ASA DAPを導入してAnyConnectのMACアドレ スを特定する

内容 <u>はじめに</u> 前提条件 要件 <u>使用するコンポーネント</u> <u>背景説明</u> 設定 <u>ネットワーク図</u> <u>ASAでの設定</u> <u>ASDMでの設定</u> 確認 <u>シナリオ1-致するDAPは1つだけです</u> <u>シナリオ2:デフォルトのDAPが一致しています</u> <u>シナリオ3:複数のDAP(Action : Continue)が一致</u> <u>シナリオ4:複数のDAP(Action :Terminate)が一致しています。</u> <u>一般的なトラブルシューティング</u> <u>関連情報</u>

はじめに

このドキュメントでは、AnyConnect接続に使用されるデバイスのMACアドレスを確認するため に、ASDM経由でダイナミックアクセスポリシー(DAP)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。 Cisco Anyconnectとホストスキャンの設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。 ASAv 9.18(4) ASDM 7.20(1) Anyconnect 4.10.07073 ホストスキャン4.10.07073 Windows 10 このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

HostScanは、AnyConnectセキュアモビリティクライアントがネットワーク上でセキュリティポ リシーを適用できるようにするソフトウェアモジュールです。ホストスキャンの処理中に、クラ イアントデバイスに関するさまざまな詳細が収集され、適応型セキュリティアプライアンス (ASA)に報告されます。これらの詳細には、デバイスのオペレーティングシステム、ウイルス対 策ソフトウェア、ファイアウォールソフトウェア、MACアドレスなどが含まれます。ダイナミッ クアクセスポリシー(DAP)機能を使用すると、ネットワーク管理者はユーザごとにセキュリティ ポリシーを設定できます。DAPのendpoint.device.MAC属性を使用して、クライアントデバイスの MACアドレスを事前定義されたポリシーと照合したり、照合したりできます。

設定

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。

	outside	-@-
192.168.1.10	192.168.1.1	

ASAv

Anyconnect PC

义

ASAでの設定

これは、ASA CLIでの最小限の設定です。

tunnel-group dap_test_tg type remote-access tunnel-group dap_test_tg general-attributes default-group-policy dap_test_gp tunnel-group dap_test_tg webvpn-attributes group-alias dap_test enable group-policy dap_test_gp internal group-policy dap_test_gp attributes vpn-tunnel-protocol ssl-client address-pools value ac_pool webvpn anyconnect keep-installer installed always-on-vpn profile-setting

ip local pool ac_pool 172.16.1.11-172.16.1.20 mask 255.255.255.0

webvpn enable outside hostscan image disk0:/hostscan_4.10.07073-k9.pkg hostscan enable anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg 1 anyconnect enable tunnel-group-list enable

ASDMでの設定

ここでは、ASDMでDAPレコードを設定する方法について説明します。この例では、 endpoint.device.MAC属性を条件として使用する3つのDAPレコードを設定します。

- 01_dap_test:endpoint.device.MAC=0050.5698.e608
- ・02_dap_test:endpoint.device.MAC=0050.5698.e605 = AnyConnectエンドポイントのMAC
- 03_dap_test:endpoint.device.MAC=0050.5698.e609

1.01_dap_testという名前の最初のDAPを設定します。

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policiesの順に 移動します。Addをクリックし、図に示すように、Policy Name、AAA Attribute、endpoint attributes、Action、User Messageを設定します。

ection Criteria efine the AAA and en elow and every endpo	dpoint attributes u int attribute has b	used to select this a been satisfied. The	access policy. A policy i se attributes can be cr	s used when a user's a eated using the tables	authorization attributes match below and/or by expanding t	the AAA attribute criteria he Advanced option to
pecify the logical expre	ession text. Ilowing AAA Attrib	utes values		and the following en	dpoint attributes are satisfied	L.
AAA Attribute	Operation	n/Value	Add	Endpoint ID	Name/Operation/Value	Add
cisco.grouppolicy	= dap_t	test_gp	Edit	device	MAC["0050.5698.e608"]	= true Edit
			Delete			Delete
						Logical On
Advanced cess/Authorization Poli onfigure access/autho	cy Attributes rization attributes	s for this policy. At	tribute values specified	here will override those	se values obtained from the A	AA system and the
Advanced cess/Authorization Poli configure access/author roup-policy hierarchy. nat are not specified in Port Forwardin	cy Attributes vrization attributes The resulting VPN n DAP).	s for this policy. At l authorization polic	tribute values specified cy is an aggregation of	here will override thos DAP attributes, AAA a	se values obtained from the A attributes, and group-policy h	AA system and the ierarchy attributes (those
Advanced cess/Authorization Pol configure access/author roup-policy hierarchy. hat are not specified in Port Forwardin Action	cy Attributes rization attributes The resulting VPN o DAP). g Lists Network /	s for this policy. At l authorization polic Bookmarks ACL Filters (client)	tribute values specified cy is an aggregation of Access Method	here will override thos DAP attributes, AAA a Secure Client Webtype ACL	se values obtained from the A attributes, and group-policy h Secure Client Filters (clientless)	AA system and the ierarchy attributes (those Custom Attributes Functions

最初のDAPの設定

AAA属性のグループポリシーを設定します。

add AAA Attribute	2	×
AAA Attribute Type: Cisco		~
Group Policy:	= ~ dap_test_gp	~
Assigned IPv4 Address:	= ~	
Assigned IPv6 Address:	= ~	
Connection Profile:	= V DefaultRAGroup	\sim
Username:	= ~	
Username2:	= ~	
SCEP Required:	= V true	\sim
	OK Cancel Help	

DAPレコードのグループポリシーの設定

エンドポイント属性のMACアドレスを設定します。

Edit Endpoint Attribute		×
Endpoint Attribute Type: Device Host Name:	= ~	
MAC Address:	- ~	0050.5698.e608
BIOS Serial Number:	= ~	
Port Number (Legacy Attribute):	= ~	
TCP/UDP Port Number:	- ~	TCP (IPv4) V
Privacy Protection:	= ~	None (equivalent to Host Scan only) $ \smallsetminus $
HostScan Version:	- ~	
Version of Endpoint Assessment (OPSWAT):	= ~	
ок са	ncel	Help

DAPのMAC条件の設定

2. 02_dap_testという名前の2番目のDAPを設定します。

ption:				ACL Priority: 0	
ction Criteria					
fine the AAA and end low and every endpoin ecify the logical expre	point attributes used to select this nt attribute has been satisfied. The scion text	access policy. A policy ese attributes can be o	reated when a user's a created using the tables	authorization attributes match below and/or by expanding th	the AAA attribute criteria ne Advanced option to
ser has ANY of the fol	lowing AAA Attributes values	\sim	and the following en	dpoint attributes are satisfied.	
AA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
sco.grouppolicy	= dap_test_gp	Edit	device	MAC["0050.5698.e605"]	= true Edit
		Delete			Delete
					Logical Op
dvanced					
dvanced					
dvanced	y Attributes				
dvanced ess/Authorization Polic nfigure access/author oup-policy hierarchy. 1	y Attributes ization attributes for this policy. Ai The resulting VPN authorization poli	ttribute values specifie	ed here will override tho	se values obtained from the A/ attributes, and group-policy hie	AA system and the erarchy attributes (those
dvanced ss/Authorization Polic nfigure access/author pup-policy hierarchy. 1 at are not specified in	y Attributes ization attributes for this policy. Ai The resulting VPN authorization pol DAP).	ttribute values specifie icy is an aggregation o	ed here will override tho	se values obtained from the A/ attributes, and group-policy hie	AA system and the erarchy attributes (those
dvanced ess/Authorization Polic nfigure access/author pup-policy hierarchy. T at are not specified in Port Forwarding	y Attributes ization attributes for this policy. A The resulting VPN authorization pol DAP). Lists Bookmarks	ttribute values specifie icy is an aggregation o Access Method	ed here will override tho of DAP attributes, AAA a Secure Client	se values obtained from the AA attributes, and group-policy hie Secure Client C	AA system and the erarchy attributes (those Custom Attributes
dvanced ess/Authorization Polic nfigure access/author pup-policy hierarchy. T at are not specified in Port Forwarding Action	y Attributes ization attributes for this policy. Af The resulting VPN authorization poli DAP). Lists Bookmarks Network ACL Filters (client)	ttribute values specifie icy is an aggregation o Access Method	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the A/ attributes, and group-policy hie Secure Client C L Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
dvanced ess/Authorization Polici nfigure access/author pup-policy hierarchy. 1 at are not specified in Port Forwarding Action	y Attributes ization attributes for this policy. At The resulting VPN authorization poli DAP). Lists Bookmarks Network ACL Filters (client)	ttribute values specific icy is an aggregation of Access Method	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the AJ attributes, and group-policy hie Secure Client C L Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
Advanced ess/Authorization Polic nfigure access/author oup-policy hierarchy. 1 at are not specified in Port Forwarding Action Action: O Continue	y Attributes ization attributes for this policy. Af The resulting VPN authorization pol DAP). Lists Bookmarks Network ACL Filters (dient) Quarantine Terminate	ttribute values specifie icy is an aggregation of Access Method	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the A/ attributes, and group-policy hie Secure Client C . Filters (dientless)	AA system and the erarchy attributes (those Custom Attributes Functions
idvanced ess/Authorization Polic nfigure access/author pup-policy hierarchy. T at are not specified in Port Forwarding Action Action: O Continue	y Attributes ization attributes for this policy. At The resulting VPN authorization pol DAP). Lists Bookmarks Network ACL Filters (client) Quarantine Terminate	ttribute values specifie icy is an aggregation of Access Method	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the AA attributes, and group-policy hie Secure Client C L Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
dvanced ess/Authorization Polic nfigure access/author pup-policy hierarchy. T at are not specified in Port Forwarding Action Action Specify the message	y Attributes ization attributes for this policy. At The resulting VPN authorization poli DAP). Lists Bookmarks Network ACL Filters (client) Quarantine Terminate that will be displayed when this rec	ttribute values specifie icy is an aggregation of Access Method) e (1) cord is selected.	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the A/ attributes, and group-policy hie Secure Client C L Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
dvanced ess/Authorization Polic nfigure access/author pup-policy hierarchy. 1 at are not specified in Port Forwarding Action Action: Continue Specify the message 1 02_d	y Attributes ization attributes for this policy. At fhe resulting VPN authorization poli DAP). Lists Bookmarks Network ACL Filters (client) Quarantine Terminate that will be displayed when this rec ap_test	ttribute values specifie icy is an aggregation of Access Method) e (i) cord is selected.	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the A/ attributes, and group-policy hie Secure Client C L Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
dvanced ess/Authorization Polici nfigure access/author pup-policy hierarchy. 1 at are not specified in Port Forwarding Action Action: O Continue Specify the message User Message:	y Attributes ization attributes for this policy. At fhe resulting VPN authorization poli DAP). Lists Bookmarks Network ACL Filters (dient) Quarantine Terminate that will be displayed when this rec ap_test	ttribute values specific icy is an aggregation of Access Method a cord is selected.	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the AJ attributes, and group-policy hie Secure Client C . Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions
dvanced ess/Authorization Polic nfigure access/author oup-policy hierarchy. T at are not specified in Port Forwarding Action Action: O Continue Specify the message User Message:	y Attributes ization attributes for this policy. Af The resulting VPN authorization poli DAP). Lists Bookmarks Network ACL Filters (dient) Quarantine Terminate that will be displayed when this rec ap_test	ttribute values specifie icy is an aggregation of Access Method a cord is selected.	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the A/ attributes, and group-policy hie Secure Client C . Filters (dientless)	AA system and the erarchy attributes (those Custom Attributes Functions
Advanced ess/Authorization Polici infigure access/author oup-policy hierarchy. 1 at are not specified in Port Forwarding Action Action: O Continue Specify the message 1 User Message:	y Attributes ization attributes for this policy. A fhe resulting VPN authorization pol DAP). Lists Bookmarks Network ACL Filters (dient) Quarantine Terminate that will be displayed when this rec ap_test	ttribute values specifie icy is an aggregation of Access Method a cord is selected.	ed here will override tho of DAP attributes, AAA a Secure Client Webtype ACI	se values obtained from the A/ attributes, and group-policy hie Secure Client C L Filters (clientless)	AA system and the erarchy attributes (those Custom Attributes Functions

2番目のDAPの設定

3. 3番目のDAPを03_dap_testという名前で設定します。

ription: ection Criteria				ACL Priority: 0	
efine the AAA and end elow and every endpoi pecify the logical expre	point attributes used to select this acc nt attribute has been satisfied. These ssion text.	ess policy. A policy attributes can be c	is used when a user's reated using the table	authorization attributes match the AAA s below and/or by expanding the Advar	attribute criteria nced option to
lser has ANY of the fol	owing AAA Attributes values $$]	and the following e	ndpoint attributes are satisfied.	
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
sco.grouppolicy	= dap_test_gp	Edit	device	MAC["0050.5698.e609"] = true	Edit
		Delete			Delata
					Delete
Advanced ess/Authorization Polic onfigure access/author	y Attributes ization attributes for this policy. Attrib	Dute values specifie	d here will override the	ose values obtained from the AAA syste	Logical Op.
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy. ⁻ at are not specified in	y Attributes ization attributes for this policy. Attrib The resulting VPN authorization policy i DAP).	oute values specifie is an aggregation o	d here will override the f DAP attributes, AAA	ose values obtained from the AAA syste attributes, and group-policy hierarchy a	Logical Op.
Advanced ess/Authorization Polic onfigure access/author oup-policy hierarchy. at are not specified in Port Forwarding Action	y Attributes ization attributes for this policy. Attrib The resulting VPN authorization policy i DAP). Lists Bookmarks Network ACL Filters (client)	oute values specifie is an aggregation o Access Method	d here will override the f DAP attributes, AAA Secure Client Webtype AC	ose values obtained from the AAA syste attributes, and group-policy hierarchy a secure Client Custom / L Filters (clientless)	End the attributes Functions

3番目のDAPの設定

4. more flash:/dap.xml コマンドを使用して、dap.xmlのDAPレコードの設定を確認します。

ASDMで設定されたDAPレコードの詳細は、dap.xmlとしてASAフラッシュに保存されます。これらの設定が完了すると、3つの DAPレコードがdap.xmlに生成されます。dap.xmlで各DAPレコードの詳細を確認できます。



注:DAPが一致する順序は、dap.xmlでの表示順序です。 デフォルトのDAP(DfltAccessPolicy)が最後に一致します。

<#root>

ciscoasa#

more flash:/dap.xml

<dapRecordList> <dapRecord> <dapName> <value>

01_dap_test

</value> <--- 1st DAP name </dapName> <dapViewsRelation> <value>and</value> </dapViewsRelation> <dapBas

dap_test_gp

< 1st DAP group policy <operation>EQ</operation> <type>caseless</type>
endpoint.device.MAC["0050.5698.e608"]
< 1st DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</operation>
02_dap_test
< 2nd DAP name <dapviewsrelation> <value>and</value> </dapviewsrelation> <dapbas< td=""></dapbas<>
dap_test_gp
< 2nd DAP group policy <operation>EQ</operation> <type>caseless</type>
endpoint.device.MAC["0050.5698.e605"]
< 2nd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</operation>
03_dap_test
< 3rd DAP name <dapviewsrelation> <value>and</value> </dapviewsrelation> <dapbas< td=""></dapbas<>
dap_test_gp
< 3rd DAP group policy <operation>EQ</operation> <type>caseless</type>
endpoint.device.MAC["0050.5698.e609"]
<pre> < 3rd DAP MAC Address condition <value>true</value> <type>caseless</type> <operation>EQ</operation></pre>

確認

シナリオ1-致するDAPは1つだけです

1. エンドポイントのMACが0050.5698.e605であり、02_dap_testのMAC条件と一致することを確認します。

2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。

🕙 Cisco	o AnyConne	ct 192.168.1.1 ×	
	Please enter	your username and password.	
_	Group:	dap_test ~	
	Username:	cisco	
	Password:	*****	1
•			
		OK Cancel	
S Cisco	o AnyConne	ct Secure Mobility Client — 🔲 🗙	
	Plea 192	: se enter your username and password. 2.168.1.1 Connect	

ユーザ名とパスワードの入力

3. Anyconnect UIで、02_dap_testが一致していることを確認します。

Cisco AnyConnect	×				
Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following		Sisco AnyConnect Secure Mobility Client	-		×
information to help you understand and remedy the security conditions: 02_dap_test		VPN: Connected to 192.168.1.1. 192.168.1.1		Disconnect	
ОК		00:00:13	1		IPv4

4. ASA syslogで、02_dap_testが一致していることを確認します。

UIでのユーザメッセージの確認



注:ASAでdebug dap traceが有効になっていることを確認します。

<#root>

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true"

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:

Selected DAPs

02_dap_test

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Dec 30 2023 11:46:11: %ASA-4-711001: dap_process_selec selected 1 records

Dec 30 2023 11:46:11: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 11:46:11: %ASA-4-711001:

シナリオ2:デフォルトのDAPが一致しています

1.02_dap_testのendpoint.device.MACの値を、エンドポイントのMACと一致しない0050.5698.e607に変更します。

2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。

3. Anyconnect接続が拒否されたことを確認します。

Cisco AnyConne	ect	×			
C Login	denied. default				
	OK				
Sisco AnyCo	onnect Secure Mol	bility Client	_		×
	VPN: Ready to connect. 192.168.1.1		~	Connect	

UIでのユーザメッセージの確認

4. ASA syslogで、DfltAccessPolicyが一致していることを確認します。



注:デフォルトでは、DfltAccessPolicyのアクションはTerminateです。

<#root>

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

"] = "true"

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: S Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Dec 30 2023 12:13:39: %ASA-4-711001: dap_process_select

selected 0 records

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001:

Selected DAPs

:

DfltAccessPolicy

Dec 30 2023 12:13:39: %ASA-4-711001: DAP_TRACE: Username: cisco, Dec 30 2023 12:13:39: %ASA-4-711001: D

シナリオ3:複数のDAP(Action: Continue)が一致

1. 各DAPのアクションと属性を変更します。

・01_dap_test: dapSelection (MACアドレス) = endpoint.device.MAC[0050.5698.e605] = AnyConnectエンドポイントのMAC アクション=続行

· 02_dap_test:

dapSelection (ホスト名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnectエンドポイントのホスト名 アクション=続行

・03_dap_test DAPレコードの削除

2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。

3. Anyconnect UIで、2つのDAPがすべて一致していることを確認します



注:接続が複数のDAPに一致する場合、複数のDAPのユーザメッセージが統合され、Anyconnect UIに同時に表示されます。

Cisco AnyConnect	×					
Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:	i	🕙 Cisco Any(Connect Secure Mobility Client			×
01_dap_test 02_dap_test			VPIE: Connected to 192.168.1.1.	~	Disconnect	
ОК		00:01:14	2010-2000-2-A		I	Pv4

UIでのユーザメッセージの確認

4. ASA syslogで、2つのDAPがすべて一致していることを確認します。

<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true" Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

...

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: S

02_dap_test

,

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4-711001: dap_process_select

selected 2 records

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:49:02: %ASA-4-711001: D

シナリオ4:複数のDAP(Action :Terminate)が一致しています

1.01_dap_testのアクションを変更します。

・01_dap_test: dapSelection (MACアドレス) = endpoint.device.MAC[0050.5698.e605] = AnyConnectエンドポイントのMAC アクション=終了

・02_dap_test: dapSelection (ホスト名) = endpoint.device.hostname[DESKTOP-VCKHRG1] = Anyconnectエンドポイントのホスト名 アクション=続行

2. エンドポイントで、Anyconnect接続を実行し、ユーザ名とパスワードを入力します。

3. Anyconnect UIで、01_dap_testのみが一致していることを確認します。



注:アクションを終了するように設定されたDAPレコードに一致する接続。終了操作の後、後続のレコードが一致しなくなりました。



UIでのユーザメッセージの確認

4. ASA syslogで、01_dap_testのみが一致していることを確認します。

<#root>

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["

0050.5698.e605

"] = "true" Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.ho

DESKTOP-VCKHRG1

" Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:

01_dap_test

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: dap_process_selec

selected 1 records

Feb 01 2024 08:55:37: %ASA-4-711001: DAP_TRACE: Username: cisco, Feb 01 2024 08:55:37: %ASA-4-711001:

一般的なトラブルシューティング

次のデバッグログは、ASAでのDAPの詳細な動作を確認するのに役立ちます。

debug dap trace

debug dap trace errors

<#root>

Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:55:37: %ASA-4-711001: endpoint.device.MAC["0050.5698.e605"] = "true" Feb

Selected DAPs

: ,01_dap_test,02_dap_test Feb 01 2024 08:49:02: %ASA-4-711001: DAP_TRACE: Feb 01 2024 08:49:02: %ASA-4

 $\underline{https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/108000-dap-deploy-guide.html {\text{tot-hId-based}} to the second seco$

<u>981572249</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。