# エラーメッセージが表示されて失敗するCERバ ックアップのトラブルシューティング

内容	
前提条件	
<u>要件</u>	
<u>使用するコンポーネント</u>	
<u>背景説明</u>	
<u>(「トラブルシューティング」)</u>	
<u>ログ収集</u>	
<u>ログ分析</u>	
<u> 是正アクション</u>	
<u>シナリオ1</u>	
<u>シナリオ2</u>	
<u>関連情報</u>	

### 概要

このドキュメントでは、Cisco Emergency Responder(CER)がバックアップに失敗し、そのステ ータスにエラーメッセージが表示される問題をトラブルシューティング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 Emergency Responder
- セキュリティ証明書の基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

Cisco Emergency Responder(CER)11.5.4.60000-5

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

クラスタモードで配備されたCERは、バックアップに失敗し、エラーメッセージ「Unable to contact server.MasterまたはLocal Agent could be down」というエラーメッセージが表示されます。

例:

lackup Statu:	5						
Refresh	Cancel						
- Status							
WARNING	3: Unable to contac	t server. Master or Lo	cal Agent cou	ld be down, Backup Completed			
-Backup deta	nils —						
Tar Filename	91	2023-06-21-08	3-02-15.tar				
Backup Devi	ice:	and the second se					
Operation:		BACKUP					
Percentage (	Complete:	52%					
Feature	Server	Component	Status	Result **	5	tart Time	Log File *
CER			0	Unable to contact server. Master or Local Agent could be down			
CER			0	Unable to contact server. Master or Local Agent could be down			
CER			0	Unable to contact server. Master or Local Agent could be down			
CER		and the second sec	0	Unable to contact server. Master or Local Agent could be down			
CER			0	Unable to contact server. Master or Local Agent could be down			
CER			0	Unable to contact server. Master or Local Agent could be down			
CER			0	Unable to contact server. Master or Local Agent could be down			
CER				onable to contact perfer haster of cocar rigent could be donn			

CERバックアップエラーメッセージ

該当するバージョンは11.x以降です。



#### ログ収集

この問題が発生した場合は、ログを収集してできるだけ多くの情報を収集し、問題の原因を特定 して、問題を解決するための正しいアクションプランを決定します。

ログを収集する前に、詳細なトレースとデバッグをアクティブにして、次の手順を実行してくだ さい。

- 1. CER Administration Webページにログインします。
- 2. System > Server Settingsの順に移動します。CERパブリッシャはデフォルトで選択されて おり、CERサブスクライバログも必要な場合は変更できます。
- 3. 「Debug Package List」セクションと「Trace Package List」セクションでSelect Allをクリ ックします。
- 4. Update Settingsをクリックします。

cisco	Cisco Emergency	Responder Administrations Solutions	on				Logged in as:	_	Navigation Searc	Cisco ER Adminis	stration About	✓ Go Logout
System 🕶	ERL • Phone Tracking • E	ERL Membership 👻 User Management 👻	Reports v	Tools 🔻	Help 👻							
Server Set	tings For CERServerGroup											
∩ Modify Se	rver Settings											
Server Na	me * Publisher											
Host Nam												
C Debug F	ackage List Select All Clea	ar All										
CER	DATABASE	CER_SYSADMIN										
CER	REMOTEUPDATE	CER_TELEPHONY										
CER	PHONETRACKINGENGINE	CER_AGGREGATOR										
CER	ONSITEALERT	CER_GROUP										
CER	CALLENGINE	CER_CLUSTER										
CER	PROVIDER	CER_ACCESSPOINT										
CER	AUDIT	CER_CREDENTIALPOLICY										
CER	APPSERVICES											
<u> </u>												
Trace Pa	ckage List Select All Clear	r All										
CER	DATABASE	CER SYSADMIN										
CER	CER REMOTEUPDATE											
CER	CER_PHONETRACKINGENGINE CER_AGGREGATOR											
CER	CER_ONSITEALERT CER_GROUP											
CER	CER_CALLENGINE CER_CLUSTER											
CER	CER_PROVIDER											
CER	AUDIT	CER_CREDENTIALPOLICY										
CER	APPSERVICES											

- Update Settings Cancel Changes -

CERデバッグおよびトレースの有効化

この時点で、問題を再現してください。

問題が複製されたら、Cisco ER Serviceability Webページから複製の試行に適用できるDRSログの収集に進み、次の手順を実行します。

- 1. NavigationからCisco ER Serviceabilityを選択します。
- 2. System Logs > Platform Logs > DRSの順に移動します。

cisco	For Cisco Unified Com	ncy	y Responder S lications Solutions	Serv	riceability		Logged in as:	Navigation Cisco ER Serviceability Go Search Documentation About Logout
Tools 👻	SNMP • System Monitor •	S	ystem Logs 👻 Help 👻					
DRS Log	Files		CER Logs	•				
Download	]		Platform Logs	•	CLI			
	File Name	7	DB Logs	•	CLM	Las	Modified 🔻 🔺	File Size 🛡 🛆
			CLI Output Files	-	Certificate Management /			
			SLM Logs	1	DDS			
				_				
					Install/Upgrade			
				_	Remote Support			

CERによるDRSログの収集

ログ分析

ログを分析すると、サーバがピアとの接続を確立しようとしている場所が表示され始め、ログに エラーの原因を示すエラーメッセージが表示されます。

CERパブリッシャDRF MAログから、次の操作を実行します。

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: Number of entries in IPSec trustStore : 1 2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient:drfQueryTruststore - 20時間ご とにトラストストアをクエリする 2023-06-21 07:58:58,168 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker:クライアントへの入出力ストリームを作成できません 致命的なアラートを受信しました:無効な証明書

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run: /IP:Portからクライアン トソケット要求を受信しました

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] – クライアント要求がクラスタ内のノード からのものかどうかを検証しています

2023-06-21 08:04:46,278 DEBUG [NetServerWorker] – 検証済みクライアント。IP =

10.10.20.25ホスト名= device.test.org。要求はクラスタ内のノードからのものです

2023-06-21 08:04:46,278 DEBUG [NetServerWorker] -

drfNetServerWorker.drfNetServerWorker:作成するソケットオブジェクトInputstream 2023-06-21 08:04:46,313 ERROR [NetServerWorker] -

drfNetServerWorker.drfNetServerWorker:クライアントへの入出力ストリームを作成できません。致命的なアラートを受信しました:無効な証明書

CERパブリッシャのDRFローカルログから:

2023-06-21 07:58:47,453 DEBUG [main] - drfNetServerClient:Reconnect, Unable to connect to host: [X], message: Connection refused (Connection refused), cause: null

証明書が正しくないため、接続が拒否されていることが、この時点まで確認できます。

バックアップ/リストア用にノード間で信頼できる接続を確立するために使用される証明書は IPSecです。この時点で、問題の原因が、期限切れのIPSec証明書か、サーバの1つに誤った証明 書が存在することに関連していることはすでに判別できます。

#### 是正アクション

- 1. すべてのCERサブスクライバノードのIPSec-trust証明書のシリアル番号(SN)を確認します 。これは、CERパブリッシャのIPSec.premのSNと一致している必要があります(シナリオ 1)。
- 2. CERパブリッシャノードでIPSec.pem証明書の有効性を確認します。日付が有効であるか、 IPSec証明書が再生成される必要があります(シナリオ2)。

#### シナリオ 1

CERが公開したサブスクライバとCERサブスクライバの間でIPSec証明書のSNが一致しません。 次の手順を実行します。

- 1. シリアル番号がCERパブリッシャのシリアル番号と一致しないCERサブスクライバの IPSec-trust証明書を削除します。
- 2. CERパブリッシャから「IPSec.pem」をダウンロードします(パス:Cisco Unified OS

Show - Settings -	Security   Software Upgrades   Set	vices 🔻 Help 🔻		
Certificate List	Certificate Management			
Generate Self.sinn	Certificate Monitor			
45 contrate contrate	Certificate Revocation			
Status	IPSEC Configuration			
i records found	Bulk Certificate Management			
Certificate List	(1 - 2 of 2)			
Find Certificate List v	where Certificate v begins with	•	Find	Clear Filter 💠 😑
Certificate *	Common Name	Type	Кеу Туре	Distribution
ipsec	and the second second	Self-signed	RSA	and the second second

Administration > Security > Certificate Management > Find

3. 信頼証明書として必要なCERサブスクライバのファイル「IPSec.pem」をパスCisco Unified OS Administration > Security > Certificate Management > Upload the certificate as IPSectrustにアップロードします。



CER ipsec.trust証明書のアップロード

4. すべてのCERノードでDRF LocalサービスとDRF Masterサービスを再起動します。

シナリオ2

IPSecは期限切れのため、再生成する必要があります。次の手順を実行します。

- 1. クラスタ内の各サーバで、Cisco Unified OS Administration > Security > Certificate Managementの順に移動します。パブリッシャから開始し、各サブスクライバを開始します
- 2. CERパブリッシャから開始して、Findをクリックし、サーバ内のすべての証明書を表示します。
- 3. 証明書「IPSec.pem」をクリックします。
- 4. これにより、証明書情報が表示され、Regenerateをクリックします。

Certificate Details for	
Regenerate 💽 Gen	erate CSR 🔋 Download .PEM File 🔋 Download .DER File
Challer	
Status Status: Ready	
Certificate Settings	
File Name	ipsec.nem
Certificate Purpose	ipsec
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly nam	e) Self-signed certificate generated by system
Certificate File Data-	
[ Version: Serial Number: SignatureAlgorithm: Issuer Name: Validity From: To: Subject Name: Key: Key value:	
Regenerate Generate	CSR Download .PEM File Download .DER File
Close	

CER ipsec.pemの再生成

- 5. 証明書がCERパブリッシャで再生成され、Successメッセージが表示されたら、CERサブス クライバノードでステップ1 ~ 4を繰り返します。
- 6. すべてのノードで証明書が再生成されたら、次のサービスを再起動します。
  - ・ CERパブリッシャのみのCisco DRF Master:
    - CER Serviceability > Tools > Control Center Services > Cisco DRF Masterに移動 します

Tools	<ul> <li>SNMP - System Monitor - System Logs - Help -</li> </ul>
Contr	ol Center
Contr	ol Center Services
Sta	rt Stop Restart Refresh
	Service Name
0	A Cisco DB Replicator
0	CER Provider
0	Cisco Audit Log Agent
0	Cisco CDP
0	Cisco CDP Agent
0	Cisco Certificate Expiry Monitor
0	Cisco DRF Local
۲	Cisco DRF Master

CER Cisco DRFマスターの再起動

• Cisco DRF Masterサービスがアクティブになったら、最初にCERパブリッシャの Cisco DRF Localを再起動します。

Tools -	<ul> <li>SNMP          <ul> <li>System Monitor              <li>System Logs              <li>Help              </li> </li></li></ul> </li> </ul>
Contro	ol Center
-Contr	ol Center Services
Star	t Stop Restart Refresh
	Service Name
0	A Cisco DB Replicator
0	CER Provider
0	Cisco Audit Log Agent
0	Cisco CDP
0	Cisco CDP Agent
0	Cisco Certificate Expiry Monitor
۲	Cisco DRF Local
0	Cisco DRF Master

CER Cisco DRFのローカル再起動

- CERパブリッシャノードでCisco DRF Localサービスがアクティブになったら、すべ てのCERサブスクライバノードでこのサービスを再起動します。
- 7. すべてのノードでサービスを再起動した後、システムの手動バックアップを実行します。
  - Disaster Recovery System > Backup > Manual Backupの順に移動します。
  - バックアップデバイス名を選択します。
  - バックアップの機能を選択します。
  - クリックしてバックアップを開始します。

## 関連情報

<u>CERのログの収集方法</u>

<u>CUCM証明書の再生成</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。