



Amazon EC2 データコレクタの設定

Cloud Insights

Tony Lavoie, Dave Grace
August 26, 2021

目次

Amazon EC2 データコレクタの設定	1
要件	1
設定	1
詳細設定	2
IAM Access Key	2
IAM ロール	2
Amazon タグを Cloud Insights アノテーションにマッピングする	3
追加リージョンを含める	3
AWS の子アカウントから収集しています	3
トラブルシューティング	4

Amazon EC2 データコレクタの設定

Cloud Insights は、Amazon EC2 データコレクタを使用して、インベントリとパフォーマンスのデータを EC2 インスタンスから取得します。

要件

Amazon EC2 デバイスからデータを収集するには、次の情報が必要です。

- 次のいずれかが必要です。
 - IAM ロール認証を使用している場合は、Amazon EC2 クラウドアカウント用の * IAM ロール *。IAM ロールは、Acquisition Unit が AWS インスタンスにインストールされている場合にのみ適用されます。
 - IAM Access Key 認証を使用している場合は、Amazon EC2 クラウドアカウントの * IAM Access Key * ID と Secret Access Key。
- 「組織のリスト」権限が必要です
- ポート 443 HTTPS
- EC2 インスタンスは、仮想マシンまたは（自然に）ホストとしてレポートできます。EBS ボリュームは、VM で使用されている仮想ディスクと、仮想ディスクの容量を提供するデータストアの両方として報告できます。

アクセスキーは、アクセスキー ID（AKIAIOSFODNN7EXAMPLE など）とシークレットアクセスキー（wJalrXUtl/K7MDENG/bPxRfCYEXAMPLEKEY など）で構成されます。Amazon EC2 SDK、REST、またはクエリ API の処理を使用している場合は、アクセスキーを使用して EC2 にプログラム経由の要求に署名します。これらのキーは、Amazon の契約に付属しています。

設定

次の表に従って、データコレクタフィールドにデータを入力します。

フィールド	説明
AWS リージョン	AWS リージョンを選択します
IAM ロール	AWS の AU で取得した場合にのみ使用します。の詳細については、以下を参照してください " IAM ロール "。
AWS IAM Access Key ID	AWS IAM Access Key ID を入力します。IAM ロールを使用しない場合は必須です。
AWS IAM Secret Access Key の略	AWS IAM Secret Access Key を入力します。IAM ロールを使用しない場合は必須です。
AWS が API 要求を課金することを理解している	このチェックボックスをオンにすると、Cloud Insights ポーリングで作成された API 要求を AWS から課金することを理解できます。

詳細設定

フィールド	説明
追加リージョンを含める	ポーリングに含める追加領域を指定します。
クロスアカウントロール	異なる AWS アカウントのリソースにアクセスするためのロール。
インベントリポーリング間隔 (分)	デフォルトは 60 です。
「除外」または「含める」を選択して、タグによる VM のフィルタリングに適用します	データの収集時にタグを使用して VM を含めるか除外するかを指定します。「含める」が選択されている場合、タグキーフィールドを空にすることはできません。
VM をフィルタするタグキーと値	+ タグのフィルタ * をクリックして、VM のキーとタグの値に一致するキーと値をフィルタリングして、対象に含める / 除外する VM (および関連ディスク) を選択します。タグキーは必須です。タグ値はオプションです。タグ値が空の場合、タグキーと一致する限り、VM はフィルタリングされます。
パフォーマンスポーリング間隔 (秒)	デフォルトは 1800 です。

IAM Access Key

アクセスキーは、IAM ユーザまたは AWS アカウントの root ユーザの長期的なクレデンシャルです。アクセスキーは、プログラムによる AWS CLI または AWS API への要求に (直接または AWS SDK を使用して) 署名するために使用します。

アクセスキーは、アクセスキー ID とシークレットアクセスキーの 2 つの部分で構成されます。IAM Role `_authentication` ではなく、`_IAM Access Key_authentication` を使用する場合は、要求の認証にアクセスキー ID とシークレットアクセスキーの両方を一緒に使用する必要があります。詳細については、の Amazon のドキュメントを参照してください "[アクセスキー](#)"。

IAM ロール

IAM Access Key 認証ではなく、`_IAM Role_authentication` を使用する場合は、作成または指定するロールにリソースへのアクセスに必要な適切な権限が割り当てられていることを確認する必要があります。

たとえば、`InstanceEc2ReadOnly` という名前の IAM ロールを作成した場合は、この IAM ロールのすべての EC2 リソースに読み取り専用リストアクセス権限を付与するようにポリシーを設定する必要があります。また、このロールがアカウント間でロールを引き受けられることができるように、STS (セキュリティトークンサービス) アクセスを許可する必要があります。

IAM ロールを作成したら、新しい EC2 インスタンスまたは既存の EC2 インスタンスを作成するときに IAM ロールを接続できます。

IAM ロール `InstanceEc2ReadOnly` を EC2 インスタンスに接続すると、インスタンスメタデータから IAM ロール名で一時的なクレデンシャルを取得し、この EC2 インスタンスで実行されているすべてのアプリケーションから AWS リソースにアクセスできるようになります。

詳細については、Amazon ドキュメントを参照してください "[IAM ロール](#)"。

注：IAM ロールは、AWS インスタンスで Acquisition Unit を実行している場合にのみ使用できます。

Amazon タグを Cloud Insights アノテーションにマッピングする

Amazon EC2 データコレクタには、EC2 で設定されているタグを使用して Cloud Insights のアノテーションを入力できるオプションがあります。アノテーションには EC2 タグとまったく同じ名前を付ける必要があります。Cloud Insights では、常に同じ名前のテキスト型アノテーションが入力され、他の型（数値、ブーリアンなど）のアノテーションの入力が「最良の試行」となります。アノテーションのタイプが異なるためにデータコレクタにデータを入力できない場合は、アノテーションを削除してテキストタイプで再作成する必要があります。

AWS では大文字と小文字が区別され、Cloud Insights では大文字と小文字が区別されないことに注意してください。そのため、Cloud Insights で「owner」という名前のアノテーションを作成し、EC2 では「owner」、「OWNER」、「Owner」という名前のタグを作成すると、いずれの EC2 バージョンの「owner」が Cloud Insight の「owner」アノテーションにマッピングされます。

追加リージョンを含める

AWS Data Collector * Advanced Configuration * セクションでは、* Include extra regions * フィールドを設定して、カンマまたはセミコロンで区切って追加のリージョンを含めることができます。デフォルトでは、このフィールドは * us- に設定されており、これによってすべての US AWS リージョンで収集されます。on_all_regions を収集するには、このフィールドを * に設定します。「* include extra regions *」フィールドが空の場合、「* Configuration *」セクションの指定に従って、「* AWS Region *」フィールドに指定されたアセットについてデータコレクタが収集されます。

AWS の子アカウントから収集しています

Cloud Insights では、1 つの AWS データコレクタで AWS の子アカウントの集合がサポートされます。この収集の設定は、AWS 環境で実行されます。

- 各子アカウントに AWS ロールを設定して、メインアカウント ID が子アカウントから EC2 の詳細にアクセスできるようにする必要があります。
- 各子アカウントには、同じ文字列としてロール名を設定する必要があります。
- Cloud Insights AWS Data Collector * Advanced Configuration * セクションの * Cross account role * フィールドに、このロール名の文字列を入力します。

ベストプラクティス：AWS Predefined_AmazonEC2ReadOnlyAccess_policy を ECS メインアカウントに割り当てることを強く推奨します。また、データソースで設定したユーザが AWS に照会するには、少なくとも、Predefined_AWSOrganizationReadOnlyAccess_policy を割り当てる必要があります。

Cloud Insights が AWS の子アカウントから収集できるように環境を設定する方法については、次のドキュメントを参照してください。

"チュートリアル：IAM ロールを使用した AWS アカウント間でのアクセスの委譲"

"AWS のセットアップ：自分が所有している別の AWS アカウントで IAM ユーザにアクセスを付与する"

"IAM ユーザに権限を委任するためのロールを作成する"

トラブルシューティング

この Data Collector の追加情報は、から入手できます ["サポート"](#) ページまたはを参照してください ["Data Collector サポートマトリックス"](#)。

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.