. С	172 24 26 0/20	EastEthernet0/20
0	172 25 51 0	172 24 100 2	Port-channel10	c c	172.24.30.0/29	Vianto
0	172.25.51.0	172.24.100.2	Dest channel10		1/2.24.10.32/2/	Vianiu
0	172.25.50.0	172.24.100.2	Port-channel10	С	172.24.100.0/30	Port-channel10
		Ap	pended Table: OSPF +	Connected routes		
	flag (string)	Ap	pended Table: OSPF +	Connected routes		
	flag (string) O E2	App v subnet (string 192,168,29,0/	pended Table: OSPF +	Connected routes ng) vout_intf (string) Vlan10	~	
	flag (string) O E2 O	App subnet (string 192.168.29.0/ 172.25.52.0	24 172.24.100.3	Connected routes ng) vot_intf (string) Vlan10 Port-channel10	~	
	flag (string) O E2 O	Apj v subnet (string 192.168.29.0/ 172.25.52.0 172.25.54.0	Dended Table: OSPF +	Connected routes ng) vout_int(string) Vian10 Port-channel10 Port-channel10	~	
	flag (string) O E2 O O	Apj v subnet (string 192.168.29.07 172.25.54.0 172.25.51.0	Dended Table: OSPF + □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Connected routes agy vout_int(string) Vian10 Port-channel10 Port-c	~	
	flag (string) O E2 O O O O	App subnet (string 192.168.29.07 172.25.52.0 172.25.51.0 172.25.51.0 172.25.50.0	Pended Table: OSPF + ■	Connected routes agi vot_int (string) Vlan10 Port-channel10 Port-c	~	
	flag (string) O E2 O O O O O O E2	App subnet (string 192.168.29.07 172.25.52.0 172.25.54.0 172.25.51.0 172.25.50.0 172.25.50.0	Dended Table:         OSPF +           ■          next_jop (st)           24         172.24.100.         172.24.100.           172.24.100.         172.24.100.         172.24.100.           172.24.100.         172.24.100.         172.24.100.           172.24.100.         172.24.100.         172.24.100.	Connected routes ng) volt_int (string) Vlan10 Port-channel10 Port-	~	
	flag (string) O E2 O O O O O E2 C	App subnet (string 192.168.29.07 172.25.52.0 172.25.54.0 172.25.50.0 172.25.50.0 172.25.32.0 172.25.32.0	Dended Table:         OSPF +           ■         next_jop (st)           172,24,103,         172,24,103,           172,24,100,         172,24,100,           172,24,100,         172,24,100,           172,24,100,         172,24,100,           172,24,100,         172,24,100,           172,24,100,         172,24,100,	Connected routes ng) ∨ out_intf (string) Vlan10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 FastEthernet0/3	~	
	flag (string) O E2 O O O O E2 C C	Ap) subnet (string 192.168.29.07 172.25.52.0 172.25.54.0 172.25.50.0 172.25.50.0 172.25.32.0 172.25.32.0 172.24.32.244 172.24.32.244	Dended Table:         OSPF +           ■         next_jop (st)           172,241.03.         172,241.03.           172,241.00.         172,241.00.           172,241.00.         172,241.00.           172,241.00.         172,241.00.           172,241.00.         172,241.00.           172,241.00.         172,241.00.           172,241.00.         172,241.00.           172,241.00.         172,241.00.	Connected routes       ng)     ∨ out_intf (string)       Vlan10     Port-channel10       Port-channel10     Port-channel10		
	flag (string) O E2 O O O O C C C C C C C	App subnet (string 192.168.29.07 172.25.52.0 172.25.50.0 172.25.50.0 172.25.50.0 172.25.20 172.24.20 24 172.24.20 172.24.30 172.24.	Dended Table:         OSPF +           □□         next_jop (st)           172,24.10.3         172,24.10.3           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.           172,24.100.         172,24.100.	ng) v out_intf (string) Vlan10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10		
	flag (string) O E2 O O O O E2 C C C C C C	App 192.168.29.07 172.25.52.0 172.25.50.0 172.25.50.0 172.25.50.0 172.25.32.0 172.24.10.24 172.24.32.24 172.24.32.24	Peended Table: OSPF + ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓	Connected routes ng) volutint(string) Vlan10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 Port-channel10 FastEthermet0/3 FastEthermet0/1 FastEthermet0/20 Vlan10		

#### The definition of Appended Table:

🔢 Table Name:	appended	_table							
🔢 Input Tables:				€					
	🥏 BJ_core_	3550				🥏 BJ_co	re_3550		
Table 1:	ospf_route	:5	~		Table 2:	connect	ted_routes	~	
Column Mapp	ing:								
Column 1:	flag (BJ_cor	re_3550.ospf_routes)	~		Column 1:	flag (BJ	core_3550.connected_routes)	~	
Column 2:	subnet (BJ	_core_3550.ospf_routes)	~		Column 2:	subnet	(BJ_core_3550.connected_rou	~	
Column 3:	out_intf (B)	_core_3550.ospf_routes)	~		Column 3:	intf (BJ_	core_3550.connected_routes)	~	
		Table 2 (connected rou)	tes)	Output (a	ppended	table)			
	Table 1 (ospf_routes) Table 2 (connected_routes)					table)			
		Table 2 (connected_rou	tes) 🥏 E	Output (a BJ_core_355	ppended_	table)			
		Table 2 (connected_rou	tes) 2 E v ip rout	Output (a BJ_core_355 te ospf	oppended_ oppended_ ospf_routes	table)			
flag (string)		v subnet (string)	tes) 🥏 E / ip rout	Output (a BJ_core_3550 te ospf , v next_jo	oppended_ ospf_routes op (string)	table)	✓ out_intf (string)		~
flag (string) O E2		v subnet (string)	tes) Z E	Output (a BJ_core_355( te ospf , next_jo 172.24	ospf_routes (string) 10.33	table)	<ul> <li>✓ out_intf (string)</li> <li>✓ Vlan10</li> </ul>		~
flag (string) O E2 O		<ul> <li>✓ Iable 2 (connected_rout</li> <li>✓ subnet (string) </li> <li>192.168.29.0/24</li> <li>172.25.52.0</li> </ul>	tes) <i>a</i> E / ip rout	Output (a BJ_core_3550 te ospf ) next_jo 172.24	ppended_ ospf_routes op (string) .10.33 .100.2	table)	<ul> <li>✓ out_intf (string)</li> <li>✓ Vlan10</li> <li>Port-channel10</li> </ul>		~
flag (string) O E2 O		<ul> <li>✓ subnet (string) ∰</li> <li>192.168.29.0/24</li> <li>172.25.52.0</li> <li>172.25.54.0</li> </ul>	es)	Output (a BJ_core_3550 te ospf ) next_jc 172.24 172.24 172.24	oppended_ ospf_routes op (string) .10.33 .100.2 .100.2	table)	Vlan10 Port-channel10 Port-channel10		~
flag (string) O E2 O O O		<ul> <li>✓ India 2 (connected_round)</li> <li>✓ subnet (string) </li> <li>✓ 192.168.29.0/24</li> <li>172.25.52.0</li> <li>172.25.54.0</li> <li>172.25.51.0</li> </ul>	es)	Output (a BJ_core_3550 te ospf , next_jc 172.24 172.24 172.24 172.24	ppended_ oospf_routes op (string) .10.33 .100.2 .100.2 .100.2	table)	<ul> <li>✓ out_intf (string)</li> <li>✓ Vlan10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> </ul>		~
flag (string) O E2 O O O O		v         subnet (string) ∰           192.168.29.0/24           172.25.52.0           172.25.51.0           172.25.50.0	es)	Output (a BJ_core_3550 te ospf , next_jc 172.24 172.24 172.24 172.24 172.24	ppended_ ospf_routes op (string) .10.33 .100.2 .100.2 .100.2 .100.2	table)	<ul> <li>out_intf (string)</li> <li>Vlan10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> </ul>		~
flag (string) O E2 O O O O O E2		■ Table 2 (connected_rout         ■ Subnet (string)         ■ 192.168.29.0/24         172.25.52.0         172.25.54.0         172.25.51.0         172.25.50.0         172.25.32.0	tes) ar E r ip rout	Output (a BJ_core_3550 te ospf ) next_jo 172.24 172.24 172.24 172.24 172.24 172.24 172.24	ppended_ ospf_routes op (string) .10.33 .100.2 .100.2 .100.2 .100.2 .100.2	table)	out_intf (string)       Vlan10       Port-channel10       Port-channel10       Port-channel10       Port-channel10       Port-channel10       Port-channel10       Port-channel10		~
flag (string) O E2 O O O O O E2 C		■ Table 2 (connected_round)         ■ show         ■ subnet (string) ●         192.168.29.0/24         172.25.52.0         172.25.54.0         172.25.51.0         172.25.50.0         172.25.32.0         172.25.32.0	tes) P E v ip rout	Output (a BJ_core_3550 te ospf , next_jc 172.24 172.24 172.24 172.24 172.24 172.24	ppended_ ospf_routes op (string) .10.33 .100.2 .100.2 .100.2 .100.2 .100.2	table)	<ul> <li>✓ out_intf (string)</li> <li>✓ Vlan10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>FastEthernet0/3</li> </ul>		~
flag (string) O E2 O O O O E2 C C		v       subnet (string) ∰         192.168.29.0/24         172.25.52.0         172.25.51.0         172.25.50.0         172.25.32.0         172.25.32.0         172.24.10.224/27         172.24.32.224/28	es)	Output (a BJ_core_3550 te ospf , next_jc 172.24 172.24 172.24 172.24 172.24 172.24	ppended_ ospf_routes op (string) .10.33 .100.2 .100.2 .100.2 .100.2	table)	<ul> <li>out_intf (string)</li> <li>Vlan10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>FastEthernet0/3</li> <li>FastEthernet0/1</li> </ul>		~
flag (string) O E2 O O O O O E2 C C C C		■ Table 2 (connected_rout         ■ subnet (string)         ■ subnet (string)         ■ 192.168.29.0/24         ■ 172.25.52.0         ■ 172.25.54.0         ■ 172.25.51.0         ■ 172.25.50.0         ■ 172.25.32.0         ■ 172.25.32.0         ■ 172.24.32.224/28         ■ 172.24.36.0/29	tes)	Output (a BJ_core_3550 te ospf , v next_jc 172.24 172.24 172.24 172.24 172.24 172.24	ppended_ ospf_routes op (string) .10.33 .100.2 .100.2 .100.2 .100.2	table)	<ul> <li>✓ out_intf (string)</li> <li>✓ Vlan10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>Port-channel10</li> <li>FastEthernet0/3</li> <li>FastEthernet0/1</li> <li>FastEthernet0/20</li> </ul>		~

The logic of Appended Table:

- 1. The output table name must follow variable naming rules.
- 2. Select the table variables for Input Table. The table variable includes a parser table, intent table, builtin table, ADT, and compound table.
- 3. **Column Mapping**: map columns of table2 to columns of table1. The column name of the Appended Table will be the same as that of Table 1.

Use Appended Table to merge rows from two tables. For example, append the connected route table and OSPF route table.

Edit Appended Tabl	e								×
iii Table Name:	appended	d_table							
input Tables:				←					
	🥏 BJ_core	_3550				💋 BJ_co	re_3550		
Table 1:	ospf_rout	es	~		Table 2:	connect	ted_routes	$\sim$	
🛃 Column Mapp	ing:								
Column 1:	flag (BL co	ore 3550.ospf routes)	~		Column 1:	flag (Bl	core 3550.connected routes)	~	Ê
									_
Column 2:	subnet (B	J_core_3550.ospf_routes)	~		Column 2:	subnet	(BJ_core_3550.connected_rou	~	ī
Column 3:	out_intf (	BJ_core_3550.ospf_routes)	~		Column 3:	intf (BJ_	core_3550.connected_routes)	~	Ē
+ Add M	apping								
					<i>~</i>				
			C	alculate	£ <u>0</u> 3				
Table 1 (ospf	_routes)	Table 2 (connected_rout	es)	Output (a	ppended_	table)			
			-	BJ_core_3550	)				
		show	ip rou	ite ospf ,	ospf_routes				
flag (string)		✓ subnet (string) 🍄		∨ next_jo	p (string)		✓ out_intf (string)	`	•
O E2		192.168.29.0/24		172.24	.10.33		Vlan10		-
0		172.25.52.0		172.24	.100.2		Port-channel10		
0		172.25.54.0		172.24	.100.2		Port-channel10		
0		172.25.51.0		172.24	.100.2		Port-channel10		
0		172.25.50.0		172.24	.100.2		Port-channel10		
O E2		172.25.32.0		172.24	.100.2		Port-channel10		
С		172.24.10.224/27					FastEthernet0/3		
С		172.24.32.224/28					FastEthernet0/1		
С		172.24.36.0/29					FastEthernet0/20		•
🕜 Help							Cancel	OK	

## 4.4.3 Sub Table Filtered by Condition

R11.1 supports defining Sub Table (Filter by Condition) to keep or remove the rows of the base table matching the conditions. The sub table can reduce the noise in the diagnosis.

Parsed Result	☐ interface_ips	<ul> <li>Base Ta</li> </ul>	able: Including	all interfaces	⊕ —
\$interface	✓ \$ip_address	✓ \$ok_	∽ \$method	✓ \$status	~
FastEthernet0/0	172.24.32.225	YES	NVRAM	up	<b>^</b>
FastEthernet0/1	172.24.31.195	YES	NVRAM	up	
FastEthernet0/0/0	unassigned	YES	unset	administratively do	wn
FastEthernet0/0/1	unassigned	YES	unset	administratively do	wn
FastEthernet0/0/2	unassigned	YES	unset	administratively do	wn
FastEthernet0/0/3	unassigned	YES	unset	administratively do	wn
Serial0/1/0	172.24.32.210	YES	NVRAM	up	•

#### Create Sub Table to only removing the interfaces without IP address

interface (string)	<ul> <li>ip_address (string)</li> </ul>	✓ ok_(string)	✓ method (string)	✓ status (string)	~
FastEthernet0/0	172.24.32.225	YES	NVRAM	up	
FastEthernet0/1	172.24.31.195	YES	NVRAM	up	
Serial0/1/0	172.24.32.210	YES	NVRAM	up	
Serial0/1/1	172.24.32.1	YES	NVRAM	down	
Loopback80000	172.24.255.8	YES	NVRAM	up	
	Sub Table: (	Only including	interfaces with ip addres	SS	

You can define the sub table (filtering row by condition):

	Add Sub Table (Filtering	g Row by Condition)					×	Output Table
	Table Name: ips	s_table					•	
a 'Only Keep' or 'Only Remove'	I Base Table: int	erface_ips			~			2 Input Table
	Filtering Logic:	nly Remove 🗸 table	rows if values match	n the below condition				Select Intent variable or
	А	ip_address	~	Equals 🗸	unassigned	~		
b Select Column from Base Table	В	Please Select	~	J		]		
	в	oolean Expression: A						
			Cal	<mark>culate</mark> හි				
	Base Table (interfac	e_ips) New Table	ips_table)					
				BJ*POP				
	interface (string)	in address (string)	show ip interf.	ace brief interface_i	ps	v protocol (string)		
	FastEthernet0/0	172.24.32.225	YES	NVRAM	up	up	~	
	FastEthernet0/1	172.24.31.195	YES	NVRAM	up	up		
	Serial0/1/0	172.24.32.210	YES	NVRAM	up	up		
	Serial0/1/1	172.24.32.1	YES	NVRAM	down	down		
	Loopback80000	172.24.255.8	YES	NVRAM	up	up		
	? Help					Cancel OK	<mark>ر م</mark>	

The key logic of Sub Table (Filtering Row by Condition):

- 1. The output table name must follow variable naming rules.
- 2. Select the table variables for Base Table. The table variable includes a parser table, intent table, builtin table, ADT, and compound table.
- 3. Filtering Logic:
  - a. Define filter rule: **Only Keep** or **Only Remove**.
  - b. The left-side field can specify the columns of the Base Table.
  - c. The right-side field can specify the Intent variable and enter a constant.

Use Sub Table to Filter Table Row by Specified Condition. For example, create a sub table to only keep the interface with the IP address configured.

dd Sub Table (Filte	ering R	low b	y Condition)									>
Table Name:	ips_t	able										
🌐 Base Table:	inter	face_	ips					~				
Filtering Logic:	Only	Keep	table rows	; if values	match	the below condition	1					
	Α	ip_a	ddress		~	Does not equal	~	unassigne	ed		~	Ē
	в	Plea	ase Select		~							
Base Table (interface_ips) New Table (ips_table)												
				show in	interf	BJ*POP ace brief === interfac	-e ins					
interface (string)		~	ip_address (string)	v ok	_ (strir	ng) v n	nethod	l (string)	~	status (string)		~
FastEthernet0/0			172.24.32.225	YE	s	N	IVRAM			up		
FastEthernet0/1			172.24.31.195	YE	S	N	IVRAM			up		
Serial0/1/0			172.24.32.210	YE	s	N	IVRAM			up		
Serial0/1/1			172.24.32.1	YE	5	Ν	IVRAM			down		
Loopback80000			172.24.255.8	YE	S	Ν	IVRAM			up		
Help										Cancel	0	к

# 4.4.4 Enhance Operation on Table

R11.1 adds table operations, "add/delete/update/query rows", on the intent table and ADT in the intent diagnosis block:

		×					
ted: 03/24/2023 11:22:45 AM							
2. Define Diagnosis							
🗋 Add Note 🛞 Add Diagnosis Can also	click a variable on the left to add automatio	n.					
Name: Untitled Diagnosis 2	Anchor: Select Variable 🗸						
Type description				Add Table Row	- Add Mate - 62 Add Diseases	n dan diak na maini ka ang ka kata ka ada a	×
				Select Table:	Critical_Routes		~
<ul> <li>If</li> </ul>				Select Operation:	Add Table Row		~
A Select Variable				Define the colur	Add Table Row		
Boolean Expression: e.g. A and B		$\downarrow$	1	Critical_Route_I	Update Table Row	tbound_Inte	erf
Than					• • •	• •	•
Intent Data View	□ Save to Embedded Incident 🔳						
Send Email							
Set Intent Baseline Operate on Table							
Advanced > Set Intent Variable	_						
Add Logic Call Qapp							
Call Webhook API							
+ Add Fiself + Add Fise		ы.					
				Note: Table opera	tion will be performed at the end of the NI execution	Cancel	к
	Cancel Apply			Note, Table opera	uon win be performed at the end of the Ni execution.		

• Add table row: Select a table and populate a new row with a specific value.

Operate on Tabl	e				×			
Select Table:	Device_Confi	g_Data			~			
Select Operation:	Select Operation: Add Table Row							
Populate New R	ow with Specifi	c Value:						
Device		Cfg_Delta		Comment				
\$this_device	~	EIGRP_Config_Delta	~		~			
Note: Table opera	tion is delayed	in the end of execution		Cancel	ОК			

• **Delete table row**: Delete table rows (Frist Row or All Rows) matching condition.

Operate on Table	×
Select Table: Incident Table	~
Select Operation: Delete Table Row	~
Delete the First Row ~ Matching Condition:	
A Status Code ~ contains ~ changed ~	- 💼
B Select Variable ~	
Boolean Expression: A	
Note: Table operation is delayed in the end of execution Cancel	ок

• **Update table row**: update the matching condition row (Frist Row or All Rows) to a certain value.

Select Table: Incident Table	
Select Operation: Update Table Row ~	
Update the First Row $\sim$ Matching Condition:	
A Status Code ~ contains ~ changed ~ 💼	
B Select Variable V	
Boolean Expression: A	
For the Selected Columns:	
Table Column Variable	
Column 1 ~ = \$number(string) ~ 🛅	
+ Add	
Note: Table operation is delayed in the end of execution Cancel OK	

• **Query table cell**: Get the first table cell to match the specified conditions.
Get Cell of Ta	able						×
Retrieve Cell \	/alue from:						
Select Table:	critical_subne	t					~
From Colun	nn: network					~	
From the Ro	ow Matching Co	ndition:					
A dev	ice	~	Equals	~	\$this_device	~	Ē
B inte	erface	~	Equals	~	fe0/0	~	<b>D</b>
c Sele	ect Variable	~					
Boolean	n Expression:	A and B					
Expression: G	Get_Table_Cell (	ritical_su	bnet, network	, <conditior< td=""><td>n: A and B&gt;)</td><td></td><td></td></conditior<>	n: A and B>)		
					Cancel	0	к
							_

For example, users can get the **Switch Port** from **One-IP Table** by end system ip address from the ServiceNow Ticket.

CLI Command Diagnosis	Network Intent (View Mode) - All Network Intents/AAppend Expression	×
BJ_core_3550 show ip route connected      J. Define Variable	Expression: + 🖸 Variable - + 🚺 Function + 🗃 Get_Table_Cell	
Summan Text Original Text	Cancel OK	:a
Select Table: One-IP Table From Column: Switch Port	* Rows	
From the Row Matching Condition:           A         IP Address         ✓         Equals           B         Select Variable         ✓	unkonw_ip     v     f	
	: Message: <i>Sintf is down</i> tatus Code for Device: tatus Code for Intent:	
Boolean Expression: A Expression: Get_Table_Cell (oneiptable, switchPort, <cor< td=""><td>ndition: A&gt;) + Add Else</td><td></td></cor<>	ndition: A>) + Add Else	

# 4.4.5 Support Built-in Table and ADT

In R11.1, Intent can use the built-in data tables (e.g., Route Table, NCT) and ADT to define diagnosis:

• Loop and analyze the built-in table data. For example, loop the OSPF Neighbor table to check the neighbor state.

Manage All Variables	×		
Device Variables Marco Variables Intent Data Table			
+ Add Compound Variable + Add Compound Table + <u>Add Built-in (</u>	Data Table		
🖌 🧐 GW2Lab 🚬 show ip ospf	neigheor		
▷ ∰ cisco_ios_osfp_nei			
🔺 🥶 GW2Lab 🕨 show ip ospf	interface brief		
🔺 🥶 GW2Lab 🔁 show ip ospf	interface		
	Select Built-in Data Table	-	×
	<ul> <li>BGP Advertised Route Table</li> <li>BGP Neighbor</li> <li>GRE Tunnels</li> <li>MPLS TE</li> <li>OSPF Neighbor</li> </ul>	Subname: Global ID_1::Global ID_2::Global	
Original Results Variable Definition			
GW2Lab#show ip ospf neighbor           Neighbor ID         Pri         State         Dead Time         Address         Interface           172.24.255.51         FULL/DR         00:00:36         172.24.10.2         GigabitEt           172.24.255.20         FULL/DR         00:00:32         172.24.30.2         GigabitEt			
		Cancel	ОК

• Handle ADT Update and ADT-based follow-up intent, and loop ADT to get the multi-line text for device config-let compliance check.

anage All Variables			×			
Device Variables Ma	arco Variables	Intent Variables				
Add Intent Variable + /	Add Intent Table	+ Automation Data Table	S	Select Reference Data Tables		
🛿 Global Varaiable 1	Type:	String Inita	l Value:10	Search		0
Global Varaiable 2	Type:	String Inita	l Value:10	4 🗌 🚞 All		
🌐 Global Table 1				C III critical application paths		
📟 Global Table 2				Global ACL Config-let		
	ths		C Refresh			
device (\$string)	acl (\$string)	entry (\$mstring)	Onerest			
CA-TOR-R1	120	permit udp any 10.8.3.0	.0.0.0.255 eg 5201			
CA-TOR-R1	194	permit udp any any eq	pop3			
CA-TOR-R1	190	permit udp any host 10	1.1.1 eq telnet			
US-BOS-SW2	120	permit udp any 10.8.3.0	.0.0.0.255 eq 5201			
US-BOS-R1	120	permit udp any 10.8.3.0	.0.0.0.255 eq 5201			
security zones of net	work					
					Cancel	ОК

# 4.5 Control the Update of Intent Baseline by Logic

R11.1 supports updating the baseline in the intent diagnosis, which allows users to reset the baseline with conditions such as:

- If configuration changes are detected.
- If the baseline has not been updated for a long time.
- If the baseline is not set at all.

ummary Text Original Text     219   router ospf 1   220   router ospf 1   221   area 31 range 10.8.0.0 255.255.0.0   redistribute bgo cosh lubhots route-map Aus-ohio.H   redistribute bgo cosh lubhots route-map Aus-ohio.H   223   network 10.8.1.0 0.0.0 255 area 0   224   default-information originate always   Config Does not equal v ospf_config B select Variable v Boolean Expression: A Then Diagnosis Message: Save to Embedded Incident = V The OSPF configuration has changed. S Set Status Code for Device: S Set Status Code for Intent: Set Status Code for Intent: Set Status Code for Intent:					2. Define Diagnosis
	ummary Text 210 pouter 221 area 5 222 redist 223 network 224 defaul	Original Text ospf 1 -id 10.10.10 1 range 10.8.0.0 255.255.0 ribute bgp 05001 subnets n + 10.8.1.0 0.0.0.255 area t-information originate al	Search .0 oute-map AwS-Ohio-M Ø ways	Q ♥ ۸	Add Note Add Diagnosis Can also click a variable on the left to add autom Loop Table Rows If  A OUS-BOS-R1 Current Baseline Select Variable Boolean Expression: A Then Diagnosis Message: Save to Embedded Incident Set Status Code for Device: Set Status Code for Device: Set Status Code for Intent: Comparison: Compariso

Users can select batch updating intent baseline based on command and device.

Lo Set Intent I	Baseline					@ >	×
Set Baseline of	All Commands $$	of	This Device	~	with	Current Value 🗸 🗸	
	All Commands		This Device			Current Value	
+ Add Elseif	This Command		All Devices			Last Value	
				_			

R11.1 also adds a setting to define whether to update the intent baseline based on the baseline age.

Setting				×
Update the intent basseline data when the age of baseline	Select ~	1	Select 🗸	
	Older Than		Hour	
	Younger Than		Day	ок
	None-Existent		Week	
			Month	

## 4.6 Intent Variable and Intent Diagnosis Block

Intent Variable and Intent diagnosis block provide a way to support:

 Analyze logic on a few previous device sections and use the intent diagnosis block to loop through the intent table to output the final diagnosis, including NI status code, diagnosis message, CSV report, or trigger follow-up.



• Intent-level of diagnosis - handle ADT update and ADT-based follow-up intent (using Macro and Intent Variable to match intents inside ADT).



## 4.6.1 Intent Variable

R11.1 allows users to define an intent-level variable (string, number, or table variable) that can be reached and modified in the intent:

- Add/remove/update the table row and use the data row of this table.
- Define the singleton variable (string or number) with an initial value and update the value in the device diagnosis.
- Create Intent-level Macro Variable to take the external incoming key metric as the input (e.g., ServiceNow ticket id) and use the metric value in the follow-up intent template.



Use the intent variable to:

• Store the device statistic data, which can be referred to by the intent status code. For example, Count the shutdown interfaces on the devices:

BJ*POP	show interface	✓ Re	trieve Live Data 🗸 Last Updat	td: 03/24/2023 01:51:44 PM		
Define Vari	able			2. Define Diagnosis		
mmary Tex	t Original Text	Search	۹ 🗸 م	Add Note  Add Diagnosis Can also click a variable on the left to a	dd autor	ane
2 Fast 29 Fast 56 Fast 80 Fast	Ethernet0/0 is up, line prot Ethernet0/1 is up, line prot Ethernet0/0/0 is administrat Ethernet0/0/1 is administrat	ocol is up ocol is up ively down, line ively down, line	Untitled Diagnosis 1	Type description		
.04 Fast 28 Fast 52 Seri 78 Seri	Ethernet0/0/2 is administrat Ethernet0/0/3 is administrat ial0/1/0 is up, line protocol ial0/1/1 is down, line protocol	ively down, line ively down, line is up ol is down	pro	☑ Loop Table Rows ,≣ intfs ∨ Table Key: intf ∨ v If		0
04 Vlar 23 Loop 42 Loop	1 is up, lime protocol is do oback1 is up, lime protocol i oback2 is up, lime protocol i	s up s up		A BIPPOP Current ~		
61 Loop 80 Loop	<pre>&gt;&gt;back3 is up, line protocol i &gt;</pre>	s up ol is up		B e Bi+POP Current ~	•	
				protocol_statue v Contains v down	~ 🗊	
				C select variable		
				Boolean Expression: A or B		
				Then		_
				all_down_interface = \$all_down_interface + 1		j
				Add Logic 🗸		
4			•	+ Add Elself + Add Else		

• Receive external incoming key metric (e.g., ServiceNow ticket id) and pass the metric value in the followup intent template. For example, check the interface state and close the ticket from ServiceNow.

	Manage All Variabl	es	
	Device Variable	es	Macro Variables Intent Variables
	+ Add Intent \	/ariab	le + Add Intent Table + Automation Data Tables
		$\backslash$	
ol	Add Intent Va	riable	×
dre #\$% 5/2	Variable Na	ame:	sv_ticket_id
DLY /25	Т	ype:	string ~
FX	Initial Va	alue:	10001
0:0 0:0 " c dro	Zet as m	acro va	ariable Cancel OK
0 p ec,	-	1	
587 0 r			
ς,	Add Outgoing Webhook		×
	Name:	Service	Now
	Description:	close se	ervicenow ticket
	URL:	Post 🕶	http://10.10.32.143/ticket/close/ticket_id
	Header:	+Add	
		Key	Value
	Json Body Sample:	1 * 4 3 4 5 6	"Licket_Id":"Sid", "device":"Sidevice", "interface":"Sintface"
	Proxy:	None	•
	Test		Cancel OK

# 4.6.2 Intent Diagnosis Block

Difference between Intent Diagnosis and Device Diagnosis:

- Each intent can have only one intent diagnosis block, which will be displayed and executed after all device diagnoses.
- Intent Diagnosis has no parser and command baseline data and includes diagnosis blocks (if/then/else).
- Device diagnosis can access all variables of the current device and intent variables. Intent diagnosis only can access intent variables.
- Device diagnosis can use all supported logic, and intent diagnosis can only use the device-independent logic, including Intent Status Code, Follow-up Intent, Send Email, Call Webhook API, Call Qapp, and Export CSV Report.

vork Intent (Edit Mode	:)					×	Intent Diagnosis Block Definition	
oute change monitoring	Published	👗 Diagnosis Tree			Run - with Live Network	Save 🛛 Help 🚍	Diagnosis1 X Diagnosis2 X +	
route table						Intent Settings	Name: Intert Status Code Summary	
Add Device						Manage All Variables		
US-BOS-R2	Type I	Description here			+ Add Config Diagnosis	Add Intent Diagnosis Block	Description: check all intent status codes created in previous device diagnos	Jes
show ip route	Type I	Description here				Switch Devices	Loop Table Rows      Gore route      Table Key: route.next.hop	
						Define Abstract	II II	
1 Protocol	Address	Age (min)	Hardware	Туре		Named Tag		
2 Internet	3.3.3.3	-	0003.0003.0003	ARPA		Intent Family >	A type V Equals V Success	
12 Internet	172.24.10.250	192	00d0.58ac.f6f2	ARPA			B status_code v Contains v No change	e
13 Internet	172.24.10.249	-	000e.d7a7.b900	ARPA		Export		
22 Internet	172.24.32.225	136	0021.5589.b900	ARPA		Save as	C Select Variable V	
26 Internet	172.24.32.226	-	0021.5589.6520	ARPA		Publish Intent	Boolean Expression: A and B	
28 Internet	172.24.36.1	-	000e.d7a7.b900	ARPA				
US-BOS-SW1		Type Descri	iption here		+ Add Config Diagnosis	* Add CLI Diagnosis	Status Code for Intent: • Alert   Status Code First EIGRP Int SintlEIGRP.Rt	1_
show ip osprinterra	ce Rischl	ijpe besch					Export to CSV Report: Define	
7 Topology-MIID	COSt DISADIO	a shutdowr	n Topology Name			OSPF Neighbor Diagnosis	CSV Name: BOS Lao CSV 12/12 - 1	
3 Enabled by it	terface config	including seco	ondary in addresses			CSV 📋 Function Call	G Follow Up Intent: @Add Network Intent Stop	
4 Loopback inte	arface is treated	as a stub Hos	at addresses				Intent: Check Interface Status 🔅	
5 Tunnel0 is up.	line protocol is	up up					Intent Cluster: Single Device Sample 🔶	
6 Internet Add	ress 10.8.1.65/30	, Area 0, Atta	ached via Network State	ement			Intent Template: BGP Check 🔅	
7 Process ID 1	, Router ID 10.11	.11.11, Networ	rk Type POINT TO POINT,	, Cost: 65			Call Qupp: Define	
8 Topology-MTI	D Cost Disa	bled Shutdo	own Topology Name				Qapp:A4_Show Interface [Cisco IOS]	
							Add Lopic 🛩	
							+ Add Elseif + Add Else	

Users can use ADT as input to define an intent diagnosis. For example, check failover link change.

Network Intent (Edit Mode)			×
Block (1)	is Tree + Auto Intent	Run with Live Network Save OH	elp 📃
Type description here		Intent Settings Lock Settings	
Add Device		Manage All Variables	
V CB BJ*POP	Type Description here	+ Add Config Diagnosis     Intent Template Settin	
show interface	Intent Diagnosis Block Definition	× Switch Devices	marten
2 FastEthernet 29 FastEthernet		ntitled Diagnos Define Abstract	
56 FastEthernet 80 FastEthernet	Diagnosis1 +	stent Variable Namod Tag	
104 FastEthernet 128 FastEthernet	Name: Diagnosis 1	Export	>
152 Seriale/1/0 178 Seriale/1/1	Baseded as	Save as	
204 Vlan1 is up, 228 Loopback1 is	Description:	Publish Intent	
242 Loopback2 is 261 Loopback3 is			
280 Loopback8000	Loop Table Rows     Select Table Variable		
	V If Automation Data Table		
	Select Variable     Define Variable		
	Boolean Expression: e.g. A and B		
	~ Then		
	Status Code for Intent: 0 Error ~ Sint/ is down		
	Add Logic v		
	+ Add Elself + Add Else		
		Cancel OK	

# 4.7 Programmable Notification to 3<sup>rd</sup>-party system

R11.1 adds three diagnosis logics: **Send Email, Call Webhook API** and **Call Qapp** so that the intent diagnosis results can be sent to users or 3rd systems via **Email, Webhook API**, and **Qapp**. (e.g., email ServiceNow to create a ticket or pass the data to Splunk via Webhook API).

The basic flow of sending diagnosis results is as follows:



### 4.7.1 Send Email

R11.1 provides an entrance for adding **Send Email** block in NI diagnosis. Users can define the email settings, such as **subject, body,** and **intent link**.

Entrance:	Email Settings:		
Intent Data View	~ Then	Send Email	×
Send Email	Send Email:	Email Template: None	~
Follow-up Intent	To: Select user or input email	To: Select user or input email	֠
Set Intent Baseline	Subject: [NetBrain] Intent Execution Issues on Device Sthis_device.	Cc: Select user or input email	֠
Advanced >	Add Logic 🗸	Bcc: Select user or input email	÷.
Add Logic 🗸		Email Subject: [NetBrain] Intent Execution Issues on Device Sthis_device.	
	+ Add Eleolf - + Add Eleo	Email Body: Include Intent Link Include Includ	ent Link
	TAUU LISCH TAUU LISC	Merge emails to same recipients from this intent into one	
	Cancel Apply	Cancel	ок

For example, send an email if the interface CRC error grows.

Name:	Check CRC Issu	le		Anchor:	~
	Check CRC Issu	le			
✓ Loop ✓ If	Table Rows ,	Interface_errors_ch	neck 🗸 🛛 Table Key:	interfacef 🐱	Q
А					
	Delta(\$crc)	~	Greater than 🗸 🗸	0	~ 🖩
В	Select Variable	~			
Bool	ean Expression	: A			
√ Then					
🗅 Diag	nosis Message:			Save to Emb	oedded Incident 🔳
	✓ The CR	C of \$this_device.\$inte	erfacef continues to gro	w.	
<mark>2</mark> 5	Set Status Code	for Device:			
0	Error 🗸	The CRC of \$this_devic	e.\$interfacef continues	to grow.	
<mark>.</mark> s	Set Status Code	for Intent:			
0	Error 🗸	The CRC of <b>\$this_devic</b>	e.\$interfacef continues	s to grow.	
🔁 Send	d Email:		🗹 Include Inter	nt Link 🗌 Include Ind	ident Link 🛛 📃
Т	o: it@sevicer	now.com			÷2
Subje	ct: [NetBrain	] The CRC of <b>\$thi</b>	s_device.\$interfac	ef continues to g	°ow.

## 4.7.2 Call Webhook

Outgoing Webhook Manager is added in the System Management. Users can refer to the defined **Webhook** in the intent without knowing the technical details, such as the **URL** and **Header**, to send diagnosis results to

## a 3<sup>rd</sup> party system.

	System Mana	agement			Sj	vstem	Admin
Н	ome Page X L	icense × Outge	oing Webhook Manag	er ×			
+ Add							
Nam	le	Description		URL			
Serv	iceNow-1	ServiceNow-1		Post: https://servicenow.	.adtrig.com/l/19%3a4683917ee74c4c88a1d214a34	8cfe16f%40thro	ead.skype
	Add Outgoing We	ebhook		×			
	Name:	Input					
	Description:	Input					
		Dest					
	URL.	Post V Imput					
	Header:	+ Add					
	_	Key	Value				
		status	1024430				
	_	Status	op.				
	Json Body Sample:	1 { 2 "event": "incident.cre	ated",				
		3 "timespan": 12312301 4 "signature": "\$msg" 5 "status": "\$status" 6 } 7 8 9 10 10 11 12					
	Proxy:	None		~			
	Test			Cancel OK			

Inside an intent, users can add a Webhook API Call block.

··· Then		$\sim$ Then				
Diagsnosis Message Intent Data View		& Webr	nook API C	all:		Ξ
Output to Embedded Incident		Select W	ebhook:	ServiceNow-1 ~	Json Body Sample	
Send Email		Body V	ariables:	Variable	Value	
Follow-up Intent				msg	Select One	~
Set Intent Baseline				status	Select One	~
Advanced > Add Logic > + Add Elseif + Add Else	Export CSV Report Write to Devicelet Operate on Table	Add Logic	~		<ul> <li>▲ BJ*POP</li> <li>▲ S Configuration</li> <li>→ policy_maps</li> </ul>	
Add Lisen FAdd Lise	Set Intent Variable	+ Add Els	seif +	Add Else	, class_maps	-
	Call Qapp Webhook API Call				policy_map     policy_map_config	pply
	Break Current Loop				Inline Function	

Use **Webhook Call** to Send Alerts to External Ticket System, for example, check application performance and return found issues to ServiceNow via calling webhook.

CLI Command Diagnosis				×
BJ_L2_Core_4 show policy-map interface	etrieve Live Data 🗸 Last l	Ipdated: 03/19/2023 04:24:12 PM		
1. Define Variable		2. Define Diagnosis		
Summary Text         Original Text         Sourch           2         FastItherret2/0/10         Gast-map: ex_voice_class((metch-all))         Gast-map: ex_voice_class((metch-all))           1         Class-map: ex_voice_class((metch-all))         Gast-map: ex_voice_class((metch-all))           16         Class-map: ex_voice_class((metch-all))         Gast-map: ex_voice_class((metch-all))           16         Class-map: ex_voice_class((metch-all))         Gast-map: class((metch-all))           17         Fattitherret2/0/24         Gast-map: class((metch-all))           18         S minute offered rate 0 bps, drop rate 0 bps         Gast-map: class((metch-all))           19         S minute offered rate 0 bps, drop rate 0 bps         Gast-map: class((metch-all))           19         S minute offered rate 0 bps, drop rate 0 bps         Gast-map: class((metch-all))           10         S minute offered rate 0 bps, drop rate 0 bps         Gast-map: class((metch-all))           10         S minute offered rate 0 bps, drop rate 0 bps         Gast-map: class((metch-all))           10         S minute offered rate 0 bps, drop rate 0 bps         S minute offered rate 0 bps, drop rate 0 bps	Q V A	Add Note Add Diagnosis Boolean Expression:  The  Diagnosis Message  Cost Dray Occur  ServiceNon  ServiceNon  G Call Webhook API: Select Webhook Body Variables: Variable Problem_D Incidenc_ID  + Add Baelf	Can also click a variable on the left to add aut Can also click a variable on the left to add aut Can also click a variable on the left to add aut Can also click a variable on the left to add aut red in class map Sclass_map of Sintf ce p occured in class map Sclass_map of Sintf te w Webhook v Ison Body Sample Value Value Value Device his_device v	
Help   Manage All Variables			Cancel	pply a

# 4.8 Schedule Intent

R11.1 supports setting the schedule to run intents. Users can schedule an intent to diagnose the transient problems, such as:

- Schedule an Intent "Monitor ASA Failover status" to continuously monitor the core application path.
- Schedule an Intent to regularly check whether the standby switch has been configured with the same ACL as the active switch.
- Schedule an Intent to ping devices before regular network changes or identify variation after network changes, then send email alerts to engineers.

Network In	tent (View Mode) - All M	Network Intents/CLI U	nReachable									×
Schedule Run	•						×	(†)	0	<b>⊮</b> }0	🔁 Edit	≡
Task Name Description Intent	Untitled-Task 1				Select			Run Run No Schedu	ow Jule Run	with Li	ve Networ	k V
Data Source		Current Baseline	2023-03-17	1	1 ~ : 12 ~	AM V						
	Time Zone: (UTC+08	:00) Beijing, Chongqinş	g, Hong Kong, Urumqi	~ 0	Cancel	Submit						

When a user defines a scheduled task:

- One scheduled intent task can only have one intent.
- Able to set the data source, execution time, and frequency (**Once, Continually, Daily,** and **Weekly**).
- For the Continually settings, users must set the end by times and end by date (cannot be longer than 2 weeks from the start). If the Times checkbox is selected, the Times\*Frequency must be less than 2 weeks.

chedule Run			
Task Name:	Untitled-Task 1		
Description:			
Intent:	Monitor QoS Drop	Select	
Data Source:	Live Network (	) Current Baseline 🚺	
Time Settings:	Once	Start: 2023-03-19	
	Continually 1		
	<ul> <li>Daily</li> </ul>	Frequency: Repeat every 30 minutes	
	O Weekly	End by: 10 Times	
		○ 2023-04-02     ○   08 ~ :   32 ~   PM ~	
	Time Zone: (UTC-08:00	) Pacific Time (US & Canada) 🛛 🗸 🕦	
		Cancel Submit	

# 4.9 API Diagnosis in Intent Definition

The Intent in the previous version supports the data retrieved from CLI and SNMP but not from APIs, which limits the intent used for the public cloud and SDN technologies. R11.1 adds support for API data, which enables the Diagnosis of SDN/Cloud Network and SPOG Data View from an external system via REST API (such as Splunk, SolarWinds, and ServiceNow). R11.1 adds a new API diagnosis type to support API diagnosis in intent. After defining the API diagnosis, a new API Diagnosis section will be added:

		×	API Dagrees	
Network Intent1	🛓 Gagenia True	Ren - 🗇 🖬 🖬 🖉 🛶 🗮	IUS-805-81 Section Name, APL. 🖌 API Adapter. Coce AD	Retrieve Data Function, Dafred     Retrieve Live Data     P     D     Lass Reserved 10/12/2020 http://d
Dwck 09PF Status for 2 devices		7.5ebet.Mag	Distance in the second s	
Add Device		14 87	2. Define Dager	sos J. Debug
Add Device     A	Oper Designed Area.	Add Carling Engenome     Add Carling Enge	Charace section     Control Control     Control Control     Control Control     Contro     Control     Contro     Control     Control	Abberg     Abberg     Abberg     Add Search Se
			Image: State	22         Assess basess: 51 (State Assess: 51 (State Asses)))))))))))))))))))))))))))))))))

 Add Retrieve Function to Retrieve data by REST API: In the API diagnosis definition, after selecting API Adapter for a specific vendor, users can define the retrieve data function to get the network data of SDN/Cloud/Other External System via REST API. The **Retrieve Data Function** is defined by Python Script, and it is defined the same as the advanced API parser.

Defin	e Variables		2. Define Diagnosis 3. Debug				
mple	Data 🚄 🛛 👝		Seorch	dd Tabl	le 💌 Add J	5ON Ta	ab
	D	Define Fur	iction to Retrieve Data	×			
į	(						
ł	"procEntity"	1	m				
4	"attribute	2	Begin Declare Variable	ine	Ада кері	aceme	su
	"admin!	3 *					
	"childAc	4	("name::"intr_table", "type::"table", "columns":[ ["name", "intr_t" "two;", "trime"]				
	"cpuPct	5	("name: init, type: string ), ("name: "init statis" "tune" "string")				
	"maxMi	7	{"name": "traffic_in_bute" "tupe": "int"].				`
	"memFi	8 -	("name": "traffic_out_byte", "type": "int")				
	"modTs	9					
	"monPc	10	1)				
	"name"	11	1		T		
	"operEr	12	End Declare		Type		
	"operSt	13			String	~	
	Status	14	def BuildParameters(context_device_name_narams).		00		
	}	16	act dn = GetDeviceProperties(context, device name, {'techName': 'Cisco ACI', 'paramType': 'SD		String	~	
	},	17	<pre>dn = get_dn['params']['dn']</pre>		501115		
)	(	18	<pre>role = get_dn['params']['role']</pre>		String	~	
	"procEntity"	19	<pre>rtn_params = [{ 'devName' : device_name, 'dn' : dn, 'role': role }]</pre>		String		
4	"attribute	20	return rtn_params				
	"admin	21	daf RakriavaDaka(ska pasara)				
	"childAd	22	do - rtn poros[/do]				
	"do": "te	25	role = rtn params['role']				
	"maxMe	25	url = '/api/mo/' + dn + '/sys/proc.json'				
	"memFi	26	rtn_params['url'] = url	10.04	d 1/20do 1/	a se la re	
9	"modTs	27		poc	J-1/1008-1/5	sys/pro	50
)	"monPc			1001	d-1/node-1/	evelore	~
	"name"			poc	1-1/1100e-1/:	systero	~
2	"operEr						
2	"operEr						

2. New **JSON Group** to parse the JSON Result: After retrieving the JSON data by the defined retrieve data function, add a new Parser Group, **JSON Group**, to parser the JSON result. JSON Group will read all the keys from the JSON result and convert the JSON result to Table Format by selecting the JSON key.

Define Variable			2.	Define Diagnosis				
aseline Data 💋	Search	۹		Define Variables 🕕	🗶 Add V	ariables 🖶 Ac	dd Paragraph 🖩 Add Tabl	e
2 { 3 "id": "/subscriptions/073e6f45-d1ae "type": "Microsoft Insight/metrics	e-40fe-93af-882:	<b>^</b>		✓ ■ app_rules_hit_count 。	2	L	Add Json Table Add Text	-
5 "name": { 6 "value": "ApplicationRuleHit",				Help		+ Start Line	Add Collector Publish Parser to Library	
<pre>7 "localizedValue": "Application 8 }, 9 "dicplayDecorpintion": "Number of ti </pre>	rules hit count			Data Scope 💿			Copy from Verified NI	>
<pre>9</pre>	tmes Application			By Path []/{)/timeseries[]	]/{}/data[]/{}		Load Parser from Library Copy Parser from NI	5
2 { 3 "metadatavalues": [], 4 "data": [				Define Variable by Selectir	ng JSON Key 💿		Export Parser Import Parser	
5 { 6 "timeStamp": "2023-	-02-09T21:30:007	Start Key 1		JSON Key	Variable		Search and Replace	
7 "total": 3 8 },		Key 2	$\Rightarrow$	timeStamp	🗸 🗢 \$timestamp	)	string 🗸 🖸	,
9 { 0 "timeStamp": "2023-	-02-09T21:31:002	DS1-End DS2-Start		Parsed Result 🔛 app_rule	es_hit_count 🗸		đ	9
1 "total": 3 2 },		Key 1		\$timestamp ቝ	~ \$	otal		
3 4 .		Key 2		2023-02-09T21:30:00Z	3			
5 "timeStamp": "2023- 6 "total": 1	-02-09T21:33:007	DS2-End DS3-Start		2023-02-09T21:31:00Z	3			
7 J		Key 1		2023-02-09T21:33:00Z	1			
99 ]		Key 2						
1 ]; 2 "errorCode": "Success" 3 }		DS3-End						
4 ]								

For example, users can build an intent with API diagnosis to monitor the number of times application rules are hit on all Azure firewalls.



# 4.10 Simplified Intent debug

R11.1 removes the old Intent Debug function since it is hard to use and maintain. Instead, R11.1 enriches the Execution Log in intent Debug Mode.

• Support the centralized viewing of home intent and follow-up intent/intent template/intent cluster execution log for multi-stage diagnosis.

letwork In	tent (View Moo	le) - All Network Inte	ents/Training/(	OSPF Route Table Chec	k		
I OSPF	Route Table Ch	neck (Published)	(	Check OSPF Status for 2 dev	vices	(†) 📃 1	🔥 0 🛛 🕹 Edit
Result: 01/	19/2022 09:15PM	✓	Incident 🗸	<b>≟</b> ⊚		Run	with Live Network
This intent	execution is finish	ed at 01/19/2022 09:16	PM with 3 errors.	You can View Execution Log			
2 Devices	3 Diagnoses	S The CRC of i	nterface FastEtherne	t0/0 has increased. 3			View
v 🔭 U	S-BOS-R2	S Hello timer	mismatch 2		please focus this devic	e`s changing.	2 Actions
⊿ ► s	how ip ospf interf	ace		1 Diagnosis	check OSPF hello time	e of interface	
1 2 12	Loopback0 is Ethernet0/1 Timer int	s up, line portoco is up,line portoco cervals configured	l is up ol is up , hello 10, I	Dead 40, wait 40, Re	transmit 5	Hello tim	er mismatch
22	Timer int	ervals configured	, hello 10, I	Dead 40, wait 40, Re	transmit 5		
🔺 🏊 s	how ip ospf			1 Diagnosis	check OSPF hello time	e of interface	
1 2 12 13	Loopback0 is Ethernet0/1 Timer int Tunne10 is u	s up, line portoco is up,line portoco cervals configured up, line protocol	l is up ol is up , hello 10, I is up	Dead 40, wait 40, Re	transmit 5	Hello time	r
22	Timer int	ervals configured	, hello 10, I	Dead 40, wait 40, Re	transmit 5		
∨ 🔗 N	BLAB-XR-P1	S Diagnosis N	ote: BJ_core 5				2 Actions
⊿ 🛌 s	how ip ospf neigh	bor		2 Diagnoses	Check OSPF Nbr uptim	ie.	
1	Protocol	Address	Age (min)	Hardware	Туре	Diagnosis	Note: Bj_cor
12	Internet	3.3.3.3	- 192	0003.0003.0003 00d0.58ac.f6f2	ARPA	The ospf	route has chan
13	Internet	172.24.10.249	-	000e.d7a7.b900	ARPA		
22	Internet	172.24.32.225	136	0021.5589.b900	ARPA		
26	Internet	172.24.32.226	-	0021.5589.b520	ARPA		
28	Internet	172.24.36.1	-	000e.d7a7.b900	ARPA		

• Support outputting richer error logs for troubleshooting intent execution.



• Support outputting richer intermediate raw data of intent execution process for debug intent.

### 4.11 Other Intent's Improvements

#### 4.11.1 Intent View

In R11.1, the UI layout of Intent View is optimized. The first layer UI displays the current running status of NI and frequently used operations. Moreover, the CSV Report is moved to the secondary menu to keep the main interface clean.



### 4.11.2 View Diagnosis Message

The Diagnosis Message dialog supports switching to view the status code and message generated by the execution of Home Intent and Follow-up Intents, and clicking the Open button can open the follow-up intent

to view the details:



#### 4.11.3 Export CSV Report to Files

In R11.1, users can specify the NetBrain Files folder for CSV reports from intent.

	0			1	
CSV report files:					
CSV					
					Ē
*CSV Name: Test 1					
*Column: column	1, column 2, column 3, colum	in 4, column 5,			
Save CSV Report t	to Files				
*Location	: Desktop\		Browse		
			k	1	
*CSV File	e: Test 1				
	The CSV file name will be rese intent template/intent cluster	t as file name + intent r r.	name when this intent is used as		
	CSV *CSV Name: Test 1 *Column: column Save CSV Report 1 *Location *CSV File	<ul> <li>CSV</li> <li>*CSV Name: Test 1</li> <li>*Column: column 1, column 2, column 3, column</li> <li>Save CSV Report to Files</li> <li>*Location: Desktop\</li> <li>*CSV File: Test 1</li> <li>The CSV file name will be resend intent template/intent cluster</li> </ul>	<ul> <li>CSV</li> <li>*CSV Name: Test 1</li> <li>*Column: column 1, column 2, column 3, column 4, column 5,</li> <li>Save CSV Report to Files</li> <li>*Location: Desktop\</li> <li>*CSV File: Test 1</li> <li>The CSV file name will be reset as file name + intent or intent template/intent cluster.</li> </ul>	CSV *CSV Name: Test 1  *Column: column 1, column 2, column 3, column 4, column 5,  ✓ Save CSV Report to Files  *Location: Desktop\  *CSV File: Test 1  • Test 1  • The CSV file name will be reset as file name + intent name when this intent is used as intent template/intent cluster.	<ul> <li>CSV</li> <li>*CSV Name: Test 1</li> <li>*Column: column 1, column 2, column 3, column 4, column 5,</li> <li>Save CSV Report to Files</li> <li>*Location: Desktop\</li> <li>*CSV File: Test 1</li> <li>The CSV file name will be reset as file name + intent name when this intent is used as intent template/intent cluster.</li> </ul>

# 4.12 Intent Replication Improvements

The configuration logic in the Intent Template Setting is improved to be more intuitive.

R11.1 makes the following improvements to the Intent Template:



- Macro variable config: config how to define Macro variables using ADT.
- **Macro Variable config of Replication for Path**: enable replication for path and how to pass a variable value to a Macro variable using built-in path variable (source, destination, source port etc.)
- **Critical Var Config**: define how to match a seed device command based on auto-test results of critical variables.
- **Intent Parser Qualification**: define intent parser qualification to filter qualified devices based on qualification to improve unnecessary command testing.
- **Cloned Intent Naming Rule**: define how cloned intent can be named with the variable value of Macro variable and path variable values.
- Automation Tag Config: configure automation tag for cloned intents.

## 4.12.1 Device Scope Configuration

For Device Scope configuration, the existing **Device Qualification** and **Filter Devices by Device Group/Sites** options are merged into one section for configuration.



Both options **A** and **B** can be defined separately with the following options:

- **Define A only**: Filter Intent Template devices based on the **Device Qualification** of the configuration item.
- **Define B only**: Filter Intent Template devices based on **Device Group/Site configuration**.
- **Define both A and B**: Filter Intent Template devices based on the intersection of A and B.
- **Both A and B are undefined**: Intent Template cannot match any device.

#### 4.12.2 Set Macro Variable

The method to set Macro Variable can be done only through GDT in the current version (the method of configuring Macro Variable through CSV file is removed. You can create a GDT table from a CSV file instead).

tent Template			×		×
Description:			two	ork Save 🕑 H	lelp ≡ ≡
De site Francisco dia Trancisco Mada Serviceo d				💑 Intent Map: MiniLAB	∽ vrk
Sevice Expansion via Template Wode Settings:					Add 🚍
A: Device Qualification: Defined 🛅 🚯		$\cdot$		+ Add CLI Diagnosis	=
B: Filter Devices by Device Groups/Sites: Sele	ect 🗸		в	Edit Diagnosis	= (/
			te S	tatus	
Macro Variables: 1 variable		Pre	view Data	CSV	
Enable Replication for Device: Match Macro	Variable				
Defin	ne Matching Macro Varia	ables			
Automatically Select All Diagnosis V.     Manually Select 0 Variables	The value of Global Data device key is tested acro	a Tables with device iss all qualified devic	key is tested based on devic es. Command is tested base	e. While the value of Glob ed on default value if no m	al Data Table without atching variable.
Intent Parser Qualification: Undefined	Seed Device	Macro Variable	Macro Variable Type	Matching Variable	
	GW2Lab				<u></u>
Cloned Intent Naming Rule: 🚯		Critical_route	string	IP(Critical Route)	~
<pre>\$nit_name</pre>					
Automation Tag for Cloned Intents: + A					
					-
	4				F
Dev	vice Key Settings: 1/1 D	evice Key Set for A	DT Decode Filter: U	ndefined	Cancel OK

Define Macro Variable for the seed device as follows:

- 1. If an ADT column is selected and the device key is configured for the ADT, all Qualified Devices will use values of the column for each device defined in ADT to test against Critical Variables.
- 2. If an ADT column is selected and no Device Key is configured for the ADT, all Qualified Devices will use all values in the ADT column for Auto Test to test against Critical Variables.
- 3. If no ADT column is selected, the default value in the Seed Intent will be used to test the effectiveness of the command for all Qualified Devices (without going through the Critical Variable check).

By default, the system will set the first available device/interface column as the default device key column. You can manually modify the device key column settings.

Device Key Settings		;	× Pr	eview Data		
Selected Table	Device Key Column					
Critical Route	Device	~ ^				×
	None					
	Device		th device	key is tested based on de	evice. While the value of Global l	Data Table without
	IP		fied devi	ces. Command is tested b	ased on default value if no mat	ching variable.
	Interface IP Interface Name	-	riable	Macro Variable Type	Matching Variable	
4						^
	Cancel	ОК	oute	string	IP(Critical Route)	~
Automation Tag for	Cloned Intents: + A					×
	Device Key Settings: 1	1/1 Device K	(ey Set for /	ADT Decode Filter:	Undefined C	Cancel OK

To reduce the possibly large number of Candidate Values to perform decoding operations, users can set a **decode flag** for the values.

Define M	atching Macro Var	riables	Diagnosis and Prevention	Und Intency Diagnosisy Chee		×	× <u>u</u>
1 The vice	value of Global Da ce key is tested aci	ita Tables with device ross all qualified devi	key is tested based on devic ces. Command is tested base	e. While the value of Global D ed on default value if no matc	ata Table without hing variable.	Save 🛛 Help 🚍	×
	Seed Device	Macro Variable	Macro Variable Type	Matching Variable			
4	😁 US-BOS-R2				*	Type to search	Q
		subnet	string	Critical Route(Device_Cri	tical_Ro v	Shared Tables      Design     L3 Design     B Device_Critical_R     Decode Flag     My Tables	loute
Device H	Key Settings: Und Automatically he Filter Logic Select the Column specified value is t	Select All Diagnosis V of or decode filter, dec false for selected colu	te Filter: Undefined ①	Ca code of the line if the	Ancel OK		
s	eed Device		Column for Filter Decode Flag(Device	_Critical_Route) v			Cancel OK
•				Cancel OK	OK		4

Users can define a filter logic for each Seed Device by selecting an ADT column. By using an ADT column with Boolean Type, it can decide whether the row will be used for decoding.

### 4.12.3 Intent Replication for Path

When an Intent Template is used for a Path, it can be used as input and passed to the Macro Variable for replication. Therefore, the ability to enable replication for Path is added here, which can replicate for Path Input.

tent Template		×	×	
Description: Input	Debug in Intent Clus	twork	Save 🕜 Help 😑	
Device Expansion via Template Mode Settings: 🕦			ntent Map: Select 🗸 🗸	vrk
A: Device Qualification: Defined	A	] 🔤 +/	Tag: + Add  Add CLI Diagnosis Edit Diagnosis	~~
lacro Variables: 3 variables Enable Replication for Device: <u>Match Macro Variable</u>	Enable Replication for Path Define Replication for Path	C Status	Code	
Enable Replication for Path Undefined	Seed Device	Macro Variable	Macro Variable Type	Matching Variable
irtical Variable Settings: 🚯	a 🤭 CA-TOR-R1			
<ul> <li>Automatically Select All Diagnosis Variables</li> </ul>		critical_description	string	Path.Source 🗸
Automatically Select All Diagnosis Variables     Manually Select 0 Variables		critical_description	string string	Path.Source
Automatically Select All Diagnosis Variables     Manually Select 0 Variables     Intent Parser Qualification: Undefined		critical_description critical_acl critical_entry	string string string	Path-Source
Automatically Select All Diagnosis Variables Annually Select () Variables Intent Parser Qualification: Undefined		critical_description critical_acl critical_entry	string string string	Path.Source
Automatically Select All Diagnosis Variables Automatically Select () Variables Intent Parser Qualification: Undefined oned Intent Naming Rule: Snit name		critical_description critical_acl critical_entry	string string string	Path.Source
Automatically Select All Diagnosis Variables  Manually Select 0 Variables  Intent Parser Qualification: Undefined  Ioned Intent Naming Rule:  \$nit_name  utomation Tag for Cloned Intents: + Add		critical_description critical_acl critical_entry	string string string	Path-Source
Automatically Select All Diagnosis Variables  Manually Select O Variables Intent Parser Qualification: Undefined  oned Intent Naming Rule:  Snit_name  utomation Tag for Cloned Intents: + Add		critical_description critical_acl critical_entry	string string string	Path-Source

When the user enables the replication for Path, a window "**Enable Replication for Path**" popups for the user to select the Path Variable used for the Seed Device Macro Variable.

Enable R	eplication for Path				>	× Select Global List Variables	×
Define	Replication for Path	n				Type to search	٩
4	Seed Device	Macro Variable	Macro Variable Type	Matching Variable	•	Shared Tables      Get and the set of t	Î
		critical_description	string	Path.Source	~	Critical Route	
		critical_acl critical_entry	string	Source		Failover Link Name	- 1
			Path Variables	Destination     SourcePort     DestinationPort     Protocol		Critical Route Secondary Device Primary Link	
	4		ADT Variables		, ·	wy Tule_Unlet_2      transport_input     exec_timeout      BGP NBR Ping Status	
				Remove Selected Variable		A . I Device I BGP_Neighbor_IP I Ping Status Cancel	ок

### 4.12.4 Intent Map Setting Configuration

monitoring	Dublick	hurd Disensei	Tree		Run	with Live Network	Enue	A Help	=
monitoring	Publish	a unagriusi	i nee		Run	• WHAT LIVE INCOMOR		Select Map	Export
								Tag: +Add	Save as
S-R2		Type Description h	re		(	* Add Config Diagnosis	🖿 + Add CLI D	iagnosis	Define NI CSV Report Switch Devices
ip route		Type Description he	me				Ed	it Diagnosis	Define Abstract
rotocol	Adda	Intent Map Settings		>	<		OSPF Nbr Dow	m 6	Intent Family Define Macro Variable
sternet	172.	Draw Devices on Map					Message 🖸 0	ata View	Named Tag
iternet	172.	<ul> <li>Intent Devices</li> <li>Intent Data View D</li> </ul>	vevices Only		←				Intent Template
iternet	172.	Auto link devices with	IPv4 L3 Topology	~					Publish Intent
S-R10		Extend at most 3	neighbor devices f	for each member device		Add Config Diagnosis	Add CLI D	iagnosis	
ip route				Cancel OK			Ed	it Diagnosis	
rotocol	Addr	ess Age (mi	in) Hardware	Туре			OSPF Nbr Dow	m	
iternet iternet	3.3.	3.3 - 24.10.250 192	0003.0003. 00d0.58ac	.0003 ARPA .f6f2 ARPA			Diagnosis Not	e ew	

The Intent Map configuration in the Intent Template is moved to the **Intent Map settings** inside the Intent.

When generating Cloned Intent, the Cloned Intent Setting will be set according to the **Intent Map Settings** in the Seed Intent.

### 4.12.5 Configuration of Critical Variables

The configuration of Critical Variables is consistent with the configuration items of the improved Intent Cluster. The logic is consistent for generating Cloned Intent for PAF/TAF, and the match is determined based on the Boolean expression of all Critical Variables.

Users can select any variable as the Critical Variable and combine them with the Boolean operations (AND/OR).

Boolean Algebra	=	CLI Command	Critical Variables	Replicate
A	=	a show version	1 Variables Selected	
🥥 В	=	1.3.6.1.2.1.2.2.1	A 🖸 💷 show version	
0 C	=	🔛 \$cpu_oid  \$mem_oid	day 🖂 🖂	
🥝 D	-	1.3.6.1.2.1.2.2.1.12	minutes	
🥏 E	-	🖽 show process cpu	week	
Ø F	=	🖽 show interface	1 Variables Selected	
🥏 G	-	1.3.6.1.2.1.2.2.1.2.1	1 Variables Selected	
📀 н	=	Configuration	1 Variables Selected	
Boolean Expression:	A or B			

A Replicate checkbox is added to each device section, indicating whether the corresponding CLI/Config will be replicated. Dependencies across CLI Command will be passed through even if not selected for replication.

#### 4.12.6 Intent Parser Qualification:

An option **Intent Parser Qualification** is added in the intent template settings to reduce the possibly large number of commands during the decoding process. With this option checked, the devices will be filtered according to the qualification defined in the **Intent Parser Qualification** (for example, per different Vendor Devices).

Cirtical Variable Settings: 🚯	
Automatically Select All Diagnosis Variables	
O Manually Select 0 Variables	
Intent Parser Qualification: Undefined	

A: Device Qualification: Defined 📾 🚯	Intent Pa	arser Qualification			
B: Filter Devices by Device Groups/Sites: Select ∨	Define	Qualification for In	tent Parser		
		Seed Device	Command	Qualification	
Macro Variables: 3 variables		😋 CA-TOR-R1			
			Configuration	Undefined	
Enable Replication for Device: Match Macro Variable					
Enable Replication for Path: Undefined					
Cirtical Variable Settings: 🚯					
Automatically Select All Diagnosis Variables					
O Manually Select 0 Variables					
Intent Parser Qualification: Undefined		4			
Cloned Intent Naming Rule: ()					Cancel
<pre>\$nit_name</pre>					
Automation Tag for Cloned Intents: + Add 🔳					
		Cancel	ок		
		_	_		

For each command and each Seed Device, users can define the following:

• **Device Type Qualification:** Specifies the Device Type Qualification that will be effective for Device Types.

## 4.12.7 Cloned Intent Name Rule

To make the name of Cloned Intent more meaningful, users can define the rule to name the cloned intent. The following variables be inserted into the name:

- NIT\_name
- Macro Variable Name
- Path variables (application\_name and path\_name)

Intent Template	Define Link to Variable	×
Description: Input	🖌 🔯 Macro Variable	
Device Expansion via Template Mode Settings: ()	▲ CA-TOR-R1 Image: Critical_description	
A: Device Qualification: Defined 🗃 🚯	critical_acl	
	application_name     path_name	
Macro Variables: 3 variables	🛃 nit_name	
Enable Replication for Device: Match Macro Var		
Cirtical Variable Settings: 🕦	Link Text:	
Automatically Select All Diagnosis Variables     Manually Select 0 Variables		
Intent Parser Qualification: Undefined	Cancel OK	
Cloned Intent Naming Rule: () \$nit_name \$		
Automation Tag for Cloned Intents: + Add 🗐	Cancel OK	

# 4.13 Intent Decode and Baseline Improvements

R11.1 improves Intent Decode and Baseline Service to remove the complexity in understanding the Intent Decode/Baseline and the Intent Decode cycle. The key improvements are:

1. Added detailed status indicators to the column Intent Decoding
2. Updated Intent Decoding and Baseline Settings pane.

In	stalled Intents	Published Intents	Preventive Au	utomation via ADT	Auto Intent	NetBrain Download			
lten	ns: 154 + Add Inte	ent							
	Intent Name	Locat	ion	Intent	Mode	Intent Baseline	In	tent Decoding	Auto Intent
	Eddy								
	<mark>Anti</mark> -drift	All Ne	etwork Intents/En	igineer/Ed Templ	ate	Manual	La	ast Decoded at 02:14 PM 04/1.	🥑
	yu_d_lab1								
	<mark>Anti</mark> _drift	All Ne	etwork Intents/Au	itomation Templ	ate	Manual	La	ast Decoded at 11:17 AM 04/1.	
								$\mathbf{N}$	
								$\mathbf{N}$	
								\ \	
Int	ent Name: Anti-dr	ift							
Inte	ent Name: Anti-dr	ift						1 Intent Decoding Str	NEW
Int	ent Name: Anti-dr	ift Network Intents/Engine	er/Eddy	Triggered	Automation	Preventive Automation	Cloned Intents	1 Intent Decoding Sta	NEW atus
Inte	ent Name: Anti-dr Location: All N Intent Mode: Tem	i <b>ft</b> Network Intents/Engine	er/Eddy	Triggered	Automation	Preventive Automation	Cloned Intents	Intent Decoding Sta	NEW atus
Int	ent Name: Anti-dr Location: All N Intent Mode: Tem	ift Vetwork Intents/Engine- uplate	er/Eddy	Triggered Items: 212	Automation	Preventive Automation 2 Intent Decoding a	Cloned Intents	Intent Decoding Sta Update	NEW atus
	ent Name: Anti-dr Location: All N Intent Mode: Tem Intent Decoding	rift Network Intents/Engine uplate	er/Eddy Decode Now	Triggered Items: 212 Cloned Int	Automation	Preventive Automation 2 Intent Decoding a Device	Cloned Intents and Baseline Set	1 Intent Decoding Sta tings Created	atus
Int	ent Name: Anti-dr Location: All N Intent Mode: Tem Intent Decoding O Recurring Deco	r <b>ift</b> Network Intents/Engine Iplate Ide	er/Eddy Decode Now	Triggered Items: 212 Cloned Int	Automation Rent	Preventive Automation 2 Intent Decoding a Device 1	Cloned Intents and Baseline Set	Intent Decoding Sta update tings Created 02:46 P	<b>NEW</b> atus
Inte	ent Name: Anti-dr Location: All N Intent Mode: Tem Intent Decoding O Recurring Deco Select	rift Network Intents/Engine uplate Ide	er/Eddy Decode Now	Triggered Items: 212 Cloned In Anti-drif	Automation ent t 1 t 3	Preventive Automation 2 Intent Decoding a Device 1 1 1	Cloned Intents and Baseline Set	Intent Decoding Sta tings Created 02:46 P 02:46 P 02:46 P	Atus Atus I At M 04/17/2023 M 04/17/2023
	ent Name: Anti-dr Location: All N Intent Mode: Tem Intent Decoding Recurring Deco Select Update Inte One-Time Deco	rift Network Intents/Engine aplate Ide Int Baseline Periodically Ide 106 Dev	er/Eddy Decode Now	Triggerec Items: 212 Cloned Int Anti-drif Anti-drif Anti-drif	Automation ent t 1 t 3 t 4	Preventive Automation Preventive Automation Decoding a Device 1 1 1 1 1 1	Cloned Intents and Baseline Set	1 Intent Decoding State tings Created 02:46 P 02:46 P 02:46 P	Atus NEW I At M 04/17/2023 M 04/17/2023 M 04/17/2023
	Intent Name: Anti-dr Location: All N Intent Mode: Tem Intent Decoding Recurring Deco Select Update Inte One-Time Deco	rift Network Intents/Engine Inplate Inde Int Baseline Periodically Inde 106 Dev	er/Eddy Decode Now	Triggered Items: 212 Cloned Im 1 Anti-drif 1 Anti-drif 1 Anti-drif 1 Anti-drif	Automation Rent t 1 t 3 t 4 t 2	Preventive Automation 2 Intent Decoding a Device 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Cloned Intents and Baseline Set	Intent Decoding State tings Created 02:46 P 02:46 P 02:46 P 02:46 P	Atus NEW Atus NEW I At M 04/17/2023 M 04/17/2023 M 04/17/2023 M 04/17/2023
	ent Name: Anti-dr Location: All N Intent Mode: Tem Intent Decoding Recurring Deco Select Update Inte © One-Time Deco	rift Vetwork Intents/Engine- aplate Ide It Baseline Periodically Ide 106 Dev	er/Eddy Decode Now	Triggered Items: 212 Cloned Ini I Anti-drif I Anti-drif I Anti-drif I Anti-drif I Anti-drif	Automation rent t 1 t 3 t 4 t 2 t 5	Preventive Automation 2 Intent Decoding a Device 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Cloned Intents and Baseline Set	Update           Update           02:46 P           02:46 P	Atus NEW atus NEW I At M 04/17/2023 M 04/17/2023 M 04/17/2023 M 04/17/2023 M 04/17/2023

#### 🛂 Intent Based Automation Center

## 4.13.1 Intent Decode / Baseline Settings Adjustment

R11.1 version adds the option, **Update Intent Baseline Periodically**, under Recurring Decode.

After selecting **Recurring Decode**, users can select a timer and check **Update Intent Baseline Periodically**.

Intent Name: BGP Check 1						
Location:	All Network In	tents/home-netwo	rk			
Intent Mode:	Template					
Intent Decodi	ng:		Decode Now			
Recurrin	g Decode	0 Device	s decoded			
Select			~			
One-Tim	te Intent Baselir e Decode	ne Periodically				

The logic is:

- The intent Baseline cycle is completely consistent with the Intent Decode cycle, and there is no longer a scenario of an inconsistent Intent Decode/Baseline cycle as in the previous version.
- Intent Decode is completely decoded according to the period selected here, and there is no longer a minimum daily period limit.

### 4.13.2 Intent Decode Displaying Status

More intent decoding statuses are added:

Aborted at xxx: No Qualified Devices – A corresponding status label is added when the Intent Decode task ends due to no qualified devices. If the decoding result is 0 devices, "O Devices decoded..." is displayed next to the Recurring Decode field.

<ul> <li>Default</li> </ul>						
Application Check	All Network Intetns/Libra	ary Templat	e Recurring	L	ast Decode at 9:0	0pm 6/3/2022
BGP Check 1	All Common Intents/hon	ne Templat	e Manual	Α	Aborted at 9:00pm 6	
						-
Intent Name: BGP Che	ck 1					
Location: All Network	k Intents/home-network		Cloned NI			
Intent Mode: Template			ltem: 8 🛛 🔭			
Intent Decoding:	Decod	le Now	Cloned Intent	De	vices	Created At
Recurring Decode	0 Devices deco	ded	I HSRP Check 1			
Select		~	I HSRP Check 2			
			I HSRP Check 3			
	senne Periodicany		I HSRP Check 4			
<ul> <li>One-Time Decode</li> </ul>			I HSRP Check 5			
			I HSRP Check 6			

- Not Started: The Decode Task has not started.
- **Decode Now task scheduled at xxx:** The task is scheduled in the future.
- **50/180 devices processed... 24 devices matched:** The Decode Task is going, showing the total number of devices (180), the number of devices that were already decoded (**50**), and the number of matched devices (24).
- Last decoded at 06:50:30 PM 12/2/2022: The date and time that the task was done.

#### 4.13.3 Intent Decode Results Improvements

If the Intent Decode process succeeds the command test but fails the Critical Variable test, the result will still be stored to be used by Auto Intent. This scenario will result in a situation where a Command Test is successful, but Create NI is **NO** (due to a failure in the Critical Variable result). And when the user hovers over the **Create Intent**, it will display a prompt "**Command tested successfully with default macro variable value of Seed NI**".

Last Decode Task Run at 03/	20/2023 05:35:15 AM V	iew Decode Task Cre	ation Log			
Total Decoded Devices: 173 Filter:			No,All Trigger Sources,Auto In	~	Search	Q 😋 Refresh
Matched Device	Matched Seed Device	Matched Comma	✓ No		Decoded At	Baseline Data Updated A
US-BOS-SW5	CA-TOR-R1	Configuration	All Trigger Sources		0/2023 05:33:56 AM	03/20/2023 05:33:44 AM
US-NYC-R1	CA-TOR-R1	Configuration	Auto Intent Only		0/2023 05:33:56 AM	03/20/2023 05:33:45 AM
EIGRP-R10	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:43 AM
OSPFv3-R30	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:47 AM
OSPFv3-R14	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:45 AM
VXLAN-MGMT	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:45 AM
F5-SW2	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:45 AM
ASA@Switch	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:45 AM
BJ_Acc_Sw4-bbb-eee-ii-J	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:51 AM
OSPFv3-R16	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:46 AM
MPLS-CLOUD-R40	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:45 AM
JMPLS-R2	CA-TOR-R1	Configuration	All Trigger Sources	03/2	0/2023 05:33:56 AM	03/20/2023 05:33:45 AM 🖕

## 4.13.4 Show Decode Results for API Parser

When displaying the **results** of the API parser, the API names and the API parser may be the same but **correspond** to different parameters. If users hover the cursor over the matched command, the **Parameters** of the API parser are displayed.

.ast decoded Task a	t 07/22/2022 10:20:30 AM	Vlew Decode Task Creation	Log		
Total Decoded Devic	es: 3		🗌 Int	tent Creation Only	earch C
Matched Devices	Matched Seed Device	Matched Command	Create Intent	Last Decoded At	Baseline Data U
R1	Seed Device1	show ip route summary	Yes	07/21/2022 04:33:2	2 PM 07/22/2022 10:2
R1	Seed Device2	show ip route 10.10.10.1	Yes	07/21/2022 04:33:2	2 PM 07/22/2022 10:2
R2	Seed Device1	API Diagnosis 1	No	07/21/2022 04:33:2	2 PM 07/22/2022 10:2
		Parameters Interface: f0	: //1		

When users click on the API Parser in the Matched Command column, it pops up a window with the Baseline data:

耳 Intent Library			
Installed Intents	NetBrain Download Shared Intents		
Items: 3 + Add Inter	nt Filter: All 🗸 Search	۹	
<ul> <li>Intent Name</li> </ul>	show ip route 10.10.10.1 ×	×	Automat
▲ Group1		er result	
L1 Check	show ip route 10,10,10,1 V Execution Time: 10/3/2022, 7:16:58 API P	O Refresh	
L2 Check	Search 🗔 🔽 🔨 Match Whole Word	tod At	
- Default	1 "atheliutes", /	IO AM	
Application Check 1	a "adminst" "enabled",	IO AM	
bur check i	5 "cpuPct": "4", 6		
	7 "dn": "topology/pod-1/mode-1/sys/proc", 8 "attributes": {		
	9 10 "adminSt": "enabled", 11		
	12 "cpuPct": "4", 13 "dn"- "torpology/pod_1/pode_1/ges/proc".		
Intent Name: BGP Ch	14 un · copology/pours/mon-1/wyo/plot, 15		
Location: All Netwo	17 18		
Intent Mode: Template			Refresh
latest Decedias			ed Time
Intent Decoding:			
Recurring Decode			
One-Time Decode			
Intent Timer:			

## **5** Automation Bot

Automation Bot can be used to build an interactive, multi-step automation chatbot and execute multiple intent-based automations to solve real-world challenges without using NetBrain IE system UI. Using a chatbot doesn't require NetBrain know-how or any seat license and is a great way to provide self-service to a large audience.

Automation bot is considered a new event to launch automation in PDAS. The use cases of the Automation Bot:

- Use a Bot to deliver the dynamic map for specific IT objects, such as applications, data centers, sites, and device groups.
- Use a Bot to execute various diagnoses on a network by following a simple chat conversation.
- Use a Bot to prompt end users to interactively provide input devices and other related data to execute intent.
- Share important findings in the Bot with others for collaboration.

## 5.1 Use Chat Bot (End User)

The end user uses a web-based chatbot to complete the self-service automations. The chatbot can be opened within the NetBrain IE system or a bot URL from others sharing from the bot editor.



With a chatbot, users can:

- 1. Follow the conversation by clicking the button prompted by Bot to follow the conversation flow.
- Interactively select or input value for automation execution: depending on the automation flow defined by the power user, end users might provide the following input to trigger the network intent for diagnosis:
  - Single selection and Multiple selections. For example, select one device or select multiple devices for NIT replication.

• Power users can allow end users to input string directly in the drop-down box instead of selecting an existing item from the list.

	Berlin-R2	
		Q
	156 Items	
02:	3750SR12	
	aci-l30ut-246	
	aci-L3Out-249	
	aci-L3OUT-50.23	
	📨 ACI-QA-SW1	
	🐵 AS30000	
	🥬 Baraccuda-FW	
	😁 Berlin-R1	
	😢 Berlin-vEdge	
	BOS-N9K-L3OUT	

• Input text in the chat input box directly.

- 3. The chat input box at the bottom
  - Users can enter the text in the field instead of clicking the button.
  - Users can type"/" to show all built-in commands.

/logout	
/show flowchart	
/show incident link	
/restart	

4. Sessions: Every chat session will be saved automatically. Users can view previous sessions and start a new session at any time.

	Hello World Session 4 🗸		Ę	í
	+ New Session			
Welcome to NetBrain Automation Bot. I'll assist you	Session 4	get started, tell me what you'd li		
ke to check.	Session 1			
02:18 PM	Session 2			
NY_DC1 L2 General Check	Session 3			
Critical Application				
O2:18 PM				

5. Publish the current session with important findings to others for collaboration.

## 5.2 Chatbot Creation Flow

Power users can use Automation Bot Manager to build the bot conversation flow via just drag-and-dropping a node to the flow. The system provides the following types of nodes:

🔍 Autom	ation Bot Manager	
←	Routing Check /	න් 🌑 Enabled 🖉 Share Save
• 1	Design the flow with automation nodes and flow control nodes	★ ★ ②+ 100% □
Intent	▶ Start	2 Define automation input and output
Intent Template	BOP Check	Intent Template All Network Intent/Demo/Case 5/Route Summary Check Select
Automation Data Table	OSPF Route Change?     BGP Route Change?	Replicated Device Data Source
E -	× ,	Associate with system Lata: device
Condition	Vis Int OSIPF Nor Change?	Chat Preview OSPF Route Change?
	No Vis	Intent: Route Summary Check Dagnosed Scount, of Jill, devices devices, found Scount, of error_m     estages error messages on Scount, of error_devices devices.
	101 OSPF Config Change? 111 OSPFLSD8 Check 101 BGP Config Change?	No OSPF Route Change Detected. Go to [BGP Check].

#### 5.2.1 Intent (NI) Node

If power users do not want end users to interactively change devices for the intent during using this Bot, use the intent node.

For example, power users create a series of intents for **NY\_DC1** network daily checks and troubleshooting. The best way to enable end users to leverage this automation knowledge in their daily work is for power users to group these intents into a bot. Power users don't need end users to change the target devices defined in the intent. End users just need to chat with this Bot without accessing the NetBrain IE system and execute the pre-defined automation to ensure everything works as expected.



## 5.2.2 Intent Template (NIT) Node

When power users want end users to interactively change devices and other input data for the macro variables to replicate the intent for execution, use the Intent Template node. The Intent devices and macro variable value can be replaced by other devices and data for replication. During end user interactions with the Bot, it will guide the end user to interactively provide input devices and macro variable value for intent template replication.

For example, create a bot to guide end users to draw the multicasting tree of the source/group that end users interactively specify and execute multicasting diagnosis.



### 5.2.3 Automation Data Table (ADT) Node

ADT provides a flexible way to organize and extend the critical network assets and their associated intent and map. Two typical use cases can be achieved by ADT node:

- Use the ADT node to deliver a map.
- Use the ADT node to dynamically search matched critical assets and execute its associated intent automation.

For example, create a bot to deliver a critical application path map to bot end users.



#### 5.2.4 Condition Node to Control Flow

A completed conversation flow usually consists of multiple steps. Power users can connect multiple automation steps with conditions to decide the next flow to send users in an automation flow based on the previous diagnosis result. For example, if a previous diagnosis detects an error, go to flow1; if there is no error, go to flow2. No condition is also available to connect automations without any condition, and the system will execute multiple intents individually.

For example, use condition node to control: if OSPF errors are detected after a Routing Check, then go to OSPF detailed check branch; if BGP errors are detected, then go to BGP detailed check branch; if no error is detected, then go to critical application check.



## 5.2.5 Selection Node

Power users can leverage the selection node to organize bot conversation flow by grouping automations. Just double-click the node to rename it. No additional settings are needed.



## **5.3 Additional Features**

The system provides the following functions to help users manage the bots:

- 1. Lock/Unlock a bot with/without a password to avoid unauthorized modification.
- 2. Enable/Disable a bot.

3. Share the Bot and control which user roles can access this Bot, and whether to allow the session feature and show flowchart command in the end user chat console interface.

Share Bot		×
Copy link to share		
http://192.168.31.46/bot/100016	Сору	
Manage user access by roles		
Domain Admin		
Engineer		
Network Change Approver		
Network Change Creator		
Network Change Executor		
Portal Temp User		
Allow users to manage and publish sessions Allow users to view bot flowchart		)
Allow users to view bot flowchart	0	

4. Customize Bot Login Page Logo, Content, and About Bot Content for different purposes.

# 6 Report and Dashboard

NetBrain system lacks a function to view the results across the whole network in the early versions. R11.1 adds the Report and Dashboard with two capabilities:

- Organize, analyze, and share data from different NetBrain automation assets, such as thousands of ADT Intent results.
- Provide a visual display of multiple automation results from PDAs on a single GUI.

The picture below illustrates an example that uses Report and Dashboard to analyze Intent results and visually display the data to help monitor a network's failover designs.

Network Intent (View Mode) - Shared Network	Intent Clusters/WZ/ACL_enforcement/ACL_enforcer	ment_BOS	Application Path Historical Verifica	tion Report 🕚			
ACL_enforcement_BOS			Report Input: Path Name: 3 Applicat	tions, 0 Path + 1 additional inp	iuts		
Result: 03/25/2023 03:15 PM V	Embedded Incident 🗸 👗 🎝	•	Date: All 🗸				
Intent Type: Member Intent This intent execution is finished at 03/25/202	3 03:15 PM with 14 errors. You can View Execution	n Log	Pivot Table				
805			Verification Date Path Result Failed Succ	ceeded			
2 Devices 1 Diagnosis     Automation Tag     S US-BOS-R2: W0 Diagnoses tech.co	S) The acl 101 match with the failover device US-BC m	JS-R2 14	2023-03-23 5 2023-03-24 1	2 2			
Last Modified: 03/23/2023 04:57 PM     Configuration Diagnosis	0 Diagno	ises					
363 pccess-list 1 permit 10.0.1.4 364 access-list 1 permit 10.0.1.2 365 access-list 1 permit 10.0.1.2 366 access-list 1 permit 10.0.3.2 367 access-list 100 permit 0.0.3.2 368 access-list 100 permit 0.0 permit 0.0 368 access-list 100 permit 0.0 permit 0.0 370 access-list 100 permit 0.0 permit 0.0 371 access-list 100 permit 0.0 permit 0.0 372 access-list 100 permit 0.0 permit 0.0 373 access-list 100 permit 0.0 permit 0.0 374 access-list 100 permit 0.0 permit 0.0 374 access-list 100 permit 0.0 permit 0.0 permit 0.0 374 access-list 100 permit 0.0 375 access-list 100 permit 0.0 375 access-list 100 permit 0.0 375 access-list 100 permit 0.0 375 access-list 0.0 3	6 00 01 01.0.1.26 any 10.0.3.30 0.0.0.255 eq 5201 10.0.3.10 0.0.0.255 eq 5405 host 10.1.1.1 eq telnet y nog ti 102 established	Intent R	esults to Report				
372 access-list 192 permit tcp an 373 access-list 193 permit tcp an	y any eq www y any eq smtp		Report Table				
374 access-list 194 permit tcp an 375 access-list 195 permit udp an	y any eq pop3 y any eq domain		Application Name	Path Name		Verified Time	
376 access-list 195 permit udp an 377 access-list 195 permit tcp an	y eq domain any y any eq domain		Voice	Voice Path		3/23/2023, 2:46:37 PM	
378 access-list 195 permit tcp an	y eq domain any		Webex	Webex Path		3/23/2023, 2:51:26 PM	
			Webex	Webex Path		3/23/2023, 2:54:04 PM	
Monitor Failover Design Description:		Re Re	port to Dashboard			🖌 Edit	aç
Failover Devices with Problems	3/25/2023, 3:34:09 PM View Report	The Result of Application Ve	rification		3/	/25/2023, 3:34:09 PM Vie	ew Report
1	2	Last Verified Time: All ~		Failed Succeeded			
	4	2		2023-03-24			
Policy Config Checking Results	3/25/2023, 3:34:05 PM View Report	ACL Config Checking Results	3/25/2023, 3:34:05 PM View	w Report BGP Config	Checking Results 3/	/25/2023, 3:34:05 PM Vie	ew Report
Date: All ~		Date: All 🗸		Date: All ~			
Sum of Intent Alert Status Code	Total Alerts	Sum of Intent Alert Status Cod	e	Sum of Ir	ntent Alert Status Code	Total Alerts	
Sum of Intent Success Status C	21 Alerts	Sum of Intent Success Status (	21 Aler	rts + Sum of Ir 20 10 0	nent Success Status C	28 Ale	erts

Besides the example mentioned above, other common use cases for the Report and Dashboard:

- Capture the Configuration Drifts for Outage Prevention
- Capture transient problems for Diagnosis Automation
- Perform Security Assessment for Network Security
- Display the result of Change Management Tasks for Protective Change
- Display the application information for Application Performance

## 6.1 Key Components to View Report and Dashboard

## 6.1.1 Key Components to View Report

🚺 Report Manager	😢 Report Info Bar 🛛 🌔	3 Report Input	Report Filter 🛛  6	Pivot Table ( 6 Report	🕜 Drill-down Actions
🔒 Report Manager	<u>۱</u> آ (	T 1	· •	<b>†</b>	<b></b>
Type to search Q S «	Application Path Historical Verification Rep	oprt 📵		Last Updated on: 3/21/2023, 10:57:19 PM	tun Edit
Sharek Réports (24)     Gamee Réports (24)     Application Path Historical Wontoring Report     Application Path Historical Wontoring Report     Application Path Historical Wontoring Report     Application Path List Wontoring Report     Application Path List Wontoring Report     Application Path List Want Z days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface CRC Error In Last 7 days Report     Check Interface Childron Security Assessment (4)     Route Leaking Check In This Week     SMMPG Enabled Check In This Week	Report Input:         Path Name: 3 Applications: 0 P.           Date: All ✓         Pivot Table           Privot Table         2023-03-23           2023-03-23         S	ah ] [+1 additional inputs ]			
<ul> <li>Unencrypt Username Check in This Week</li> <li>Outage Prevention - Failover Failure (8)</li> </ul>	Report Table	Varified Time	Dath Result	Application Name	5 C
Check ACL Configuration	Path Name	Verified Time	Path Result	Application Name	
Citica Bor Comg Citica Policy Config Critical Application Report	Webex Path Webex Path	3/23/2023, 2:51:26 PM 3/23/2023, 2:51:26 PM 3/23/2023, 2:54:04 PM	Failed Succeeded	Webex Webex	
Critical Succeed Application Report  Tritical Succeed Application Report  Tritical Succeed Application  For Succeed Application  Succeed Application  Comparison  Succeed Application  Succeed Applic	Web Path Web Path	3/23/2023, 3:42:43 PM 3/23/2023, 3:50:43 PM	Failed	Webex Web	
MITEST	Web Path Web Path Voice Path	3/23/2023, 4:59:05 PM 3/24/2023, 10:15:23 AM 3/24/2023, 10:25:32 AM	Failed Failed Succeeded	Web Web Voice	
					· · ·

The GUI of the View Report page consists of seven key components:

- 1. **Report Manager**: Lists all the accessible reports in the domain. From the Report Manager, users can choose a report for viewing, editing, or renaming; or create new folders and reports.
- 2. **Report Info Bar**: Display the basic information of the report, such as the title and last update time. You can mouse over the info icon to view more information, including the report's creator, last modified by and last modified time. It also provides the option to edit or run the Report.
- 3. **Report Input**: Display the Report Input and the criteria to select and generate the report data.
- 4. **Report Filter**: Filters used to refine the report data or narrow it down to subsets of report data.
- 5. **Pivot Table**: Display the Pivot Table, which helps analyze and summarize information from a large amount of Report data.
- 6. **Report:** Display the content of the report.

7. **Drill-down Actions:** Hyperlinks in report columns that are linked to other NetBrain features for users to drill down to underlying data.



#### 6.1.2 Key Components to View Dashboard

The graphic user interface of the View Dashboard page consists of four key components:

- 1. **Dashboard Info Bar**: Displays the basic information of the Dashboard, such as title and description. It also provides the option to edit, share or update the Dashboard.
- 2. **Dashboard Pane:** Major components of the Dashboard that display report data in various charts.
- 3. Drill-down Actions: Hyperlinks in report columns linked to other NetBrain features.
- 4. **View Report**: Display the report data used for the Dashboard Pane in a pop-out window.

## 6.2 Key Components to Create the Report and Dashboard

The user flow to create the Report and Dashboard:



## 6.2.1 Key Components to Create a Report

1 Rep	ort Property 3	Repor Repor Drill-d	t Settings: t Columns and own Action	Pivot Tabl	e Settings	2 Report Input						
	BGP Config Checking for WAN Link Description							Report Filter (1)		Cancel	Save	Save and Run
	Edit Report Properties            SearchQ.         D. Refresh            Coutomized Reid         + Add            Searche Bete         + Add            Metwork Insert         -	Report Inter	put: A AND B 🗶 Name (default) Column: BGP Config Ch	B Execution Time From 2023-01-01	X to 2023-12-31	Drag and drop fields here						Apply
	Intent Name Intent Type	Pivot Ta	e Settings	Previewing	a limited number of	records. Run the report to see a	Il records.					
Report Field Tree		Rows S D Columns Values # S Sho	cure Date × brag and drop fields here brag and drop fields here in thrant Alert Status Co m Intern Alert Status Co m Intern Status Status × Co	Prive Table Execute Date 2023-03-14 2023-03-15	Sum of Intent Alert S	tatus Code Count Sum of Inten 7 13	Totais t Success Sterus Code Count 7					
	# Intent Success Status Code Count S Intent Status Code Summary	Report S Columns	ettings	Report Intent Name	1	Execution Time	Intent Status Code Summary	Intent Alert Status	ode Count Inten	t Success Status Co	de Count Total A	lert Count
			tent Name 📑 😒 🖂	BGP Config	Check for NYC Edg	3/15/2023, 11:18:55 PM	US-NYC-R1 BGP Config Not Cha	0	1		0	-
		() E	ecution Time 🛛 🕒 🗙	BGP Config (	Check for NYC Edg	3/15/2023, 11:18:11 PM	JMPLS-R1 BGP Config Not Chan	- 0	1		0	
0		SIn	tent Status Code Su 🕒 🗙	BGP Config 0	Check for NYC Edg	3/15/2023, 9:00:22 PM	JMPLS-R1 BGP Config Not Chan	- 0	1		0	
Report —		# In	tent Alert Status Cod 🥵 🖂	BGP Config 0	Check for NYC Edg	3/15/2023, 5:04:10 PM	JMPLS-R1 BGP Config Not Chan	- 0	1		0	
		# In	tent Success Status C 🕓 🖂	BGP Config (	Check for NYC Edg	3/15/2023, 4:21:42 PM	BGP Config Not Change	0	0		0	
		# Te	tal Alert Count 🛛 🕒 🗙	BGP Config 0	Check for NYC Edg	3/15/2023, 4:20:58 PM	BGP Config Not Change	0	0		0	
			Drag and drop fields here	BGP Config 0	Check for NYC Edg	3/15/2023, 2:16:48 PM	BGP Config Not Change	0	0		0	
				BGP Config 0	Check for NYC Edg	3/15/2023, 2:16:37 PM	US-NYC-R1 BGP Config Change	d 1	0		2	
				BGP Config 0	Lneck for Toronto	ar 15r2u23, 11:19:06 PM	CA-TUR-RT BGP Config Changer	1	0		Z	-

The GUI of the Report editor consists of 3 major areas and 4 basic settings. You can define a basic report by defining the following four settings:

- 1. **Report Property:** Define the basic properties of a report, including report name, creation method and Report Field Tree. Report Objects and Report Fields define the Report Field Tree.
  - **Report Object**: Report Objects are analogous to database tables that organize NetBrain data by categories, such as Device Property, Change Management, and Intent Property.

- Report Field: Report Fields are analogous to columns in database tables. Each Report Object has multiple Report Fields. For example, the Intent Property Object has Report Fields such as Intent name, creation time, Intent type, etc.
- 2. **Report Input:** Define the Report rows with filtering criteria. Each report has one built-in default input that can be edited but not deleted; additional report inputs can be added by drag-and-dropping Report Fields to the Report Input area. The logical relationships between each input can also be defined.
- 3. **Report Settings:** Define the Report Columns and Drill-down Actions.
  - Report Columns: Define the Report Columns by drag-and-drop available Report Fields from Report
     Field Tree to the Report Column area.
  - **Drill-down Actions**: Define user interactions with the Report, such as opening the Device detail pane or the Network Change Manager. Those interactions will appear as hyperlinks in the Report columns for viewers to click.
- 4. **Pivot Table Settings:** Define the Rows, Columns and Values of the Pivot Table.

These four settings help to define the three major areas on the Report Editor page:

- **Report Field Tree**: Report Field Tree lists all the available fields that can be used in the Report, including Customized Fields defined by users and built-in Report Fields defined by Report Property.
- **Pivot Table**: Pivot Table helps aggregate the report data by selecting Report Fields to help analyze and summarize information from the Report. It can also be used in Dashboard to create charts.
- **Report:** The report area displays limited sample data of the report. The Report rows are defined by Report Input, and the Report columns are defined by Report Columns.

Besides the four basic settings mentioned above, the following advanced settings are offered as an extension to the basic Report functionality:

1 Customized Field				(2) R	eport Filter 🗿 Au	ito-update	
BGP Config Checking for WAN Link Description:				1	teport Filter (1) Auto-u	pdate Cancel Save	Save and Run
Kitt Report Properties      Kertch.     Cli Customized Reid     + Add     Execute Date     Hearter Heart	Report Input: AAND B Z A Intent Name (servult) Intent Column: BGP Config Ch	Execution Time X From 2023-01-01 to 2023-12-31	Drag and drop fields here				Apply
I Intent Name	Pivot Table Settings	Previewing a limited number	of records. Run the report to see a	l records.			
Intent Type Intent Map	Rows	Pivot Table					::
S Intent Tags	S Execute Date ×			Totals			
S Creator Creation Time	Drag and drop fields here	Execute Date Sum of Intent Alert	Status Code Count Sum of Inten	Success Status Code Count			
5 Modifier	Columns	2023-03-15	13	7			
Modify Time     Motify Time     Motion Result (Intent Name)     Summany	Drag and drop fields here						
I Intent Name	Values + Add						
Execution Time     # Total Alert Count	# Sum: Intent Alert Status Co $ imes$						
Source	# Sum: Intent Success Status $ imes$						
# Intent Status Code Count # Intent Alert Status Code Count	show: Grand Total Subtotal						
# Intent Success Status Code Count	Report Settings	Report					8
5 Intent Status Code Summary	Columns	Intent Name	Execution Time	Intent Status Code Summary	Intent Alert Status Code Count	Intent Success Status Code Count	Total Alert Count
	🚺 Intent Name 🛛 😫 🖂	BGP Config Check for NYC Edg	3/15/2023, 11:18:55 PM	US-NYC-R1 BGP Config Not Cha	- 0	1	0
	€ Execution Time	BGP Config Check for NYC Edg	3/15/2023, 11:18:11 PM	JMPLS-R1 BGP Config Not Chan	- 0	1	0
	S Intent Status Code Su 🕒 🗙	BGP Config Check for NYC Edg	3/15/2023, 9:00:22 PM	JMPLS-R1 BGP Config Not Chan	- 0	1	0
	# Intent Alert Status Cod 喀 🛛	BGP Config Check for NYC Edg	3/15/2023, 5:04:10 PM	JMPLS-R1 BGP Config Not Chan	- 0	1	0
	# Intent Success Status C 🕞 🔀	BGP Config Check for NYC Edg	3/15/2023, 4:21:42 PM	BGP Config Not Change	0	0	0
	# Total Alert Count 🛛 🕓 🖂	BGP Config Check for NYC Edg	3/15/2023, 4:20:58 PM	BGP Config Not Change	0	0	0
	Drag and drop fields here	BGP Config Check for NYC Edg	3/15/2023, 2:16:48 PM	BGP Config Not Change	0	0	0
		BGP Config Check for NYC Edg	3/15/2023, 2:16:37 PM	US-NYC-R1 BGP Config Changed	E 1	0	2
		BGP Config Check for Toronto	3/15/2023, 11:19:06 PM	CA-TOR-R1 BGP Config Changed	1	0	2

- **Customized Field:** Define customized fields besides built-in Report Fields using calculations, functions, and conditions.
- **Report Filter:** Define filters for users to drill down data when viewing a Report or Dashboard.
- **Auto-update:** Besides running Report manually, users can update the Report data automatically on the specified frequency.



## 6.2.2 Key Components to Create a Dashboard

The GUI of the Report editor consists of 2 major areas: Report Tree and Dashboard Pane.

- **Report Tree**: Lists all the available reports that can be used in the Dashboard. Drag and drop a report to the pane area on the right to add a Dashboard pane.
- **Dashboard Pane**: A Dashboard pane is defined by the data source and chart settings. Each pane can have a different report from Report Tree as its data source. Also, different chart types are provided to satisfy different use case scenarios, such as Line Charts, Gauge charts, Pie charts, etc. Besides the chart, each pane could have an optional call-out chart to help provide extra information.

## 6.3 Create Report

The report organizes data from different automation assets into reports, such as device, intent, application, change management, and site. Besides that, the Pivot Table feature in Report can help further analyze and summarize the report data.

### 6.3.1 Define Report Properties

When creating a new Report from Report Manager, the Report Properties window will automatically pop out, then you can follow the steps on GUI to define the Report Properties. There are three steps to define the Report Properties:

- **Basic Settings**: The name and description of the Report.
- **Report Properties**: Select the Primary Object, Related Object and their relationships.
  - Report Object: Report Objects are analogous to database tables that organize NetBrain data by categories, such as Device Property, Change Management, and Intent Property. Each report must select one Primary Report Object and can also have up to three Related Report Objects.
  - **Primary Object**: Primary Object defines the main subject of the report. Each report must have and can only have one Primary Object.
  - Related Object: Related Objects can supplement the main subject's information. Other Report
     Objects can be added to Report as Related Objects via a lookup relationship.
- **Report Fields**: Preview the Report Fields of the Report and add Related Fields if necessary.

#### 6.3.1.1 Report Object

Report Objects are analogous to database tables that organize NetBrain data by categories. The Report Object includes multiple Report Fields that can be used as Report Columns to build report content. In R11.1, the system provides Report Objects for device, intent, application, change management and site. We will continue to provide more report objects in the future release. As illustrated in the picture below, the blue box represents a Report Object, such as Network Intent, which contains multiple Report Fields such as **Intent Name, Intent Type, Intent Map**, etc. The Report Fields will be listed in Report Field Tree for use in the Report.



Report Objects are mainly used in Report Properties to help define the basic data structure of a report. Users must select one Primary Object and can add up to three Related Objects for the report.

Report Properties - Edit Report	×
1 Define Basic Settings	~
2 Define Report Objects	^
Primary Object defines the main subject of the report. You can add other related report objects via lookup relationship.	
Primary Object:       Network Intent Result ~         Application Path       Image: Application Path Historical Result         Application Path Intent Result       Image: Application Path Last Result         Change Management Implemented Device       Image: Application Path Intent Result	
< Previous Next >	
3 Define Report Fields	~
Cancel Sa	ave

Each report must have and can only have one **Primary Object**. The major purpose of the report should determine Primary Objects. For example, for a report of Intent Results, Report Object **Network Intent Result** should be selected as Primary Object. After the Primary Object is selected, the Report Fields under the Report Object will be listed in Report Field Tree for use in the Report.

Report Properties - Edit Report		×
1 Define Basic Settings	~	
2 Define Report Objects	^	
Primary Object defines the main subject of the report. You can add other related report objects via lookup relationship.		
Primary Object: Network Intent Result ~		∠ Edit Report Properties
+ Add Related Object		Customized Field + Ac
		Network Intent Result     Summary     Intent Name     Secution Time     # Total Alert Count     Source     # Intent Status Code Count     # Intent Status Code Count     # Intent Status Code Count     \$ Intent Status Code Count     \$ Intent Status Code Summary
< Previous	Next >	
3 Define Report Fields	~	
	Cancel Save	

#### 6.3.1.2 Lookup Relationships between Report Objects

In the database, the Report Objects are related via **Lookup Relationships**. Through the lookup relationship, different Report Objects are related via key Report Fields so that multiple Report Objects can be used in the same report.

The diagram below illustrates an example of the Report Objects and their relationships. The Network Object B (*Network Intent Result*) lookup to A (*Network Intent*) via Report Field *Intent Name*, and A (*Network Intent Result*) can be considered as the Parent Object to B (*Network Intent*). Similarly, Report Object C (*Network Intent Device Result*) lookup to B (*Network Intent Result*) via Report Field *Intent Name*. The B (*Network Intent Result*) can be considered as the Parent Object to C (*Network Intent Result*).

Please note that this lookup relationship is one-way, so it makes a difference when adding related objects and related fields in Report Property.



#### 6.3.1.3 Define Complex Report Using Multiple Report Objects

For Reports that require complex data structures, users can have multiple Report Objects in a Report by adding Related Report Objects via a lookup relationship. Also, users can add up to three Related Fields to provide additional context to the Report. And the Primary Object should be the Report Object that occupies the highest level in the hierarchy of the Report Object relationship.

Report Properties - Edit Report	×
1 Define Basic Settings	~
2 Define Report Objects	^
Primary Object defines the main subject of the report. You can add other related report objects via lookup relationship. Parent Object	
Primary Object: Network Intent	
Related Object: Network Intent Result (Intent Name) ~   A to B Relationship: <ul> <li>Each "A" record must have at least one related "B" record.</li> <li>"A" records may or may not have related "B" records.</li> </ul> Child Object Child Object	
< Previous Next >	
3 Define Report Fields	~
Cancel Sa	ave

For example, to build a report that includes **Intent type**, **Intent results**, and **Intent device results** as report columns, use three Report Objects: **Network Intent**, **Network Intent Result** and **Network Intent Device Result**. Report Object A (*Network Intent*), which occupies the highest level in the lookup relationship, is selected as Primary Object, then Report Object B (*Network Intent Result*) is added as a Related Object, and Report Object C (*Network Intent Device Result*) is added last.

Define Rep	ort Objects	
rimary Object	t defines the main subject of the report. You can add other related report objects via lookup relationship.	
A		
Primary (	Object: Network Intent	
B	alsted Object: Network Intent Result (Intent Name)	
	A to B Relationship:	
	Each "A" record must have at least one related "B" record.	
	"A" records may or may not have related "B" records.	
L		
(	C	
	Related Object: Network Intent Device Result (Intent Result Su 🗸 🐣	
	B to C Relationship:	
	Each "B" record must have at least one related "C" record.	
	<ul> <li>"B" records may or may not have related "C" records.</li> </ul>	
	···· No Related Object Can be Added	
	< Pre	vious Next >

The Selected Report Object and the report fields under them will help form the barebone of the Report Field Tree, which specifies the basic data structure of the report. The picture below illustrates the relationship between the Report Object definition in Report Property and the Report Field Tree formed accordingly.



#### 6.3.1.4 Define Report Fields

All Report Fields of the selected Report Objects are listed to provide a preview of the Report Field Tree. Besides these Report Fields, users can also add Related Fields to help provide additional information to the report.

To add Related Fields, select the Report Object. The drop-down list will list all the Parent Objects of Report Object A.

Report Properties - Edit Report	×			Sure and han
Define Basic Settings	~			^
Define Report Objects				
	_			Apply
3 Define Report Fields	^			
25 Fields Define the fields to be used in the report.				к л К 3
Source	• U	IS-BOS-R2	US-BOS-SW1	US-BOS-SW2
# Intent Status Code Count	Add Relate	ed Fields	Parent Obj	ect ×
# Intent Alert Status Code Count	Report	Object. Dev	ice (Device Name)	~
# Intent Success Status Code Count Lookup Relationship	Related	Fields:		
5 Intent Status Code SummarChild Object	neidee o		Management IP Management Interface	
C Network Intent Device Result (Intent Result Summary) (8)     + Add Related Fields			S Vendor	
S Intent Result Summary			S Model	
I Intent Name			<ul> <li>Sub Type</li> </ul>	
() Execution Time			Software Version	
Sevice Name			Site Name	
# Device Status Code Count			S Location	
H Device Alert Status Code Count			S Contact	
# Device Success Status Code Count			System Memory Size	-
S Device Status Code Summary			(	Cancel Save
< Previous Next >			1	
			1	
Cancel	ve		1	Ţ

## 6.3.2 Define Report Input

Report Input defines the report rows with filtering criteria. It selects the data in the NetBrain database, and only records meeting the criteria specified in Report Input are included in the report. Each report has one built-in default input and can have multiple additional report inputs.

Intent Name (default) All Intents Intent Name		Drag and drop	p fields here
Scope:	All Intents All Intents Specific Inter Specific Inter	ıt It within ADT	~

Default Input is included in the report by default and cannot be deleted. It helps provide first-level filtering to narrow down the data scope. The default input is usually related to the Primary Object of the report. For example, if the Primary Object of the report is Network Intent, then the default input is Intent Name, allowing you to select the desired Intent by name or by ADT.



Besides default input, you can add multiple additional inputs by drag-and-drop Report Fields from the Report Field Tree to Report Input. For example, to filter the report content by execution time, you can drag and drop *execution time* to Report Input and set the time range as *This Month*.



The relationship between Report Inputs can be managed by clicking the edit icon beside the logical expression. Please note that the default input will always have an 'AND' relationship with the other additional inputs.

### 6.3.3 Define Report Columns

By drag-and-drop report fields from the Report Tree to Report Columns, users can define the report's columns. Users can also adjust the column orders by moving the report fields up and down in the Report Columns.



Besides built-in report fields, users can define customized fields using formulas and use them in the report. There are two ways to define a customized field: **Calculated Field** and **Conditional Field**.

### 6.3.3.1 Calculated Field

Calculated Field allows you to define a customized field using functions and mathematical and logical operators. To define the formula, select the available functions and fields from the tree on the left side and insert them into the formula. All the report fields in the Report Field Tree can be used except for other customized fields.

Besides the standard mathematical formula and logical operators, the following functions are supported for this release:

Function Name	Example	Description
ToString	<i>string</i> <b>ToString</b> ( <i>number</i> or <i>datetime</i> or <i>boolean</i> \$input)	Converts a number, a datetime or a boolean to string format.
Duration	number Duration (datetime \$startDate, datetime \$endDate, string \$unit)	Calculate the time difference between the start date and the end date. The output is calculated by the unit and given in number format. Supported unit includes week, day, hour and minute.
Year	<i>number</i> <b>Year</b> ( <i>datetime</i> \$date)	Subtract the year from a date

Month	<i>number</i> <b>Month</b> ( <i>datetime</i> \$date)	Subtract the month from a date, a number between 1(January) and 12(December)
Day	number <b>Day</b> (datetime \$date)	Subtract the day from a date, a number between 1 and 31
Hour	<i>number</i> <b>Hour</b> ( <i>datetime</i> \$date)	Subtract the hour from a date, a number between 0 and 23
WeekofYear	<i>number</i> <b>WeekofYear</b> ( <i>datetime</i> \$date)	Subtract the week from a date, a number between 0 and 53
Now	datetime <b>Now</b> ()	Returns the current time in datetime format
Ceil	<i>number</i> <b>Ceil</b> ( <i>number</i> \$input)	Returns the smallest integer that is greater or equal to the given number.
Floor	<i>number</i> <b>Floor</b> ( <i>number</i> \$input)	Returns the largest integer that is smaller or equal to the given number.
IF	number or string or datetime <b>IF</b> ( <i>logical expression</i> \$expression, \$value_if_true, \$value_if_false)	First verifies if an expression is true or false, then returns a given value based on the verification result. The data type of variable \$value_if_true and \$value_if_false should be the same.

#### 6.3.3.2 Conditional Field

Unlike Calculated Field, which is based on user-defined formulas, Conditional Field provides quick and easy-touse UI-based conditions for the most common customized fields. For the Conditional Field, the report field can only be of data type **'number'**, **'picklist' and 'DataTime'**.

#### 6.3.4 Pivot Table

A **pivot table** is a data summarization and analysis tool that organizes, summarizes, and analyzes data from a report. In a Pivot Table, data is organized into rows and columns, and users can reorganize the data to look at different aspects of it, enabling users to identify trends and patterns in the data and perform various calculations and comparisons.

There are two primary purposes for the Pivot table:

- To analyze large amounts of data in a Report by summarizing it into a more manageable and meaningful format.
- To assist in defining the Dashboard by providing the data needed for Dashboard charts.

In the report editor page, drag-and-drop fields from Report Field Tree to Pivot Table Settings to define the Rows and Columns of Pivot Table. Then click **+Add** to define the values of the Pivot Table.

ក្កភ មុន OSPF Config Checking for WAN Link	Description:					Report Filter (1)		Cancel Save	Save and Run
Z Edit Report Properties	« C Refresh	Report Input: Intent Na	Intent Colum	an: OSPF Config C + 1 additional input	s				~
Customized Field	+ Add	Pivot Table Settings		Previewing a limited number of rec	ords. Run the report to see all reco	rds.			
S Execute Date  It is in the internet  It is internet Name  It is internet Name		Rows		Pivot Table					
		E Everyte Date				Totals			
		Drag and drop fields he		Execute Date Sum of Intent Alert Statu	s Code Count Sum of Intent Succ	ess Status Code Count			
Intent Type			ias nere	2023-03-14	2				
S Intent Tags		Columns		2023-03-15	4	3			
S Creator	Drag-and-drop	Drag and drag Falds have		2023-03-21		3			
( Creation Time		brag and drop ne	ius nere						
S Modifier		Values	+ Add						
( Modify Time		H Curry January Marso Co							
Network Intent Result (Intent Name)		# Sum: Intent Alert Su	stus co ×						
S Summary		# Sum: Intent Success	Status X						
Execution Time		show: 🗌 Grand Total	Subtotal						
# Total Alert Count	1 11	Report Settings		_					
<ul> <li>Source</li> </ul>		Columns							
# Intent Status Code Count				Report					0
# Intern Alert Sastus Code Court # Intern Stoces Satus Code Court E Intern Status Code Summary		1 Intent Name	喀 🖂	Intent Name	Execution Time	Intent Status Code Summary	Intent Alert Status Code	Count Intent Suc	cess Status Code Count
		Execution Time	🕓 🖂	OSPE Config Check for NYC Edge	3/21/2023, 10:22:32 AM	US-NYC-R1 OSPF Config Not Change	0	1	
		S Intent Status Code S	iu 👒 🖂	OSPF Config Check for NYC Edge	3/15/2023, 5:06:46 PM	US-NYC-R1 OSPF Config Not Change	0	1	
		# Intent Alert Status C	lod_ 🕓 🖂	OSPF Config Check for NYC Edge	3/15/2023, 2:50:17 PM	OSPF Config Not Change	0	0	
		# Intent Success Status C ▷ × Drag and drop fields here	is C 🏊 🖂	OSPF Config Check for Toronto Edg	e 3/21/2023, 10:22:41 AM	CA-TOR-R1 OSPF Config Not Change	0	1	
			lds here	OSPF Config Check for Toronto Edg	e 3/15/2023, 5:07:22 PM	CA-TOR-R1 OSPF Config Not Change	0	1	
				OSPF Config Check for Toronto Edg	e 3/15/2023, 2:42:43 PM	OSPF Config Not Change	0	0	
				OSPF Config Check for Boston Edge	3/21/2023, 10:22:12 AM	US-BOS-R1 OSPF Config Not Change	• 0	1	
				OSPF Config Check for Boston Edge	3/15/2023, 5:06:15 PM	US-BOS-R1 OSPF Config Not Change	0	1	
				OSPF Config Check for Boston Edge	3/15/2023, 5:05:45 PM	US-BOS-R2 OSPF Config Changed	2	0	
				OSPF Config Check for Boston Edge	3/15/2023, 2:14:29 PM	US-BOS-R2 OSPF Config Changed	2	0	
				OSPE Config Check for Boston Edge	3/14/2023. 10:36:20 PM	US-BOS-R1 OSPF Config Changed	1	0	*
#### 6.3.4.1 Pivot Table Rows

The rows in Pivot Table represent the categories by which the data is grouped and summarized. Any available fields in the Report Field Tree can be used as Pivot Table rows. As illustrated in the picture below, the Rows for Pivot Table will become the first column in Pivot Table.



A Pivot Table can have multiple grouping by rows. It provides a multi-layer of data grouping and can be used to drill down into more details. Each Pivot Table can have up to four groupings by Rows or columns. When there are multiple rows in a Pivot Table, the data is grouped hierarchically based on the order of rows. Each row represents a grouping level, with the first row being the highest level and the last row being the lowest level. As the picture below illustrates, the Pivot Table will group the data first by Creator, then by CreateDate. Each Row will represent a grouping level, with the Creator row being the highest level and the CreateDate Row being the lowest.



#### 6.3.4.2 Pivot Table Columns

Like Pivot Table Rows, the Column in Pivot Table also allows you to group data by certain report fields. Pivot Table Columns provide another way to aggregate data and help you identify important trends that may not be obvious when viewing data by rows. The Pivot Table will create a new column for each unique value in the selected report fields when grouping by columns. The Pivot Table will then display the summary data for each column.

Pivot Table Settings	😔 Previewing a limit	he report to see all records.						
Rows	Pivot Table							
Intent Name	Intent Name	execution date	2023-03-23	2023-03-24				
	AUL_Er	nforcement	4	0				
Drag and drop fields here	ACL_enfo	2	0					
Columns	ACL_enfo	2	0					
Sexecution date X	Add 1	1	0					
	BGP_Conf	iguration_BOS	4	0				
Drag and drop neids here	BGP_Cont	4	0					
Values + Add	Call C	)арр Сору	0	4				
# Count: Device Alert Status C ×	Fake - Slow Application	n Interface CRC Error Check	0	7				
	Fake - Slow Applicati	on Interface Usage Check	0	14				
snow:Grand TotalSubtotal	Fake_BGP_C	onfiguration_BOS	4	0				

Like Pivot Table Rows, a Pivot Table can have multiple groupings by columns. Each Pivot Table can have up to four groupings by Rows or columns. When there are multiple columns in a Pivot Table, the data is grouped hierarchically based on the order of columns. As illustrated in the picture below, the Pivot Table will group the data by execution date, then by Site Name.

Pivot Table Settings		Previewing a limited number of records. Run the report to see all records.								
Rows		Pivot Table								
	executi	on date		2023-03-2	23		2023-	03-24		
Drag and drop fields here		Sit	e Name	CXL-Lab	Multicast-Lab	NIC-Demo2-Lab	null	CXL-Lab	Multicast-Lab	
			Totals	106	4	22	4	317	2	
Sexecution date	× ×									
Values	+ Add									
# Count: Device Alert Status C	×									
show: 🗌 Grand Total 🗌 Subto	tal									

#### 6.3.4.3 Pivot Table Values

In Pivot Table, the Values are the numerical data being summarized and displayed. When defining values for Pivot Table, you can choose one or more report columns to use as Values. Then you can also specify the calculation method for the Values, such as **sum, average, minimum, count**, etc. The available calculation method varies depending on the data type of the Report Field selected.

These Values are displayed in the body of the Pivot Table, with Rows and Columns defining the categories or dimensions you want to analyze.

Pivot Table Settings	Previewing	Previewing a limited number of records. Run the report to see all records.						
Rows	Pivot Table							
Sevecution date V			Totals					
	execution date	Count of Device Alert Status Code Count	Count of Device Success Status Code Count					
Drag and drop fields here	2023-03-23	132	132					
Columns	2023-03-24	348	348					
Drag and drop fields here								
Values + A	dd							
# Count: Device Alert Status C $ imes$								
# Count: Device Success Stat $\times$								
show: 🗌 Grand Total 🗌 Subtotal								

## 6.3.5 Drill-down Actions

Drill-down actions in the Report provide navigation from Report data to related NetBrain features by hyperlinks in report columns, providing deeper insights for Reports by drilling down into the underlying data.

🕵 Report Manager								
Type to search Q 🖸 «	Check OoS D	rop in las	t 7 days Report	Network Intent (View Mode) - All Netw	vork Intents/WZ/Slow Application QoS D	Drop		
🖌 🔟 Shared Reports (24)								
🖌 📹 Application Performance - Continuous Monitoring (4)	Report Input:	Intent	Name: Intent: Slow Applic	I Slow Application QoS Drop	Э			ក្រា 🛄 o 🔥 o 🗶 Edit 🗄
Application Path Historical Monitoring Report	Davide All re-							
Application Path Historical Verification Report	Device: All ~			Result: 03/25/2023 06:11 PM ¥	Embedded Inciden	tv 👗	<u>.</u> •	Run vith Live Network
Application Path Last Verification Report	Pivot Table							
Application Pathl Last Monitoring Report		Device	CATOR	This intent execution is finished at u	3/25/2023 06:11 PM with 0 errors. You	can view Exect	ution Log	
Diagnosis Automation - Transient Problem (6)				4 Devices 3 Diagnoses	S No Queue Drops Detected	in Class video	0	View~
Check CPU Utilization in Last 7 days Report			Sum of Device Alert Su Status Code Count 5		sor			3
Check Interface CRC Error In Last 7 days Report	3/24/2023 12:38	:15 AM	0	• • • • • • • • • • • • • • • • • • •	102			
Check OoS Drop in last 7 days Report	3/24/2023 12:41	:46 AM	0	No content has been added.				
Intent Alert Summary	3/24/2023 1:11:	01 AM	0		100			
Voice Application	3/24/2023 1:41:	01 AM	0	V CO US-BOS-R2	S No Queue Drops Detected	in Class vídeo	0	
A Metwork Security - Continuous Security Assessment (4)	3/24/2023 2:11:	01 AM	0					
Route Leaking Check in This Week	3/24/2023 2:41:	02 AM		show policy-map interface e0/1				
SNMPv2 Enabled Check in This Week	3/24/2023 3:11:	01 AM	0	6 Class-map: video (m	6 Class-map: video (match-any)			No Queue Drops Detected in Class
Telnet Enabled Check in This Week	3/24/2023 3:41:	01 AM	0	20 Class-map: Signal (	(match-all)			
Unencrypt Username Check in This Week	Report Table			22 5 minute offered 32 Class-map: voice (m	rate 0000 bps, drop rate 0000 bps match-any)			No Queue Drops Detected in Class
🖌 📰 Outage Prevention - Failover Failure (8)	1			34 5 minute offered	rate 0000 bps, drop rate 0000 bps			🎦 No Queue Drops Detected in Class
Check ACL Config	intent Name		Executo	46 Class-map: data (ma 48 5 minute offered	rate 0000 bps, drop rate 0000 bp;			No Queue Droos Detected in Class -
📴 Check BGP Config	Slow Applicati	ion QoS Dr	op 3/24/203	58 Class-map: general	(match-all)			
Check Policy Config	Slow Applicati	ion QoS Dr	op 3/24/20	70 Class-map: class-de	rate 0000 bps, drop rate 0000 bps sfault (match-any)			No Queue Drops Detected in Class
Critical Application Report	Slow Applicati	ion QoS Dr	op 3/24/20:	72 5 minute offered	rate 1000 bps, drop rate 0000 bps			🗅 No Queue Drops Detected in Class
Critical Failed Application Report	Slow Apolicati		00 3/24/202					
Critical Succeed Application Report	Plane Amelicani				S No Oueue Droot Detected	0		
Pallover Device Into	Slow Applicati		op 3/24/204	• • • • • • • • • • • • • • • • • • •	Tol no drene proba perected	0		
Problem Fallover Devices	Slow Applicati	ion QoS Dr	op 3/24/20:	a 🗖 abau sallar maa labadaa				
MI TEST	Slow Applicati	ion QoS Dr	op 3/24/20	Show policy-map interface	reu/2	1 Diagnosis		
My Reports (0)	Slow Applicati	ion QoS Dr	op 3/24/20:	6 Class-map: video ( 8 5 minute offered	(match-any) d rate 0000 bps, drop rate 0000 bp	5		No Queue Drops Detected
and the second	Slow Applicati	ion QoS Dr	op 3/24/20;	20 Class-map: Signal 22 5 minute offered	<pre>(match-all) i rate 0000 bps, drop rate 0000 bp (match-all)</pre>	25		No Queue Drops Detected

There are six types of actions to select from for Drill-down actions. Besides that, you can also select one of the Report Columns as the parameter for the Drill-down actions. The parameter defines the details of the Drill-down Actions, such as the name of the Intent to be opened.

- **Open Configuration File** Open the configuration file for the device. The parameter defines the value of the device name.
- **Open Intent Details** Open the Network Intent in View Mode. The name of the Intent is defined by the parameter.
- **Open Diagnosis Tree** Open the Diagnosis Tree of an Intent execution result. The name of the Intent and execution time of the result are defined by the parameter.
- **Open Path Overview** Open the Path Overview pane. The name of the Path and Verified Time is defined by the parameter.
- **Open Change Management Task** Open the Change Management Task. The name of the Change Management Task is defined by the parameter.
- **Open Map** Open the map in another window. The map name is defined by the parameter.



## 6.3.6 Report Filter

Report Filters can filter the report data by certain criteria when viewing a report. There are two purposes for using Report Filters:

- Helps users to sort through a large amount of data and focus on important information.
- Displays data from different perspectives or scopes to help identify the trends or patterns that may not be obvious when viewing the report.

🚉 Report Manager																
Type to search Q S «	Check (	CPU Utiliz	ation in Last	7 days Rep	ort 📵						Li	ast Updated on	: 3/24/2023, 9:3	37:49 AM	Run	Edit
a 📶 Shared Reports (24)															_	
a 📫 Application Performance - Continuous Monitoring (4)	Report I	Input:	ntent Name: I	ntent: Slow Ap	plication CPU.	+ 1 addit	tional inputs									~
Application Path Historical Monitoring Report		and an and a second secon														
Application Path Historical Verification Report	Device: All ~						Date:	All 🗸								
Application Path Last Verification Report	Pivot T.	All														53
Application Pathl Last Monitoring Report		CA-TOR-R1														
a 🗾 Diagnosis Automation - Transient Problem (6)		CA-TOR-SV	V1	-R1	CA-TC	DR-SW1	CA-1	OR-SW2	US+E	BOS-R1	US-B	BOS-R2	US-B	OS-SW1	US-BO	DS-SW2
Check CPU Utilization in Last 7 days Report		CA-TOR-SV	/2	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of	Sum of
📋 Check Interface CRC Error in Last 7 days Report		US DOS D	12	Device Success	Device Alert	Device Success	Device Alert	Device Success	Device Alert	Device Success	Device Alert	Device Success	Device Alert	Device Success	Device Alert	Device Success
Check Interface Utilization in Last 7 days Report	Executio	03-B03-R		tatus Code	Count	Status Code	Count	Status Code	Count	Status Code	Count	Status Code	Count	Status Code	Count	Status Code
🔁 Check OoS Drop in last 7 days Report 🔍	Time	US-BOS-R	2	Count		Count		Count		Count		Count		Count		Count
📋 Intent Alert Summary	3/24/2023 Al	3 12:36:36 M	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Voice Application	3/24/202	3 1:09:05														
🖌 🗾 Network Security - Continuous Security Assessment (4)	A	М	0	1	0	1	(	1	0	1	0	1	0	1	0	1
📋 Route Leaking Check in This Week	3/24/202	3 1:39:04	0	1	0	1		1	0	1	0	1	0	1	0	1
SNMPv2 Enabled Check in This Week	AI	м														
Telnet Enabled Check in This Week	3/24/202 Al	3 2:09:05 M	0	1	0	1		1	0	1	0	1	0	1	0	1
📋 Unencrypt Username Check in This Week	Report T	Table														K 3
a 🗾 Outage Prevention - Failover Failure (8)								Participant Contraction Contraction Contraction Contraction								
📋 Check ACL Config	Intent Na	ame		Exec	ution Time		C	Device Name Device			Device Alert Status Code Count Device Success Status Code Cou				ount	
Check BGP Config	Slow Ap	plication C	PU Check	3/24	/2023. 9:09:03	AM		CA-TOR-R1 0					1			
Check Policy Config	Slow Ap	plication C	PU Check	3/24	/2023, 9:09:03	AM		A-TOR-SW1	70R-SW1 0					1		
Critical Application Report	Slow Ap	-	PUI Check	3/24	/2023 0-00-03	AM		CL TOD CH/2						1		
Critical Failed Application Report	SIOWAP	plication c	FUCHECK	2124	2023, 5.05.03	7500		0K-54/2			0			1		
Critical Succeed Application Report	Slow Ap	oplication C	PU Check	3/24	/2023, 9:09:03	AM		JS-BOS-R1			0			1		
Failover Device Info	Slow Ap	oplication C	PU Check	3/24	/2023, 9:09:03	AM		JS-BOS-R2			0			1		
Problem Failover Devices	Slow Ap	plication C	PU Check	3/24	/2023, 9:09:03	AM		JS-BOS-SW1			0			1		
🗐 New Report	Clow Ap	plication (	DU Chack	2/24	/2022 0-00-02						0					
🔯 NI TEST	SIOW AP	plication c	PO CHECK	3/24	2023, 9:09:03	0.00		/3-003-5WZ			U		1			
My Reports (0)	Slow Ap	oplication C	PU Check	3/24	/2023. 8:39:06	AM	(	CA-TOR-R1			0 1		1			
	Slow Ap	plication C	PU Check	3/24	/2023, 8:39:06	AM		CA-TOR-SW1			0			1		

You can define up to three Report Filters for each Report on Edit Report Page. Each Report Filter has three key elements:

Define Report Filters X	Check CPU Utilization in Last 7 days Report <b>1</b>	
Device Date + Filter Field: Filter Name:	Report Input:         Intent Name: Intent: Slow Application CPU         + 1 addit	ional inputs
Device Name V Device		
Filter Value: +Add	Pivot T. All	
CA-TOR-R1 CA-TOR-SW1	CA-TOR-SW1	CA-TO
CA-TOR-SW2 US-805-R1 US-805-R2	Executio Time CA-TOR-SW2 US-BOS-R1 US-BOS-R2 CA-TOR-SW2 US-BOS-R2 Count	Sum of Device Alert Status Code Count
Cancel OK		

- **Field** Select one of the Report Columns as Field from the drop-down list to define which Report Column the filtering criteria is applied to.
- **Filter Name** Define the name of the Report Filter displayed on the View Report page.
- **Filter Value** –Define the options in the drop-down list for Report Filters. Click on +Add to add Filter Values. You can add up to ten Filter Values for each filter.



## 6.3.7 Run Report

Once the report is defined, you can run it to generate the data. The Report Edit page only provides a preview of the limited number of sample data, and you need to run the report to achieve accurate and complete data.

There are two ways to run a report: manually run it through the Save and Run button, and schedule to run it through Auto-update.

Check OoS Drop in last 7 days Report	Description:					ŭ		Rep	ort Filter (2)	Auto-update	Cancel	Save	Save and Run
Edit Report Properties	»	Report Input: Intent Na Inter	nt: Slow Aj	oplication QoS	i [+ 1	additional inputs				2			<b>1</b>
Customized Field	+ Add	Pivot Table Settings Setving a limited number of records. Run the report to see all records.											
Metwork Intent Device Result     S Intent Result Summary     Intent Name		Rows	Pivot Table										
	() Execution Time	×		Device Name	CA-T	OR-R1	US-BOS-R1		US-BOS-R2		US-BOS-SW1		
Execution Time     Device Name		Drag and drop fields here		Execution		Sum of Device Alert Status	Sum of Device Success Status	Sum of Device Alert Status	Sum of Device Success Status	Sum of Device Alert Status	Sum of Device Success Status	Sum of Device Alert Status	Sum of Device Success Status
Device Name # Device Status Code Count		Columns		Time 3/24/2023	12:38:15	Code Count	Code Count						
# Device Alert Status Code Count		管 Device Name	×	AM		•	Ŭ	14	Ŭ	0	Ŭ		
Device Success Status Code Count     S Device Status Code Summary		Drag and drop fields here		3/24/2025 AN	12.41.40	0	6	0	12	0	6	0	0
		Values	+ Add	3/24/2023 1	:11:01 AM	0	6	0	12	0	6	0	0
		# Sum: Device Alert Status Co.	. ×	3/24/2023 1	:41:01 AM	0	6	0	12	0	6	0	0
		# Sum: Device Success Status .	×	3/24/2023 2	:11:01 AM :41:02 AM	0	6	0	12	0	6	0	0
		show: 🗌 Grand Total 🗌 Subt	otal	3/24/2023 3	:11:01 AM	0	6	0	12	0	6	0	0 -

# 6.4 Create Dashboard

The Dashboard visually displays multiple reports in different charts for a specific purpose.

## 6.4.1 Chart

The dashboard uses various charts to display the analyzed result of the Report. Based on different pivot table settings, Dashboard provides a **column chart, bar chart, line chart, metric chart, gauge chart, pie chart** and **table chart** to display data.



As illustrated in the table below, the data that can be selected and used in the chart directly relates to the Pivot Table settings in the report.



Chart, Column Chart Gauge Chart	Edit Pane - BGP Config Checking for WAN link Types:  Types:  Excert and the second sec	<ul> <li>The x-axis of the line chart can be one or more of the Pivot Table Rows.</li> <li>The y-axis of the line chart can be one or more of the Pivot Table Values.</li> <li>The series of the line chart can be one or more of the Pivot Table Columns.</li> <li>Check Show Call-out to display call-out on the chart. You can display the call-out on the right or bottom of the chart.</li> <li>Check Show Legend to display the data legends on the chart. You can display the legend on the chart's top, right, or bottom.</li> <li>Check Show Data Label to display the data details on the chart.</li> </ul>
	BGP Config Checking for WAN link Title BGP Config Checking for WAN link Measure Sum: Intent Alert Status Code Count ✓ Data Range 0	of the grand totals of Pivot Table values, whether the total is enabled in Pivot Table. • You can modify the data range, colors, and labels for Gauge Chart.

Metric Chart	Report   BGP Config Checking for WAN link   Title   BGP Config Checking for WAN link   Fields   1 Sum: Intent Alert Status Code Count ~   ~ Intent Alert Status Code Count ~   2 Sum: Intent Success Status Code Count ~   ~ Intent Success Status Code Count ~   + Add	<ul> <li>The data of the Fields in the Metric Chart can be one of the grand totals of Pivot Table values, whether the grand total is enabled in Pivot Table or not.</li> <li>You can modify the data, colors, and labels for Fields in Metric Chart.</li> <li>You can add more than one Field in one Metric Chart.</li> </ul>
Pie Chart	Report         BGP Config Checking for WAN link         Title         BGP Config Checking for WAN link         Measure         Sum: Intent Alert Status Code Count         Sliced By         Execute Date         Show Call-out on Right ✓          Show Legend on Top ✓         Show Data Label	<ul> <li>The Measure of the Pie Chart can be one of the Pivot Table Values.</li> <li>The 'Sliced By' of the Pie Chart can be one of the Pivot Table Rows or Columns.</li> <li>Check Show Call-out to display call-out on the chart. You can display the call-out on the right or bottom of the chart.</li> <li>Check Show Legend to display the data legends on the chart. You can display the legend on the chart's top, right, or bottom.</li> <li>Check Show Data Label to display the data details on the chart.</li> </ul>

Table Chart	Report   BGP Config Checking for WAN link   Title   BGP Config Checking for WAN link   Row   100   Sort by   Intent Name   Show Call-out on Right <	<ul> <li>The Table Chart can display the top N records of the report, where N can be specified by users.</li> <li>The Table Chart can be sorted by one of the Report Columns in ascending or descending order.</li> </ul>
	□ Show Call-out on Right ∨ ∠	

## 6.4.2 Call-Out

Besides the chart, each dashboard pane can have one call-out to help provide additional information. There are two main purposes for using the call-out:

- Provide additional details that are not obvious from the chart.
- Highlight important data or trends in the chart.

Edit Pane: The Last Monitoring Result of Application	<b>=</b>				
Report					
Application Pathl Last Monitoring Report	The Last Monitor	ing Result of Applicat	ion		
Title		_			
The Last Monitoring Result of Application			3 Alerts Fou	und	
Fields + Add Sum: Intent Alert Status Code Count >		2	8 Diagnose	s Passed	
✓ Alerts Found					
(2) Sum: Intent Success Status Code Count ~			Top 3 Alerts		
Diagnoses Passed	Intent Name	Intent Map	Execution Time	Intent Alert Status Cod	e Ci Intent Success Status Codi
	Voice Path	Voice Path	3/24/2023, 3:42:17 PM	9	22
	Webex Path	Webex Path	3/24/2023, 10:16:31 AM	8	0
	Webex Path	Webex Path	3/24/2023, 11:44:21 AM	6	6
Z Show Call-out on Bottom 🗸 🗶					

Cancel Save

## 6.4.2.1 Define Metric Call-out

This type of call-out displays numerical data along with their corresponding units of measurement. It helps highlight important data in a clear and concise format.

Edit Pane: ACL Config Checking Results			
турев: 🛫 🌆 🧖 123 📻 🌑 🏢 🖉	Edit Call-out X	ACL Config Checking Results	<b>∠</b> ×
Report Check ACL Configuration	Format: 123	<ul> <li>Sum of Intent Alert Status Code Count</li> <li>Sum of Intent Success Status Code C</li> </ul>	Total Alerts
Title ACL Config Checking Results	Caption: Total Alerts	6	
X-axis Execution Date	1 Sum: Intent Alert Status Code Count ~	4	
Y-axis Sum: Intent Alert Status Code Count, Sum: Intent Succesv	✓ Alerts	2	
Series v		2023-03-23 2023-03-24 2023-03-25	
<ul> <li>Show Call-out on Right          <ul> <li>Show Legend on Top              </li> <li>Show Data Label</li> </ul> </li> </ul>			
	Cancel Ok		

Select the Metric Chart as the format in the Edit Call-out window to define a Metric Call-out. There are two key elements for Metric Call-out:

- **Captions** Captions are descriptive labels on the top of the Call-out. It helps provide an overview of the content or purpose of a call-out.
- **Fields** Fields are the data displayed in the Metric Call-out. Each Metric Call-out can have up to six Fields, while each Field displays one summarized data from the report. You can define a unique background color and label each field to help annotate the data.

#### 6.4.2.2 Define Table Call-out

This type of call-out displays the top-N records of the original report. It helps provides additional details for the chart.

To define the Table Call-out, select the Table Chart as the format in the Edit Call-out window. There are three key elements for a Table Call-out:

- **Captions** Captions are descriptive labels that help provide an overview of the content or purpose of the call-out.
- **Row** Row defines how many rows of data appear in the Table Call-out.
- **Sort by** Sort by defines by which report column the report data is sorted. You can choose to sort it in ascending or descending order.

Edit Pane: The Last Monitoring Result of Application		
Types:	Edit Call-out	×
Report		
Application Pathl Last Monitoring Report	Format: 123	
Title	Caption: Top 3 Alerts	
The Last Monitoring Result of Application	Row 3	
Fields + Add		
Sumi Intent Alert Status Code Countas	Sort by Intent Alert Status Cod V Descending V	
(1) Sum: Intent Alert Status Code Count V		I
V Alerts Found		
	<b>7</b>	
2 Sum: Intent Success Status Code Count 🗸		
Diagnoses Passed		
	Cancel	k
Show Call-out on Bottom 🗸 🖌	Calcel	IX.

# 6.4.3 Refresh Dashboard

Dashboard caches report data in the back end for faster loading speed. Refresh the Dashboard from the dropdown menu to get the latest report data and update the dashboard accordingly.

Monitor Failover Design Description:		∠ Edit do •••
Failover Devices with Problems PM View Report	The Result of Application Verification Last Verified Time: All  Failed Failed Failed	Succeeded
1 Policy Config Checking Results 3/25/2023, 3:34:05 PM View Report Over All or	ACL Config Checking Results     3/25/2023, 334:05 PM     View Report	BGP Config Checking Results 3/25/2023, 3/34:05 PM View Report
Total Alerts Total Alerts Total Alerts Total Alerts Alerts	Total Alerts Sum of Intent Alert Status Code Sum of Intent Success Status C 10 5 6 10 10 10 10 10 10 10 10 10 10	Total Alerts Sum of Intent Alert Status Code Sum of Intent Success Status C 20 10 10 10 10 10 10 10 10 10 1

# 6.5 Report and Dashboard Examples

## 6.5.1 Monitor Failover Failure for Outage Prevention

Failover design is essential to network outage prevention to ensure the reliability of critical network services. However, sometimes failover failure could happen due to inadequate testing or configuration errors. To monitor the failover designs and find potential risks in advance, a dashboard could be built to answer the following question:

How is the robustness of the failover design in the network?

To answer this question, a few follow-up questions could be asked:

• Are the ACLs consistent between the primary and failover devices?

- Are the BGP configurations consistent between the primary and failover devices?
- Are the policy maps consistent between the primary and failover devices?
- Which devices have potential risks?
- When are the risks detected?
- Is there any impact on critical applications?

For each follow-up question, you can build a report to answer it. Then a dashboard could summarize and display those reports on a single screen.

Monitor Failover Design Description:						2 8	idit ag
Failover Devices with Problems	3/25/2023, 3:34:09 PM View Report	The Result of Application Verifica	tion			3/25/2023, 3:34:09 PM	View Report
	2	Last Venfied Time: All ~ 3 2		Failed	Succeeded		
Policy Config Checking Results	1 3/25/2023, 3:34:05 PM View Report	ACL Config Checking Results	3/25/2023, 3:34:05 PM	202 View Report	3-03-24 BGP Config Checking Results	3/25/2023, 3:34:05 PM	View Report
Date: All 🗸	Total Alaste	Date: All 🗸	Total Alor	de .	Date: All 🛩	Total	Maste
• Sum of Intent Alert Status Co + Sum of Intent Success Status	21 Alerts	Sum of Intent Alert Status Co Sum of Intent Success Status	21	Alerts	• Sum of Intent Alert Status Co + Sum of Intent Success Status 20 10 0 0 0 0 0 0 0 0 0 0 0 0 0	28	Alerts

## 6.5.2 Automate Diagnosis of Transient Problems

Diagnosing transient problems can be challenging because they occur intermittently or briefly, making them difficult to reproduce and troubleshoot. An Intent is scheduled to run every 10 minutes to troubleshoot the slowness in the voice application. A dashboard can be built to answer the following questions:

What are the possible causes of slowness in the voice application?

To answer this question, a few follow-up questions could be asked:

• Is there high CPU usage in Voice Application?

- Is there QoS drop in Voice Application?
- Is there high interface usage in Voice Application?
- Are there interface CRC errors in Voice Application?
- When are the alerts detected?
- How many alerts in total are detected?

Reports and Dashboards can be created to analyze and display the results from the following Intents:

- **Check CPU Utilization**: This Path Intent is scheduled to collect results of the command, show process CPU, for all the devices in the path and generate an alert if the CPU usage is above 80%.
- **Check QoS Packet Drop**: This Path Intent is scheduled to generate an alert whenever there is a QoS packet drop for all devices in the path.
- **Check Interface Usage:** This Path Intent is scheduled to monitor the interface usage for all the devices in the path and generate an alert if the interface usage is above 70%.
- **Check Interface CRC Error**: This Path Intent is scheduled to check the interface CRC error for all the devices in the path. It will generate an alert if there is any CRC error detected.

For each follow-up question, you can build a report to answer it. Then a dashboard could summarize and display those reports on a single screen.

Troubleshoot Slow Voice Application for i	ncident Description:						🖊 Edit	ao
Slow Application Info				3/24/2023, 12:11:44 AM	View Report	Alert Detection Count	3/24/2023, 2:50:12 PM	w Report
Application Name Path Name	Path Type Sour	rce Source Device	Destination	Destination Device	Reference Map			
Voice Voice Path	Unicast 10.8.	3.200 10.8.3.200	10.8.1.26	Webex-Server	Voice Path	0	40 60 80 0	
High CPU Usage Alert		3/24/2023, 9:37:49 AM	View Report	OoS Drop Aler	t		3/26/2023, 1:12:49 PM View	w Report
Device: All V	Date	£ All ∽		Device: All 🗸		Date: All 🗸		
0 0 0 0 0 0 0 0	0 0 0 0 0 0 0		0 0 0 0	0 0 0			0 0 0 0 0 0 0	0 0 0
3,14,100,100,100,100,100,100,100,100,100,	2 1213 1214 2124 2124 2124 2124 2124 212	512 1013 1013 1013 1013 1013 1013 1013 10	223 124 12023 12013 12013	3/26/2013 2013/26/2013	2023 1023 1013 1013 1013 1013 326 326 316 316 318 318 31	5002 1002 1002 1002 1002 1002 1002 1002	201310 202 210 210 200 200 200 200 200 200 2	312612923
High Interface Usage Alerts		3/24/2023, 2:18:29 PM	View Report	Interface CRC	Error Alerts		3/24/2023, 2:18:27 PM View	w Report
Device: All V	Date	s All 🗸		Device: All 🗸		Date: All 🗸		

# 6.5.3 Perform Security Assessment for Network Security

Network Security Assessment is critical to maintaining a secure and resilient network infrastructure. To conduct the security assessment regularly, a series of Network Intents are scheduled to run weekly. A dashboard can be built to answer the following questions:

Is there any security weakness in the network?

To answer this question, a few follow-up questions could be asked:

- Can the allowed devices successfully access the devices in the security zone?
- Are the disallowed devices successfully blocked by the security zone?
- Is there any configuration drift in the security zone?

ecurity Assessment Dashboa	ard Description:						Edit Update
Security Zone - Allowed	Network Alert in This Month	ı	4/17/2023, 5:09:01 PM View Report	Security Zone - Disallow Result: All ~	ed Network Alert in T	This Month	4/18/2023, 5:42:31 AM View Report
	0	2 3			0	2 2 3	
	The Lat	est 3 Detections				The Latest 3 Detections	
Intent Name	Execution Time	Intent Alert Status Code Count	Intent Status Code Summary	Intent Name	Execution Time	Intent Alert Status Code Count	Intent Status Code Summary
Check Production Zone of US-	4/17/2023, 5:01:55 PM	0	Validation Disallow Network is C	Check Production Zone of US	4/18/2023, 2:01:56 AM	1	Validation Disallow Network is in
Check Enterprise Zone of US-N	I 4/8/2023, 8:59:43 PM	0	Validation Disallow Network is C	Check Enterprise Zone of US-N.	4/8/2023, 9:00:09 PM	1	Validation Disallow Network is in
Check DMZ Zone of US-NYC-Pa	a 4/8/2023, 8:59:34 PM	1	Validation Allow Network is inco	Check DMZ Zone of US-NYC-Pa	4/8/2023, 8:59:53 PM	0	Validation Disallow Network is C
Security Zone - Anti-drift Result: All 🗸	ft Device In this Month						4/18/2023, 5:40:45 AM View Report
						The Latest 3 Detection	
	1	2		Intent Name Execution Tir	ne Device Name	Device Alert Status   Device Success Stat	evice Status Code Alert Detection
				NYC Security Zo 4/18/2023, 2	02: US-NYC-Paloalto	. 0 8 A	ccess-internet 0
	0	0					

## 6.5.4 Perform Continuous Monitoring of Application Performance

Continuous Monitoring of critical applications and paths can help identify potential problems, improve performance, and analyze network traffic patterns. Two Intent are scheduled to run continuously to monitor

the key applications Voice Path and Webex Path in the network. A dashboard can be built to answer the following questions:

Are there any potential problems in critical applications?

To answer this question, a few follow-up questions could be asked:

- Which applications failed to be verified that require attention?
- Which applications are verified successfully?
- For the application failed to be verified, are there any failed to ping destination issues?
- For the application failed to be verified, are there any ACL misconfigurations?

For each follow-up question, you can build a report to answer it. Then a dashboard could summarize and display those reports on a single screen.

pplication Continuous Monitoring Description:		🖌 Edit 🛛 🖉
The Last Verification Result of Application 3/24/2023. 10:29:19 AM View Report	The Historical Verification Result of Application Date: All ~  Falled • Succeeded  Succeeded Succeeded  Succeeded  Succeeded Succeeded  Succeeded  Succeeded  Succeeded  Succeeded  Succeeded  Succeeded  Succeeded  Succeeded  Succeeded Succeeded  Succeeded Succeeded Succeeded Succeeded Succeeded Succeeded Succeeded Succeeded Succeeded Succeeded Succeeded Succeede	3/24/2023. 10:26:46 AM View Report
The Last Monitoring Result of Application     3/24/2023. 0:00445 PM     View Report       Path Name: All >     23     Alerts Found       28     Diagnoses Passed	The Historical Monitoring Alerts of Application Date: All ~ 60 0 2023-03-23 2023-03-24	3/24/2023, 5:11:20 PM View Report
Top 3 Alerts	Top 3 Alerts	Total Alext Count
inclusion many exception may international international code con international code	Voice Path Voice Path 3/24/2023, 3:42:17 P/	M 18
Voice Path Voice Path 3/24/2023, 3:42:17 PM 9 22		
Voice Path         Voice Path         3/24/2023, 3:42:17 PM         9         22           Webex Path         Webex Path         3/24/2023, 10:16:31 AM         8         0	Webex Path Webex Path 3/24/2023, 10:16:31 /	AM 16

# 7 Other Enhancements

# 7.1 Domain Setup and Data Accuracy Improvements

## 7.1.1 Discovery and Fine Tune Improvements

#### 7.1.1.1 Unknown IP and Do-Not-Scan Improvement

After the discovery, many entries will be generated in the table **Fine Tune\Devices to be Discovered**. Some of these IP addresses are not accessible or invalid, which makes cleaning up this table difficult. R11.1 provides automated ways to clean up these entries.

 Changed the field name, Missed Devices to Inaccessible Devices, and Unknown IPs to Devices to be Discovered.

: Domain Management				
Start Page Fine Tune X	42			
	G Refresh	Items: 6		
<ul> <li>Live Access</li> <li>All Discovered Devices (172)</li> </ul>		Hostname	Management IP	Device Type
CLI Configuration Devices (161)		AWS-EAST-Vedge	192.168.28.4	Viptela vEdge
SNMP Configuration Devices (9) Others (2)		Azure-cEdge	4.4.4.111	Cisco Router
Inaccessible Devices (6)		Berlin-vEdge	10.8.12.33	Viptela vEdge
Unknown SNMP SysObjectID (4)		London-vEdge	10.8.12.37	Viptela vEdge
Devices to be Discovered (612)		Paris-vEdge	10.8.12.41	Viptela vEdge
NUP (427)     Routing Neighbor (16)		Tokyo-vEdge	10.8.12.45	Viptela vEdge
<ul> <li>Routing Table (35)</li> </ul>				
Others (134)				
SSH Fingerprint Check Failed (0)				
🔺 📶 Network and Topology				
Duplicated IP and Subnet Manager				

- 2. Automatically add MPLS PE IPs to the **Do-Not-Scan** table after creating and updating MPLS Cloud. The PE IPs already in the **Devices to be Discovered** table will be removed.
- 3. After the Generic Device is added, the IP address belonging to the Generic Device will be automatically deleted from the **Devices to be Discovered** table.

 Provide a System Plugin, *Auto\_Clear\_NDP*, that automatically runs after the discovery to move the entries from the **Devices to be Discovered/NDP table** to the **Do-Not-Scan table**.

The *Auto\_Clear\_NDP* plugin matches the keyword in the description column and moves them to the Do-Not-Scan table to reduce the noise. The user can modify the keyword, for example, Linux, IP Phone, etc.

rt tage Ne Tune Vugen Manager Discover Schedule Task cover bevices via SMMP/CLI Network Settings Method: Discover Va Seed Routers O San IP Range Access Mode: SMMP and SSH/Telnet O Discovery Depths: 30 IP Hoomanne: Leg To 10 10 12 2001; 1: Mr CH I Performanne: Le	Domain Management	i 				
tore the set of the second base	t Page Fine Tune X Plugir	n Manager X Discover X Scher	dule Task $ imes$			
scorer Devices via SHMP/CLU Network Settings Method: © Discovery Via Seed Routers © San P Range Access Mode: NMP and SSH/Tellnet © © Discovery Depthe 30 PHOsename: eg: 10.11.0.11; 2001; 1; 107;01 scorer Devices via API • Select API Servers Cleck Select API Servers to add servers. © Benchmark Task: select <b>out servers</b> • Select <b>Select API Servers</b> to add servers. • Select <b>Select API Select API Servers</b> to add servers. • Select <b>Select </b>	over		View His	storical Result: Select 🕜 Help		
Method:	scover Devices via SNMP/CLI Netw	ork Settings				
IP/Hostmane:	Method: ( Discover via Seed	Routers 🔿 Scan IP Range Acce	ss Mode: SNMP and SSH/Telnet 🗸 🚯	Discovery Depth: 30		
PMosename to the set of the second part of the seco		· ·				
iscover Devices via API + Select API Servers API Servers Cick: Select API Servers Benchmark: Task: select Advanced Options Set Discovery Advanced Options Set Discovery Set Discovery Advanced Options Set Discovery Advanced Options Set Discovery Advanced Options Set Discovery Advanced Options Set Discovery Advanced Options Set Discovery Advanced Options Set Discovery Set Disco	IP/Hostname: e.g. 10.10.10.1; 2001::	1; NY_R1			Import IP List 🗸	
API Servers Cick Select API Servers' to add servers. Benchmark Task: Select API Servers' to add servers. Benchmark Task: Select API Servers' to add servers. Advanced Options	iscover Devices via API + Soloct ADI	I Servers				
API Servers: Citck Select API Servers' to add servers. Benchmark Task: Select  Advanced Options  Start Discovery  Advanced Options Select Plugin  Advanced Plugin		56765				
Benchmark Task     Advanced Options        Advanced Options     Advanced Options        Advanced Options           Advanced Options </td <td>API Servers: Click 'Select API Server</td> <td>s' to add servers.</td> <td></td> <td></td> <td></td> <td></td>	API Servers: Click 'Select API Server	s' to add servers.				
Benchmark lask     Select     Advanced Options     Advanced Options <td></td> <td></td> <td></td> <td>Start Discouper</td> <td></td> <td></td>				Start Discouper		
• Advanced Options         • Margined System UserOncomy DupprixMus (See,NP) More         • Buitten PugnerMutssource Discover, mutissource         • Buitten PugnerMutssource Discover, mutissource         • None	Benchmark Task:	select V	Advanced Options V	Start Discovery		
Decision Prote After execution geno Sequential V      Action	Select Plugin + Add Execution Point	0	+	× Auto_Cl	car_NDP	Sam
R Eneber     Lossenian     Marin     Description_Opcode Group       B Bulletin Plugins/NB_System_Uker/Discovery_Plugins/NAuro_Clear_NOP     None     This plugin.       B Bulletin Plugins/NB_System_Uker/Discovery_multisource     None     NA	Execution Point: After executing discovery     + Add Plugin		Execution order of this execution point: Sequ	Jential Y		
Image: State Plagers NB_System_Uker/Discovery_Plagers/NkurS_State     None     This plage N/A       Image: State Plagers/NB_System_Uker/Discovery_multisource     None     N/A	Enable Location	Meut	Descriptio Device Group	P	"IP Phone", "Linux"	3
C Buitten Flagfrach Rig System Use MKR SpassBetriere None NA     Buitten Flagfrach Rig System Use MKR SpassBetriere None NA     Buitten Flagfrach Multisource/Discover_multisource None NA	Built-in Plugins/NB_System_U	Jse/Discovery_Plugins/Auto_Clear_NDP None	This plugi N/A	4	Lu	
	Built-in Plugins/NB_System_U	Jse/AWS_PostRetrieve None	Handle A N/A			
	Built-in Plugins/Multisource/	Jiscover_multisource None	N/A			
Canzal						
						Cancel

5. Record the IP source in the Do-Not-Scan Table to help the user understand where the IP is from.

List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S     List the IP address, subnets or devices, R1     List the IP address, subnets or devices, R2     List the IP address, subnets or devices, R2     List the IP address, subnets or device types you do not want to discover via Telnet/SSH/S	$\times$		
5 Items       + Add       Import       Export         IP or Subnet •       Description       Source Te         30.30.30.30/32       IP found from To be Discovered Devices: bos_core-r20       All Technol         30.30.30.32/32       IP found from Unknown SNMP SysObjectID: 21F3A-37       All Technol         30.30.30.34/32       IP found from MPLS Cloud: AT&T_MPLS       All Technol         30.30.30.35/32       IP found from All Discovered Devices: R1       All Technol         30.30.30.36/32       IP found from Inaccessible Devices: R2       All Technol	<ol> <li>List the IP address,</li> </ol>	subnets or device types you do not want to discover via T	elnet/SSH/S
IP or Subnet •       Description       Source Te         30.30.30/32       IP found from To be Discovered Devices: bos_core-r20       All Technol         30.30.30.32/32       IP found from Unknown SNMP SysObjectID: 21F3A-37       All Technol         30.30.30.34/32       IP found from MPLS Cloud: AT&T_MPLS       All Technol         30.30.30.35/32       IP found from All Discovered Devices: R1       All Technol         30.30.30.36/32       IP found from Inaccessible Devices: R2       All Technol	5 Items + Add	🔁 Import	📑 Export
30.30.30.30/32IP found from To be Discovered Devices: bos_core-r20All Technol30.30.30.32/32IP found from Unknown SNMP SysObjectID: 21F3A-37All Technol30.30.30.34/32IP found from MPLS Cloud: AT&T_MPLSAll Technol30.30.30.35/32IP found from All Discovered Devices: R1All Technol30.30.30.36/32IP found from Inaccessible Devices: R2All Technol	IP or Subnet +	Description	Source Tee
30.30.30.32/32       IP found from Unknown SNMP SysObjectID: 21F3A-37       All Technol         30.30.30.34/32       IP found from MPLS Cloud: AT&T_MPLS       All Technol         30.30.30.35/32       IP found from All Discovered Devices: R1       All Technol         30.30.30.36/32       IP found from Inaccessible Devices: R2       All Technol	30.30.30.30/32	IP found from To be Discovered Devices: bos_core-r20	All Techno
30.30.30.34/32     IP found from MPLS Cloud: AT&T_MPLS     All Technol       30.30.30.35/32     IP found from All Discovered Devices: R1     All Technol       30.30.30.36/32     IP found from Inaccessible Devices: R2     All Technol	30.30.30.32/32	IP found from Unknown SNMP SysObjectID: 21F3A-37	All Techno
30.30.30.35/32     IP found from All Discovered Devices: R1     All Technol       30.30.30.36/32     IP found from Inaccessible Devices: R2     All Technol	30.30.30.34/32	IP found from MPLS Cloud: AT&T_MPLS	All Techno
30.30.36/32 IP found from Inaccessible Devices: R2 All Technol	30.30.30.35/32	IP found from All Discovered Devices: R1	All Techno
	30.30.30.36/32	IP found from Inaccessible Devices: R2	All Techno
		<ul> <li>List the IP address,</li> <li>List the IP address,</li> <li>Items + Add</li> <li>IP or Subnet -</li> <li>30.30.30.30/32</li> <li>30.30.30.32/32</li> <li>30.30.30.34/32</li> <li>30.30.30.35/32</li> <li>30.30.30.36/32</li> </ul>	<ul> <li>List the IP address, subnets or device types you do not want to discover via Tr</li> <li>List the IP address, subnets or device types you do not want to discover via Tr</li> <li>Items + Add  IP or Subnet • Description</li> <li>30.30.30.30/32 IP found from To be Discovered Devices: bos_core-r20</li> <li>30.30.30.32/32 IP found from Unknown SNMP SysObjectID: 21F3A-37</li> <li>30.30.30.34/32 IP found from MPLS Cloud: AT&amp;T_MPLS</li> <li>30.30.30.35/32 IP found from All Discovered Devices: R1</li> <li>30.30.30.36/32 IP found from Inaccessible Devices: R2</li> </ul>

5

- When the Source Device is deleted from the domain, its associated entries in the **Devices to be Discovered** table are automatically cleared.
- 7. Add Rediscover Selected Source Devices function in the Devices to be Discovered table, which will launch a new discover task using the Source Device as the seed and the depth set to 1. After rediscovering the source device, the system automatically clears the associated entries that are no longer in the Source Device's NDP table.

	Domain Managemer	nt				Q Support	Tenant: demoTe	nant Do	main: demo	Domain 🚊	Danny.Gan@n	et ?	Net3
tart P	Page Fine Tune X												
		🕤 Refresh	Items: 421					Redisc	over All	Search	C	A B B	<b>8</b> H
i Li	ive Access	A	ID Address	Source Device	Source Interface	Interface Descrip	Description (Douis	o Namo Jat	orfaco Diatfo	(111)	Reason		Die
4	All Discovered Devices (172)		in Address	Source Device	Source interface	interface beachp.	Description (Devic	e Name, mo	eriace, Fiacio		Reason		01.
	CLI Configuration Devices (1)	61)	10.1.1.13	IPv6Lab-SW8	Ethernet0/0 (10.1.1		IPv6Lab-R4.netbra	iin.com,Ethe	rnet0/1,Linux	Unix	Ping Faile	d, SNMP Faile	d 3/
	SNMP Configuration Devices	; (9)	10.1.1.2	IPv6Lab-MPLS	Ethernet0/3 (10.1.1		IPv6Lab-R_IPv4.ne	tbrain.com,	View Edge	Device Configu	ration	SNMP Faile	d 3/
	Others (2)		10.1.1.235	IPv6Lab-SW11	Ethernet0/2 (2020:		IPv6Lab-SW9.netb	rain.com,Et	Move Selec	ted IPs to Do N	ot Scan IP List	SNMP Faile	d 3/1
	Inaccessible Devices (0)		10.1.1.248	IPv6Lab-MPLS	Ethernet0/2 (10.1.1		R-vrftest.netbrain.	com.Ethern	Delete from	n Tabl		SNMP Faile	d 3/1
	Onknown Styler Sysobjectib (4)     Devices to be Discovered (612)		10.1.1.240	IDu6Lab MDLS	Ethernet0/2 (10.1.1		P19 pathrain com	Ethornot0/2	Discover Se	elected IPs		SNIMD Faile	4 2/
-	NDP (427)		10.1.1.249	IPVOLAD*IVIPES	Ethernetorz (10.1.1		Krainetorain.com	cuterneco/s	Rediscoven	Selected Sourc	e Devices	Sivivie Falle	
	Routing Neighbor (16)	_	10.1.1.5	IPv6Lab-MPLS	Ethernet0/1 (10.1.1		IPv6Lab-R4.netbra	iin.com,Ethe	Live Access	Log		SNMP Faile	d 3/1
			10.10.12.9	ITE_SW1	Vlan3 (172.16.10.2/		BUR12-LAB-SW1.k	o,Gi2 0/15,			Ping Faile	d, SNMP Faile	d 3/1
	Domain Manage	ment				🙆 Su	pport Tenant: d	moTenant	1, LANX DIRix		Ping Faile	d, SNMP Faile	d 3/1
					•				1,Linux Unix		Ping Faile	d, SNMP Faile	d 3/1
-	Start Page Fine Tune $ imes$	Discover ×			<b>2</b>				hernet0/2,Lin	ux Unix	Ping Succ	eeded, SNMP.	3/1
[	Discover					View Hist	orical Result: Select	? Help	hernet0/0,Lin	ux Unix	Ping Succ	eeded, SNMP.	3/1
	Discover Devices via SNMP/CLI	Network Setting	ts						n,Ethernet0/	),Linux Unix	Ping Faile	d, SNMP Faile	d 3/1
			_					.thraid	Thernet0	/0 Linux Unix	Ping Faile	d SNMP Faile	4 3/1
	Method: 💿 Discover v	ia Seed Routers	Scan IP Range	Access	Mode: SNMP and SSH	Telnet 🗸 🚯	Discovery Depth:	1			Di Su		
							-	torainte	m,Ethernet0	/0,Linux Unix	Ping Faile	d, SNMP Faile	a 3/1
	IP/Hostname: IPv6Lab-SW8							:tbrain.d	MP, Ethernet0	/0,Linux Unix	Ping Faile	d, SNMP Faile	d 3/1
	Discover Devisor via API	last ADI Convers							om,Ethernet0	/0,Linux Unix	Ping Faile	d, SNMP Faile	d 3/1
	Discover Devices via virt 1 5	lect AFI Dervers							m,Ethernet0	/0,Linux Unix	Ping Faile	d, SNMP Faile	d 3/1
	API Servers: Click 'Select A	PI Servers' to add ser	vers.						n,Ethernet0/	),Linux Unix	Ping Faile	d, SNMP Faile	d 3/1
	Benchmark	Task: select		~	Adva	nced Options 🗸	Start Disc	overy					

## 7.1.1.2 System Validation Improvements

R11.1 adds new error types to improve the CLI, API and server access errors. Also, the recommendation of existing error types is updated to guide the users more accurately in solving live access issues in the Data Accuracy Wizard pane.



## 7.1.1.3 Discover a Device with Duplicate IP

R11.1 provides an option in the Advanced Settings of Domain Management to enable the discovery of duplicate IPs in such customer networks. This option can be used to discover the device which has duplicated interface IP address (the management IP address must be unique). By default, this option is disabled. Enabling this option will impact the discovery performance.

::: Domain Management	🖉 Support Tenant: Tenant1 Domain: Domain1 🛓 admin 🛛 NetBrdin
Start Page Advanced Settings ×	
Build L3 Topology Option	Management Interface Selection Order     •       Enter the Interface type order for batch setting the management Interface     •       management,loopback;vlan;ve;ethernet     Apply
Build L2 Topology Option	Discovery and Scan Continue to discover, if the IP to be discovered is not duplicated with the existing device management IP. (Used for the situation that device management IP has a duplicate with other devices' interface IP.)
Only save One-IP table entries that have values in Switch Port or DNS Name parameter	Polling Order
Configure Alert Email for Qapp Compose emails in this format during each interval: Merge all alerts in one email Separate alert emails for different tasks Separate alert emails for different objects Duplicate an alert in emails when alert count increases by	<ul> <li>Trying to login device directly, then login via Jumpbox</li> <li>Trying to login device via Jumpbox, then login directly</li> <li>If ping falls, don't try Telnet/SSH in Tune Live Access and Seed Discovery</li> <li>If ping falls, don't try SNMP/Telnet/SSH in Scan IP Range</li> </ul> Third Party Telnet/SSH Tool <ul> <li>Enable Telnet/SSH CLI via third party tool</li> </ul> SSH Fingerprint Check
Ωνε	□ Enable SSH Hingerprint Check and Auto Fill-In Fingerprint Key to the Devices

## 7.1.1.4 Import Devices Via Config Files/Pre-defined CSV

R11.1 provides two built-in plugins to import inaccessible devices to the NetBrain system.

• Import Devices via Config Files:

The plugin, *Import\_DeviceData\_From\_Files*, under the folder /All Plugin/Built-in

**Plugins/Plugin\_Features/Import\_Baseline/** in the **plugin manager**, imports the devices by the configuration file.

rch Q 🕃 Refres	In the second se	6
All Plugins	Description Input main.py +	
🔺 📶 Built-in Plugins		
🖻 📶 Multisource	Normal 💠 Sans Serif 🗧 🎽 🖪 🛛 🖳 😌 🤧 🗞 🖹 🗮 🚍	
Image:		
Platform_Certification	Add the device to your NetBrain system.	
Plugin_Features	Flow to implement this plugin:	
Clean_Invalid_Data		
Dry_Run_NIC	<ol> <li>to get started, you need to prepare the following "device/ist.csv" tile to list the information you want to import to Netsrain system: For example:</li> </ol>	
Export_Baseline	A B C	
Feature_Design	1 DeviceName DeviceType	
🕨 📶 Hostname_Change	2 Netbrain Router Cisco Router	
🔺 🔝 Import_Baseline	3 Netbrain_SW Cisco IOS SWItch	
	4	
Import Configuration	The first column must be the device name, and the second column must be the device type(ignore case)	
Import Configuration	The first column must be the device name, and the second column must be the device type(ignore case)	
Import Configuration Import_DeviceData_From_Files Import_DeviceData_From_Local	The first column must be the device name, and the second column must be the device type(ignore case)     Create folder to import devicelist.csv and device name folders.     For example.	
Import_Configuration Import_DeviceData_From_Files Import_DeviceData_From_Local Import_GenericDevice_From_Files	The first column must be the device name, and the second column must be the device type(ignore case) Create folder to import devicelist.csv and device name folders. For example:  Exampl	
Import_Configuration Import_DeviceData_From_Files Import_DeviceData_from_Local Import_Gener/Clevice_From_Files Platform_Validation		
Immort_Configuration     Import_DeviceData_From_Files     Import_DeviceData_From_Local     Import_CenericDevice_From_Files     Import_CenericDevice_From_Files     Import_CenericDevice_From_Files	The first column must be the device name, and the second column must be the device type(ignore case) Create folder to import devicelist csv and device name folders. For example:  RetBrain South Anything and Create Map.  RetBrain South Anythi	
Immort Configuration     Import_DeviceData_From_Files     Import_OeviceData_From_Local     Import_GenericDevice_From_Files     Import_GenericDevice_From_Files     Import_GenericDevice_From_Files     Import_GenericDevice_From_Files     Split_Zone     Samples	The first column must be the device name, and the second column must be the device type(ignore case) Create folder to import devicelist.csv and device name folders. For example:  Files > Desktop Files > Desktop Search.	
Import_Configuration  Import_DeviceData_From_Files  Import_GenericDevice_From_Files  Pattorm_Validation  Split_Zone  Split_Zone  Split_Zone  Split_Split_Senarios	The first column must be the device name, and the second column must be the device type(ignore case)  2. Create folder to import device is the many folders. For example:  Files > Desistop  Fi	
Import_Cenificuation     Import_DeviceData_From_Files     Import_DeviceData_From_Local     Import_GenericEDevice_From_Files     Import_GenericEDevice_From_Files     Split_Zone     Split_Zone     Split_Zone     More Support Security	The first column must be the device name, and the second column must be the device type(ignore case)  2. Create folder to import deviceilst.csv and device name folders. For example:  Files > Desktop  Files > D	
Import_Configuration     Import_DeviceData_From_Files     Import_Cener/Cevice_From_Files     Import_Cener/Cevice_From_Files     Patform_Validation     Split_Zone     Spplit_Zone     Special_Scenarios     My Plugins     Acure_VRT_154		
Import_Configuration     Import_DeviceData_From_Files     Import_DeviceData_From_Files     Import_GenericDevice_From_Files     Import_GenericDevice_From_Files     Split_Zone     Split_Zone     Special_Scenarios     My Plugins     Arrure_VRT_154     Import_Configuration	The first column must be the device name, and the second column must be the device type(ignore case)  C. Create folder to import deviceilist.csv and device name folders. For example:  Files > Desktop  Files > Desktop  Files > Desktop  Files > Desktop  Files > Diffice Device:  Files > Diffice De	
Import_Configuration     Import_DeviceData_From_Files     Import_DeviceData_From_Files     Import_GenericDevice_From_Files     Import_GenericDevice_From_Files     Split_Zone     Split_Zone     Split_Zone     Split_Some Some Some Some Some Some Some Some	The first column must be the device name, and the second column must be the device type(ignore case)  a. Create folder to import device is cave and device name folders. For example:  Files > Desistop  Files > Desistop  Files > Desistop  Files > Device Group  Sincurén  Files > Discurént Files  Files > Device Group  Sincurén  Files > Discurént File  Files > Device File  Files > Device File  Files > Discurént File  Files > Discurént File  Files > Device File  Files > Discurént File  Files > Discurént File  Files > Device File  Files > Discurént File  File  Files > Discurént File  File  Files > Discurént File	
Import_Configuration     Import_DeviceData_From_Files     Import_DeviceData_From_Files     Import_CenterDevice_From_Files     Import_CenterDevice_From_Files     Split_Cone     Split	The first column must be the device name, and the second column must be the device type(ignore case) 2. Create folder to import deviceilist.csv and device name folders. For example:	
Import_Configuration     Import_DeviceData_From_Files     Import_DeviceData_From_Local     Import_Gener(Device_From_Files     Sell_Zone     Samples     Special_Scenarios     My Plugins     Arure_VRT_154     Import_Configuration	The first column must be the device name, and the second column must be the device type(ignore case) a. Create folder to import deviceilst case and device name folders. For example:	
Import_Configuration     Import_DeviceData_From_Files     Import_GenericDevice_From_Files     Import_GenericDevice_From_Files     Split_Zone     Split_Zone     Split_Sone     Special_Scenarios     My Plugins     Azure_VRT_154     Import_Configuration	The first column must be the device name, and the second column must be the device type(ignore case) a. Create folder to import device is case and device name folders. For example:	

• Import Devices via Pre-defined CSV

The plugin *Import\_GenericDevice\_From\_Files*, under the folder **/All Plugin/Built-in Plugins/Plugin\_Features/Import\_Baseline/** in the **plugin manager**, imports the devices by CSV file.

The CSV file must contain the following information:

- If there is no IP address, the corresponding physical interface data will be generated.
- If there is an IP address, the corresponding physical and IP interface data will be generated.

# The fields *DeviceName, ManagementIP, DeviceType, DriverName,* and *IntfName* are required. The other fields are optional.

DeviceName	ManagementIP	DeviceType	DriverName	IntfName	IPv4Address	IntfType	IntfVrf	IntfMode	IntfVlan
Device1	10.10.10.10	Cisco IOS Switch	Cisco IOS Switch	Ethernet0/0	192.168.25.1	VLAN	global_vrf		40
Device2	11.11.11.11	Juniper Router	Juniper Router	Ethernet0/1		Physical		access	100

# 7.1.2 Benchmark Improvements

R11.1 made the following improvements on the scheduled benchmark task:

- Remove the BGP Advertised Route Table from the System Table since we already have the NCT Table with the same information. Collecting the same data twice is a waste of resources and timeconsuming.
- Modify the data collecting logic for BGP Advertised Route Table and BGP All VPNv4 Advertised Route Table in the Server Benchmark to only collect the data on the MPLS CE device and the BGP neighbor connected to MPLS Cloud. This logic also applies to Public Cloud VRT. The related nodes in Public Cloud are:
  - o AWS: DX Router, VGW
  - Azure: MSEE, Virtual Network Gateway, and VPN Gateway
  - o GCP: Cloud Router, Partner Interconnect, and VPN Gateway
- Add Circuit Breaks

Collecting a large amount of data may be time-consuming, which could cause Server Benchmarks to run for several hours without completion. This delay in updating critical data such as topology could affect the regular system operations. However, by implementing a Circuit Break, the initial Server Benchmark may take longer to complete as it detects and records the big data items. The Circuit Break Benchmark can then collect these items at a lower frequency, resulting in smoother and quicker subsequent Server Benchmarks. Refer to <u>Circuit Break in Server Benchmark</u> for more information.

# 7.2 Topology Accuracy Improvements

## 7.2.1 Open Topology Improvements

The Open Topology team has continuously improved and updated the main logic of the Open Topology algorithm:

- Improve the Proxy ARP in the VLAN Group algorithm to support more complex network situations.
- Support "Generic Device" in Open Topology.
- Optimize the performance.
- Use the Adaptive Plugin to address more customer cases, including:
  - Improve the HA support for more Vendors and technologies.
  - Improve the VSS/VDS logic.
  - Support the sub-Interface case with Duplicate IP in different VRFs.
  - Support the Palo Alto Firewall using L2 Zone to connect different VLANs.
- Remodel the Virtualization model to restrict the related interfaces to the Child device only.
- Provide more plugins to improve the troubleshooting ability.

## 7.2.2 One IP Table Improvement

Certain IP/MAC entries in the One IP table do not have a corresponding switchport because of the NDP neighbor in the domain. Due to this, users cannot determine the connected switchport and hence cannot locate the IP/MAC in their network. To solve this issue, R11.1 adds two columns, **gateway** and **possible switch port** into One IP table.

One-IP Table								🕑 Help 🔺 🔍 🗙
Resolve All DNS	Show Unknown	End System Only						
Items: 129							Search by IP/I	MAC/LAN/DNS Name Q 🕴 🕚
IP Address	LAN Segment	MAC Address	Vendor	Switch Port	Possible Switch Port	VLAN ID DNS Name	Gateway	Description Data Sour
172.24.101.51	172.24.101.0/24	00b0.c275.8c00	Cisco Systems, Inc	BJ-L2-Core-A.FastEth	BJ-L2-Core-A.FastEthernet0/15	10		Port_con_Juniper_"n ARP Ta 🔷
172.24.101.52	172.24.101.0/24	0010.0b0e.27ff	Cisco Systems, Inc	BJ-L2-Core-A.FastEth	BJ-L2-Core-A.FastEthernet0/15	10		Port_con_Juniper_"n ARP Ta
172.24.101.61	172.24.101.0/24	001c.0fe2.55c6	Cisco Systems, Inc	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.62	172.24.101.0/24	0023.0502.de41	Cisco Systems, Inc	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.64	172.24.101.0/24	0cb6.d2f8.1d20	D-Link International	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.65	172.24.101.0/24	d478.569e.2b40	Avaya Inc	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.66	172.24.101.0/24	d478.569e.0e40	Avaya Inc	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.67	172.24.101.0/24	001c.73ac.b5a6	Arista Networks	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.68	172.24.101.0/24	001c.737a.2ea4	Arista Networks	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.74	172.24.101.0/24	085b.0e5c.e895	Fortinet, Inc.	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/15	10		connect to BJ-3750-1 ARP Ta
172.24.101.229	172.24.101.0/24	0000.0c5c.d8c3	Cisco Systems, Inc	BJ_L2_Core_6.FastEth	BJ_L2_Core_6.FastEthernet0/16	10		connect to Rack_Con ARP Ta

# 7.2.3 Remove Zone Selection from Add Topology Link

Each VLAN Group generates a zone in the Open Topology, causing many zones in the domain. R11.1 removed the zone selection and media option from **Add Topology Link** UI. Users **can add point-to-point L3 and L2** links only.

Add Topology Link			×
Default Zone 🗸			
First Device	Interface	Second Device By Device V	Interface
Search Q	Search Q	Search Q	Search Q
.EMU_NAT_R11		.EMU_NAT_R11	
_for_AWS_IGW		_for_AWS_IGW	
_for_Azure_Internet_Cloud		_for_Azure_Internet_Cloud	
_for_Google_Cloud_Internet_Cloud		_for_Google_Cloud_Internet_Cloud	
00:00:00:00:00		00:00:00:00:00	
10.88.16.1		10.88.16.1	
10.88.19.1		10.88.19.1	
100G-02-GABM-HV-A		100G-02-GABM-HV-A	
50:02:00:07:00:01		50:02:00:07:00:01	
50:02:00:07:00:02		50:02:00:07:00:02	
5101_Router		5101_Router	
7750SR12		7750SR12	
a01231414014001-device0		a01231414014001-device0	
ACI-L3OUT-246		ACI-L3OUT-246	
			Cancel Connect

# 7.3 Circuit Break in Server Benchmark

Collecting a large amount of data may be time-consuming, which could cause Server Benchmarks to run for several hours without completion. This delay in updating critical data such as topology could affect the regular system operations. However, by implementing a Circuit Break, the initial Server Benchmark may take longer to complete as it detects and records the big data items. The Circuit Break Benchmark can then collect these items at a lower frequency, resulting in smoother and quicker subsequent Server Benchmarks.

The Domain admin can use Circuit Break to detect and record large data items in the regular Benchmark task and move them to the Circuit Break Benchmark automatically for low-frequency data collection, which will ensure the regular Benchmark operates at a faster pace. Take the following steps to configure the circuit break:

- 1. Enable/Disable the Circuit Break function globally.
- 2. Define the global threshold of Circuit Break checking.
- 3. Define the scheduling of the Circuit Break Benchmark and view the current status.
- 4. Review all device data items that are triggered by the Circuit Break threshold.
- 5. Review and update customized Circuit Break threshold settings for the individual device data item.

Domain Managem	lent					Support Tenant: shared_tenant Domain	: shared_domain	danny	10 NC
art Page Fine Tune X	Schedule Task × Advanced Settings >	Circuit Break Manager X							
Global Setting									
🛞 Enable Circuit Break 🛛 💽	Triggered Threshold If Data Size is Greater or Equal to:	0.00976 MB Apply	Task Schedule: Weekly Cu	errent Status: Idle 🌒 🦷 Run Now	/ SRefresh				
Benchmark Circuit Break A	list of all device data items that are triggered by	the circuit break threshold	4	Circuit Break Records			Search	Q B	50
Device	Data	Data Size (MB)	Retrieval Time	Last result	Last Retrieve Time	Circuit Break Threshold			
VPL5_CE12	MAC Table	0.01	0m 7s	Succeeded	3/14/2023, 12:02:12 PM	Data Size ? 0 MB			
VRF-P	MAC Table	0.01	0m 43s	Succeeded	3/14/2023, 12:02:04 PM	Data Size ? 0 MB			
Bur-isp-gw1	MAC Table	0.01	0m 18s	Succeeded	3/14/2023, 12:02:00 PM	Data Size ? 0 MB			
VRF-CE4	MAC Table	0.01	0m 44s	Succeeded	3/14/2023, 12:02:00 PM	Data Size ? 0 MB			
Sanjose_Core	MAC Table	0.02	1m 42s	Succeeded	3/14/2023, 12:01:54 PM	Data Size ? 0 MB			
Sanjose_Core	Route Table	0.01	0m 41s	Succeeded	3/14/2023, 12:01:54 PM	Data Size ? 0 MB			
QinQ+MGMT	MAC Table	0.04	0m 32s	Succeeded	3/14/2023, 12:01:52 PM	Data Size ? 0 MB			
Emu_NB_NYC_MGMT	MAC Table	0.02	0m 31s	Succeeded	3/14/2023, 12:01:52 PM	Data Size ? 0 MB			
VRF-PE2	MAC Table	0.01	1m 20s	Succeeded	3/14/2023, 12:01:49 PM	Data Size ? 0 MB			
VRF-PE2	Route Table	0.01	1m 18s	Succeeded	3/14/2023, 12:01:49 PM	Data Size ? 0 MB			
Individual Setting A list of the	e threshold settings for individual device data		•	Individual Threshold	•				
2 Items 👔 Delete All			•	Setting for Device D	ata		Search	Q	G Refres
)evice	Data			Data Size (MB)		Circuit Break Threshold			
BJ_L2_Core_4	Rout	e Table		0.01		Data Size is Unlimited			
BJ_L2_Core_5	Rout	e Table		0.01		Data Size ≥ 20 MB			

## 7.3.1 Circuit Break Global Settings

By default, the Circuit Break function is turned OFF, and it can be turned ON when there is a large amount of data in the user network, causing delays or inability to complete the Server Benchmark.

:	ii Doi	main Manageme	ent	🝳 Sup
	Start Page	Schedule Task $~ imes$	Circuit Break Manager $ imes$	
	Global Se	tting	·	
	ကြို့ Enab	le Circuit Break 🛛 🚺	Triggered Threshold 50 MB	Apply

The Circuit Break uses the data size as the threshold for retrieving live data in the Server Benchmark. The default system-wide threshold is 50 MB.

Do	main Manageme	nt	o Sup
Start Page	Schedule Task $~ imes$	Circuit Break Manager $ imes$	
Global Se	etting	,	
င့်ဦး Enab	ole Circuit Break 🛛 🚺	Triggered Threshold     50       If Data Size is Greater or Equal to:     50	MB Apply

The Circuit Break will check the following data retrieved in the Server Benchmark:

• Each data item in the Retrieve Live Data section, including the System Tables and NCT Tables.

Edit Benchmark	Task
Task Name:	Basic System Benchmark Description: Default system benchmark task
Frequency	Device Scope Retrieve Live Data CLI Commands Additiona
Stop :	retrieving after Hours 0 Minutes
⊿ — Bu	ailt-in Live Data
	Configuration File
	MAC Table
	STP Table
	Inventory Information of Device/Interface/Module
	CT Table
<b>Z</b> A	Access Policy
<b>Z</b> 4	ARP Switch Table
<b>V</b> /	ARP Table[Mac Learning Type]
<b>Z</b> /	AWS ELB Listener Table
<b>Z</b> /	AWS ELB Target Group Table
<b>Z</b> 4	AWS Endpoint Service Table
<b>Z</b> /	AWS ENI Interface Table
<b>Z</b> /	AWS Firewall Policy Table
<b>Z</b> /	AWS Firewall Stateful Rule Table

• Each CLI Command in the CLI Commands section.

Task Name:	Basic System Benchmark	Description: Default	system benchmark task		
Frequency	Device Scope	Retrieve Live Data	CLI Commands	Additi	onal Operations after Benchmark
Enter Com	nmands				
Enter Co	mmand	Select Devic	е Туре	✓ Add	
Comma	and			Device Type	
show ve	ersion			3Com Switch;Ar	ista Switch;Aruba IAP;Aruba LWAF
show in	terface			Arista Switch	

The data size is the size of the raw data in each item listed above for an individual device. If a data item has sub-items, the data size is the total amount of all raw data of the main item and sub-items.

For example: If R1 has 5 VRFs configured, the Route Table of R1 will include one default routing table and 5 VRF routing tables. The data size of the Route Table for R1 is the total amount of the default routing table plus 5 VRF routing tables.

## 7.3.2 Execute Circuit Break Check in Server Benchmark

When executing Server Benchmark, two checks need to be performed for each data to be collected:

- Before collecting each piece of data, check whether it has been recorded in the Circuit Break Manager. If it has been recorded, do not collect it.
- After collecting each data, check whether it triggered the Circuit Break threshold. If triggered, record it in Circuit Break Manager.

## 7.3.3 Manage Circuit Break Data

All Device Data items that trigger Circuit Breaks in Server Benchmark will be recorded in the Circuit Break Manager.

Domain Manager	ment				🙆 Supp	ort Tenant: shared_tenant Domain	: shared_domain 🚨 danny 🕜 I
tart Page Fine Tune X	Schedule Task X Advanced Setting	IS X Circuit Break Manager X					
Global Setting	Triggered Threshold If Data Size is Greater or Equal t	to: 0.00976 MB Apply	Task Schedule: Weekly C	rrent Status: Idle 🜖 Run Now	ि Refresh		2 Search and Filter items in the data
Benchmark Circuit Break	A list of all device data items that are triggere	ed by the circuit break threshold	Sort by Each Colur	n			Search 🔍 📴 🖏
Device	Data	Data Size (MB)	Retrieval Time	Last result	Last Retrieve Time	Circuit Break Threshold	
B VPLS_CE12	MAC Table	0.01	0m 7s	Succeeded	3/14/2023, 12:02:12 PM	Data Size ? 0 MB	
VRF-P	MAC Table	0.01	0m 43s	Succeeded	3/14/2023, 12:02:04 PM	Data Size ? 0 MB	3
Bur-isp-gw1	MAC Table	0.01	0m 18s	Succeeded	3/14/2023, 12:02:00 PM	Data Size ? 0 MB	Export to CSV F
VRF-CE4	MAC Table	0.01	0m 44s	Succeeded	3/14/2023, 12:02:00 PM	Data Size ? 0 MB	
SanJose_Core	MAC Table	0.02	1m 42s	Succeeded	3/14/2023, 12:01:54 PM	Data Size ? 0 MB	
SanJose_Core	Route Table	0.01	0m 41s	Succeeded	3/14/2023, 12:01:54 PM	Data Size ? 0 MB	
QinQ-MGMT	MAC Table	0.04	0m 32s	Succeeded	3/14/2023, 12:01:52 PM	Data Size ? 0 MB	
Emu_NB_NYC_MGMT	MAC Table	0.02	0m 31s	Succeeded	3/14/2023, 12:01:52 PM	Data Size ? 0 MB	
VRF-PE2	MAC Table	0.01	1m 20s	Succeeded	3/14/2023, 12:01:49 PM	Data Size ? 0 MB	
VRF-PE2	Route Table	0.01	1m 18s	Succeeded	3/14/2023, 12:01:49 PM	Data Size ? 0 MB	
ndividual Setting A list of t	the threshold settings for individual device da	ata					
2 Items 📲 Delete All							Search Q 😋 Refr
		Data		Data Size (MB)		Circuit Break Threshold	
evice							
evice BJ_L2_Core_4		Route Table		0.01		Data Size is Unlimited	

Users can set individual Device Data of the Circuit Break thresholds according to their actual situation. For example, if the data size for the routing table of the core router is larger than the default Circuit Break threshold, but the user still wants to get data in the Server Benchmark, it can be achieved by modifying the thresholds.

Start Page Circuit Break Ma	anager	<							
Global Setting		Triggered Threshold If Data Size is Greater or Equal to: 0.00097 MB Apply Task Schedule: C	nce Cu	urrent Status: Idle 🌒 🦳 Run Noi	N C Refres	h			
Benchmark Circuit Break	A list of all	device data items that are triggered by the circuit break threshold				Search	2 ۵	3 8	0
Device	Data	Circuit Break Threshold Setting	×	st Retrieve Time	Circuit Break Thresh	old			
aci-QA-SW1	FHRP Tal			2/2023, 12:13:48 PM	Data Size >= 0 MB				
Cisco-10W-ARP	ARP Tabl	Choose Setup Type: 1 Item Select	ted	22/7 23, 12:13 View Device Log	e >= 0 MB				
Cisco-10W-ARP	MAC Tab	F		Edit Threshold	e >= 0 MB				
Cisco-10W-ARP	NDP Tab	Oata Size is Unlimited		22/2023, 12:13:4	e >= 0 MB				
Cisco-10W-ARP	Route Ta			2/2023, 12:13:44 PM	Data Size >= 0 MB				
an NATT-MGMT	FHRP Tal	O Data Size is Greater or Equal to: 50 MB	_	22/2023, 12:13:39 PM	Data Size >= 0 MB				÷
		Cancel OK							

- Choose the "Data Size is Unlimited", which means that this data item does not run Circuit Break checking, which is the default selection.
- The "Data Size is Greater or Equal to" can be chosen to assign a specific data size value to the data item.

# 7.3.4 Run Circuit Break Benchmark

Dom	ain Management 🙆 Support Tenant: shared_tenant Domain: shared_domain 🙎 danny	😗 Net
itart Page	Fine Tune × Schedule Task × Advanced Settings × Circuit Break Manager × Schedule Setting and Task	
Global Setti	ng Running Status	
င့်၌ Enable	Circuit Break D Triggered Threshold 0.00976 MB Apply Task Schedule: Weighty Current Status: Idle 🕕 Run Now 😋 Refresh	
Cir	cuit Break Threshold Setting	×
Benchm 19 Items	Stop retrieving after Hours O Minutes 2 The time limit for data retrival	G Ø
Device		
Emu_N	Start Date: 2023-03-12 💼 🗆 End Date: 2023-03-13 📾 Time Zone: (UTC-05:00) Eastern Time (US & Canada) 🗸 🚺	
😁 VRF-PE:		
🕲 VRF-PE:	Once 3 Schedule Settings	
😁 bjta002	Weekly Every: 1 weeks on:	
S VRF-CE	🔿 Monthly 🗹 Sunday 🗹 Monday 🗹 Tuesday 🗹 Wednesday 🗹 Thursday 🗹 Friday 🗹 Saturday	
NHRP-S	Start Time Everyday: 10 V : 16 V AM V Use Current Time	
Individu		
2 Items		Refresh
Device		
a Bj_L2_C		
BJ_L2_C		
	Cancel Submit	

- 1. When the Circuit Break function is enabled, the system will automatically create a Circuit Break Benchmark task, and all device data items in the Circuit Break table will be included in this task.
- 2. In some user networks, device access is allowed only within a specified time range. The "Stop retrieving after" option can define the time limit for data collection.
- 3. Using a lower frequency to collect the device data items in the Circuit Break Benchmark task is recommended. Circuit Break Benchmark supports run Once (manual execution), Weekly and Monthly.

Information summary can be viewed after the Circuit Break Benchmark is finished.

Global Setting							
爵 Enable Circuit Break	Triggered Thresh	old 0.00097	MB Apply	Task Schedule:	Once Current Status: Idle 🕵 Run Now	Refresh	
Panchmark Circuit Pr	ante a tra di la da da da sera	that are triggered by the circuit	heast thrashold	1	Last Run Time: 3/22/2023, 12:10:19 PM Duration: 3m 56s		
6984 Items	eak A list of all device data items	unat are triggered by the tirtuit	oreak threshold	i	Total Items Retrieved: 755 Total Data Size: 118.55 MB	Sea <mark>r</mark> ch	9 8 8 6
6984 Items Device	Data	Data Size (MB)	Retrieval Time	Last result	Total Items Retrieved: 755 Total Data Size: 118.55 MB Next Run Time: 1/2/3000, 12:00:00 AM	Sector	Q B 8 (
6984 Items Device ACI-QA-SW1	Data FHRP Table	Data Size (MB) 0.00	Retrieval Time	Last result	Total Items Retrieved: 755 Total Data Size: 118.55 MB Next Run Time: 1/2/3000, 12:00:00 AM	Seo ch cuit Break Threshold	9.00
6984 Items Device ACI-QA-SW1 Cisco-10W-ARP	Data FHRP Table ARP Table	Data Size (MB) 0.00 61,47	Retrieval Time 1m 32s 0m 31s	Last result	Total Items Retrieved: 755 Total Data Size: 118.55 MB Next Run Time: 1/2/3000, 12:00:00 AM 	Search cuit Break Threshold	Q B S (

# 7.4 System-wide Intent Execution Workload Control

The system is expected to process the intent execution from different sources efficiently, and meanwhile, the stable operation of the system will not be affected by a large number of requests.

Moreover, the priority of intents and urgency to run intents differ. For example, an intent of compliance checks may be executed once a month, and their delay time can be long, such as 1 week, while the intents to help troubleshoot must be executed in a short time.

R11.1 introduces a new setting for intent: *max\_execution\_delay,* and the system utilization can also be controlled in this version:

- Inside Intent, a field "*max\_execution\_delay*" has been added for the maximum time gap of a NI from submission to execution. By default, it is set as 5 minutes. When executing an intent, the service will check if the interval between the current time and the submission time is greater than the max execution delay time. If so, it means the intent was submitted too long ago, and the execution of the intent will be aborted.
- Before each NI is executed, it will be checked whether it needs to be executed: If the same NI has been
  executed before and there is a result, then the execution of the same NI within the max execution delay
  time will be skipped, and the result of the previous NI will be reused for the new execution request. If
  the system is still executing an NI and receives the same NI execution request, the execution of the

subsequent NI request will be skipped if the request time interval is within **2** \* *max\_execution\_delay*, and the result of the previous NI execution will be reused.

- The backend process can monitor the system utilization (server CPU, memory, etc.) in real-time. Requests will be processed only when the utilization is within the specified range (80%, configurable in the database), preventing the system from being busier by more requests.
- The intent requests have priority: all intent execution requests from PAF are submitted to the backend system for execution at LOW priority, while those from TAF are at HIGH priority (priority is divided into SUPPER, HIGH, and LOW).
- To protect the system from being overwhelmed by the API requests, users can set the API request threshold (5000 in the API request queue, configurable in the database by the system administrator) that the system can accept. If the accumulated API request exceeds the threshold, the API requests from the 3rd-party system will be discarded and cannot enter the system.
- Users can set the number of waiting tasks supported by TAF to prevent the impact of many tasks. By default, the number of waiting tasks is up to 30 in a worker server, and this value can be configured in the database.

# 7.5 Lock and Single Editing Control

The files of many key features (Network Intent/Map/Bot/ADT...) in NetBrain can be created by a user and used by many others. R11.1 improves the lock/unlock function with the editing rights control function in NetBrain.

Lock a File by User1	
Lock Settings $ imes$	
Lock Last Modified by James Green on 9/2/2023	Provide Password to Edit by User2
O Without Password	Verify
With Password: Confirm Password:      Lock Annotation:      This file is currently locked by James Green whom you can contact to get more details.	This file is currently locked by James Green whom you can contact to get more details. Please enter password to continue: *** Cancel Continue
Cancel OK	
- Users with editing rights can lock a file with or without a password.
- Other users who want to edit the file must provide the password if needed.
- The creator and users with the "Domain Admin" role can freely edit a file without a password.

### 7.5.1 Lock Function

The Lock function protects users' important files from being modified casually. Here are two typical use scenarios for applying this function:

- The creator of a file (such as intent and map) can lock it with a password to prevent other users from modifying it.
- For teamworking, the creator of a file locks it with a password and shares it with other team members.
   Users who are not team members can only view the file.

Users can lock files with or without a password and provide lock annotation to other users. If the file is locked with a password, other users can edit the file after entering the password.

Lock Settings	×
Lock Last Modified by James Green on 9/2/2023	
O Without Password	
With Password:     Confirm Password:	
Lock Annotation:	
This file is currently locked by James Green whom you can contact to get more details.	
Cancel OK	

- The information about who modified the lock settings and the modification time are displayed on the Lock Settings dialog.
- To define the lock settings, users must meet one of the following conditions:
  - A creator of the file.

- A user (who is not the creator of the file) with Editing Rights, e.g., the "Shared Resource and File Management" privilege.
- A user with the "Domain Admin" role.
- The lock settings of the original file will not be kept in the new one after saving as or copying the file. However, the settings will be kept after the file is exported/imported.

## 7.5.2 Single-editing Control

Users in the same domain may simultaneously operate with the same file in NetBrain. If several users edit the file simultaneously, the file may be overwritten or cannot be saved. To address this issue, we introduce "Single-editing Control" to ensure that only one user can edit a file simultaneously.





#### 7.5.3 Related Features

The above logic can be applied to Network Intent/Map/ADT/Bot/Network Intent Cluster in R11.1. However, there may be adjustments for every feature based on each one's specificity.

Feature	Lock Function	Single-editing Control
Network Intent	Editing Rights: "Shared Resource and File Management" privilege.	The same as the
	When to Verify: users click "Edit", e.g.	basic concept.

	Network Intent (View Mode) - All Network Intents/R&D/Zhao Xu/Multicast Tree Copy X	
	I Multicast Tree Copy (Published) (7) □ 0 🖒 0 📈 Edit 🗮	
	Result: 03/24/2023 02-23 PM 👻 👩 Embedded Incident 🗸 🛣 🏵 Run 👻 with Live Network	
	This intent execution is finished at 03/24/2023 02:23 PM with 9 errors. You can View Execution Log  1 Denice. Enhancement 2021 1 1 to real after particular the tradition of the barreline of the tradition of the	
	Control - Durge over      Control - The group 224 https://www.control.metr	
Мар	Editing Rights: Map Owner	Use the "Map
	When to Verify: users click "Save", e.g.	Owner" control as
	📽 Stencils 🐛 Map 🗰 Network 🥶 Guidebook   😥 + 140% 🐵 😫 < 🗙	before.
	Save Map (Ctrl+S)	
ADT	Editing Rights: "Shared Resource and File Management" privilege.	This concept is
(Automation	When to Verify: users click "Enable Editing", e.g.	not used in R11.1.
Data Table)	📆 Automation Data Table Manager	
	Search Q C « 🖷 Automation Data Table Builder Last Updated at: 3/3/2022 3:30 PM No Scheduled Update 💽 Update Now	
	Shared Tables     Items: 6 Rows 7 Column     O This ADT is locked     Enable Editing     X	
	Im Security Zones of network     Device     Image: Solution of the solution	
	AB Tables      My Tables  Blue e0/1 12.10.10.10/24 Check Interface Status2There aren't	
Bot	Editing Rights: "Shared Resource and File Management" privilege.	The same as the
	When to Verify: users click "Edit", e.g.	basic concept.
	Example 1 - NY, DC1 Network Automation Last edited by: Chris. Zhao@netbr C Enabled & Share Edit	
	Usage: Used 4 times by 2 users         20	
	► Start	
	W DCI 12 General Check	
Network Intent	Editing Rights: "Shared Resource and File Management" privilege.	The same as the
Cluster	When to Verify: users click "Save", e.g.	basic concept.
	👶 2-WAN Link Failover Check 🗶 🛛 Help Author: NetBrain Cancel Save As Save	Check the
	Description: In this sample, each Member NI contains 4 devices of 2 sites and every 2 devices are active and standby device are sective and standby even active active and sta	condition when
		clicking "Save"
	2. Seed NI 3. Seed Logics	

## 7.6 Support Plus

Support Plus aims to check the health status of NetBrain IE systems online/offline so that system improvements can be made promptly according to the report.

In R11.1, Support Plus provides more metrics in the report, helping customers monitor and have better insights into the system's health and performance.

	🉀 Alert Rules	G Refresh 🗕 admin 🔻	😮 Help
	Search Dee	Delete Aged Data	0
c 15	Search Kep	Support Log	~
Created Time	Last Updated Time	Support Dius	
2022-11-18 10:50:50 AM	2022-11-18 10:51:52 AM		
2022-11-17 03:38:32 PM	2022-11-17 03:38:35 PM	Log Analysis	
2022-11-10 10:56:43 AM	2022-11-10 10:56:50 AM	Log Out	
2022-11-02 01:41:47 PM	2022-11-02 01:41:50 PM		
2022-10-31 11:16:10 AM	2022-10-31 11:16:13 AM		

Number	System Health List	ltems
1	Server Firewall & Port Information	<ul> <li>Check if the firewall of each server is turned on and if the port of each component is open.</li> <li>Whether the firewall is enabled</li> <li>Whether the incoming ports of MongoDB, Elasticsearch, RabbitMQ, and Redis are open</li> <li>Whether the outgoing port of the Front Server and the incoming port of the Front Server Controller are open</li> <li>Whether the outgoing ports of SMTP and IMAP are open</li> </ul>
2	External Network connectivity	<ul> <li>Check the network connectivity required for specific needs:</li> <li>Whether the email-sending port is connected</li> <li>Whether Teams can be connected to the Internet</li> <li>Whether ShareFile can be connected to the Internet</li> </ul>

3	Multi-DC Configuration	<ul><li>Whether Multi-DC is implemented</li><li>Whether Multi-DC is configured properly</li></ul>
4	Auto Data Clean Check	<ul> <li>List the time when the data clean was last executed. Users can determine if the data clean works properly from it.</li> <li>List the data clean status of each data type, i.e., whether it's enabled</li> <li>List the clean rule for each data type, i.e., when the old data should be deleted</li> </ul>
5	Notification Setting	<ul> <li>Check if the System Email Setting has been enabled and defined.</li> <li>Check if the Service Monitor Alert Setting has been defined. The email receiver and the alert rule must be defined.</li> </ul>
6	Auto-update Information	<ul><li>Check if the auto-update has been enabled.</li><li>Check the last result for auto-update</li></ul>
7	MongoDB	<ul> <li>MongoDB Metrics         <ul> <li>Check the status of the replica set</li> <li>Check the status and role(master/secondary/arbiter) of each node</li> <li>The number of currently open files</li> <li>If the Majority Read Concern has been enabled for the MongoDB cluster</li> </ul> </li> <li>MongoDB Data Size Check: The data size in each domain</li> <li>MongoDB Slow Queries: Slow queries and their correlated metrics</li> </ul>
8	RabbitMQ	<ul> <li>RabbitMQ Metrics:</li> <li>Check the status of the RabbitMQ cluster</li> </ul>

RabbitMQ Queue Check: Check if there is an abnormal queue in
RabbitMQ and if consumers exist

#### 7.7 Auto Update Improvements

In previous versions, all system admins received an email notification when a system update succeeded or failed, or when a new patch was available. In R11.1, a system admin can select who will receive these emails. Only the selected users can receive the notifications. Admins can make the selection at any time, and the selection will be applied when the next update is performed.

System Management		_				🔔 admin 🛛	og Out	19 NG
ne Page 🛛 License 👋 Tena	nts X User Accounts X Proxy Manager X Front	t Server (	Controllers ×	Email Settings × Adva	nced Settings × System U	odate ×		
	Current Version: 10.1.9.0 0				Email Notification: 2 Users			G Refres
	Successfully installed version 10.1.9.0.							
	1/17/2023, 3:04:13 PM Executor: admin			View Test Results	View Installation Log			
	Automatically check the latest version Last checked on: 1/1	17/2023, 5	5:36:39 PM		Check Update Now			
	Download and Install Platform Resources Automatical	Select U	sers for Email Notifi	cation 2				×
	Latest Available Version: 10.1.9.1  Release Note	2 Users	Selected 🚯			Search		٩
			Username	Email	Phone Number	Description		
			admin	@netbrainte	ch.com	description		
			nguo	@gmail.	com	NB@331Share		
	View Update History							
								or

Running the pre-check before auto-update can verify the environment's readiness, preventing issues such as malfunctions of the service monitor.

To prompt users to run the pre-check tool, a pop-up window will appear when they upload a patch and click **Schedule**. Clicking the **running the pre-check tool** link in the window will take users to a webpage with the user guide, which includes instructions for completing the system and environment check.

## 7.8 New Vendor Support

#### 7.8.1 Support NSX-T

R11.1 supports NSX-T with the following functions:

- Discover NSX-T components such as T0/T1 Gateways, Segments, N-VDS Transport Nodes, Edge Nodes, etc. This enriched data helps understand better the network's configuration, dependencies, and potential bottlenecks.
- Create the map to visualize the NSX-T infrastructure, such as the topology of Logic Components like T0/T1 Gateways, Segments and Virtual Machines, which provides a comprehensive view of the network topology, enabling users to identify and troubleshoot potential issues in their NSX-T environment.





• Discover the AB path between the two endpoints inside or outside the NSX-T networks. The path calculation can also support checking DFW Policy, Gateway Policy, NAT and Load Balancer, which can help analyze the security, traffic flow or load balancing quickly and visually.



• View NSX-T operation status by applying data views driven by the API parser.

### 7.8.2 Other Device Type Support

Besides NSX-T, R11.1 also supports the following new device type:

- Juniper MIST: support the discovery of Juniper MIST AP and the L2 Wireless Topology.
- **Aruba Orchestrator** (Silver Peak, or Aruba SD-WAN): supports Aruba WAN Optimizer and Router. The system retrieves the configuration files, routing tables, APR tables, and NDP tables through the API.
- **Fortinet SD-WAN**: support the discovery of the ForiManager and Forinet ForiGate Firewall through API and retrieve the configuration files and routing tables through API.

## 7.9 Security Improvement

R11.1 resolved the following CVEs in R11.1 from 3rd Party Libraries (C/H/M/L is the priority, meaning Critical/High/Medium/Low):

CVE-2021-29921 C       Python       3.10.9         CVE-2022-37454 C	CVE	Associated Library	Fixed version
CVE-2021-23336 M	CVE-2021-29921 C CVE-2022-37454 C CVE-2020-27619 C BZip2 in Python (CVE-2019-12900) C CVE-2015-20107 H CVE-2022-0391 H CVE-2022-0391 H CVE-2020-10735 H CVE-2020-10735 H CVE-2022-42919 H CVE-2022-45061 H CVE-2021-3737 H Zlib in Python (CVE-2018-25032) H CVE-2021-3733 M CVE-2021-3426 M CVE-2021-23336 M	Python	3.10.9

CVE	Associated Library	Fixed version
CVE-2021-4189 M CVE-2013-0340 M		
CVE-2022-35737 <b>H</b>	SQLite3	3.40.0
<u>CVE-2020-10543</u> <b>H</b> <u>CVE-2020-10878</u> <b>H</b> <u>CVE-2020-12723</u> <b>H</b>	Perl	5.32.1.1
<u>CVE-2022-29117</u> H	Microsoft.Owin	4.2.2
<u>CVE-2022-41881</u> <b>H</b>	Netty-Codec-Haproxy	4.1.90
<u>CVE-2022-41854</u> M <u>CVE-2022-38752</u> M	SnakeYAML	1.33
<u>CVE-2022-38900</u> H	Decode-URI-Component	0.2.2
CVE-2022-24999 <b>H</b>	QueryString	6.11.0
CVE-2022-0536 M	Follow-Redirects	1.15.2
<u>CVE-2022-21189</u> C	Dexie.js	3.2.2
CVE-2022-31160 M	JQuery UI	1.13.2
<u>CVE-2021-32840</u> <b>C</b> <u>CVE-2021-32842</u> <b>M</b>	SharpZipLib	1.3.3
CVE-2021-44732 C CVE-2021-43666 H CVE-2020-36475 H CVE-2020-36476 H	MbedTLS (used in Redis C++ client)	Removed from 10.1.9/R11.1 Replaced with () redis- plus-plus

CVE	Associated Library	Fixed version
CVE-2020-36478 <b>H</b>		
CVE-2020-22741 H		
CVE-2020-36426 H		
CVE-2020-36477 M		
CVE-2021-24119 M		
CVE-2020-10941 M		
CVE-2019-16910 M		

# 8 Cases Resolved in R11.1

The followings are customer cases resolved in R11.1 since the last major release of R11. Please note that this is a completed list.

- Case **00153154**: Fixed the issue that the dynamic search with an IP address is not working when proceeding with the site segregation operation due to an Elasticsearch synchronization problem.
- Case **00152949**: Support for manual gateway selection in path calculation.
- Case **00150847**: It takes a long time to log in if there are many domains.
- Case **00153653**: Benchmark task running for 24+ hours when updating site maps.
- Case 00151489: Unable to run password change scripts on Cisco Routers and Switches due to lack of <send enter>.
- Case **00152785**: CLI access issue with HP ProCurve Switch caused by vt100 context handle logic error.
- Case **00153828**: Velocloud Path tracing is not working with SDWAN devices via Live Data source.
- Case **00153762**: Aruba WLC configuration file update failed due to an extra underline in the hostname.
- Case 00153684: PAF not displaying/sending alerts.
- Case **00153578**: Search/Map for End Hosts not working properly.
- Case **00154011**: Incorrect switchport info on One-IP Table and wrong I2 connections to other switches.
- Case **00152299**: Site Visio maps size is 0 KB when exported using benchmark task.
- Case **00153524**: MPLS Cloud path failing no route to next hop device.
- Case **00152920**: Benchmark takes a long time due to CLI threads reinitiating issue.
- Case **00153517**: Recurring decode not running without selecting update baseline.
- Case **00153256**: Cannot search some devices in Site search and global search if the config files are larger than 16MB.

- Case **00152886**: Show counters with the Include bar for only "0 0 0 0" cannot be displayed in the runbook.
- Case **00151857**: Incorrect L2 topology and One IP table entries based on PAN virtual Mac.
- Case **00146775**: Portal SSO Integration Support.
- Case **00150245**: L3 topology for the switch device is not built for the IP unnumbered interfaces.
- Case **00152343**: Unify search return data format by adding object-group and object network.
- Case **00151947**: Decommissioned devices are removed from Missed Devices table after System Benchmark.
- Case **00149717**: New API for Domain Metrics Plugin.
- Case **00152482**: Sites display problem when moving devices from Unsigned to leaf sites.
- Case **00152335**: Failed to update device info due to null PyFuncContext.
- Case **00151710**: Configuration comparison does not work properly if API config is selected for Firepower.
- Case **00151988**: Schedule Task Succeeded with warnings due to exceptional data in HP switch configurations.
- Case **00150356 & 00150449**: Error while exporting Site details in Excel File format.
- Case **00151491**: Integrating Audit and system monitor logs to Splunk.
- Case **00151991**: The help link is incorrect on the Missed Device page.
- Case **00151600**: Checkpoint NCT Policy Table not complete after live path.
- Case **00151420**: NI Global Data Table Subtable showing empty.
- Case **00150970**: Remove "The site was rebuilt" messages received on ALL site maps.
- Case **00151563**: Delete old, cached files to reduce swap usage on the Worker server automatically.
- Case **00150778**: New plugin API to delete all Fine Tune-unknown ip.
- Case **00151110**: L2 topo build stuck during the benchmark.

- Case **00149980**: MongoDB high disk utilization due to data clean not working for some domains.
- Case **00150996**: Solve domain creating performance issue.
- Case **00150951**: L2 topology build takes a long time during the Benchmark.
- Case **00076382**: New feature to export the user list in NetBrain.
- Case **00150652**: Add support for new BGP peer template command to MPLS L3 VPN Cloud.
- Case **00150108**: Getting UnicodeDecodeError when tracing path using current baseline.
- Case **00147921**: Unable to generate domain health report with error message "The domain health report is being created by other users. Please try again later. "
- Case **00148718**: Support Ignore config block (multi-lines) for Comparison logic.
- Case **00150652**: Add support for new BGP peer template command for MPLS L3 VPN Cloud.
- Case **00148962**: The user can not choose the email subject identifier.
- Case **00150179**: IP from one IP table cannot be displayed on the map with the error message "TypeError: Cannot read properties of undefined (reading 'id')".
- Case **00150219**: Servers getting disconnected in the service monitor due to ES performance problems.
- Case **00149896**: SNMP access timed out for Cisco Meraki Firewall and Cisco ACI Leaf Switch, Spine, APIC in Validation.
- Case **00150400**: Path failure due to setting the wrong port mode after switchport command Arista Switch.
- Case **00148570**: Device login session is not cleaned in front server Juniper Router.
- Case **00148665**: Support a new format when building the cloud routing table and comparing as a path.
- Case **00150277**: Miss L2 topology from the Palo Alto Firewall to the Juniper EX SW.
- Case **00149376**: Inaccessible devices not being sent to the "Missed Devices" list.
- Case **00149138**: Velocloud Exception: in ngJson::Value::asCString(): requires string Value.

- Case **00149745**: Triggered Diagnosis events are long pending and are not getting through.
- Case **00149286**: Error while making API calls to Netbrain due to duplicate site name.
- Case **00149220**: MPLS path not working as expected due to destination IP load logic defect.
- Case **00149388**: Policy Table Comparisons are not working on Checkpoint firewalls.
- Case **00149507**: VRT in Business Cloud missing B Routes from CE device BGP Advertised Route.
- Case **00149714**: Azure route lookup should check the route AS-Path value to show the active path with a bold line.
- Case **00150041**: Change Management templates don't load due to multiple selection templates.
- Case **00148553**: Add more error logs for SNOW app integration.
- Case **00149469**: Portal login issue with access code with error message "The user has no permission to login".
- Case **00148694**: The Next hop device is not available in the routing table as the next hop IP is a duplicated IP on the HA device interface.
- Case **00148841**: The uploaded logo does not appear on the login page.
- Case **00149016**: Guidebook diagram fails to initialize.
- Case **00149340**: NCT Compare is not working on some Azure nodes due to duplicate data in the data engine.
- Case **00149419**: L2 topology building time is long, and the performance needs to be optimized.
- Case **00148659**: Cisco ACI Leaf Switches are wrongly shown in the Missed Devices after being rediscovered.
- Case **00148786**: More missing switch port entries are found in the One IP table due to the L2 logic changes since IEv10.
- Case **00148915**: Feature request–API for retrieving portal access key.
- Case **00149122**: Request to restrict API access to the parser if the user does not have private resource management permission.

- Case **00147645**: The device count shown in the Fine Tune result, and Inventory Report is different. A plugin is provided to delete duplicated devices.
- Case **00148655**: Duplicated VRF subtables are shown in the BGP Received Route table, but there is only one VRF subtable Fortinet FortiGate Firewall.
- Case **00148735**: The Interface description in the subnet manager is not populated properly.
- Case **00148339**: NIC Failed to update Baseline with an error "An item with the same key has already been added."
- Case **00147510**: Support Office 365 SMTP/IMAP OAuth2.0.
- Case **00147590**: Webserver shut down with the error "Cannot read configuration file".
- Case **00147284**: Display N/A instead of retrieval failure since Interface Information is not defined in the End System driver.
- Case **00147917**: Fail to update Palo Alto configuration with empty hostname error due to large configuration file not saved in drive in time.
- Case **00146200**: Checkpoint Opsec manager is not working.
- Case **00147939**: Entries in One IP-table doubling during the build process.
- Case **00147709**: Management ip disappears in Tune live device of the silver peak.
- Case **00147678**: Ping result inconsistency in Device Log and Fine Tune Report.
- Case **00146542**: Cisco Meraki Firewall CLI Config Retrieval Failed.
- Case **00148399**: There is no topology for the Baracuda firewall due to failure to parse interface information.
- Case **00145332**: SNMP proxy forwarder support for Netbrain Front Server.
- Case **00147739**: Config parser does not show data for Cisco IOS XR device for IEv10.1.
- Case **00147366**: Benchmark crash in Build VLAN Group step.
- Case **00144319**: Unable to Delete Parser in the Shared Folder, error "Unable to perform the operation due to invalid Knowledge Cloud authentication".

- Case **00147123**: No L2 Topo for ACI leaf device's specific VPC port. The physical interface on the VPC port needs to be displayed on the ACI leaf device.
- Case **00147473**: Traceroute node throws an unknown error because Traceroute is not using the login script from the driver.
- Case **00147701**: Getting ACI L2 neighbor servers with BOND. The physical interface on the VPC port needs to be displayed on the ACI leaf device.
- Case **00133340**: Add export to Excel for Audit Log.
- Case **00144876**: [Public Cloud] Add Northbound API to Edit API Server Include/Exclude VNets.
- Case **00145923**: All Palo Alto firewall configs retrieve failed in benchmark and discovery.
- Case **00146264**: Cannot import Automation Library caused by the security policy.
- Case **00146624** Netbrain is not loading the config for the selected dates.
- Case **00146335**: Benchmark succeeded even though vCenter failed due to insufficient license.
- Case **00146657**: Issues with L3 mapping NIC.
- Case **00146729**: Last Accessed Time in Fine Tune wording issue.
- Case **00146771**: Subtask LiveRetrieveMultiDevice ended but failed with an error.
- Case **00146846**: Unable to create Device Health report with error "Failed to generate a new report".
- Case **00146928**: Support Full-Text Search.
- Case **00147153**: Unable to create Device Health report with error "Failed to generate a new report" due to multiple records isCurent=true in DB.
- Case **00147233:** Import ticket does not work.
- Case **00144967** Path failure for ACI endpoints with traceback error in next hop check due to too many subnets in one VLAN interface.
- Case **00146043**: Cannot adjust the L2 connections for the port channel link.

- Case 00146048: Basic System benchmark warning "Subtask BuildVlanGroup ended, but failed with error..."
- Case **00146603:** Schedule discovery Discovery over node license limit not saved.
- Case **00145635**: Device cannot be found during Dynamic Discovery for MPLS cloud.
- Case **00146157**: Interface parsing issues- Aryaka SD-WAN.
- Case **00145165**: Unable to pull any data(config, route) from Aryaka SDWAN devices via SNMP.
- Case **00145496**: Network Change stuck on one device when checking Pre-check Hostname before Execution.
- Case **00145854**: Unable to find Layer2 after benchmark due to an error when dealing with HRSP data.
- Case 00145352: Unable to create Device Health report with error "Failed to generate a new report".
- Case 00145634: Resolve Latest CLI Configuration Retrieval Failed on Palo Alto Firewall.
- Case **00144583**: L2 Path failing -Fortinet FortiGate Firewall.
- Case **00144445**: Benchmark error Subtask BuildVlanGroup ended but failed with an error.
- Case **00143758**: Site Maps L2 & L3 connection is not populating post 10.1 version upgrade.
- Case **00143492**: Path is not moving forward to Viptela boxes.
- Case **00144180**: Ignored DAW alerts still making devices red on site maps.
- Case 00144384: Getting Old Domain Health Report While Exporting.
- Case **00142952**: The map data was not completely exported.
- Case **00143818**: Dynamic Map L3 Topology-PortChannel Links Issue.
- Case **00144150**: Retrieve live Data won't run when we play runbook.
- Case **00143667**: Path not working after upgrade due to MPLS Cloud L3 Topo issue.
- Case **00143693**: Adding cloud objects to L2 site maps.
- Case **00143844**: Benchmark Timeout error due to too many NetScreen Firewalls having the same IP.

- Case **00142752**: Benchmark is slow because all the telnet sessions are taken and not released automatically.
- Case **00143017**: After upgrade, unable to collect logs on Dell EMC switches when the last line contains 'bel' char(0x07).
- Case **00143316**: Path gateways must always be selected, even for old paths.
- Case **00143450**: SSH connection failed when setting "version=1" in fix\_livesetting.ini on Linux FS.
- Case **00143637**: When calculating a path, the gateway resolve is very slow due to too many interfaces in one device.