cisco.



Cisco SD-Access ファブリックからのデータの収集と分析

ファブリックデータ収集の概要 2 ファブリックデータ収集ツールの使用 2 バンドルの分析 5 改訂: 2021 年 10 月 15 日

ファブリックデータ収集の概要

ファブリックデータ収集ツールを使用すると、Cisco Software-Defined Access(SD-Access)ファブリックからデータを 簡単に収集することができます。ツールはコマンドのプリセットリストを使用して、選択したすべてのデバイスに接続 します。また、ツールはこれらのコマンドを実行して出力をバンドルします。このアプローチの主な利点は、すべての ファブリックデバイスからほぼ同時に大量の情報が収集されることです。ファブリック内部で問題が発生した場合は、 後で原因と解決策を分析することができます。ツールは自動的に情報を収集するため、その時点でのファブリックの状 態のスナップショットを提供します。

ファブリックデータ収集ツールの使用

次の手順は、Fabric Data Collectionツールの使用方法を示しています。

手順

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (=) をクリックして選択します[Tools] > [Network Reasoner] の 順に選択します。

Cisco DNA Center				Q (?) (2)			
印 Design 〒 Policy 문 Provision		Discovery Topology Command Runner	Take a Tour 💿 Learn More				
 ∠ Assurance 2 Workflows 3 Tools C Platform O Activity 	> > >	License Manager Template Editor Model Config Editor Wide Area Bonjour Security Advisories Network Reasoner	P2 View Details	Trends and Insights Last 30 Days Throughput Coverage Capacity View Details			
E Reports	Sign Out						

ステップ2 [Network Reasoner] ウィンドウには、Network Reasoner ツールのコレクションがあります。[Validated Tools] 領域で、Fabric Data Collection ツールを見つけます。



Q 🕐 🖉

Be Insightful with Network Reasoner

Automated Cisco expertise brought to your network through the Network Reasoner to proactively evaluate your network, or to reactively diagnose complex problems.

	۲	7
CPU Utilization Troubleshoot causes for high CPU Utilization on a device	Fabric Data Collection Collect show command outputs from network devices to troubleshoot issues in a Fabric	Power Supply Determine the root cause for power supply problems on a device.
Affected Devices: 0/last 24 hrs 🕦 Network Impact: Low	network Network Impact: Low	Affected Devices: 0/last 24 hrs ① Network Impact: Low
<u> </u>	t↓	

ステップ3 [Fabric Data Collection] をクリックします。[Fabric Data Collection] ウィンドウが表示されます。

ステップ4 左側のペインでロケーションサイトを選択し、ツールに使用するデバイスを選択します。

ステップ5 サイトとデバイスを選択すると、ツールがアクティブになります。[Troubleshoot] をクリックします。

■ Cisco DNA Center	Tools · Network Re	easoner • Fabric D	ata Collection		Q 🕐 🖉	
Network Reasoner > Fabric Data Collection	L. C.					
Eq. Find Hierarchy	Devices (10)					
 	Tilter Tag Device Troubleshoot 10 Selected			Last updated: 10:53 AM 🛛 📿 Refresh		
√	Device Name 🔺	IP Address	Device Type	Site	Reachability 🛈	
> @ Peg	☑ 3850XS_2 ⊖	172.31.255.5	Switches and Hubs	/Brussels/Peg	Reachable	
> & Brussels-Test	✓ 9500_VSL Θ	172.31.255.2	Switches and Hubs	/Brussels/Peg	Reachable	
> 🎄 France > 💩 Ghana	✓ C9407R ⊖	172.31.255.12	Switches and Hubs	/Brussels/Peg	Reachable	
> 🕸 India	✓ FE2050 ☺	172.31.255.50	Switches and Hubs	/Brussels/Peg	Reachable	
> 🖓 L2Brussels	✓ Ø FE2053 Θ	172.31.255.53	Switches and Hubs	/Brussels/Peg	🔗 Reachable	

ステップ6 ツールは、その動作中にデバイスのタイプとファブリック内でのデバイスのロールを判別します。この情報を使用して、デバイスで実行するコマンドと実行しないコマンドがツールにより評価されます。この評価により、デバイスはデバイスのロールに関連するコマンドのみを実行できます。



ステップ7 ツールが出力の収集を完了すると、[Conclusions] タブで結果を確認できます。[Fabric Data Collection] ウィ ンドウの [Root Cause Analysis] 領域で、[Conclusions] タブをクリックします。その他の Network Reasoner ツールが、Fabric Data Collection ツールから受信したデータの分析を提供します。[Conclusions] タブで、バ ンドルファイルをダウンロードします。

=	Cisco DNA	Center Tools	Network Reasoner - Fabric Data Collection	Q	?		
Netv	vork Reasoner >	Fabric Data Collect	ion			×	
ΞQ	Find Hierarchy						
~ &	🗄 Global	Root Cause Analysis Last Run: Jun 24, 2021 10:57 AM			Run Again		
	Unassigned	Reasoning Activity Conclusion	s (1)				
~	🖉 🚳 Brussels						
	> 🖻 Peg	 Download the command ou 					
>	🛞 Brussels2	View Relevant Activities					
>	💩 Brussels-Te						
>	💩 France		Was this sutamated root cause and	lucic ha	Inful?		
>	💩 Ghana		was this automated FOOL cause and	iyata ne	ipidi:		
>	💩 India						
>	💩 L2Brussels						

- **ステップ8** [Conclusions] タブでファイル名をクリックし、収集されたすべての出力を含むファイルをダウンロードします。
- ステップ9 tar コマンドを使用するなど、さまざまな方法でバンドルを取得できます。バンドルファイルが取得される と、ツールが実行されたデバイスのホスト名に対応するさまざまな.txt ファイルが tar コマンドに表示され ます。これらのテキストファイルには、実行されたコマンドと出力が含まれています。これらのテキスト ファイルは通常のテキストファイルです。

#########-M-K4K6:cmd bundle ########\$ tar -xzvf cmd output 9f7962c3-c54a-4a76-9642-05ddf0ca23ae.tar.gz

```
x FE9200-02.txt
x FE2053.txt
x FE9404 1.txt
x FE9200-30.txt
x 9500 VSL.txt
x FE2050.txt
x 3850XS 2.txt
x FE9200-28.txt
x C9407R.txt
#########-M-K4K6:cmd bundle #######$ ls
3850XS 2.txt
                      FE9200-02.txt
9500 VSL.txt
                      FE9200-28.txt
C9407R.txt
                       FE9200-30.txt
FE2050.txt
                       FE9404 1.txt
FE2053.txt
                       cmd output 9f7962c3-c54a-4a76-9642-05ddf0ca23ae.tar.gz
```

バンドルの分析

すべてのデバイスのバンドルファイル内には、すべてのコマンドを含むテキストファイルがあり、任意のテキストエ ディタで表示できます。コマンドは、ほぼ同時にすべてのデバイスで実行されます。この簡単なプロセスにより、さま ざまなデバイスの出力を比較できます。たとえば、エッジデバイスのリストマップキャッシュを、コントロールプレー ンノードからの情報と比較できます。バンドルファイルには複数の機能にまたがる情報が含まれているため、バンドル が取得された時点で SD-Access ファブリックを分析できます。これには、Locator/ID Separation Protocol (LISP) テーブ ル、IP ルーティングテーブル、認証情報、Cisco Trusted Security (CTS) 情報、デバイス設定、さまざまなプラット フォームコマンドなどの情報が含まれます。

バンドルを分析するには、次の2つの方法があります。

- •手動分析を使用して、さまざまなテーブルを比較します。
- SDA_Digger ツールなどのツールを使用してバンドルファイルを分析します。このツールは、特定のイベントと不 整合を検出してアラートを発します。また、分析中に検出された内容の概要も示されます。

次の例は、SDA Digger ツールの出力を示しています。

#########-M-K4K6: #########\$ python3 SDA_Digger.py -b ~/cmd_bundle Session Analysis: CP session to 3850XS_2 not present on FE9200-02 Session Analysis: CP session to 3850XS 2 not present on FE9404 1 Session Analysis: Checked LISP sessions on 8 nodes towards 2 CP nodes. Found 8 sessions, missing 2, failures 0 LISP Database Analysis: d037.4544.5f3e/48 : In LISP database on FE2050(172.31.255.50) CP node: 9500 VSL reports RLOC 10.48.91.173 LISP Database Analysis: d037.4544.5f3e/48 : In LISP database on FE2050(172.31.255.50) CP node: 9500 VSL reports RLOC 10.48.91.173 LISP Database Analysis: Number of EID checked 91, failed 1 LISP Database Analysis: Number of Local EID 29 LISP Database Analysis: Number of Devices checked 8 Map Cache Analysis : Device: FE9200-28 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 23:49:05, Uptime: 1w3d, Map Cache Analysis : Device: FE9200-02 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 04:56:04, Uptime: 1wld, Map Cache Analysis : Device:9500_VSL reporting 4099:172.27.0.0/24 with RLOC 172.31.255.201 in map-cache entry

not present on CP nodes. Expires in 05:28:49, Uptime: 1d18h,

Map Cache Analysis : Device: FE9404_1 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 23:50:19, Uptime: 1w3d,

Map Cache Analysis : Device: FE2053 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 07:52:07, Uptime: 6d16h,

Map Cache Analysis : Device:FE2050 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 06:12:07, Uptime: 1w0d,

Map Cache Analysis : Device:C9407R reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 23:50:09, Uptime: 1w3d,

Map Cache Analysis : Device:FE9200-30 reporting 4099:172.28.253.1/32 with RLOC 172.31.255.2 in map-cache entry not present on CP nodes. Expires in 00:00:00, Uptime: 00:00:00,

Map Cache Analysis : Found 149 entries, verified 22 entry on 8 devices with 8 failures

MTU Analysis: System MTU in fabric 9100, configured on 7 devices, misconfigured on 0 devices

Device-tracking analysis: Verified 7 edge devices with SVI info, 32 success, 0 mismatches 0 info missing Reachability Analysis: Fabric Devices with full (/32) reachabily 8, devices without full reachability 0, not checked 0 CTS Analysis: verified CTS on 9 nodes, 0 failures found

SVI Analysis: Device FE2050 has inconsistent Interface Vlan configuration with all other edge devices SVI Analysis: Analyzed Interface Vlan config on 7 , found inconsistency on 1

このテクニカルノートで説明されている SDA_Digger ツールは公開されており、https://github.com/michelpe/SDA_Digger からダウンロードできます。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意(www.cisco.com/jp/go/safety_warning/)をご 確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、 日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合が ありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サ イトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、 弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, およびCisco Systems ロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。 「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R) この資料の記載内容は2008 年 10月現在のものです。 この資料に記載された仕様は予告なく変更する場合があります。

··|···|·· cisco.

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
 http://www.cisco.com/jp
 お問い合わせ先:シスコ コンタクトセンター
 0120-092-255 (フリーコール、携帯・PHS含む)
 電話受付時間:平日 10:00~12:00、13:00~17:00
 http://www.cisco.com/jp/go/contactcenter/