デジタルネットワークアーキテクチャ(DNA)セン ターのLAN自動化のヒントとテクニック

内容

概要 数珠 前提条件 要件 背景説明 はじめる前に LAN Automationの実行中に実行される手順は何ですか。 トラブルシューティングダイアグラム DNA Center 1.1 LAN Automation関連ログ DNA Center 1.2 LAN Automation関連ログ DNA Center 1.x公開キーインフラストラクチャ(PKI)関連ログ フローチャートに示されているtcpdumpの実行方法を教えてください。 コピーしようとしているbridge.pngファイルは何ですか。 セキュアソケットレイヤ(SSL)通信が期待どおりに動作しない場合のキャプチャの例(この記事に 添付されている.pcapファイル全体) 不正な証明書 考えられる原因: ブラウザを使用して証明書を確認します キャプチャ例 解決方法. DNA Centerが接続をリセットします 考えられる原因: キャプチャ例 証明書関連の問題に関するPnPエージェントでの便利なdebugコマンド 以前に確立された認証済みセッションキーの応答がありません LANの自動化とスタック構成の検討事項 スタックでLANオートメーションを行う方法 LAN自動化タスクにインポートできるホスト名マップファイルの形式は? /mvpnpは1.2のどこに行きましたか。 インベントリエラー

<u>接続は存在しますが、PKI証明書はPnPエージェントに正常にプッシュされません</u>

概要

このドキュメントでは、LANオートメーションがデジタルネットワークアーキテクチャ(DNA)センターで想定どおりに動作しない場合の問題の診断に役立つローカルエリアネットワーク (LAN)オートメーションの概要について説明します。

数珠

<u>プラグアンドプレイ(PnP)エージェント:</u>構成や証明書なしで電源を入れたばかりの新しいデバイ スで、DNA Centerによって自動的に設定されます。

<u>シードデバイス:DNA</u> Centerが既にプロビジョニングし、Dynamic Host Configuration Protocol(DHCP)サーバーとして機能するデバイス。

前提条件

要件

LANオートメーションとプラグアンドプレイソリューションに関する一般的な知識があることが 強く推奨されます。は、LANオートメーションの概要を示していますが、DNA Center 1.0をベー スにしていますが、DNA Center 1.1以降にも同じ概念が適用されます。

背景説明

LAN自動化は、アンダーレイルーティングプロトコルとしてISISを使用してネットワークデバイ スを設定およびプロビジョニングできる、ほぼゼロタッチ導入ソリューションです。

はじめる前に

LAN Automationを実行する前に、PnPエージェントにNVRAMにロードされている証明書がない ことを確認してください。

```
Edge1#dir nvram:*.cer
Directory of nvram:/*.cer
Directory of nvram:/
                                    <no date> IOS-Self-Sig#1.cer
   4 -rw-
                820
                                    <no date> kube-ca#468ACA.cer
                 763
   6 -rw-
   7
                882
                                    <no date> sdn-network-#616F.cer
     -rw-
   8 -rw-
                807
                                    <no date> sdn-network-#4E13CA.cer
2097152 bytes total (2033494 bytes free)
Edge1#delete nvram:*.cer
[プロビジョニング(Provisioning)] > [デバイス(Devices)] > [デバイスインベントリ(Device
Inventory)]ページで、要求されていないデバイスがないことを確認します。
```



CSCvh68847<u>が原因</u>一部のスタックは要求されていない状態のままになり、 ERROR_STACK_UNSUPPORTEDエラーメッセージが表示されることがあります。このメッセ ージは、LANオートメーションがデバイスを単一のスイッチのようにプロビジョニングするよう に要求しようとすると発生します。ただし、デバイスはCatalyst 9300スイッチスタックであるた め、LANオートメーションはデバイスを要求できず、デバイスは要求されていないものとして表 示されます。同様に、PnPはスタックであるため、デバイスを要求しないため、デバイスはプロ ビジョニングされません。

LAN Automationの実行中に実行される手順は何ですか。

DNA Centerは、シードデバイスにDHCP設定をプロビジョニングします。シードデバイスが取得 するIPアドレスの範囲は、サイトのIPアドレスプールを予約したときに定義した初期プールのセ グメントです。このプールは/25以上である必要があります。

注:このプールは3つのセグメントに分割されます。 1. PnPエージェントのVLAN 1にプッシュされるIPアドレス。 2. PnPエージェントのLoopbac0にプッシュされるIPアドレス。 3.シードまたは他のファブリックデバイスに接続するリンク上のPnPエージェントにプッシ ュされる/30 IPアドレス。

DNA CenterがPnPエージェントをプロビジョニングするには、シードデバイスが受信する DHCP設定で、nノードクラスタの場合は、DNA Centerエンタープライズ向けネットワークイン ターフェイスカード(NIC)のIPアドレスまたは仮想IP(VIP)アドレスを指定する必要があります。

PnPエージェントが起動しても、設定はありません。したがって、すべてのポートがVLAN 1の一 部です。その結果、デバイスはDHCPディスカバリメッセージをシードデバイスに送信します。 シードデバイスは、LAN自動化プール内のIPアドレスのオファーを使用して応答します。

LAN自動化の初期シーケンスを理解したので、プロセスが期待どおりに動作しない場合は、トラ ブルシューティングを行うことができます。

トラブルシューティングダイアグラム



DNA Center 1.1 LAN Automation関連ログ

- network-orchestration-service
- pnp-service

DNA Center 1.2 LAN Automation関連ログ

リリース1.2ではPNPサービスがなくなったため、LANオートメーションのトラブルシューティン グを行う際には、次のサービスを探す必要があります。

- ネットワークオーケストレーション
- ネットワーク設計
- connection-manager-service
- onboarding-service (これは1.1に相当する古いpnp-serviceです)

DNA Center 1.x公開キーインフラストラクチャ(PKI)関連ログ

- apic-em-pki-broker-service
- apic-em-jboss-ejbca

フローチャートに示されているtcpdumpの実行方法を教えてください。

sudo tcpdump -i <DNA Center fabric's interface> host <PnP Agent ip address> -w
/data/tmp/pnp_capture.pcap

*これを停止するには、Ctrl+Cを使用します

これにより、pnp_capture.pcapファイルが/data/tmp/に保存されます。セキュアコピー(SCP)コマ ンドを使用してDNA Centerからファイルをコピーするか、次のコマンドを使用してDNA Centerからファイルを読み取る必要があります。

\$ sudo tcpdump -ttttnnr /data/tmp/pnp_capture.pcap [sudo] password for maglev: reading from file capture.pcap, link-type EN10MB (Ethernet) 2018-03-08 20:09:27.369544 IP 192.168.31.1 > 192.168.31.10: ICMP host 192.168.1.2 unreachable, length 36 2018-03-08 20:09:39.369175 IP 192.168.31.1 > 192.168.31.10: ICMP host 192.168.1.2 unreachable, length 36 2018-03-08 20:09:44.373056 ARP, Request who-has 192.168.31.1 tell 192.168.31.10, length 28 2018-03-08 20:09:44.374834 ARP, Reply 192.168.31.1 is-at 2c:31:24:cf:d0:62, length 46 2018-03-08 20:09:50.628539 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [S], seq 1113323684, win 29200, options [mss 1460, sackOK, TS val 274921400 ecr 0, nop, wscale 7], length 0 2018-03-08 20:09:50.630523 IP 192.168.31.1.22 > 192.168.31.10.57234: Flags [S.], seq 2270495802, ack 1113323685, win 4128, options [mss 1460], length 0 2018-03-08 20:09:50.630604 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [.], ack 1, win 29200, length 0 2018-03-08 20:09:50.631712 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [P.], seq 1:25, ack 1, win 29200, length 24

コピーしようとしているbridge.pngファイルは何ですか。

DNA Centerに含まれる191バイトのイメージファイルで、HTTP(証明書を使用しない)または HTTPS(証明書を使用する)を使用してコピーし、DNA CenterとPnPエージェント間の通信をテ ストします。

セキュアソケットレイヤ(SSL)通信が期待どおりに動作しない場 合のキャプチャの例(この記事に添付されている.pcapファイル 全体)

不正な証明書

考えられる原因:

• DNA Centerの証明書の[サブジェクト代替名(SAN)]フィールドに正しいIPアドレスがありません。

証明書のSANフィールドを確認するには、次の手順を実行します。

ブラウザを使用して証明書を確認します



virtual, across campus, branch, WAN and cloud.

- · Add site locations on the network
- · Designate golden images for device families
- Create wireless profiles of SSIDs

lig www	www.cisco.com								
www.cisco.com Root certificate authority Expires: Wednesday, June 5, 2019 at 18:26:44 Central Daylight Time * Details expand									
	Extension	Subject Alternativ	ve Name (2.5.29.17)						
	Critical	NO							
	IP Address	10.88.244.133							
	IP Address	10.88.244.135							
	IP Address	10.88.244.138	SAN						
	IP Address	192.168.31.11	Field						
	IP Address	192.168.31.12							
	IP Address	192.168.31.14							
	IP Address	192.168.31.77							

		🙋 💿 🚞 🗋 🔀 🤇	🖢 🤜 🍳 🤰 🛓	🛓 🐔 👱 🗔 📗	_	27	II				
s	ssi 🛛 🖾 👘										
No.	1	Time	Source	Destination	Protocol Lenn	gth /	Info				
F	1	2018-03-08 14:10:11.073236	192.168.31.1	192.168.31.10	TLSv1.2 2	201 /	Client Hel	llo			
1	2	2018-03-08 14:10:11.079597	192.168.31.10	192.168.31.1	TLSv1.2 20	/95 /	Server Hel	llo, Certificate,	Server	Key Exchange, Ser	ver Hello Done
L	3	2018-03-08 14:10:11.092431	192.168.31.1	192.168.31.10	TLSv1.2	65	Alert (Lev	vel: Fatal, Descr	iption:	Bad Certificate))
	Frama	2: 55 butos on wise (520 bit	102 100 21 1	102 100 21 10	TLC1 0 0	01	Client Hell	11.			
2	Fame	3: 65 Dytes on wire (520 bits	(), 65 bytes captured	(520 D1ts)	1.00 (00.Ed.72.cf						
	thern	et 11, Src: 20:31:24:01:02	2 (20:31:24:01:02),	, Dst: 00:50:73:00:07	190 (00:20:13:00	c//	:90)				
- P - R	302.10	/ Virtual LAN, PRI: 0, CFI: 0,	, ID: 0								
- ▶	intern	<pre>iet Protocol Version 4, Src: 7</pre>	192.168.31.1, Dst: 197	2.168.31.10							
- F	fransm	Aission Control Protocol, Src	Port: 31441, Dst Port	t: 443, Seq: 144, Ack	: 2042, Len: 7						
Ψ.	Secure	a Sockets Layer									
	TLS'	v1.2 Record Layer: Alert (Lev	vel: Fatal, Descriptic	on: Bad Certificate)							
	C	Content Type: Alert (21)									
	V	Version: TLS 1.2 (0x0303)									
	1	Length: 2									
		Alert Message									
		Level: Fatal (2)									
		Description Bad Certificat	te (42)								

解決方法.

サードパーティCA(認証局)がある場合は、DNA CenterのIPアドレスとVIPが含まれた証明書が 提供されていることを確認してください。サードパーティCAがない場合、DNA Centerは証明書 を生成できます。このプロセスの手順については、Cisco TACにお問い合わせください。

DNA Centerが接続をリセットします

考えられる原因:

DNA CenterはデフォルトでTLS v1.2のみをサポートします。

これを回避するには、このガイドに従ってDNA CenterでTLS v1を使用できるようにしてください

キャプチャ例

		<u>a</u> 💿 🖿 [ै 🤇 🔶 🖷) 🖀 🐔 🛓 📃	•		II			
A	pply a	display filter <೫/>									
No.		Time		Source	Destination	Protocol	Length	Info			
	4	2018-03-14 08:20:2	1.563736	10.213.1.20	10.213.1.223	SSL	120	Client Hello			
	5	2018-03-14 08:20:2	1.563773	10.213.1.223	10.213.1.20	TCP	54	443→49365 [ACK	Seq=1 Ack=67	Win=29200 Len=0)
L	6	2018-03-14 08:20:2	1.563926	10.213.1.223	10.213.1.20	тср	54	443→49365 [RST	, ACK] Seq=1 Ac	ck=67 Win=29200	Len=0
F F E E E E E E E E E E E E E E E E E E	<pre>b 2018-03-14 00:2011:123 10:213:122 10:213:123 10:213:120 TCP 54 443:49305 [ACK] Seq=1 ACk=67 Win=29200 Len=0 Frame 4: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) Ethernet II, Src: CiscoInc_cf:90:41 (dc:ce:c1:cf:90:41), Dst: 38:00:4d:9c:3b:b8 (38:00:4d:9c:3b:b8) Internet Protocol Version 4, Src: 10:213:1.20, Dst: 10:213:1.223 Transmission Control Protocol, Src Port: 49365, Dst Port: 443, Seq: 1, Ack: 1, Len: 66 Secure Sockets Layer * SSL Record Layer: Handshake Protocol: Client Hello Content Type: Handshake (22) Version TLS 1.0 (0x0301) Length: 61 * Handshake Type: Client Hello (1) Length: 57 Version: TLS 1.0 (0x0301) * Random Session ID Length: 0 Cipher Suites (9 suites) Compression Methods Length: 1 * Compression Methods (1 method)</pre>										

証明書関連の問題に関するPnPエージェントでの便利なdebugコ マンド

- debug crypto pki transactions
- debug ssl openssl
- debug ssl openssl errores

- debug ssl openssl errors
- · debug crypto pki api
- debug crypto pki transactions
- debug ssl openssl msg

以前に確立された認証済みセッションキーの応答がありません

理論上は、[Provisioning] > [Devices] > [Device Inventory]ページで未請求のデバイスを表示する必要はありませんが、このページから未請求のデバイスを削除した後も、デバイスがhttps://<DNA Center ip>/mynpに表示される問題があります。このシナリオが発生し、PnPログに次のようなログが表示される場合、またはGUIに次のようなログが表示される場合は、デバイスがPnPで未請求として表示されないことを確認します。

ERROR | qtp604107971-170 | | c.c.e.z.impl.ZtdHistoryServiceImpl | Device authentication status has changed to Error(PNP response com.cisco.enc.pnp.messages.PnpBackoffResponse is missing previously established authenticated session key) | address=192.168.31.10, sn=FCW212XXXX

LANの自動化とスタック構成の検討事項

- DNA Center 1.2では、スタックはフルリングである必要があります(2メンバーのスタックに 1本のスタックケーブルが機能しない場合があります)。
- スタックデバイスは、LANの自動化によって迅速に要求する必要があります。これは約10分 未満です。
- DNA Centerに接続されると、PnPでUnclaimedと表示されます。 PnPは、スタックの判別に 10分間の時間枠を使用し、期限が切れると、LANオートメーションの未請求セクションに残 ります。

RCAまたはPnPログがある場合は、未請求のデバイスメッセージを検索できます。

more pnp.log | egrep "(Received unclaimed notification|ZtdDeviceUnclaimedMessage)" メッセージがない場合、要求されていないデバイス通知はDNA Centerに到達せず、PnPはこれを 要求できません。

スタックでLANオートメーションを行う方法

- 1. シードデバイスへのアップリンクをシャットダウンします。
- 2. DNA CenterでLAN Automationを開始します。
- 3. スタックからスタートアップコンフィギュレーションを削除します。# write erase
- 4. NVRAMからすべての証明書を削除します。# delete nvram:*.cer
- 5. vlan.datファイルを削除します。# delete flash:vlan.dat
- 6. プライマリスイッチから、スタンバイスイッチの証明書を削除します。**# delete stby**nvram:*.cer
- a.スタックケーブルを外します。

b.各メンバスイッチのコンソールにログインします。

c.証明書を削除します。# delete nvram:*.cer

d.flas vlanデータベースを削除します。# delete flash:vlan.dat

e.スタックケーブルを再接続します。

7.リブートします。

8.スイッチがスタックとして登録されるまで待ち、すべてのメンバを起動し、初期設定ダイアロ グを開始します。

%INIT: waited 0 seconds for NVRAM to be available

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: 9.シードデバイスへのアップリンクを有効にします。# no shutdown

LAN自動化タスクにインポートできるホスト名マップファイルの 形式は?

DNA Centerでは、次の例に示すように、ホスト名とシリアル番号(ホスト名、シリアル番号)を 含むCSVファイルが必要です。

А	В				
Edge1	FCW2048Cxxx				
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx				
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx				
Edge4	FXS2131Qxxx				

スタックLANオートメーションでは、CSVファイルを使用して、1行に1つのホスト名と複数のシ リアル番号を入力できます。シリアル番号はカンマで区切る必要があります。詳細については、 添付のCSVファイルを参照してください。

/mypnpは1.2のどこに行きましたか。

次のいずれかの方法でPnPにアクセスします。

- Webブラウザで、https://<DNA Center IP>/networkpnpと入力します
- DNA Centerホームページから、次のネットワークプラグアンドプレイツールを選択します。



BETA

Network Plug and Play

A simple and secure approach to provision networks with a near zero touch experience.

または、https://<DNA Center IP>/networkpnpにアクセスします

インベントリエラー

LAN Automation S	tatus			×
		Configuration		
Site:	1412 Main Campus			
Primary Device:	PRHINTERMEDIATE1 piedmonthospita	il.org		
Secondary Device:	none			
IP Pool:	PRH-provisioning-pool 10.87.2.0/23	3		
Device Prefix:	piedmont			
Interfaces:	TenGigabitEthernet2/0/7			5
		Logs		\$
Message				Timestamp +
Started the Network	Orchestration Session with primary devic	e: b967ae20-7ff4-4807-b656-f41f060d7f18	2018-0	06-20 17:32:05.63
		Devices		
	0	0	1	
	Completed	In Progress	Error	
Name	Address	Serial	Status D	
electropet 27		FCW2202G0BM	Inventory Error	

インベントリエラーは、LANオートメーションによって要求され、設定を受信した後、デバイス がインベントリに追加されることを意味します。通常、このエラーは、設定、ルーティング、ま たはCLIクレデンシャルの問題が原因で発生します。

LAN Automationを使用して正しいデバイスを起動しようとしていることを確認するには、優先接 続プロトコル(SSHまたはTelnet)を使用して、デバイス上のloopback 0インターフェイスの IPアドレスにリモートアクセスします。

接続は存在しますが、PKI証明書はPnPエージェントに正常にプ ッシュされません

途中のデバイスで、DNACとPnPエージェント間のパケットの*Don't Fragment(*DF)ビットがオンに なる場合があります。これにより、1500バイトを超えるパケット(通常は証明書を含むパケット)が廃棄される可能性があるため、LAN Automationが完了しない可能性があります。DNA Centerのオンボーディングログに見られる一般的なログの一部を次に示します。 errorMessage=Failed to format the url for trustpoint

この場合の推奨処置は、DNA CenterとPnPエージェントの間のパスで、system mtu 9100コマンドを使用してジャンボフレームが通過できるようにすることです。

Switch(config)# system mtu 9100