

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7614177号
(P7614177)

(45)発行日 令和7年1月15日(2025.1.15)

(24)登録日 令和7年1月6日(2025.1.6)

(51)国際特許分類

F I

G 0 6 F 9/50 (2006.01) G 0 6 F 9/50 1 2 0 A

請求項の数 20 (全53頁)

(21)出願番号	特願2022-508586(P2022-508586)	(73)特許権者	502303739
(86)(22)出願日	令和2年8月7日(2020.8.7)		オラクル・インターナショナル・コーポ
(65)公表番号	特表2022-544762(P2022-544762		レイション
	A)		アメリカ合衆国 9 4 0 6 5 カリフォル
(43)公表日	令和4年10月21日(2022.10.21)		ニア州 レッドウッド ショアーズ, メー
(86)国際出願番号	PCT/US2020/045514		ル ストップ 5 オーピー7 オラクル パ
(87)国際公開番号	WO2021/030219		ークウェイ 5 0 0
(87)国際公開日	令和3年2月18日(2021.2.18)	(74)代理人	110001195
審査請求日	令和5年7月24日(2023.7.24)		弁理士法人深見特許事務所
(31)優先権主張番号	62/884,931	(72)発明者	ゴヤール, アロック
(32)優先日	令和1年8月9日(2019.8.9)		アメリカ合衆国、9 4 0 6 5 カリフォ
(33)優先権主張国・地域又は機関	米国(US)		ルニア州、レッドウッド・シティ、オ
(31)優先権主張番号	62/884,933		ラクル・パークウェイ、5 0 0、オラク
(32)優先日	令和1年8月9日(2019.8.9)		ル・インターナショナル・コーポレイシ
	最終頁に続く		ョン
			最終頁に続く

(54)【発明の名称】 クラウドインフラストラクチャ環境におけるタグベースのリソース制限または割り当てのためのシステムおよび方法

(57)【特許請求の範囲】

【請求項1】

関連付けられるクラウドインフラストラクチャ環境におけるリソース使用のタグベースの制御のためのシステムであって、

1つ以上のマイクロプロセッサを含むコンピュータと、
前記関連付けられるクラウドインフラストラクチャ環境において定義されるテナンシと、
前記コンピュータと作動的に結合されるメモリデバイスとを備え、前記メモリデバイスは、前記テナンシにおけるリソース使用の前記タグベースの制御を提供するために前記コンピュータによって実行可能な論理を記憶し、前記メモリデバイスは、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表す、タグベースの割り当てデータを記憶し、

前記テナンシにおいてリソースをプロビジョニングする要求が受信され、前記要求は、前記要求の要求特性を表す要求特性データを含み、

前記要求の前記要求特性に対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量が判断され、判断された使用量は前記複数のタグベースの割り当て量と比較され、

前記リソースをプロビジョニングする前記要求は、前記判断された使用量が前記複数のタグベースの割り当て量のうちの1つを超えることに基づいてドロップされる、システム。

【請求項2】

前記テナンシは、前記リソースを格納する複数のコンパートメントを備え、前記複数の

コンパートメントの各コンパートメントは、他のコンパートメント内のリソースの1つ以上の他のセットに対する、前記各コンパートメント内のリソースのセットの隔離を提供し、

前記要求の前記要求特性に対応する前記リソースタグに関連付けられる、前記テナンシにおける前記リソースの前記使用量は、前記複数のコンパートメントにわたってまとめて判断され、前記複数のコンパートメントにわたってまとめて判断された前記使用量は、前記テナンシの前記複数のタグベースの割り当て量と比較され、

前記リソースをプロビジョニングする前記要求は、前記複数のコンパートメントにわたってまとめて判断された前記使用量が前記複数のタグベースの割り当て量のうちの1つを超えることに基づいてドロップされる、請求項1に記載のシステム。

【請求項3】

前記メモリデバイスに記憶された前記タグベースの割り当てデータは、前記テナンシの対応する複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表し、

前記テナンシにおいて前記リソースをプロビジョニングする前記要求の前記要求特性データは、前記要求されたリソースの第1のリソースタイプを表すリソースタイプデータを含み、

前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量が判断され、判断された使用量は前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較され、

前記第1のリソースタイプの前記リソースをプロビジョニングする前記要求は、前記第1のリソースタイプに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、ドロップされる、請求項1または2に記載のシステム。

【請求項4】

前記メモリデバイスに記憶された前記タグベースの割り当てデータは、前記テナンシの対応する複数のユーザグループに割り当てられた前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表し、

前記テナンシにおいて前記リソースをプロビジョニングする前記要求の前記要求特性データは、前記リソースを要求する前記システムのユーザに割り当てられたユーザグループカテゴリを表すユーザグループデータを含み、

前記ユーザグループカテゴリに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量が判断され、判断された使用量は前記ユーザグループカテゴリを割り当てられた前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較され、

前記リソースをプロビジョニングする前記要求は、前記ユーザグループカテゴリに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記ユーザグループカテゴリに割り当てられた前記テナンシにおけるリソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、ドロップされる、請求項1～3のいずれか1項に記載のシステム。

【請求項5】

前記メモリデバイスに記憶された前記タグベースの割り当てデータは、前記テナンシの複数のユーザグループに割り当てられた、前記テナンシの複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、タグベースの割り当て量を表し、

前記テナンシにおいて前記リソースをプロビジョニングする前記要求の前記要求特性データは、i) 前記要求されたリソースの第1のリソースタイプを表すリソースタイプデータと、ii) 前記リソースを要求する前記システムのユーザに割り当てられた第1のユーザグループカテゴリを表すユーザグループデータとを含み、

前記第1のユーザグループカテゴリにプロビジョニングされる前記第1のリソースタイ

10

20

30

40

50

プに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量が判断され、判断された使用量は前記第1のユーザグループカテゴリに割り当てられた前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較され、

前記リソースをプロビジョニングする前記要求は、前記第1のユーザグループカテゴリにプロビジョニングされる前記第1のリソースタイプに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記第1のユーザグループカテゴリに割り当てられた前記第1のリソースタイプの、前記テナンシにおける前記リソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、ドロップされる、請求項1～4のいずれか1項に記載のシステム。

10

【請求項6】

前記メモリデバイスに記憶された前記タグベースの割り当てデータは、前記テナンシの複数のユーザグループに割り当てられた、前記テナンシの複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、タグベースの割り当て量を表し、

前記テナンシのリソース使用量を追跡する第1の要求が受信され、前記第1の要求は、第1のユーザグループカテゴリおよび第1のリソースタイプを表す要求特性データを含み、

前記第1のユーザグループカテゴリによってプロビジョニングされる前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの第1の使用量が判断され、

リソース使用追跡データが、前記第1のユーザグループカテゴリによってプロビジョニングされる前記第1のリソースタイプの、前記テナンシにおける前記判断されたリソースの第1の使用量に基づいて生成される、請求項1～5のいずれか1項に記載のシステム。

20

【請求項7】

前記リソースをプロビジョニングする前記要求は、前記判断された使用量が前記複数のタグベースの割り当て量のうちの1つを超えることに基づいてドロップされ、

前記テナンシの前記リソースをプロビジョニングするオーバーライド要求が受信され、

前記リソースは、前記システムが前記オーバーライド要求を受信することに基づいて選択的にプロビジョニングされ、

前記システムが前記オーバーライド要求を受信したことに応答して前記リソースが選択的にプロビジョニングされることに基づいて、リソース使用過剰データが生成される、請求項1～6のいずれか1項に記載のシステム。

30

【請求項8】

関連付けられるクラウドインフラストラクチャ環境におけるリソース使用のタグベースの制御のための方法であって、

1つ以上のプロセッサと、コンピュータに作動的に結合されるメモリデバイスとを備える前記コンピュータが、前記関連付けられるクラウドインフラストラクチャ環境においてテナンシを提供することを含み、前記メモリデバイスはタグベースの制御論理を記憶し、前記方法はさらに、

タグベースの割り当てデータを前記メモリデバイスに記憶することを含み、前記タグベースの割り当てデータは、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表し、前記方法はさらに、

40

前記テナンシにおいてリソースをプロビジョニングする要求を受信することを含み、前記要求は、前記要求の要求特性を表す要求特性データを含み、前記方法はさらに、

前記1つ以上のプロセッサが前記タグベースの制御論理を実行することによって、前記要求の前記要求特性に対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することと、

前記1つ以上のプロセッサが前記タグベースの制御論理を実行することによって、前記判断された使用量を前記複数のタグベースの割り当て量と比較することと、

前記1つ以上のプロセッサが前記タグベースの制御論理を実行することによって、前記判断された使用量が前記複数のタグベースの割り当て量のうちの1つを超えることに基づ

50

いて、前記リソースをプロビジョニングする前記要求をドロップすることを含む、方法。
【請求項 9】

前記テナンシを提供することは、前記リソースを格納する複数のコンパートメントを提供することを含み、前記複数のコンパートメントの各コンパートメントは、他のコンパートメント内のリソースの 1 つ以上の他のセットに対する、前記各コンパートメント内のリソースのセットの隔離を提供し、

前記使用量を判断することは、前記複数のコンパートメントにわたってまとめて、前記要求の前記要求特性に対応する前記リソースタグに関連付けられる、前記テナンシにおける前記リソースの使用量を判断することを含み、

前記比較することは、前記複数のコンパートメントにわたってまとめて判断された前記使用量を、前記テナンシの前記複数のタグベースの割り当て量と比較することを含み、

前記ドロップすることは、前記複数のコンパートメントにわたってまとめて判断された前記使用量が前記複数のタグベースの割り当て量のうちの 1 つを超えることに基づいて、前記リソースをプロビジョニングする前記要求をドロップすることを含む、請求項 8 に記載の方法。

【請求項 10】

前記タグベースの割り当てデータを記憶することは、前記テナンシの対応する複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することを含み、

前記要求を受信することは、前記要求されたリソースの第 1 のリソースタイプを表すリソースタイプデータを含む要求を受信することを含み、

前記判断することは、前記第 1 のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することを含み、

前記比較することは、前記判断された使用量を、前記第 1 のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、第 1 のタグベースの割り当て量と比較することを含み、

前記要求をドロップすることは、前記第 1 のリソースタイプに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記第 1 のリソースタイプの、前記テナンシにおける前記リソースプロビジョニングの前記第 1 のタグベースの割り当て量を超えることに基づいて、前記要求をドロップすることを含む、請求項 8 または 9 に記載の方法。

【請求項 11】

前記タグベースの割り当てデータを記憶することは、前記テナンシの対応する複数のユーザグループに割り当てられた、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することを含み、

前記要求を受信することは、前記リソースを要求するユーザに割り当てられたユーザグループカテゴリを表すリソースタイプデータを含む要求を受信することを含み、

前記判断することは、前記ユーザグループカテゴリに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することを含み、

前記比較することは、前記判断された使用量を、前記ユーザグループカテゴリに割り当てられた前記テナンシにおけるリソースプロビジョニングの、第 1 のタグベースの割り当て量と比較することを含み、

前記要求をドロップすることは、前記ユーザグループカテゴリに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記ユーザグループカテゴリに割り当てられた前記テナンシにおけるリソースプロビジョニングの前記第 1 のタグベースの割り当て量を超えることに基づいて、前記要求をドロップすることを含む、請求項 8 ～ 10 のいずれか 1 項に記載の方法。

【請求項 12】

前記タグベースの割り当てデータを記憶することは、前記テナンシの複数のユーザグループに割り当てられた、前記テナンシの複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、タグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することを含み、

前記要求を受信することは、i) 前記要求されたリソースの第1のリソースタイプを表すリソースタイプデータと、ii) 前記リソースを要求するユーザに割り当てられた第1のユーザグループカテゴリを表すユーザグループデータとを含むリソースタイプデータを含む要求を受信することを含み、

前記判断することは、前記第1のユーザグループカテゴリにプロビジョニングされる前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することを含み、

10

前記比較することは、前記判断された使用量を、前記第1のユーザグループカテゴリに割り当てられた前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較することを含み、

前記要求をドロップすることは、前記第1のユーザグループカテゴリにプロビジョニングされる前記第1のリソースタイプに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記第1のユーザグループカテゴリに割り当てられた前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、前記要求をドロップすることを含む、請求項8～11のいずれか1項に記載の方法。

20

【請求項13】

前記方法はさらに、

前記テナンシの複数のユーザグループに割り当てられた、前記テナンシの複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、タグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することと、

前記テナンシのリソース使用量を追跡する第1の要求を受信することとを含み、前記第1の要求は、第1のユーザグループカテゴリおよび第1のリソースタイプを表す要求特性データを含み、前記方法はさらに、

前記第1のユーザグループカテゴリによってプロビジョニングされる前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの第1の使用量を判断することと、

30

前記第1のユーザグループカテゴリによってプロビジョニングされる前記第1のリソースタイプの、前記テナンシにおける前記判断されたリソースの第1の使用量に基づいて、リソース使用追跡データを生成することとを含む、請求項8～12のいずれか1項に記載の方法。

【請求項14】

前記方法はさらに、

前記テナンシの前記リソースをプロビジョニングするオーバーライド要求を受信することと、

前記オーバーライド要求を受信することに基づいて前記リソースを選択的にプロビジョニングすることと、

40

前記オーバーライド要求を受信したことに応答して前記リソースが選択的にプロビジョニングされることに基づいて、リソース使用過剰データを生成することとを含む、請求項8～13のいずれか1項に記載の方法。

【請求項15】

関連付けられるクラウドインフラストラクチャ環境におけるリソース使用のタグベースの制御のための命令を有するプログラムであって、前記命令は、コンピュータによって実行されると、前記コンピュータにステップを実行させ、前記ステップは、

1つ以上のプロセッサと、コンピュータに作動的に結合されるメモリデバイスとを備える前記コンピュータが、前記関連付けられるクラウドインフラストラクチャ環境において

50

テナンシを提供することを含み、前記メモリデバイスはタグベースの制御論理を記憶し、前記ステップはさらに、

タグベースの割り当てデータを前記メモリデバイスに記憶することを含み、前記タグベースの割り当てデータは、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表し、前記ステップはさらに、

前記テナンシにおいてリソースをプロビジョニングする要求を受信することを含み、前記要求は、前記要求の要求特性を表す要求特性データを含み、前記ステップはさらに、

前記1つ以上のプロセッサが前記タグベースの制御論理を実行することによって、前記要求の前記要求特性に対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することと、

前記1つ以上のプロセッサが前記タグベースの制御論理を実行することによって、前記判断された使用量を前記複数のタグベースの割り当て量と比較することと、

前記1つ以上のプロセッサが前記タグベースの制御論理を実行することによって、前記判断された使用量が前記複数のタグベースの割り当て量のうちの1つを超えることに基づいて、前記リソースをプロビジョニングする前記要求をドロップすることを含む、プログラム。

【請求項16】

前記テナンシを提供することは、前記リソースを格納する複数のコンパートメントを提供することを含み、前記複数のコンパートメントの各コンパートメントは、他のコンパートメント内のリソースの1つ以上の他のセットに対する、前記各コンパートメント内のリソースのセットの隔離を提供し、

前記使用量を判断することは、前記複数のコンパートメントにわたってまとめて、前記要求の前記要求特性に対応する前記リソースタグに関連付けられる、前記テナンシにおける前記リソースの使用量を判断することを含み、

前記比較することは、前記複数のコンパートメントにわたってまとめて判断された前記使用量を、前記テナンシの前記複数のタグベースの割り当て量と比較することを含み、

前記ドロップすることは、前記複数のコンパートメントにわたってまとめて判断された前記使用量が前記複数のタグベースの割り当て量のうちの1つを超えることに基づいて、前記リソースをプロビジョニングする前記要求をドロップすることを含む、請求項15に記載のプログラム。

【請求項17】

前記タグベースの割り当てデータを記憶することは、前記テナンシの対応する複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することを含み、

前記要求を受信することは、前記要求されたリソースの第1のリソースタイプを表すリソースタイプデータを含む要求を受信することを含み、

前記判断することは、前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することを含み、

前記比較することは、前記判断された使用量を、前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較することを含み、

前記要求をドロップすることは、前記第1のリソースタイプに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記第1のリソースタイプの、前記テナンシにおける前記リソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、前記要求をドロップすることを含む、請求項15または16に記載のプログラム。

【請求項18】

前記タグベースの割り当てデータを記憶することは、前記テナンシの対応する複数のユーザグループに割り当てられた、前記テナンシにおけるリソースプロビジョニングの、複

10

20

30

40

50

数のタグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することを含み、

前記要求を受信することは、前記リソースを要求するユーザに割り当てられたユーザグループカテゴリを表すリソースタイプデータを含む要求を受信することを含み、

前記判断することは、前記ユーザグループカテゴリに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することを含み、

前記比較することは、前記判断された使用量を、前記ユーザグループカテゴリに割り当てられた前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較することを含み、

前記要求をドロップすることは、前記ユーザグループカテゴリに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記ユーザグループカテゴリに割り当てられた前記テナンシにおけるリソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、前記要求をドロップすることを含む、請求項15～17のいずれか1項に記載のプログラム。

【請求項19】

前記タグベースの割り当てデータを記憶することは、前記テナンシの複数のユーザグループに割り当てられた、前記テナンシの複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、タグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することを含み、

前記要求を受信することは、i) 前記要求されたリソースの第1のリソースタイプを表すリソースタイプデータと、ii) 前記リソースを要求するユーザに割り当てられた第1のユーザグループカテゴリを表すユーザグループデータとを含むリソースタイプデータを含む要求を受信することを含み、

前記判断することは、前記第1のユーザグループカテゴリにプロビジョニングされる前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの使用量を判断することを含み、

前記比較することは、前記判断された使用量を、前記第1のユーザグループカテゴリに割り当てられた前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て量と比較することを含み、

前記要求をドロップすることは、前記第1のユーザグループカテゴリにプロビジョニングされる前記第1のリソースタイプに対応する前記リソースタグに関連付けられる、前記テナンシにおける前記判断されたリソースの使用量が、前記第1のユーザグループカテゴリに割り当てられた前記第1のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの前記第1のタグベースの割り当て量を超えることに基づいて、前記要求をドロップすることを含む、請求項15～18のいずれか1項に記載のプログラム。

【請求項20】

さらに、

前記テナンシの複数のユーザグループに割り当てられた、前記テナンシの複数のリソースタイプの、前記テナンシにおけるリソースプロビジョニングの、タグベースの割り当て量を表す、タグベースの割り当てデータを、前記メモリデバイスに記憶することと、

前記テナンシのリソース使用を追跡する第1の要求を受信することとを含み、前記第1の要求は、第1のユーザグループカテゴリおよび第1のリソースタイプを表す要求特性データを含み、さらに、

前記第1のユーザグループカテゴリによってプロビジョニングされる前記第1のリソースタイプに対応するリソースタグに関連付けられる、前記テナンシにおけるリソースの第1の使用量を判断することと、

前記第1のユーザグループカテゴリによってプロビジョニングされる前記第1のリソースタイプの、前記テナンシにおける前記判断されたリソースの第1の使用量に基づいて、リソース使用追跡データを生成することとを含む、請求項15～19のいずれか1項に記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

著作権通知

この特許文献の開示の一部は、著作権保護の対象となる資料を含む。著作権保有者は、この特許文献または特許開示の、それが特許商標庁の特許ファイルまたは記録に現れているとおりの、何人による複写複製にも異議を唱えないが、それ以外の場合にはすべての著作権をどのようなものであろうと所有する。

【0002】

関連出願に対する優先権主張および相互参照：

本出願は、2019年8月9日に出願された「SYSTEM AND METHOD FOR TAG BASED RESOURCE LIMITS OR QUOTAS IN A CLOUD INFRASTRUCTURE ENVIRONMENT」と題される米国仮特許出願第62／884，931号、および2019年8月9日に出願された「SYSTEM AND METHOD FOR TAG BASED REQUEST CONTEXT IN A CLOUD INFRASTRUCTURE ENVIRONMENT」と題される米国仮特許出願第62／884，933号に対する優先権の利益を主張し、上記の各出願は、参照によりその全体が本明細書に組み込まれる。

【0003】

本出願は、2020年8月5日に出願された「SYSTEM AND METHOD FOR TAG BASED RESOURCE LIMITS OR QUOTAS IN A CLOUD INFRASTRUCTURE ENVIRONMENT」と題される米国特許出願第16／986，158号、および2020年8月5日に出願された「SYSTEM AND METHOD FOR TAG BASED REQUEST CONTEXT IN A CLOUD INFRASTRUCTURE ENVIRONMENT」と題される米国特許出願第16／986，160号に対する優先権の利益も主張し、上記の各出願は、参照によりその全体が本明細書に組み込まれる。

【0004】

技術分野

本明細書で説明される実施形態は、概して、サービスとしてのインフラストラクチャ（Infrastructure as a Service）（IaaS）等のクラウドインフラストラクチャ環境に関し、特に、そのようなクラウドインフラストラクチャ環境内でリソース制約を提供するためのシステムおよび方法を提供するためのシステムならびに方法に関する。

【背景技術】

【0005】

背景：

クラウドインフラストラクチャ環境は、ユーザおよびクライアント（本明細書を通して、「クライアント」および「顧客」という用語は互換的に用いることができる）が、高度に利用可能なホストされた環境において広範囲のアプリケーションおよびサービスを構築ならびに実行することを可能にする、補完的クラウドサービスのセットを備えることができる。

【0006】

年々、ますます多くの事業および組織が、ミッションクリティカルなアプリケーションおよびシステムをクラウドインフラストラクチャ環境に移行させている。このシフトの理由は様々である。例えば、多くの事業は、オンプレミスインフラストラクチャを運用し、維持し、増築するコストおよび複雑さを低減するために、クラウドに移動している。同様に、クラウドインフラストラクチャは、より迅速な情報技術（IT）配信機構も可能にする。いくつかの事業および組織は、さらに、クラウドインフラストラクチャ環境を、より敏捷なシステムに適合することによって、競争で優位に立つ手段として見る。

【0007】

IaaS（Infrastructure as a Service）モデル内では、クラウドプロバイダは、従来の設定では、各顧客／クライアントの場所においてオンプレミスとなるであろうインフ

10

20

30

40

50

ラストラクチャ構成要素を提供、ホスト、および管理することができる。従来ではオンプレミスで提供されるそのような構成要素は、ハードウェア、例えば、データウェアハウスおよびデータセンター、サーバ、ストレージ、ネットワーキングハードウェア、ならびに仮想化ソフトウェア等のソフトウェアを含むことができる。

【0008】

IaaSプロバイダは、従来ではオンプレミスであらうハードウェアおよびソフトウェアを提供することに加えて、それらのクライアントおよび顧客にサービスを提供することもできる。例として、クライアントおよび顧客は、彼らのIaaSサブスクリプションを彼らのニーズに適合するように調整することを可能にされ得、次いでこれは、詳細で分解された課金および請求を可能にする。IaaSは、負荷分散、冗長性、複製、回復などの機能もサポートできる。そのようなサービスは、（顧客ではなく）IaaSプロバイダによって提供およびサポートされるため、これは、クライアントおよび顧客を、彼らのサービスのための自動化およびオーケストレーションにさらにプッシュすることによって、彼らの事業を改善することに、より集中させる。

【0009】

クラウドインフラストラクチャは、ユーザおよびクライアントが、従来の企業アプリケーションを、クラウドネイティブアプリとともに、すべて同じプラットフォーム上でシームレスに実行することを可能にし、運用オーバーヘッドを低減し、両方のタイプのワークロード間の直接接続性を可能にする。

【発明の概要】

【課題を解決するための手段】

【0010】

概要：

クラウドインフラストラクチャ環境においてタグベースのリソース制限または割り当てを設けるためのシステムおよび方法が本明細書で説明される。本明細書に記載のシステムおよび方法は、クラウドインフラストラクチャ環境においてタグベースのリソース制限／割り当てをサポートする。細かい粒度のアプローチは、複数のコンテナに跨がるタグに基づいてリソース制限を設けることができる。タグは、主にリソース管理において用いられる機構であり、クラウドプロバイダはそれらをコスト管理のためにも用いる。システムおよび方法は、タグを通してグループレベルでコストを制御するための機構を作成することができる。システムおよび方法は、クラウドインフラストラクチャ環境のためのコンパートメント割り当てを設ける。

【0011】

クラウド管理者は、既存のクラウドにおいてリソース使用を制限する能力を有するが、それは上位レベルにおいてのみであり、特定のユーザ、特定のリソースおよびリソースタイプ、またはコンテナ階層構造のレベルにおけるリソースを考慮しない。ある実施形態に従うと、リソースはタグに関連付けられ、その結果、それらの使用は、必要または所望に応じて、リソースレベルで制御され、追跡され、および／または他の態様で扱われ得る。リソース割り当ておよび／または制限を設けることにより、管理者などは、ユーザのリソース使用を適切なレベルに制限することができ、微調整されたコスト制御が可能になる。

【0012】

ある実施形態に従うと、顧客は、アカウント作成時にクラウドインフラストラクチャ環境によって定義されるサービスレベル制限を割り当てられることができる。これらのサービスレベル制限は、顧客がテナンシ全体にわたって作成することができるリソースの総数（例えば、複数のコンパートメントを有する複数のリージョンにわたり、複数のコンテナに跨がる）を制限する。テナンシおよびコンパートメント管理者は、タグベースのリソース割り当てを利用して、リソース固有の制限を設定することができる。リソースに関連付けられるタグに基づくそのような制限がないと、インスタンスを起動する権限を付与されたユーザは、テナンシ全体においてすべての利用可能な容量を消費し得る。タグベースのリソース制限は、この問題を解決し、サービス制限とは異なり、例えば、コンソール、S

DK、またはAPIを介して、クライアントおよび顧客によって設定ならびにカスタマイズされる。タグベースのリソース制限は、サービス制限の上に適用され、ネスト化されたコンパートメント階層を通して継承され得る。これは、コンパートメント管理者が、リソース消費を制限し、許容可能なリソース使用の周りに境界を設定することを可能にする。

【図面の簡単な説明】

【0013】

【図1】ある実施形態に係る、クラウドインフラストラクチャ環境を提供するためのシステムを示す図である。

【図2】ある実施形態に係る、クラウドインフラストラクチャ環境内にクラウドインフラストラクチャリージョンを提供するためのシステムを示す図である。

10

【図3】ある実施形態に係る、クラウドインフラストラクチャリージョンに跨がるポリシー管理ならびに制御のためにコンパートメント、コンパートメントポリシー、サブコンパートメント、およびサブコンパートメントポリシーの間の関係を示すクラウドインフラストラクチャ環境システムを示す図である。

【図4】コンパートメントを移動させるときのコンパートメント、コンパートメントポリシー、サブコンパートメント、およびサブコンパートメントポリシーの間の関係を示すクラウドインフラストラクチャ環境400を示す図である。

【図5】コンパートメントを移動させるときのポリシーの意味を示すクラウドインフラストラクチャ環境500を示す図である。

【図6】例示的な実施形態による、定義済みタグの対を示す図である。

20

【図7】例示的な実施形態による、たとえばリソースタグおよびリソース要求コンテキストタグを含むタグに基づいてクラウドインフラストラクチャ環境においてリソースに対する割り当てまたは制限を実施するシステムのアーキテクチャを示す図である。

【図8】クラウドインフラストラクチャ環境におけるリソースのプロビジョニングなどの使用を制限するために要求コンテキストタグおよび／またはリソースタグを用いるシステムを示す図である。

【図9】一実施形態による、クラウドインフラストラクチャ環境においてリソース要求コンテキストタグベースの制限／割り当てを設けるシステムの機能概略図である。

【図10】例示的な実施形態による、要求コンテキストに基づいてクラウドインフラストラクチャ環境においてリソースをプロビジョニングすることを制限するかまたはそれに割り当てを課すための方法を示す流れ図である。

30

【図11】一実施形態による、クラウドインフラストラクチャ環境においてタグベースのリソース制限／割り当てを設けるシステムの機能概略図である。

【図12】例示的な実施形態による、リソースタグに基づいてクラウドインフラストラクチャ環境においてリソースをプロビジョニングすることを制限するかまたはそれに割り当てを課すための方法を示す流れ図である。

【発明を実施するための形態】

【0014】

詳細な説明：

本明細書の実施形態によれば、「ベアメタルホスト」、「ベアメタルインスタンス」、または「ベアメタル計算インスタンス」という用語は、クラウドインフラストラクチャ環境による使用のために提供される物理ホスト（「ベアメタル」）マシンを指し得る。ベアメタル計算インスタンスは、ハイパーバイザなしでベアメタルサーバ上で直接動作する。ベアメタルインスタンスがプロビジョニングされると、ユーザ／クライアントは、物理CPU、メモリ、およびネットワークインターフェイスカード（NIC）の唯一の制御を維持することができる。ユーザ／クライアントは、あたかも自分自身のデータセンターで動作するハードウェアであるかのように、各物理マシンの全能力を構成し利用することができる。ユーザ／クライアントは、物理マシンを他のテナントと共有しない。

40

【0015】

本明細書の実施形態によれば、クラウドインフラストラクチャ環境は、リージョンおよ

50

び可用性ドメインにおいて物理的にホストされ得る。用語「リージョン」は、局所化された地理的エリアを指すことができる。用語「可用性ドメイン」は、あるリージョン内に位置する1つ以上のデータセンターを意味することができる。リージョンは、1つ以上の可用性ドメインから構成される。クラウドインフラストラクチャは、仮想クラウドネットワークのようにリージョン固有、または計算インスタンスのように可用性ドメイン固有であり得る。可用性ドメインは、互いに隔離され、フォールトトレラントであり、同時に故障したり、別の可用性ドメインの故障によって影響を受ける可能性が低い。ユーザ／クライアントが自分のクラウドサービスを構成すると、ユーザ／クライアントは、複数の可用性ドメインを用いて、高い可用性を保証し、リソース障害から保護することができる。いくつかのリソースは、インスタンスおよびそれに付随するストレージボリューム等、同じ可用性ドメイン内で作成されなければならない。

10

【0016】

本明細書の実施形態によれば、「レルム」という用語は、リージョンの論理的な集まりを指すことができる。レルムは互いに隔離されており、いかなるデータも共有しない。クライアントのテナンシは、単一のレルム内に存在し、そのレルムに属するリージョンの各々へのアクセスを有することができる。レルムは、例えば、商業的リージョンおよび行政クラウドリージョンのために提供されることができる。

【0017】

本明細書の実施形態によれば、「コンソール」という用語は、ユーザ／クライアントがクラウドインフラストラクチャ環境にアクセスし、それを管理するために用いることができる（たとえば、ウェブベースの）ユーザインターフェイスを指すことができる。

20

【0018】

本明細書の実施形態によれば、「テナンシ」という用語は、クラウドインフラストラクチャ環境内の安全かつ隔離されたパーティションを指すことができる。クライアント／ユーザがクラウドインフラストラクチャ環境についてサインアップすると、クラウドインフラストラクチャ環境は、そのユーザ／クライアント（または彼らの会社）のためにテナンシを作成することができる。テナンシは、ユーザ／クライアントが自分のクラウドリソースを作成、編成、および管理する場所であり得る。

【0019】

本明細書の実施形態によれば、「コンパートメント」という用語は、管理者によって許可が与えられた特定のグループによってのみアクセスされ得る関連リソース（インスタンス、仮想クラウドネットワーク、ブロックボリュームなど）の集まりを指すことができる。コンパートメントは、クライアント／ユーザが、彼らのクラウドリソースを編成し、それらへのアクセスを制御することを可能にする。クライアント／ユーザがコンソールにおいてリソースで作業し始めると、コンパートメントは、クライアント／ユーザが見ているものについてフィルタを提供することができる。

30

【0020】

本明細書の実施形態によれば、「テナンシ」という用語は、テナントのクラウドリソースのすべてを含むルートコンパートメントを指すことができる。テナンシ（ルートコンパートメント）および対応するポリシー内に追加のコンパートメントを作成して、各コンパートメント内のリソースへのアクセスを制御することができる。ユーザ／クライアントが、インスタンス、ブロックボリューム、またはクラウドネットワーク等のクラウドリソースを作成すると、ユーザ／クライアントは、リソースがどのコンパートメントに属すべきかを指定することができる。

40

【0021】

本明細書の実施形態によれば、「仮想クラウドネットワーク」という用語は、インスタンスが動作する、サブネット、ルートテーブル、およびゲートウェイを含む、従来のネットワークの仮想バージョンを指すことができる。クラウドネットワークは、単一のリージョン内に存在するが、そのリージョンのすべての可用性ドメインを含む。クラウドネットワークにおいて定義される各サブネットは、単一の可用性ドメイン内にあるか、またはそ

50

のリージョン内のすべての可用性ドメインにわたるかのいずれかであり得る。少なくとも1つの少なくとも1つのクラウドネットワークは、インスタンスが起動され得る前にセットアップされ得る。

【0022】

本明細書の実施形態によれば、「インスタンス」という用語は、クラウド内で動作する計算ホストを指すことができる。クラウドインフラストラクチャ環境インスタンスは、ユーザ／クライアントが、従来のソフトウェアベースの仮想マシンとは対照的に、ホストされた物理ハードウェアを利用することを可能にし、それによって、増加したセキュリティおよび性能を提供することができる。

【0023】

本明細書の実施形態によれば、「イメージ」という用語は、例えば、LINUX（登録商標）など、インスタンスのためにオペレーティングシステムおよび他のソフトウェアを定義する仮想ハードドライブのテンプレートを指すことができる。インスタンスが起動されると、そのイメージを選択することによって、その特性を定義することができる。イメージのセットを提供することができ、同じソフトウェアおよびカスタマイズでインスタンスを用いるために、（例えば、テンプレートとして）すでに構成されている既存のインスタンスからイメージを用いることができる。

【0024】

本明細書の実施形態によれば、「シェイプ」という用語は、インスタンスに割り当てられるCPUの数およびメモリの量の仕様を指すことができる。負荷分散において、シェイプは、入口+出口トラフィックのためのロードバランサの予めプロビジョニングされた合計最大容量（帯域幅）を決定することができる。利用可能なシェイプは、例えば、100 Mbps、400 Mbps、および8000 Mbpsを含むことができる。

【0025】

本明細書の実施形態によれば、「キーペア」という用語は、クラウドインフラストラクチャ環境で用いられる認証機構を指すことができる。キーペアは、秘密鍵ファイルと公開鍵ファイルとからなる。公開鍵はアップロードされることができ、一方秘密鍵はユーザ／クライアントのデバイス上に保持される。秘密鍵は、パスワードのように、ユーザ／クライアントに秘密である。キーペアは、インスタンスSSHキーペアおよびAPI署名キーペアなどの異なる仕様に従って生成され得る。インスタンスSSHキーペアは、インスタンスへのセキュアシェル（SSH）接続を確立するために用いられる。インスタンスがプロビジョニングされると、公開鍵が提供され得、公開鍵は、インスタンスの承認されたキーファイルに保存される。インスタンスにログオンするために、秘密鍵が提供され、それは公開鍵で検証される。API署名キーペアは、PEM（プライバシー拡張メール）フォーマットであり、API要求を提出するときにユーザ／クライアントを認証するために用いられる。

【0026】

本明細書の実施形態によれば、「ブロックボリューム」という用語は、クラウドインフラストラクチャ環境インスタンスのために永続的ブロックストレージを提供する仮想ディスクを指すことができる。ブロックボリュームは、例えばデータおよびアプリケーションを記憶するために、例えばコンピュータ上の物理ハードドライブと同様の方法で、用いることができる。ボリュームは、データの損失なしに、あるインスタンスから分離され、別のインスタンスにアタッチされることができる。

【0027】

本明細書の実施形態によれば、「オブジェクトストレージ」という用語は、データをオブジェクトとして記憶および管理するために用いられ得るストレージアーキテクチャを指し得る。データファイルは任意のタイプであり得る。データがオブジェクトストレージにアップロードされると、それは任意の場所からアクセスすることができる。オブジェクトストレージは、大量のデータを記憶する必要がある、そのデータがあまり頻繁に変化しないときに、用いることができる。オブジェクトストレージのための典型的な使用は、デー

10

20

30

40

50

タバックアップ、ファイル共有、非構造化データ（例えば、ログおよびセンサ生成データ）の記憶を含むが、これらに限定されない。

【0028】

本明細書の実施形態によれば、「バケット」という用語は、データおよびファイルを記憶するための論理コンテナを指すことができる。バケットは、無制限の数のオブジェクトを含むことができる。

【0029】

上述のように、クラウドインフラストラクチャ環境は、ユーザおよびクライアントが、高度に利用可能なホストされた環境において広範囲のアプリケーションおよびサービスを構築ならびに実行することを可能にする、補完的クラウドサービスのセットを備えることができる。

10

【0030】

図1は、一実施形態による、クラウドインフラストラクチャ環境を提供するためのシステムを示す。

【0031】

ある実施形態に従うと、いくつかのハードウェアおよびソフトウェアリソース112上で実行することができるクラウドインフラストラクチャ環境100は、コンソールインターフェイス102とAPI104とを備えることができる。加えて、クラウドインフラストラクチャ環境100は、いくつかのガバナンスサービス110と、アイデンティティおよびアクセス管理（IAM）サービス120と、プロビジョニングサービス130とをサポートすることができる。クラウドインフラストラクチャ環境100はまた、たとえば、コンピュータリソース層150、ネットワークリソース層160、およびストレージリソース層170などの層において、いくつかのリソース140をサポートすることができる。クラウドインフラストラクチャ環境100はまた、例えば、概してリソース140に関連付けられるリソースタグ140a、コンピュータリソース150に関連付けられるコンピュータリソースタグ150a、ネットワークリソース160に関連付けられるネットワークリソースタグ160a、およびストレージリソース170に関連付けられるストレージリソースタグ170aを含む、リソースの各々に関連付けられるいくつかのタグをサポートすることもできる。

20

【0032】

ある実施形態に従うと、デバイスハードウェア（プロセッサ、メモリなど）12を有するコンピューティングデバイス10などのクライアントデバイスは、たとえばワイドエリアネットワーク（WAN）、ローカルエリアネットワーク（LAN）、またはインターネットなどのネットワークを介してクラウドインフラストラクチャ環境と通信することができる。クライアントデバイスは、管理者アプリケーション14を備えることができ、それは、ユーザインターフェイス16を備えることができる。

30

【0033】

ある実施形態に従うと、クラウドインフラストラクチャ環境内では、テナンシをサポートすることができる。登録および展開時に、クライアント／顧客ごとにテナンシを作成することができる。これは、クラウドインフラストラクチャ内に、クライアントが自分のクラウドリソースを作成、編成、および管理することができるセキュアかつ隔離されたパーティションを備えることができる。

40

【0034】

ある実施形態に従うと、コンソールインターフェイス102およびAPI104は、クライアントに、インフラストラクチャ環境のそれぞれの部分に対するアクセスおよび制御を与える。ある実施形態に従うと、コンソールインターフェイスは、クライアントに、リソース、インスタンス、クラウドネットワーク、およびストレージボリュームを作成ならびに管理させるとともに、クライアントに関連付けられるユーザを管理させ、クライアント範囲内に許可を設定させる、直感的なグラフィカルインターフェイスを含むことができる。同様に、API104は、例えばHTTPS（ハイパーテキスト転送プロトコルセキ

50

ユア)を利用するREST APIを含み得る。

【0035】

ある実施形態に従うと、コンソールインターフェイスまたはAPIの一例は、構成管理ツール(たとえばAnsible)とすることができる。構成管理ツールは、クラウドインフラストラクチャプロビジョニング、オーケストレーション、および構成管理のために用いることができる。構成管理ツールは、クライアントが、クラウドインフラストラクチャの構成およびプロビジョニング、ソフトウェアアセットの展開および更新、ならびに複雑な動作プロセスのオーケストレーションを自動化することを可能にすることができる。

【0036】

ある実施形態に従うと、クラウドインフラストラクチャ環境のガバナンスサービス110は、クライアントが単純なリソース管理を可能にし、コストを管理し、クラウドインフラストラクチャへのアクセスを制御するのを助けるツールをクライアントに提供する。例として、ガバナンスサービスはタグ付けを提供し、このタグ付けは、クライアントが情報上または動作上の理由で彼らのリソースにタグを適用することを可能にすることができる。定義済みタグは、正しくないタグがリソースに適用されることを回避するように制御され得る。タグはまた、管理スクリプトのために柔軟なターゲット化機構を提供することもできる。同様に、ガバナンスサービスは、予算管理を可能にし、実費および予測費をすべて1つの場所から追跡することができる。これにより、クライアントは、費用分析ダッシュボードで使用の上に留まり、コンパートメントおよびタグによってフィルタリングして、部門、チーム、およびプロジェクトによる支出を分析することができる。そのようなデータは、詳細なリソース利用報告ならびに既存のクラウド管理およびビジネスインテリジェンスツールとの統合のためにエクスポートすることもできる。ガバナンスサービスはまた、クラウドインフラストラクチャエンタイトルメントならびにコンパートメントにわたるセキュリティ、コンプライアンス、およびリソース最適化のために後で検索され、記憶され、分析され得るイベントを記録することもできる。

【0037】

例示的な実施形態によれば、ガバナンスサービスは、クライアント、管理者などが、リソースがインスタンス化されているときに情報上または動作上の理由で彼らのリソースにタグを適用することを可能にするタグ付けを提供する。さらなる例示的な実施形態によれば、ガバナンスサービスはまた、リソースがインスタンス化された後に、クライアントおよび他者が情報上または動作上の理由で彼らのリソースにタグを適用することを可能にし、それによって、タグを用いてシステムにおけるリソース割り当てまたは制限の遡及的实施を可能にする、タグ付けを提供する。

【0038】

ある実施形態に従うと、アイデンティティおよびアクセス管理(IAM)サービス120は、IAMサービスにおける各クライアント/顧客/ユーザについて、ユーザクレデンシャル(たとえばユーザ名およびパスワード)に関連付けられて、ユーザプロファイルを作成することができる。クライアントは、IAMサービスを介してクラウドインフラストラクチャにおいて管理者特権も付与され得る。

【0039】

ある実施形態に従うと、アイデンティティおよびアクセス管理サービスは、クラウドインフラストラクチャ環境と統合することができる。クライアント登録で、IAMサービスは、アイデンティティサービスにおいて別のユーザクレデンシャルを作成することができ、それは、次いで、クラウドインフラストラクチャサービスへのシングルサインオンおよび追加のクラウドサービスへのアクセスを可能にすることができる。

【0040】

ある実施形態に従うと、プロビジョニングサービス130は、たとえばリソース140内などのクラウドインフラストラクチャサービス内にテナンシをプロビジョニングすることができる。プロビジョニングサービスは、例えば、コンソールインターフェイスを通して、またはAPI104等の1つ以上のAPIを介して、アクセスおよび制御することが

10

20

30

40

50

できる。プロビジョニングサービスは、クライアントが、インスタンスと称され得る計算ホストをプロビジョニングおよび管理することを可能にし得る。クライアントは、計算およびアプリケーション要件を満たすために必要に応じてインスタンスを起動することができる。クライアントがインスタンスを起動した後、プロビジョニングされたインスタンスは、例えば、クライアントデバイスからアクセスされることができる。プロビジョニングサービスはまた、インスタンスの再起動、インスタンスからのボリュームのアタッチおよびデタッチ、ならびにインスタンスの終了を提供することができる。

【0041】

ある実施形態に従うと、クラウドインフラストラクチャ環境によって提供されるリソース140は、計算リソース層150、ネットワークリソース層160、およびストレージリソース層170などの複数の層に分割することができる。

10

【0042】

ある実施形態に従うと、計算リソース層150は、たとえばベアメタルインスタンス152、仮想マシン154、エッジサービス156、およびコンテナ158などのいくつかのリソースを含み得る。計算リソース層は、例えば、ベアメタル計算インスタンスをプロビジョニングおよび管理し、オンプレミスデータセンターと同様に、アプリケーションを展開および実行するために必要に応じてインスタンスをプロビジョニングするために用いることができる。例示的实施形態によるクラウドインフラストラクチャ環境100は、例えば、ベアメタルインスタンス152、仮想マシン154、エッジサービス156、およびコンテナ158を含むコンピュータリソース150と関連付けられるコンピュータリソースタグ150aを含む、リソースの各々と関連付けられるいくつかのタグ140aをサポートする。

20

【0043】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、計算リソース層内の1つ以上の物理ホスト（「ベアメタル」）マシンの制御を提供することができる。ベアメタル計算インスタンスは、ハイパーバイザなしでベアメタルサーバ上で直接動作する。ベアメタル計算インスタンスがプロビジョニングされると、クライアントは、物理CPU、メモリ、およびネットワークインターフェイスカード（NIC）の唯一の制御を維持することができる。ベアメタル計算インスタンスは、構成され、各物理マシンの全能力を、あたかもそれがオンプレミスの自身のデータセンターで動作するハードウェアであるかのように、利用することができる。したがって、ベアメタル計算インスタンスは、一般に、テナント間では共有されない。

30

【0044】

ある実施形態に従うと、ベアメタル計算インスタンスは、ソフトウェアベースの仮想環境とは対照的に、関連付けられた物理ハードウェアを介して、高レベルのセキュリティおよびパフォーマンスを提供することができる。

【0045】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、計算リソース層内においていくつかの仮想マシンの制御を提供することができる。仮想マシン計算ホストは、例えば、仮想マシン動作システムおよび他のソフトウェアを決定することができるイメージから起動することができる。仮想マシンインスタンスに利用可能なリソースのタイプおよび量は、例えば、仮想マシンが起動されたイメージに基づいて判断され得る。

40

【0046】

ある実施形態に従うと、仮想マシン（VM）計算インスタンスは、物理ベアメタルハードウェア上で動作する独立したコンピューティング環境を含み得る。仮想化は、互いに隔離された複数のVMを実行することを可能にする。VMは、例えば、物理マシン全体の性能およびリソース（CPU、メモリ、ネットワーク帯域幅、ストレージ）を必要としないアプリケーションを実行するために用いることができる。

【0047】

いくつかの実施形態では、仮想マシンインスタンスは、ベアメタルインスタンスと同じ

50

ハードウェア上で実行することができ、これは、同じクラウド最適化ハードウェア、ファームウェア、ソフトウェアスタック、およびネットワーキングインフラストラクチャを用いることに影響を及ぼすことができる。

【0048】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、計算リソース層内にいくつかのグラフィカル処理ユニット（GPU）計算インスタンスを提供することができる。高速化される計算は、あらゆるサービスにわたって一貫して高速なインフラストラクチャを必要とする。GPUインスタンスを用いて、クライアントは、より効率的に大量のデータセットを処理および分析することができ、それらを、複雑な機械学習（ML）、人工知能（AI）アルゴリズム、および多くの産業用HPCアプリケーションに対して有用にする。GPU計算インスタンスは、仮想化された計算インスタンス（複数のGPU計算インスタンスが同じベアメタルハードウェアを共有する）として、または各GPU計算インスタンスについて専用ハードウェアを提供するベアメタルインスタンスとして、プロビジョニングすることができる。

10

【0049】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、計算リソース層内にいくつかのコンテナ化された計算インスタンスを提供することができる。スタンドアロンコンテナエンジンサービスを用いて、コンテナ化されたアプリケーションを構築し、クラウドに起動することができる。コンテナサービスは、例えば、クラウドネイティブアプリケーションを構築、展開、および管理するために用いることができる。コンテナサービスは、コンテナ化されたアプリケーションが必要とする計算リソースを指定することができ、次いで、コンテナエンジンは、プロビジョニングサービスを介して、（例えば、テナンシのコンテキストにおいて）クラウドインフラストラクチャ環境内で用いるために必要とされる計算リソースをプロビジョニングすることができる。

20

【0050】

ある実施形態に従うと、用いることができるそのようなコンテナサービスエンジンの1つは、ホストのクラスタにわたるコンテナ化されたアプリケーションの展開、スケーリング、および管理を自動化するためのオープンソースシステムであるKubernetesである。そのようなコンテナサービスは、アプリケーションを構成するコンテナを、容易な管理および発見のために、論理ユニットにグループ化することができる。

30

【0051】

ある実施形態に従うと、ネットワークリソース層160は、たとえば仮想クラウドネットワーク（VCN）162、ロードバランサ164、エッジサービス166、および接続サービス168などのいくつかのリソースを含み得る。例示的な実施形態によるクラウドインフラストラクチャ環境100は、たとえば、概してリソース140に関連付けられるリソースタグ140aと、仮想クラウドネットワーク（VCN）162、ロードバランサ164、エッジサービス166、および接続サービス168に関連付けられるネットワークリソースタグ160aとを含む、リソースの各々に関連付けられるいくつかのタグをサポートする。

【0052】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、ネットワーキングリソース層において、いくつかの仮想クラウドネットワーク162を提供することができる。仮想クラウドネットワークは、クライアントインスタンスが動作できるサブネット、ルートテーブル、およびゲートウェイを含む従来のネットワークの仮想バージョンを含むことができる。クラウドネットワークは、単一のリージョン内に存在するが、そのリージョンのすべての可用性ドメインを含む。クラウドネットワークにおいて定義される各サブネットは、単一の可用性ドメイン内にあるか、またはそのリージョン内のすべての可用性ドメインにわたる（推奨）かのいずれかであり得る。少なくとも1つのクラウドネットワークを、インスタンスを起動する前に構成することができる。ある実施形態では、VCNは、公衆トラフィック、VPN接続、または高速接続サービスを処理して、オンプレミスネッ

40

50

トワークを安全に拡張するよう、インターネットゲートウェイを介して構成することができる。

【0053】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、ネットワーキングリソース層において、いくつかのロードバランサ164を提供することができる。負荷分散サービスは、1つのエン트리ポイントから、仮想クラウドネットワーク（VCN）から到達可能な複数のサーバへの、自動化されたトラフィック分配を提供することができる。様々な負荷分散が、パブリックまたはプライベートIPアドレス、およびプロビジョニングされた帯域幅を提供することができる。

【0054】

ある実施形態に従うと、ロードバランサは、リソース利用、スケーリングを改善し、高い可用性を確保するのに助けることができる。複数の負荷分散ポリシーを構成ことができ、アプリケーション固有の健全性チェックを提供して、ロードバランサがトラフィックを健全なインスタンスにのみ向けることを確実にすることができる。ロードバランサは、不健全なアプリケーションサーバが保守のためにサービスから取り除かれる前に不健全なアプリケーションサーバからトラフィックを排出することによって、保守ウィンドウを縮小することができる。

【0055】

ある実施形態に従うと、負荷分散サービスにより、VCNに関連したパブリックまたはプライベートロードバランサの作成が可能になる。パブリックロードバランサは、インターネットからアクセス可能なパブリックIPアドレスを有する。プライベートロードバランサは、VCN内でのみ可視であるホスティングサブネットからのIPアドレスを有する。複数のリスナが、IPアドレスについて、異なるトラフィックの層（例えば、層4および層7（TCPおよびHTTP）トラフィック）を負荷分散トランスポートするよう、構成され得る。パブリックおよびプライベートの両方のロードバランサは、VCNから到達可能な任意のバックエンドサーバにデータトラフィックをルーティングすることができる。

【0056】

ある実施形態に従うと、パブリックロードバランサは、インターネットからトラフィックを受け入れることができ、着信トラフィックのためのエン트리ポイントとしての役割を果たすパブリックアドレスを割り当てられるパブリックロードバランサを作成することができる。

【0057】

ある実施形態に従うと、パブリックロードバランサは範囲がリージョナルである。リージョンが複数の可用性ドメインを含む場合、パブリックロードバランサは、例えば、リージョナルサブネット、または各々が別個の可用性ドメインにある2つの可用性ドメイン固有（AD固有）サブネットを有することができる。リージョナルサブネットでは、ロードバランサは、一次ロードバランサおよびスタンバイロードバランサを、各々異なる可用性ドメインにおいて作成して、可用性ドメイン機能停止中であってもアクセス可能性を保証することができる。負荷分散が複数のAD固有サブネットにおいて形成される場合、一方のサブネットは一次ロードバランサをホストすることができ、他方のサブネットはスタンバイロードバランサをホストすることができる。一次ロードバランサが故障した場合、パブリックIPアドレスは二次ロードバランサに切り替わることができる。サービスは、2つのロードバランサを等価物として扱う。

【0058】

ある実施形態に従うと、リージョンが1つの可用性ドメインのみを含む場合、サービスは、一次ロードバランサおよびスタンバイロードバランサの両方をホストするために、リージョナルであれAD固有であれ、1つのサブネットのみを必要とする。一次ロードバランサおよびスタンバイロードバランサは、各々、割り当てられたフローティングパブリックIPアドレスに加えて、ホストサブネットからのプライベートIPアドレスを有することができる。可用性ドメイン機能停止がある場合、ロードバランサはフェイルオーバーを有

10

20

30

40

50

さない。

【0059】

ある実施形態に従うと、プライベート負荷分散はまた、ロードバランサをインターネットから隔離し、セキュリティ姿勢を単純化するようにも提供され得る。ロードバランササービスは、着信トラフィックのためのエントリポイントとして機能するプライベートアドレスをロードバランサに割り当てることができる。

【0060】

ある実施形態に従うと、プライベートロードバランサは、あるサービスによって、1つのサブネットのみに対応して一次ロードバランサとスタンバイロードバランサとの両方をホストするよう、作成され得る。ロードバランサは、ホストサブネットの範囲に応じて、リージョナルであり得るかまたはAD固有であり得る。ロードバランサは、ホストサブネットを含むVCN内からのみ、またはセキュリティルールによってさらに制限されるとおりに、アクセス可能である。

【0061】

ある実施形態に従うと、割り当てられたフローティングプライベートIPアドレスは、ホストサブネットに対してローカルである。一次ロードバランサおよびスタンバイロードバランサは、各々、ホストサブネットから追加のプライベートIPアドレスを必要とする。

【0062】

ある実施形態に従うと、可用性ドメイン機能停止がある場合、マルチADリージョン内のリージョナルサブネットにおいて作成されたプライベートロードバランサは、フェイルオーバー能力を提供する。AD固有サブネットにおいて、または単一の可用性ドメインリージョン内のリージョナルサブネットにおいて作成されたプライベートロードバランサは、可用性ドメイン機能停止にตอบสนองしてフェイルオーバー能力を有さない。

【0063】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、ネットワーキングリソース層においていくつかのエッジサービス166を提供することができる。概して、エッジサービスは、クライアントがドメインおよびエンドポイントを管理、セキュリティ保護、および維持することを可能にする、いくつかのサービスを備える。これらは、例えば、DNS（ドメイン名システム）、DDoS（分散型サービス妨害）保護、電子メール配信などを含む。これらのサービスは、クライアントが性能を最適化し、サイバー攻撃を阻止し、通信をスケール変更することを可能にする。

【0064】

ある実施形態に従うと、クラウドインフラストラクチャ環境は、ネットワーキングリソース層においていくつかの接続サービス168を提供することができる。そのような接続サービスは、クライアントデータセンターまたは既存のネットワークとクラウドインフラストラクチャ環境との間に専用のプライベート接続を作成するための容易な方法を提供することができる。接続サービスは、広帯域幅、および信頼できる一貫したネットワークを提供することができる。

【0065】

ある実施形態に従うと、ストレージリソース層170は、たとえばブロックボリューム172、ファイルストレージ174、オブジェクトストレージ176、およびローカルストレージ178などのいくつかのリソースを含み得る。例示的な実施形態によるクラウドインフラストラクチャ環境100は、例えば、概してリソース140に関連付けられるリソースタグ140aと、ブロックボリューム172、ファイルストレージ174、オブジェクトストレージ176、およびローカルストレージ178に関連付けられるストレージリソースタグ170aとを含む、リソースの各々に関連付けられるいくつかのタグをサポートする。

【0066】

ある実施形態に従うと、ブロックボリューム172は、広範囲のI/O集約的ワークロードをサポートする高性能ネットワークストレージ容量を提供する。クライアントは、ブ

10

20

30

40

50

ロックボリュームを用いて、計算インスタンスの記憶容量を拡張し、計算インスタンスにわたって移行することができる耐久性のある永続的なデータストレージを提供し、大きなデータベースをホストすることができる。

【0067】

ある実施形態に従うと、ファイルストレージ174により、クライアントは、スケーラブルで分散型の企業グレードのネットワークファイルシステムを作成することができる。ファイルストレージは、セマンティクス、スナップショット能力、およびデータ保存時の暗号化をサポートする。

【0068】

ある実施形態に従うと、オブジェクトストレージは、非構造化データに対して高スループットストレージを提供する。オブジェクトストレージサービスは、大量の分析データ、または画像および映像のような豊富なコンテンツのための、ほぼ無制限の記憶容量を可能にする。ブロックボリュームは、追加の耐久性のためにオブジェクトストレージにバックアップされることができる。

10

【0069】

ある実施形態に従うと、ローカルストレージ178は、たとえば、I/O集約型アプリケーション用のソリッドステートドライブの形態で高速かつ信頼性のあるストレージを提供することができる。これらは、例えば、ベアメタルインスタンス内に設けることができる。ローカルストレージは、VMおよびベアメタル計算インスタンスに対して高いストレージ性能を提供する。いくつかの例は、リレーショナルデータベース、データウェアハウス、ビッグデータ、分析、AI、およびHPCアプリケーションを含む。

20

【0070】

図2は、ある実施形態に係る、クラウドインフラストラクチャ環境内にクラウドインフラストラクチャリージョンを提供するためのシステムを示す図である。

【0071】

ある実施形態に従うと、図1において上述したクラウドインフラストラクチャ環境のインスタンスは、クラウドインフラストラクチャリージョン220と呼ばれる異なるリージョンにおいてホストされることができる。これらは、上述のように、コンソール、SDK、またはAPIを介して、インターネット210などのネットワークを介して顧客ネットワーク200によってアクセスすることができる。各クラウドインフラストラクチャリージョンは、管理サービス222と、計算サービス224と、ストレージサービス226と、エッジサービス228と、ネットワークサービス230と、物理インフラストラクチャ232とを備えることができる。

30

【0072】

ある実施形態に従うと、クラウドインフラストラクチャは、リージョンおよび可用性ドメインにおいてホストされることができる。リージョンは、局所化された地理的エリアとすることができる。可用性ドメインは、リージョン内に位置する1つ以上のデータセンターとすることができる。リージョンは、1つ以上の可用性ドメインから構成される。大抵のクラウドインフラストラクチャリソースは、仮想クラウドネットワークなどのリージョン固有であるか、または計算インスタンスなどの可用性ドメイン固有のいずれかであり得る。可用性ドメイン間およびリージョン間のトラフィックは暗号化される。

40

【0073】

ある実施形態に従うと、可用性ドメインは、互いに隔離され、フォールトトレラントであり、障害が同時に生ずる可能性が非常に低い。可用性ドメインは、電力もしくは冷却などのインフラストラクチャ、または内部可用性ドメインネットワークを共有しないので、リージョン内の1つの可用性ドメインにおける障害は、同じリージョン内の他のものの可用性に影響を及ぼす可能性が低い。

【0074】

ある実施形態に従うと、同じリージョン内の可用性ドメインを低レイテンシの広帯域幅ネットワークによって互いに接続することができ、これにより、インターネットおよびオ

50

ンプレミスへの高可用性接続性を提供し、高可用性および災害復旧の両方のために複数の可用性ドメインにおいて複製されたシステムを構築することができる。

【0075】

ある実施形態に従うと、リージョンは他のリージョンから独立しており、地理的に（たとえば国または大陸にわたって）分離されることができる。これは、次いで、あるアプリケーションが最も頻繁に利用される可能性が最も高いリージョン内における当該アプリケーションの展開につながる。

【0076】

しかしながら、ある実施形態に従うと、アプリケーションは、さまざまな理由により、異なるリージョンにおいて展開されもし得る。これは、例えば、気象システムなどのイベントがリージョンをオフラインで取るときリスク軽減を含むことができる。加えて、アプリケーションは、課税ドメインまたは他の事業もしくは社会的基準などの戦略的な理由で他のリージョンに展開されることができる。

【0077】

ある実施形態に従うと、リージョンにわたって利用可能ないくつかのサービスがある。これらは、例えば、管理サービス222、計算サービス224、ストレージサービス226、エッジサービス228、およびネットワークサービス230を含む。

【0078】

ある実施形態に従うと、コンパートメントにより、クライアントは、クラウドリソースを編成し、それに対するアクセスを制御することが可能になる。コンパートメントは、管理者によって許可が与えられた特定のグループによってのみアクセスされ得る関連リソース（インスタンス、仮想クラウドネットワーク、ブロックボリュームなど）の集まりである。例えば、1つのコンパートメントは、例として、会社の人事（HR）システムの制作物を構成するすべてのサーバおよびストレージボリュームを含み得、他のコンパートメントは、各々、さらなる例として、会社の法務、マーケティング、経理、営業、および情報技術（IT）システムに別々に専用とすることができる。ある例では、そのコンパートメントに対する許可を有するユーザのみが、それらのサーバおよびボリュームを管理し、および／またはそれらにアクセスすることができる。さらなる例では、コンパートメントは、会社の人事（HR）システム、および法務、マーケティング、経理、営業、および情報技術（IT）システムの収集の制作物を構成するすべてのサーバならびにストレージボリュームを含むことができる。ある例では、それらのリソースの部分に対する許可を有するユーザのみが、サーバおよびボリューム上でそれらの部分を管理し、および／またはそれらにアクセスすることができる。

【0079】

例示的实施形態のコンパートメントは、1つ以上の論理グループを備え、必ずしも物理メモリコンテナではないが、所望または必要に応じて、物理メモリコンテナであり得る。コンソール内で作業するとき、コンパートメントは、見られることを可能にされるものについてのフィルタとして作用することができる。コンパートメントは、クラウドリソースのために用いられ得る主要構築ブロックであり、それらは、リソースを編成および隔離して、それらのリソースへのアクセスを管理およびセキュリティ保護することをより容易にするために用いられ得る。

【0080】

ある実施形態によると、コンパートメントは、いくつかの層を有することができる。例えば、テナンシは、クライアントのクラウドリソースのすべてを保持するルートコンパートメントと見なすことができる。ルートコンパートメント（テナンシ）内に追加のコンパートメントを作成することができ、対応するポリシーを作成して、各コンパートメント内のリソースへのアクセスを制御することができる。クライアントが、計算、ストレージ、VCN、IPアドレスおよび／もしくはDNSインスタンス、ブロックボリューム、またはクラウドネットワークなどのクラウドリソースを作成するとき、そのようなリソースは、特定のあるコンパートメントまたは複数のコンパートメントに向けられ得る。コンパー

10

20

30

40

50

トメントは、リージョンに跨ることができる。

【0081】

障害ドメイン

ある実施形態に従うと、障害ドメインは、可用性ドメイン内のハードウェアおよびインフラストラクチャのグループ化を含むことができる。各可用性ドメインは、3つの障害ドメインを含むことができる。障害ドメインは、インスタンスが単一の可用性ドメイン内の同じ物理ハードウェア上にないように、インスタンスが分散されることを可能にする。ある障害ドメインに影響を及ぼすハードウェア障害または計算ハードウェア保守は、他の障害ドメインにおけるインスタンスに影響を及ぼさない。

【0082】

ある実施形態に従うと、計算、ベアメタルDBシステム、または仮想マシンDBシステムインスタンスなどのリソースの配置は、任意で、起動時に障害ドメインまたは新たなインスタンスを指定することができる。リソースは、配置後に、リソースを現在の障害ドメインで終了し、リソースの新たなインスタンスを別の障害ドメインで起動することによって、障害ドメインを追加的に変更することができる。

【0083】

ある実施形態に従うと、障害ドメインは、予期せぬハードウェア障害からの保護および保守による計画された機能停止からの保護といった多くの理由で利用することができる。

【0084】

可用性

ある実施形態に従うと、サービス可用性を提供することができる。クラウドインフラストラクチャ環境内のリージョンは、以下を含むコアインフラストラクチャサービスおよびリソースを提供することができる：

- ・計算：計算（ベアメタルおよびVM, DenseIOおよび Standard）、Kubernetesのためのコンテナエンジン、レジストリ...
- ・ストレージ：ブロックボリューム、ファイルストレージ、オブジェクトストレージ、アーカイブストレージ
- ・ネットワークング：仮想クラウドネットワーク、負荷分散、高速接続
- ・データベース：データベース、Exadataクラウドサービス、自律データウェアハウス、自律トランザクション
- ・処理
- ・エッジ：DNS
- ・プラットフォーム：アイデンティティおよびアクセス管理、タグ付け、監査

ある実施形態に従うと、上記サービスおよびリソースは一般に利用可能であり得るが、他のサービスおよびリソースも（例えば、リージョナルな需要または顧客要求に基づいて）追加的に利用可能であり得る。例として、新たなクラウドサービスは、リージョナルな顧客需要、適用可能な場合には規制遵守を達成する能力、リソース可用性、および他の要因を含む様々な考慮事項に基づいて、リージョンにおいてできるだけ迅速に利用可能にされ得る。低レイテンシの相互接続バックボーンのため、顧客は、クラウドサービスが自分の本拠リージョンで利用可能でないときに、それらを他の地理的リージョンで効果的な結果を伴って用いることができるが、ただし、データレジデンシー要件がそうすることを妨げないことを条件とする。

【0085】

ある実施形態に従うと、リソース可用性は、グローバルな可用性、リージョナルな可用性、単一リージョン可用性、およびドメイン可用性のコンテキストにおいて考慮することができる。概して、IAMリソースは、グローバルに利用可能であり、DBシステム、インスタンス、およびボリュームは、実行可能性ドメインに固有である。他のほとんどのリソースはリージョナルである。

【0086】

ある実施形態に従うと、グローバルに利用可能なリソースの例には、API署名キー、

10

20

30

40

50

コンパートメント、動的グループ、フェデレーションリソース、グループ、ポリシー、タグ名前空間、タグキー、およびユーザを含むことができる。

【0087】

ある実施形態に従うと、リージョナルに利用可能なリソースの例には、アラーム、アプリケーション、バケット（バケットはリージョナルなリソースであるが、APIコールのための正しいリージョン固有のオブジェクトストレージURLを用いると、バケットは任意の位置からアクセスできる）、クラスタ、クラウドイベントルール、顧客構内機器（CPE）、DHCPオプションセット、動的ルーティングゲートウェイ（DRG）、暗号化キー、関数、イメージ、インターネットゲートウェイ、ジョブ、キーボルト、ロードバランサ、ローカルピアリングゲートウェイ（LPG）、メトリック、NATゲートウェイ、ネットワークセキュリティグループ、ノードプール、ons-subscriptions、ons-topics、リポジトリ、予約されたパブリックIP、ルートテーブル、セキュリティリスト、サービスゲートウェイ、スタック、サブネット（サブネットが作成されると、それはリージョナルまたは可用性ドメインに固有であると宣言され得る）、仮想クラウドネットワーク（VCN）、およびボリュームバックアップ（ボリュームバックアップは、新たなボリュームとして、それらが格納される同じリージョン内の任意の可用性ドメインに復元することができる）などが含まれ得る。

10

【0088】

ある実施形態に従うと、可用性ドメイン固有リソースの例は、DBシステム、一過性のパブリックIP、インスタンス（インスタンスは、同じ可用性ドメイン内のボリュームにアタッチすることができる）、サブネット（サブネットが作成されると、それはリージョナルまたは可用性ドメインに固有であると宣言され得る）、およびボリューム（ボリュームは、同じ可用性ドメイン内のインスタンスにアタッチすることができる）を含み得る。

20

【0089】

コンパートメント

ある実施形態に従うと、管理者は、クラウドインフラストラクチャ環境内においてコンパートメントを管理することができる。

【0090】

ある実施形態に従うと、タグを、コンパートメント内のリソースに適用することができる。タグは、例えば、事業ニーズスキーマなどのスキーマに従ってリソースを編成するために用いることができる。タグはリソースの作成時にリソースに適用されることができ、またはタグは既存のリソース上で更新されることができる。リソースの各々に関連付けられるタグは、例えば、概してリソース140に関連付けられるリソースタグ140a（図1）、コンピュータリソース150に関連付けられるコンピュータリソースタグ150a、ネットワークリソース160に関連付けられるネットワークリソースタグ160a、およびストレージリソース170に関連付けられるストレージリソースタグ170aを含んでもよい。

30

【0091】

ある実施形態に従うと、コンパートメントは、クラウドインフラストラクチャの構築および編成にとって重要である。リソースをコンパートメント間で移動させることができ、（例えば、ユーザインターフェイスを介して）表示し、現在のリージョン内でコンパートメントによって編成することができる。リソースで作業し、およびリソース管理する場合、まずコンパートメントを選択することができる。

40

【0092】

ある実施形態に従うと、コンパートメントはテナンシ幅であり、リージョンに跨ることができる。コンパートメントが作成されると、コンパートメントは、テナンシが加入されるあらゆるリージョン内で利用可能にされることができる。

【0093】

ある実施形態に従うと、コンパートメントを削除することができる。コンパートメントを削除するために、コンパートメントは、削除に先立って、その中のすべてのリソースを

50

除去されることができる。

【0094】

ある実施形態に従うと、コンパートメントを削除するアクションは、非同期とすることができ、ワーク要求を開始する。コンパートメントの状態は、ワーク要求の実行中に「削除」に変わる。ワーク要求が失敗した場合、コンパートメントは削除されず、アクティブ状態に戻る。

【0095】

ある実施形態に従うと、クラウドインフラストラクチャ環境内に作成される各コンパートメントは、あるプロパティを有することができる。例えば、各コンパートメントに、一意の識別子（ID）を割り当てることができる、加えて、随意に、変更可能な記述および名前を提供することができる。ある実施形態に従うと、サブコンパートメントは、ベースコンパートメントの下に階層的に定義することができる。

【0096】

ある実施形態に従うと、コンパートメントおよびサブコンパートメントに対するアクセスならびに制御は、管理者または十分なクレデンシャルを有する他のユーザに限定することができる。クレデンシャルは、異なるレベルのコンパートメントアクセスに関連付けることができる。例えば、管理者は、すべてのコンパートメントを閲覧し、およびそれらにアクセスし、ならびにテナンシの任意のコンパートメント内のリソースで作業する許可を有することができるが、アクセスがより制限されたユーザは、そのようなレベルのアクセスおよび制御を有さない。

【0097】

図3は、一実施形態による、クラウドインフラストラクチャリージョンに跨がるポリシー管理および制御のためにコンパートメント360、コンパートメントポリシー365、サブコンパートメント370、およびサブコンパートメントポリシー375の間の関係を示すクラウドインフラストラクチャ環境300を示す。

【0098】

ある実施形態に従うと、上述したように、図1において上述したクラウドインフラストラクチャ環境のインスタンスは、クラウドインフラストラクチャリージョン320、330、340、350などの異なるリージョンにおいてホストされ得る。これらは、上述のように、コンソール、SDK、またはAPIを介して、インターネット等のネットワーク302を介して顧客ネットワーク301によってアクセスされることができる。

【0099】

ある実施形態に従うと、顧客ネットワーク301は、たとえば単一のコンピュータ、顧客コンピュータのネットワーク、または他のそのようなネットワークを含み得る。

【0100】

ある実施形態に従うと、図には示されていないが、各クラウドインフラストラクチャリージョンはいくつかのサービスを含み得、各サービスは、管理サービス、計算サービス、ストレージサービス、エッジサービス、ネットワークサービス、および物理インフラストラクチャなどのいくつかのリソースを含む。

【0101】

ある実施形態に従うと、クラウドインフラストラクチャは、リージョンおよび可用性ドメインにおいてホストされることができる。リージョンは、局所化された地理的エリアとすることができ、可用性ドメインは、リージョン内に位置する1つ以上のデータセンターとすることができ、リージョンは、1つ以上の可用性ドメインから構成される。大抵のクラウドインフラストラクチャリソースは、仮想クラウドネットワークなどのリージョン固有であるか、または計算インスタンスなどの可用性ドメイン固有のいずれかであり得る。可用性ドメイン間およびリージョン間のトラフィックは暗号化される。

【0102】

ある実施形態に従うと、可用性ドメインは、互いに隔離され、フォールトトレラントであり、障害が同時に生ずる可能性が非常に低い。可用性ドメインは、電力もしくは冷却な

10

20

30

40

50

どのインフラストラクチャ、または内部可用性ドメインネットワークを共有しないので、リージョン内の1つの可用性ドメインにおける障害は、同じリージョン内の他のものの可用性に影響を及ぼす可能性が低い。

【0103】

ある実施形態に従うと、同じリージョン内の可用性ドメインを低レイテンシの広帯域幅ネットワークによって互いに接続することができ、これにより、インターネットおよびオンプレミスへの高可用性接続性を提供し、高可用性および災害復旧の両方のために複数の可用性ドメインにおいて複製されたシステムを構築することができる。

【0104】

ある実施形態に従うと、リージョンは他のリージョンから独立しており、地理的に（たとえば国または大陸にわたって）分離されることができる。これは、次いで、あるアプリケーションが最も頻繁に利用される可能性が最も高いリージョン内における当該アプリケーションの展開につながる。

【0105】

しかしながら、ある実施形態に従うと、アプリケーションは、さまざまな理由により、異なるリージョンにおいて展開されもし得る。これは、例えば、気象システムなどのイベントがリージョンをオフラインで取るときリスク軽減を含むことができる。加えて、アプリケーションは、課税ドメインまたは他の事業もしくは社会的基準などの戦略的な理由で他のリージョンに展開されることができる。

【0106】

ある実施形態に従うと、リージョンにわたって利用可能ないくつかのサービスがある。これらは、例えば、管理サービス、計算サービス、ストレージサービス、エッジサービス、およびネットワークサービスを含む。

【0107】

ある実施形態に従うと、コンパートメントにより、クライアントは、クラウドリソースを編成し、それに対するアクセスを制御することが可能になる。コンパートメントは、管理者によって許可が与えられた特定のグループによってのみアクセスされ得る関連リソース（インスタンス、仮想クラウドネットワーク、ブロックボリュームなど）の集まりである。コンパートメントは、物理的なコンテナではなく、論理的なグループと考えることができる。コンソール内で作業するとき、コンパートメントは、見られることを可能にされるものについてのフィルタとして作用することができる。

【0108】

ある実施形態によると、コンパートメントは、いくつかの層を有することができる。例えば、テナンシ305は、クライアントのクラウドリソースのすべてを保持するルートコンパートメントと見なすことができる。コンパートメントは、コンパートメント360がテナンシコンパートメントの下レベルであり、サブコンパートメント370がコンパートメント360の下追加の層であるように、階層的態様で編成することができる。ある実施形態に従うと、各コンパートメントは、コンパートメントポリシー365およびサブコンパートメントポリシー375などの1つ以上のコンパートメントポリシーに関連付けることができる。テナントコンパートメントポリシーは、図に示されていない。

【0109】

ある実施形態に従うと、コンパートメントまたはサブコンパートメント、たとえばコンパートメント360およびサブコンパートメント370の作成中、作成時、または作成後に、コンパートメントポリシー365およびサブコンパートメントポリシー375などのポリシーを、各コンパートメントおよびサブコンパートメントについて記述／作成することができる。ポリシーが適所にない場合、コンパートメントおよび／またはサブコンパートメントへのアクセスは、テナンシ305レベルにおいて許可を有するユーザに制限され得る。

【0110】

ある実施形態に従うと、コンパートメント内におけるコンパートメント（すなわち、サ

10

20

30

40

50

ブコンパートメント)の作成時に、サブコンパートメントは、その階層の上位のコンパートメントからアクセス許可を継承する。

【0111】

ある実施形態に従うと、コンパートメントまたはサブコンパートメントポリシーを作成すると、そのポリシーは、それがどのコンパートメントにアタッチするかを示す仕様を含み得る。そのような仕様は、ポリシーのサブシーケンス制御、修正、または削除のためのアクセスを制限する制御を含み得る。いくつかの実施形態では、ポリシーは、テナンシ、親コンパートメント、またはポリシーが向けられる特定のコンパートメントにアタッチされ得る。

【0112】

ある実施形態に従うと、新たなリソースをコンパートメントに配置することができる。これは、新たなリソースの作成時にターゲットとされるコンパートメントを指定することによって達成することができる(コンパートメントは、リソースを作成するために必要な情報の1つである)。これは、コンソールインターフェイスを介して達成することができる。

【0113】

ある実施形態に従うと、既存のリソースを異なるコンパートメントに移すこともできる。ほとんどのリソースは、それらが作成された後に移動され得る。あるコンパートメントから別のコンパートメントに移動することができないリソースは少数である。

【0114】

ある実施形態に従うと、いくつかのリソースはアタッチされたリソース依存関係を有し、いくつかはアタッチされたリソース依存関係を有さない。親リソースが移動するとき、すべてのアタッチされた依存関係が同じように振る舞うわけではない。

【0115】

ある実施形態に従うと、いくつかのリソースについて、アタッチされた依存関係は親リソースとともに新たなコンパートメントに移動する。親リソースは直ちに移動するが、場合によっては、アタッチされた依存関係は非同期的に移動し、移動が完了するまで新たなコンパートメント内においては可視ではない。

【0116】

ある実施形態に従うと、他のリソースについては、アタッチされたリソース依存関係は新たなコンパートメントには移動しない。このようなアタッチされたリソースは、独立して移動させることができる。

【0117】

ある実施形態に従うと、リソースが新たなコンパートメントに移動された後、その新たなコンパートメントを管理するポリシーが即座に適用され、そのリソースへのアクセスに影響を与える。コンパートメント編成の構造に応じて、メータリング、課金、および警報も影響を受ける可能性がある。

【0118】

ある実施形態に従うと、作成後、コンパートメントを、たとえば同じテナンシ内の異なる親コンパートメントに移動させることができる。コンパートメントを移動させると、コンパートメントのコンテンツ(サブコンパートメントおよびリソースを含む)のすべてがコンパートメントとともに移動する。

【0119】

図4は、ある実施形態に係る、クラウドインフラストラクチャ環境内でのコンパートメント移動のためのシステムを示す図である。

【0120】

ある実施形態に従うと、上述したように、図1において上述したクラウドインフラストラクチャ環境400のインスタンスは、異なるリージョンにおいてホストされ得る。テナンシ405、コンパートメントA460およびコンパートメントB470などのコンパートメントは、クラウドインフラストラクチャ環境内に画定することができ、これらのコン

10

20

30

40

50

パートメントは、リージョンに跨ることができる。そのようなコンパートメントは、上述のように、コンソール、SDK、またはAPIを介して、インターネット等のネットワーク402を介して顧客ネットワーク401によってアクセスされることができる。

【0121】

ある実施形態に従うと、顧客ネットワーク401は、たとえば単一のコンピュータ、顧客コンピュータのネットワーク、または他のそのようなネットワークを含み得る。

【0122】

ある実施形態に従うと、コンパートメントにより、クライアントは、クラウドリソースを編成し、それに対するアクセスを制御することが可能になる。コンパートメントは、管理者によって許可が与えられた特定のグループによってのみアクセスされ得る関連リソース（インスタンス、仮想クラウドネットワーク、ブロックボリュームなど）の集まりである。コンパートメントは、物理的なコンテナではなく、論理的なグループと考えることができる。コンソール内で作業するとき、コンパートメントは、見られることを可能にされるものについてのフィルタとして作用することができる。

【0123】

ある実施形態によると、コンパートメントは、いくつかの層を有することができる。例えば、テナンシ405は、クライアントのクラウドリソースのすべてを保持するルートコンパートメントと見なすことができる。コンパートメントは、コンパートメントA460およびコンパートメントB470がテナンシコンパートメントの下レベルであり、サブコンパートメントA465がコンパートメントAの下に画定され、サブコンパートメントB475がコンパートメントBの下に画定されるように、階層的様式で編成することができる。ある実施形態に従うと、各コンパートメントは、1つ以上のコンパートメントポリシー（図示せず）に関連付けることができる。

【0124】

ある実施形態に従うと、たとえばテナンシ内に画定されたコンパートメントは、たとえばコンパートメントまたはサブコンパートメントを再画定することによって移動させることができる。

【0125】

ある実施形態に従うと、コンパートメントを移動させるために、十分な許可を有する要求を受け取ることができる。すなわち、当該要求は、例えば、現在のコンパートメントおよび移動コンパートメントの宛先コンパートメントに対する最も低い層で共有された親コンパートメントに関する「全リソース管理」許可を有するグループに属するユーザからの要求である。

【0126】

すなわち、例えば、サブコンパートメントA465をコンパートメントA460からコンパートメントB470に移動する（465から476に移動する）要求は、ユーザから十分な許可とともに受信されなければならない。テナンシ405は、送信元コンパートメントであるコンパートメントA460および宛先コンパートメントであるコンパートメントB470の両方の最も低い層で共有された親コンパートメントであるため、図に示されるように、サブコンパートメントAを移動させる要求は、テナンシ405のコンパートメント内で「全リソースを管理する」許可を有するユーザから受信されなければならない。

【0127】

ある実施形態に従うと、別の例では、サブコンパートメントA465をコンパートメントAからコンパートメントBに移動させる要求が、コンパートメントA内の「全リソースを管理する」許可のみを有するユーザから受信された場合、その要求は失敗し得、なぜならば、ユーザからの要求は、宛先コンパートメント、すなわちコンパートメントB内のリソースを管理することができないからである。

【0128】

ある実施形態に従うと、コンパートメントを新たな親コンパートメントに移動させると、新たな親コンパートメントのアクセスポリシーが有効となり、前の親コンパートメント

10

20

30

40

50

のポリシーはもはや適用されない。場合によっては、階層を指定するポリシーとともに入れ子にされたコンパートメントを移動させるとき、それらのポリシーは整合性を保証するために自動的に更新され得る。

【0129】

したがって、ある実施形態によると、以前にサブコンパートメントAに適用されたコンパートメントA460のコンパートメントポリシーは、サブコンパートメントAのコンパートメントBへの移動にはもはや適用されないであろう。次いで、コンパートメントBのコンパートメントポリシーが、代わりにサブコンパートメントAに適用される。これは、以下の図でさらに説明される。

【0130】

図5は、クラウドインフラストラクチャ環境内のコンパートメント移動中のポリシー管理および施行のためのシステムを示す。

【0131】

一実施形態によれば、より具体的には、図5は、コンパートメントが移動されるコンパートメント階層と、異なるポリシーに関する結果とを示す。

【0132】

ある実施形態に従うと、上述したように、図1において上述したクラウドインフラストラクチャ環境500のインスタンスは、異なるリージョンにおいてホストされ得る。テナンシ505、コンパートメントA560およびコンパートメントB565、ならびにコンパートメントD566等のコンパートメントは、クラウドインフラストラクチャ環境内で画定することができ、これらのコンパートメントは、リージョンに跨ることができる。そのようなコンパートメントは、上述のように、コンソール、SDK、またはAPIを介して、インターネット等のネットワーク502を介して顧客ネットワーク501によってアクセスされることができる。

【0133】

ある実施形態に従うと、顧客ネットワーク501は、たとえば単一のコンピュータ、顧客コンピュータのネットワーク、または他のそのようなネットワークを含み得る。

【0134】

ある実施形態によると、コンパートメントは、いくつかの層を有することができる。例えば、テナンシ505は、クライアントのクラウドリソースのすべてを保持するルートコンパートメントと見なすことができる。コンパートメントは、コンパートメントA560がテナンシの下レベルであるように、階層的に編成することができる。次いで、コンパートメントB565およびコンパートメントD566は、コンパートメントA560の下にさらに別のレベルとして編成されるが、サブコンパートメントC570は、最初はコンパートメントBの下レベルとして示される。ある実施形態に従うと、各コンパートメントは、コンパートメントBポリシー582、コンパートメントAポリシー580、およびコンパートメントDポリシー583などの1つ以上のコンパートメントポリシーに関連付けることができる。そのようなポリシーは、例えば、コンパートメントへのアクセスのためのユーザ／クライアント許可、ならびに任意の所与のコンパートメント内のリソースへのアクセスおよびそれらリソースの制御のための許可を管理することができる。上述のように、コンパートメントポリシーは、コンパートメントB565にアクセスするユーザが、コンパートメントAポリシー580に加えてコンパートメントBポリシー582によって管理／制限されているコンパートメントB565との対話を有するように、互いに追加（すなわち「スタック」）することができる。

【0135】

ある実施形態に従うと、たとえば、コンパートメントBポリシー582が、あるグループ、グループ1がコンパートメントA-B内のインスタンスファミリーを管理することを可能にすると仮定する（コンパートメント階層は、コンパートメントAのサブコンパートメントであるコンパートメントBを含む）。

【0136】

ある実施形態に従うと、コンパートメントDポリシー583は、別のグループ、グループ2がコンパートメントA-D内のインスタンスファミリーを管理することを可能にすることも仮定する（コンパートメント階層は、コンパートメントAのサブコンパートメントであるコンパートメントDを含む）。

【0137】

ある実施形態に従うと、コンパートメントCがコンパートメントBからコンパートメントDに移動されると、グループ1のメンバーは、もはやコンパートメントC内のインスタンスファミリーを管理することはできず、グループ2のメンバーが、今度は、コンパートメントC内のインスタンスファミリーを管理することができる。

【0138】

ある実施形態に従うと、ある状況において、コンパートメントを移動させると、あるポリシーを自動的に更新することができる。例えば、移動されるコンパートメントまでのコンパートメント階層を指定するポリシーは、ポリシーが現在のターゲット親の共有先祖にアタッチされると、自動的に更新され得る。

【0139】

再び図5を参照すると、例えば、一実施形態によれば、コンパートメントAポリシーは、あるグループ、グループXのメンバーがコンパートメントB:C内のバケットを管理することを可能にすると仮定する。コンパートメントCをコンパートメントDに移動すると、コンパートメントBとコンパートメントDとの間の共有先祖（コンパートメントA）のため、コンパートメントAポリシーは、グループXのメンバーがコンパートメントD:C内のバケットを管理することを可能にするように、自動的に更新され得る。

【0140】

ある実施形態に従うと、テナンシにアタッチされたポリシーは同様に、コンパートメントがテナンシ内を移動すると、自動的に更新されることができる。

【0141】

しかしながら、ある実施形態に従うと、コンパートメントの移動で、すべてのポリシーが自動的に更新されるわけではない。例えば、図5を参照すると、コンパートメントCがコンパートメントBからコンパートメントDに移動される状況において、コンパートメントBポリシーは、（移動前に）コンパートメントC内のバケットの管理を可能にすると仮定する。コンパートメントCが移動される場合、コンパートメントBポリシーは自動的に更新されない。代わりに、ポリシーは、もはや有効ではなく、（例えば、手動または自動で）除去され得る。

【0142】

タグベースのリソース制限／割り当て

ある実施形態に従うと、クラウド管理者は一般に、既存のクラウドにおけるリソース使用を制限する能力を有していない。ユーザにリソースを作成するための許可を与えることにより、ユーザは、事前定義されたアカウント限度まで任意の数のリソースを作成することが可能になる。タグベースのリソース制限または割り当ては、コンパートメント内でリソースを作成または使用する能力に、微調整されたコスト制御を可能にする適切なレベルへの制限を課すことを可能にする。

【0143】

ある実施形態に従うと、顧客は、アカウント作成時にクラウドインフラストラクチャ環境によって定義されるサービスレベル制限を割り当てられることができる。これらのサービスレベル制限は、顧客がテナンシ全体にわたって（例えば、複数のコンパートメントを伴う複数のリージョンにわたって）作成することができるリソースの総数を制限する。テナンシおよびコンパートメント管理者は、タグベースのリソース制限または割り当てを利用して、リソース固有の厳しい制限を設定することができる。個々のリソースに対するそのようなコンパートメント制限がなければ、インスタンスを起動することを承認されたユーザは、テナンシ全体においてすべての利用可能な容量を消費し得る。タグベースのリソース制限または割り当ては、この問題を解決し、サービス制限とは異なり、例えば、コン

10

20

30

40

50

ソール、SDK、またはAPIを介して、クライアントおよび顧客によって設定およびカスタマイズされる。タグベースのリソース制限または割り当ては、サービス制限の上に適用され、ネスト化されたコンパートメント階層を通じて継承され得る。これは、クラウド管理者がリソース消費を制限し、許容可能なリソース使用の周りに境界を設定することを可能にする。

【0144】

ある実施形態に従うと、タグベースのリソース制限または割り当ては、テナントおよびコンパートメント管理者に、クラウドインフラストラクチャ環境においてリソースがどのように消費されるかをよりよく制御させ、管理者が、たとえばコンソール、SDK、もしくはAPIを用いて、ユーザまたはユーザのグループにリソースを容易に割り当てることを可能にする。コンパートメント割り当ては、テナント内でのクライアントの支出を管理するための強力なツールセットである。

10

【0145】

ある実施形態に従うと、クライアントがテナンシにおいて複数のコンパートメントにわたってリソース（例えば、インスタンス、VCN、ロードバランサ、およびブロックボリューム）を有する場合、特定の目的のために用いられるリソースを追跡すること、またはそれらを集約すること、それらについて報告すること、もしくはそれらについてバルクアクションをとることは困難になり得る。タグ付けは、クライアントがキーおよび値を定義し、それらをリソースに関連付けることを可能にする。タグは、リソースの編成およびリスト化を支援するために用いることができる。一般に2種類のタグ、すなわち自由形式タグおよび定義済みタグがあるが、例示的な実施形態によれば、他のタイプのタグも可能である。

20

【0146】

ある実施形態に従うと、自由形式タグはキーおよび値からなることができる。例えば、「環境：制作」は自由形式タグの例であり、「環境」はキーであり、「制作」は値である。複数の自由形式タグを単一のリソースに適用することができる。

【0147】

ある実施形態に従うと、定義済みタグは、自由形式タグよりも多くの特徴および制御を提供する。クライアントが定義済みタグキーを作成する前に、定義済みタグに対してタグ名前空間を設定することができる。名前空間は、タグキーのセットのためのコンテナと考えることができる。定義済みタグは、誰があなたの定義済みタグを適用することができるかに対する制御を可能にするポリシーをサポートする。タグ名前空間は、クライアントがポリシーを適用することができるエンティティである。

30

【0148】

ある実施形態に従うと、定義済みタグをリソースに適用するために、ユーザはまずタグ名前空間を選択し、次いで名前空間内でタグキーを選択し、次いでユーザは値を割り当てることができる。管理者は、どのグループのユーザが各名前空間を用いることを許されるかを制御することができる。例示的な実施形態によれば、タグは、リソースが作成される際にリソースに適用されてもよい。別の実施形態では、タグは、リソースがプロビジョニングされた後にリソースに適用されてもよく、それによって、タグを用いるシステムにおけるリソース割り当てまたは制限の遡及的实施を可能にする。ある実施形態に従うと、タグを用いて、コスト管理および／またはリソース管理を可能にすることができる。このように、タグは、コストを追跡するために用いられ得る。

40

【0149】

図6は、一実施形態による2つの定義済みタグを示す。2つのタグ名前空間、名前空間1 600および名前空間2 620（例えば、名前空間1は「営業」であり得、名前空間2は「人事」であり得る）が設定される。タグキー605、610、625、および630は、名前空間において定義される。各名前空間内では、タグキーは一意であり得るが、タグキー名は名前空間にわたって繰り返され得る。例えば、両方の名前空間は、「環境」と名付けられたキーを含むことができる。

50

【0150】

ある実施形態に従うと、多くのクラウドプロバイダは、容量不足からの保護のためにサービス制限を設ける。しかしながら、多くの場合、クライアントは、自分自身がリソース過剰にならないように制限を設定することも望む。1つのそのようなアプローチは、グループレベルで制限を指定することである。グループは、ユーザ、リソース、またはユーザが指定したい任意のもののセットを含むことができる。グループレベル制限は、特定のテナンシ／アカウントの管理者／ユーザによって設定される。

【0151】

ある実施形態に従うと、一例として、テナンシ管理者またはグループ管理者は、それらのクラウドコストを制御するために、グループレベルで制限を構成することができる。これは、クラウドリソースが、特定のグループ内で作成されるリソースと関連付けられるドルコストに変換される使用データを放出する際に、そのグループが、テナンシまたはアカウント管理者によって設定される使用制限を超えないことの保証を、顧客／会社に与える。この意味で、グループは、コストセンターグループと考えることができ、なぜならば、そのグループのメンバーによって作成されるリソースのクラウドコストのすべてが、単一の集約された一括料金として顧客／会社に割り当てられたり、または単一のグループアカウントに対して集約されるなどするからである。

【0152】

しかしながら、ある実施形態によれば、管理者がコストを制御するための非常に単純な機構が存在するため、問題が存在する。例として、管理者は、特定のグループを含むかまたはリソース過剰から除外することができ、または管理者は、アクセスを拒否することによってリソースを作成する特定のユーザを除外することができる。しかしながら、これらは粒度の粗い機構であり、顧客は概して、彼らのクラウドリソースを管理するための柔軟性およびより良好な制御を彼らに与える細かい粒度の機構を指定する能力を有しているというわけではない。

【0153】

ある実施形態に従うと、細かい粒度のアプローチは、タグに基づいてリソース制限を設けることができ、特定のグループの1人以上のメンバーによってプロビジョニングされ得るリソースのすべてが、そのグループを表すコストセンタータグに関連付けられるか、またはさもなければコストセンタータグを提供される。この性質のコストセンタータグは、リソース管理における使用のための機構を提供し、クラウドプロバイダは、コスト管理のためにもそれらを用いる。システムおよび方法は、タグを通してグループレベルでコストを制御するための機構を作成することができる。例として、ユーザは、以下のような細かい粒度のルール／ポリシーを指定することができる：

Set limits <resource type> to 10 in group A where target.resource.tag = "finance"
(制限<リソースタイプ>をグループAにおいて10に設定し、ターゲットリソースタグ＝「財務」である)

ある実施形態に従うと、タグはリソースに関連付けることができ、上記アプローチを用いて、タグは、顧客をグループレベルでリソース過剰から保護することができる。上記の例では、タグ値がグループAにおいて「財務」である場合、ユーザメンバーは、<リソースタイプ>の10を超えるインスタンスを作成することはできないことになる。グループレベルでコストを制限するこのアプローチは、コストおよびリソース使用をより良く管理するために、細かい粒度の機構をクライアントに提供する。

【0154】

ある実施形態に従うと、システムは、クラウドインフラストラクチャ環境において、リソース要求コンテキストタグベースの限度／割り当てを設ける。システムは、要求コンテキストに基づいてクラウドインフラストラクチャ環境におけるリソースのプロビジョニングを制限するかまたはそれに割り当てを課すための方法を実行する。

【0155】

ある実施形態に従うと、システムは、クラウドインフラストラクチャ環境においてタグ

10

20

30

40

50

ベースのリソース制限／割り当てを設ける。システムは、リソースタグに基づいてクラウドインフラストラクチャ環境においてリソースをプロビジョニングすることを制限するかまたはそれに割り当てを課すための方法を実行する。

【0156】

ある実施形態に従うと、高度にセキュアな環境では、顧客は、リソースおよび顧客のデータへのアクセスをセキュリティ保護したいと望む。例として、顧客は、彼らのリソースを、高機密性、機密性、制限付き、公開などとして分類することによって保護し、ユーザに対して、制約に従ったユーザのクリアランスに基づいて、アクセスを許可する。分類されたリソース／データへのアクセスを有するユーザは、情報漏洩がないことを確実にし、共有コンテキスト内においてデータ分類にわたるリソースへの不注意による変更を回避するために、データにアクセスする際に極めて慎重である必要がある。本明細書の実施形態は、ユーザが、所与のセッション／コンテキストについてデータ分類境界内においてアクセスを制限するかまたはリソースを修正することを可能にするための改善されたシステムおよび方法を提供するが、ユーザは、そうでなければ、より高いアクセスを有し得る。

10

【0157】

ある実施形態に従うと、クラウドアーキテクチャは、ユーザを役割内に投入することにより、ルール（役割）をベースとしたアクセス制御技術を用いて、特定のセキュリティ境界へのアクセスを制限／許可することができる。しかしながら、これらの技術は粗粒化されている。実施義務は、ユーザがアクセスしている、修正している、または実行しているものについて、ユーザが入念かつ慎重であることにある。

20

【0158】

ある実施形態に従うと、本開示のシステムおよび方法は、ユーザが意図しないときにある動作を実行するようリソースにアクセスすることからユーザを保護する。一例は、ユーザが高度に分類されたリソースへのアクセスを有するときに他の分類のデータにアクセスすることである。例えば、ユーザが、高度に分類されたリソースをフィルタリングで除去することによって、分類されていないリソースにアクセスすることのみを必要とするスクリプトを有すると仮定する。ここで、ユーザ／スクリプトは、どのデータ／リソースが分類され、どのデータ／リソースが分類されないかを知らなければならない。

【0159】

ある実施形態に従うと、別の例は、ユーザが、事業の終了後にビジネスクリティカルではないインフラストラクチャをシャットダウンすることにのみ関心があり、ビジネスクリティカルである他のリソースは稼働させ続けることを望む場合である。ここで、ユーザは、どのインスタンスをオフにすべきかを正確に知らなければならない。

30

【0160】

ある実施形態に従うと、本明細書のシステムおよび方法は、そのような問題に対する解決策を、リソースに対する1つ以上の要求に添付されるタグを介して提供する。スクリプトからの要求は、ユーザの代わりに、例えば、インスタンスをシャットダウンすること、リソースの詳細を読み出すこと、リソースを更新すること、分類されたリソースにアクセスすること等の動作を実行する。ユーザは、これらの要求を、要求コンテキストに添付された1つ以上のタグとともに送信する。要求がリソース上でアクションを実行するとき、要求コンテキストからのこれらのタグを検査することができ、次いで、たとえユーザが、最初は、ユーザが実行したい動作を実行するためのアクセスを有していたとしても、その動作を実行するためのアクセスを拒否または許可することができる。これは、ユーザがその特定のリソースに対して意図しなかった操作を行うことによる、高度に分類されたデータまたはリソースへの意図しないアクセスを回避する。これは、タグベースの自動化に該当し得る。それは、セキュリティに関連する分野だけでなく、多種多様な使用例に対応することができる。

40

【0161】

ある実施形態に従うと、リソース要求コンテキストを表すタグを用いることにより、要求を送信することによってリソースにアクセスする際に、タグを介してセキュリティ境界

50

を形成することができる。

【0162】

ある実施形態に従うと、ある動作を実行するためにユーザがリソースにアクセスしたい場合、ユーザは一般にソフトウェア開発キットを介して呼び出しを行うことができるか、またはAPI呼び出しを直接行うことになる。ユーザは、リソースに送信される要求に追加される1つ以上のタグを渡すことができる。ユーザを承認している間、リソースインプリメンテーションは、要求に関連付けられるタグを検査することができ、タグがユーザタグと一致する場合、要求は許可され、そうでない場合には、要求は拒絶／拒否される。

【0163】

図7は、例示的な実施形態による、たとえばリソースタグおよび／またはリソース要求コンテキストタグを含むタグに基づいてクラウドインフラストラクチャ環境においてリソースに対する割り当てまたは制限を実施するシステムにおいてインスタンスを起動するユーザのためのアーキテクチャフローを示す。

【0164】

ある実施形態に従うと、ステップ1において、ユーザ701は、リージョン700においてインスタンスを起動するように要求し、この要求は、リージョン700内で規定される1つ以上のタグ（例えば、自由形式タグまたは定義済みタグ）に関連付けられる。例示的な実施形態では、タグは、リソースに対するユーザからの要求のコンテキストを表す。

【0165】

ある実施形態に従うと、ステップ2において、ロードバランサ720は、パブリックプロキシAPI725のようなAPIに要求を転送する。

【0166】

ある実施形態に従うと、ステップ3において、APIは、アイデンティティデータプレーン735において認証を実行する。

【0167】

ある実施形態に従うと、ステップ4において、インスタンスを起動する要求を、計算制御プレーン（CCP）730に転送することができる。次いで、CCPは、ステップ5において、アイデンティティデータプレーンにおいて要求をさらに認証することができる。

【0168】

ある実施形態に従うと、ステップ6において、計算制御プレーンは、ユーザ701からの要求の一部であるタグに関連付けられるすべてのタグベースの制限／割り当て750を制限サービスデータプレーン740からフェッチすることができる（代替的に、フェッチ動作は、リソース制御プレーンにおいて実行され得る）。そのようなタグベースの割り当ては、例えば、テナンシ全体にわたって適用することができ、コンパートメント固有である必要はない。

【0169】

ある実施形態に従うと、ステップ7において、計算制御プレーンは、750において、要求された使用が任意のものに対するタグベースの制限／割り当てのいずれかに違反するかどうかをチェックすることができる。要求された使用がいかなるコンパートメント割り当てにも違反しない場合、要求は、例えばデータベース745に処理されることができる。要求された使用がコンパートメントツリーに沿ったタグベースの制限／割り当てのいずれかに違反する場合、要求はドロップされ得、ユーザに通知すべくメッセージが送信され得る。

【0170】

ある実施形態に従うと、タグベースの制限／割り当ては、たとえばテナンシがテナンシ内における有効化されたコンパートメントであるすべてのリージョンを含むテナンシ全体にわたって適用される。要求されたインスタンスがタグベースの制限／割り当てに違反するかどうかを判断するとき、CCPは、新たな要求が、例えばサービス開発者キット（SDK）を介して、割り当てのいずれにも違反しないことを保証することができる。要求が割り当てを超える場合、CCPは要求を落とすことができる。

10

20

30

40

50

【0171】

ある実施形態に従うと、CCPのSDKは、クラウドインフラストラクチャ環境のすべての制御プレーンに存在し得る。

【0172】

ある実施形態に従うと、CCPは、制限サービスデータプレーンと連携して、新たな要求をタグベースの制限／割り当てに対してチェックすることができる。

【0173】

ある実施形態に従うと、クライアントがクラウドリソースを作成する動作をトリガすると、要求はリソース制御プレーンに進む。リソース制御プレーンは、グループレベルで構成された制限を考慮して、リソースが安全にスピンアップされ得るかどうかを知るべく、制限サービスから尋ねる。制限サーバがリソース制御プレーンに否定／失敗応答を返す場合、リソースは作成されない。

10

【0174】

内部的に、制限サービスが要求を受信すると、制限サービスは、リソース作成に関連付けられるタグをチェックし、その特定のタグを有するリソースの現在の使用を見るために、ストアもしくはデータベースまたはメモリを参照する。タグ値がグループレベルで設定された制限を超える場合、リソース生成が失敗するようにリソース制御プレーンに失敗／否定応答を送信する。

【0175】

リソース制限／割り当てのためのタグの使用

20

図8は、クラウドインフラストラクチャ環境におけるリソースのプロビジョニングなどの使用を制限するために要求コンテキストタグおよび／またはリソースタグを用いるシステムを示す。

【0176】

ある実施形態に従うと、クライアントデバイス810は、クラウドインフラストラクチャ環境に要求811を提出することができ、要求は、たとえば要求のコンテキストを表すタグなどのタグ812に関連付けられる。クライアントデバイスは、コンソール802、API804、またはSDK806等のインターフェイスのうちの1つを介して、(デバイスハードウェア801上で動作する)クラウドインフラストラクチャ環境800に要求を提出することができる。

30

【0177】

ある実施形態に従うと、要求はリソース840に転送され得、これは、タグ付けされたリソース851～854を含む計算リソース層850、タグ付けされたリソース861～864を含むネットワークリソース層860、およびタグ付けされたリソース871～874を含むストレージリソース層870など、(上述したように)いくつかの層を含み得る。

【0178】

ある実施形態に従うと、クライアントデバイスが高いセキュリティ／優先度特権(たとえば不正保護、またはインテリジェンス)を享受する場合、クライアントデバイスは、要求に関して広範囲のタグを利用することができる。例として、要求に関連付けられるタグは、ユーザが保護されたリソースに誤って触れることから助けるために用いられ得る。例えば、コストを節約するために、特定の計算リソースを毎日午後6時以降にシャットダウンすることができる。そのような計算リソースは、低セキュアなタグを有する。しかしながら、同じシステムは、シャットダウンすることができない他の計算リソースも有する(24/7で実行されなければならない)。そのような計算リソースは、高セキュアなタグを有する。低特権計算リソースをシャットダウンするために、ユーザは、タグ付けされた要求を有することなく、各リソースに進み、シャットダウンされるべきリソースのみを選択するか、またはそうするようスクリプトを書いて、24/7を実行する必要がある高特権リソースをシャットダウンすることを回避するようにしなければならないであろう。これは、計算リソースが毎日追加および除去され得るため、これを維持すること

40

50

が困難である。

【0179】

ある実施形態に従うと、ユーザは代わりに、タグ付けされた要求を提供して低特権リソースをシャットダウンすることができる。すなわち、要求に関連付けられるタグは、午後6時にシャットダウンされ得る計算リソースと、低セキュアなタグを共有するであろう。次いで、タグは、ネットワーク内のすべてのリソースに進むことができるが、要求が有するタグを有さない高度に保護されたリソースはバイパスすることになる。このように、計算リソースをシャットダウンするタグ付き要求は、低セキュアなタグが一致する計算リソースのみをシャットダウンし、高セキュアなタグ付き計算リソースはバイパスした。

【0180】

ある実施形態に従うと、別の例として、クライアント810が高度にセキュアな計算インスタンスをブロックボリュームにアタッチすることを望むと仮定する。そのような状況では、高度にセキュアな計算インスタンスをアタッチする要求は、高セキュアなタグでタグ付けされ得る。次いで、そうすることによって、これは、高度にセキュアな計算インスタンスが、より低セキュアなタグを有するブロックボリュームにアタッチされないことを保証することができ、代わりに、要求は、高度にセキュアな計算インスタンスを、同様にタグ付けされた（高度にセキュアな）ブロックボリュームにアタッチすることしかできない。言い換えれば、要求は、高度にセキュアな計算を低セキュアなブロックボリュームにアタッチしない（タグチェックは失敗することになる）。

【0181】

要求コンテキストタグベースの制限／割り当て

図9は、一実施形態による、クラウドインフラストラクチャ環境においてリソース要求タグベースの制限／割り当てを設けるシステム900の機能概略図である。概して、クライアントデバイス810（図8）は、複数のタグ付けされたリソース940の中で新たなリソースをプロビジョニングするための要求911をクラウドインフラストラクチャ環境に提出することができる。複数のタグ付けされたリソース940は、例えば、計算リソース層850のタグ付けされた計算リソース851～854、ネットワークリソース層860のタグ付けされたネットワークリソース861～864、および／またはストレージリソース層870のタグ付けされたストレージリソース871～874のいずれかであり得る。

【0182】

例示的实施形態によると、リソースは、クラウドインフラストラクチャ環境においてプロビジョニングされるアイテムであり、例えば、いくつか例を挙げると、計算リソースタイプ、ストレージサービスリソースタイプ、VCNサービスタイプ、IPアドレスサービスタイプ、DNSサービスタイプ、DDoSサービス保護タイプ、および電子メール配信サービスタイプを含み得る、種々のタイプであり得る。本明細書における例示的な実施形態は、これらの特定のリソースタイプに限定されず、他のタイプも含み得、さらなるリソースタイプの例が、例として以下で言及される。

【0183】

【表1】

例示的なリソースタイプ
計算
ストレージ
VCN
IPアドレス
DNS

【0184】

例示的な実施形態によれば、プロビジョニングされるリソースおよびサービスはタグ付け可能である。例示的な実施形態では、リソースに対する要求およびリソースは、1つ以上のタグと関連付けられる。加えて、リソースは、それらのタグ値に基づいてグループ化され得る。本質的に、例示的な実施形態では、各プロビジョニングされたリソースと関連付けられるリソースタグは、クラウドインフラストラクチャ環境においてプロビジョニングされたリソースにアタッチされ得るか、または別様にそれらに関連付けられ得る、キー値ペアである。タグキー値ペアは、例えば、様々な会計目的を含む多くの目的のために用いられ得る。ある例では、プロビジョニングされたリソースに関連付けられるリソースキー値ペアタグは、リソースをグループ化するために用いられ、リソースタグによって提供されるグループ化は、クラウドインフラストラクチャ環境における値のすべてのコスト管理および／またはリソース管理を可能にする。

10

【0185】

クラウドインフラストラクチャ環境においてプロビジョニングされるリソースは、各リソースに割り当てられたタグ値に基づいて、または必要もしくは所望に応じて他の基準に基づいて、コンテナ942、944、946にグループ化されてもよい。例として、第1のコンテナ942は、クラウド内でプロビジョニングされ、クライアントユーザ701（図7）の会計グループと関連付けられる計算リソースおよびストレージリソースを記憶し得、第2のコンテナ944は、クラウド内でプロビジョニングされ、クライアントユーザ701の営業グループと関連付けられる計算リソースを保持し得、第3のコンテナ946は、クラウド内でプロビジョニングされ、クライアントユーザ701の人事グループと関連付けられる計算リソースを保持し得る。本明細書における例示的な実施形態は、これらのグループに限定されず、他のグループも同様に用いることができ、さらなる例示的なグループを例として以下に示す。

20

【0186】

【表2】

リソースグループの例
営業
人事
財務
経理
法務
マーケティング

30

【0187】

ある例に従うと、リソースインスタンスは、異なるコンテナ942、944、946に論理的に配置され、それにより、別々のコストセンターを提供し、各コストセンターにはタグ値が割り当てられ、エンドユーザは、さまざまなコストセンターへのアクセスについて請求され得、コストセンターのタグは、コスト管理および課金のために用いられる。一部の顧客は、彼らのエンドグループ価格内で複数のコストセンターをモデル化し得る。各コストセンターに対して別個のタグが存在してもよく、クラウドは、各タグに対して、限定されたリソースのセットを割り当ててもよい。

40

【0188】

例示的な実施形態では、1つ以上のポリシー920は、エンドユーザがアクセスについて標準契約で許可されるよりも多くのリソースにアクセスすることから自身を保護するための機構を提供し、実質的過剰は、エンドユーザが標準契約の標準契約条件下で許可されるよりも多くのリソースにアクセスすることによって生じ得る。例えば、顧客は、リソース制御プレーン930を介して、例えば、100個の計算リソース等の複数の計算リソースのプロビジョニングをアクティブにする、リソースに対する要求を送信し得、契約条件は

50

、標準レートで90個のコンピュータリソースのプロビジョニングのみを許可しており、過剰分が、この実施例では10が、顧客エンドユーザに対して追加費用を招く。

【0189】

上述したように、そしてある実施形態に従うと、細かい粒度のアプローチは、タグに基づいてリソース制限を設けることができる。タグは、主にリソース管理において用いられる機構であり、クラウドプロバイダはそれらをコスト管理のためにも用いる。システムおよび方法は、タグを通してグループレベルでコストを制御するための機構を作成することができる。例として、ユーザは、以下のような細かい粒度のルール／ポリシーを指定することができる：

Set limits <resource type> to 10 in group A where target.resource.tag = "finance" 10
(制限<リソースタイプ>をグループAにおいて10に設定し、ターゲットリソースタグ = 「財務」である)

ある実施形態に従うと、タグは、リソースおよびリソースの要求またはその両方に関連付けることができ、上記アプローチを用いて、タグは、たとえばグループレベルなどの1つ以上の選択されたレベルで顧客をリソース過剰から保護することができる。上記の例では、タグ値がグループAにおいて「財務」である場合、ユーザメンバーは、<リソースタイプ>の10を超えるインスタンスを作成することはできないことになる。グループレベルでコストを制限するこのアプローチは、コストおよびリソース使用をより良く管理するために、細かい粒度の機構をクライアントに提供する。

【0190】

例示的な実施形態によれば、第1のポリシー922は、第1のコンテナ942においてグループ化されたリソースについてグループレベルで顧客をリソース過剰から保護する。同様に、第2のポリシー924は、第2のコンテナ944においてグループ化されたリソースについてグループレベルで顧客をリソース過剰から保護し、第3のポリシー926は、第3のコンテナ946においてグループ化されたリソースについてグループレベルで顧客をリソース過剰から保護する。

【0191】

ある例に従うと、リソース要求911a~911dの各々は、要求されているリソースインスタンスのタイプを表すデータ（リソースタイプ）と、要求されているリソースインスタンスのグループを表すデータ（リソースグループ）と、リソース要求のコンテキストを表すデータ（コンテキストタグ）とを有するフィールドを含む。この点に関して、リソース要求911a~911dの各々は、要求されているリソースインスタンスのタイプを表すデータ（リソースタイプ）を有するリソースタイプフィールド912a~912dを含む。加えて、リソース要求911a~911dの各々は、要求されているリソースインスタンスのグループ（リソースグループ）を表すリソースグループフィールド913a~913dを含む。さらに加えて、リソース要求911a~911dの各々は、リソース要求のコンテキストを表す要求コンテキストデータ（コンテキストタグ）を含む要求コンテキストフィールド914a~914dを含む。

【0192】

ある例に従うと、計算制御プレーンは、ユーザ701からの要求の一部であるタグに関連付けられるすべてのタグベースの制限／割り当て950を制限サービスデータプレーン740（図7）からフェッチすることができる（代替的に、フェッチ動作は、リソース制御プレーン930において実行され得る）。そのようなタグベースの割り当ては、例えば、テナンシ全体にわたって適用することができ、コンパートメント固有である必要はない。

【0193】

ある実施形態に従うと、計算制御プレーンは、要求された使用がメモリ950において任意の割り当てまたは制限ルールについてタグベースの制限／割り当てのいずれかに違反するかどうかをチェックすることができる。要求された使用がいかなるコンパートメント割り当てにも違反しない場合、要求は、例えばデータベースに処理することができる。要求された使用がコンパートメントツリーに沿ったタグベースの制限／割り当てのいずれか

20

30

40

50

に違反する場合、要求はドロップされ得、ユーザに通知すべくメッセージが送信され得る。

【0194】

例示的な実施形態によれば、タグベースの制限／割り当ては、テナンシ内のコンパートメントに適用される。以下で説明する例示的な実施形態によれば、タグベースの制限／割り当ては、たとえば、テナンシが有効にされる本質的に複数のコンパートメントに跨がるすべてのリージョンを含む、テナンシ全体にわたって適用される。要求されたインスタンスがタグベースの制限／割り当てに違反するかどうかを判断するとき、計算制御プレーンは、新たな要求が、例えばサービス開発者キット（SDK）を介して、割り当てのいずれにも違反しないことを保証することができる。要求が割り当てを超える場合、計算制御プレーンは要求を落とすことができる。

10

【0195】

ある実施形態に従うと、計算制御プレーンのSDKは、クラウドインフラストラクチャ環境のすべての制御プレーンに存在し得る。ある実施形態に従うと、計算制御プレーンは、制限サービスデータプレーンと連携して、新たな要求をタグベースの制限／割り当てに対してチェックすることができる。

【0196】

ある実施形態に従うと、タグは、リソースおよびリソースの要求またはその両方に関連付けることができ、この手法では、タグは、リソースを不注意なアクセスから保護することができ、顧客ユーザを不注意なリソース過剰から保護することもできる。

【0197】

この点に関して、システム900は、関連付けられるクラウドインフラストラクチャ環境におけるリソース940の取り扱いを制御するために要求コンテキストタグ914a～914dを用いて提供される。システムは、関連付けられるクラウドインフラストラクチャ環境においてテナンシを定義する1つ以上のマイクロプロセッサを備える1つ以上のコンピュータを含むことができる。例示的な実施形態では、コンピュータに作動的に結合されるメモリデバイス940は、テナンシにおけるリソースの取り扱いの制御を提供するために、コンピュータによって実行可能な論理を記憶する。メモリデバイスはまた、テナンシにおけるリソースの取り扱いを可能にするための複数の必要とされるクレデンシャルゲートレベルを表すアクセス制御データ950を記憶し得る。テナンシにおいて第1のリソースを取り扱う要求911a～911dが受信され得、要求911a～911dは、要求の要求コンテキスト情報を表す要求コンテキストタグデータ914a～914dを含む。要求された第1のリソースに関連付けられる第1の特権レベル分類が判断され、要求の要求コンテキスト情報は、第1の特権レベル分類を有する、テナンシにおけるリソースの取り扱いを可能にするために、複数の必要とされるクレデンシャルゲートレベルのうちの第1の必要とされるクレデンシャルゲートレベルと比較される。例示的な実施形態によれば、第1のリソースを取り扱う要求は、第1の必要とされるクレデンシャルゲートレベルに一致する要求コンテキスト情報に基づいて選択的に許可される。

20

30

【0198】

第1のリソースを取り扱う要求は、テナンシにおいて第1のリソースをプロビジョニングする要求を含み得る。例示的な実施形態によれば、第1のリソースは、第1の必要とされるクレデンシャルゲートレベルに一致する要求コンテキスト情報に基づいて、テナンシにおいて選択的にプロビジョニングされる。

40

【0199】

例示的な実施形態によれば、テナンシにおいて第1のリソースをプロビジョニングする要求は、関連付けられるクラウドインフラストラクチャ環境における計算リソース層内の1つ以上の物理ホストマシンのユーザに制御を与えるために、テナンシにおいてベアメタル計算インスタンスをプロビジョニングする、システムのユーザからの要求を含むことができる。この例では、要求の要求コンテキストタグデータは、ユーザのユーザ識別情報を表すユーザコンテキストタグデータ913a～913dを含む。メモリデバイスに記憶されたアクセス制御データは、テナンシにおけるリソースの取り扱いを可能にするための複

50

数のユーザ必要とされるクレデンシャルゲートレベルを表すユーザアクセス制御データを含み、ユーザのユーザ識別情報は、第1の特権分類を有する、テナンシにおけるリソースの取り扱いを可能にするための複数のユーザ必要とされるクレデンシャルゲートレベルのうちの第1のユーザ必要とされるクレデンシャルゲートレベルと比較される。この例では、ベアメタル計算インスタンスは、第1のユーザ必要とされるクレデンシャルゲートレベルに一致するユーザのユーザ識別情報に基づいて、テナンシにおいてユーザに選択的にプロビジョニングされる。

【0200】

例示的な実施形態によれば、テナンシにおいて第1のリソースをプロビジョニングする要求は、第1の特権レベル分類を有する、テナンシにおける複数のリソースをプロビジョ

10

【0201】

例示的な実施形態によれば、要求の要求コンテキストタグデータは、ユーザのユーザ識別情報を表すユーザコンテキストタグデータ913a～913dを含んでもよく、第1のリソースを取り扱う要求は、テナンシにおいてプロビジョニングされ、第2の特権レベル分類に関連付けられるすべてのリソースを取り扱う要求を含んでもよい。システム900は、第2の特権レベル分類を有する、テナンシにおけるリソースの取り扱いを可能にするために、要求のユーザ識別情報を複数の必要とされるクレデンシャルゲートレベルのうちの第2の要求される要求クレデンシャルゲートレベルと比較するように動作する。システム900は、第2の必要とされるクレデンシャルゲートレベルに一致するユーザ識別情報に基づいて、テナンシにおいて、第2の特権レベル分類に関連付けられる、プロビジョ

20

【0202】

例示的な実施形態によれば、テナンシは、第2の特権レベル分類に関連付けられるリソースを格納する複数のコンパートメント942、944、946を含むことができ、複数のコンパートメントの各コンパートメントは、他のコンパートメント内の第2の特権レベル分類に関連付けられるリソースの1つ以上の他のセットに対する、各コンパートメント内の第2の特権レベル分類に関連付けられるリソースのセットの隔離を提供する。システム900は、複数のコンパートメントに跨がる第2の特権レベル分類に関連付けられる、テナンシにおいてプロビジョニングされるリソースのすべてを取り扱う要求を、第2の必要とされるクレデンシャルゲートレベルに一致するユーザ識別情報に基づいて選択的に許可する。

30

【0203】

テナンシにおいて第1のリソースを取り扱うためにシステムによって受信される要求の要求コンテキストデータは、要求されているリソースインスタンスのタイプを表すリソースタイプデータ912a～912dおよび／または要求されているリソースインスタンスのグループを表すリソースグループデータ913a～913dのうちの1つ以上を含み得る。

40

【0204】

ある実施形態に従うと、クライアントがクラウドリソースを作成する動作をトリガすると、要求はリソース制御プレーンに進む。リソース制御プレーンは、グループレベルで構成された制限を考慮して、リソースが安全にスピンアップされ得るかどうかを知るべく、制限サービスから尋ねる。制限サービスがリソース制御プレーンに否定／失敗応答を返す場合、リソースは作成されない。

【0205】

内部的に、制限サービスが要求を受信すると、制限サービスは、リソース作成に関連付けられるタグをチェックし、その特定のタグを有するリソースの現在の使用を見るために、ストアもしくはデータベースまたはメモリを参照する。タグ値がグループレベルで設定

50

された制限を超える場合、リソース生成が失敗するようにリソース制御プレーンに失敗／否定応答を送信する。

【0206】

例示的な実施形態の機能性を説明する目的のためだけであり、それを限定する目的のためではないが、第1のポリシー922は、以下のような細かい粒度のルール／ポリシーに従って、第1のコンテナ942にグループ化されたリソースについて、財務グループレベルにおいて、顧客をリソース過剰から保護することができる：

Set limits <Compute> to 10 in Container #1 (642) where target.resource.tag = "Finance"

(制限<計算>をコンテナ#1(642)において10に設定し、ターゲットリソースタグ＝「財務」である)

上記の特定の例では、ユーザは、財務コンテナ942内に10を超える計算リソースのインスタンスを作成することはできない。このようにして、コンテナ942内のリソースをプロビジョニングするための要求911dは、ポリシー922によって処理されて、いかなる過剰も被ることなく要求が実行され得るかまたは他の態様で実行され得るかどうかを判断する。

【0207】

同様に、第2のポリシー924は、以下のような細かい粒度のルール／ポリシーに従って、第2のコンテナ644にグループ化されたリソースについて、営業グループレベルにおいて、顧客をリソース過剰から保護することができる：

Set limits <db storage> to 100 in Container #2 (644) where target.resource.tag = "Operations"

(制限<dbストレージ>をコンテナ#2(644)において100に設定し、ターゲットリソースタグ＝「営業」である)

上記の例では、ユーザは、営業コンテナ644内に100を超えるストレージリソースのインスタンスを作成することはできない。このようにして、コンテナ644内のリソースをプロビジョニングするための要求911cは、ポリシー924によって処理されて、いかなる過剰も被ることなく要求が実行され得るかまたは他の態様で実行され得るかどうかを判断する。

【0208】

同様に、第3のポリシー926は、以下のような細かい粒度のルール／ポリシーに従って、第3のコンテナ946にグループ化されたリソースについて、人事グループレベルにおいて、顧客をリソース過剰から保護することができる：

Set limits <Compute> to 10 and <db storage> to 100 in Container #3 (646) where target.resource.tag = "Human Resources"

(コンテナ#3(646)において、制限<計算>を10に、および<dbストレージ>を100に設定し、ターゲットリソースタグ＝「人事」である)

上記の例では、ユーザは、10を超える計算リソースのインスタンスまたは100を超えるストレージリソースのインスタンスを人事コンテナ946に作成することはできない。このようにして、コンテナ946内のリソースをプロビジョニングするための要求911a、911bは、ポリシー926によって処理されて、いかなる過剰も被ることなく要求が実行され得るかまたは他の態様で実行され得るかどうかを判断する。

【0209】

図10は、例示的な実施形態による、例えば、要求コンテキストに基づいてクラウドインフラストラクチャ環境においてリソースをプロビジョニングすることなど、リソースを取り扱うことを制限するかまたはそれに割り当てを課すための方法1000を示すフロー図である。ここでその図を参照すると、クラウドインフラストラクチャ環境においてリソースをプロビジョニングするための要求が、ステップ1010において受信される。要求は、例えば、上述の第1の要求911aであってもよい。要求は、たとえば、要求の要求コンテキスト情報を表す要求コンテキストタグデータ914aを含み得る。

10

20

30

40

50

【0210】

ステップ1020において、要求911aが検査され、要求されたリソースに対する要求のコンテキストが判断される。判断されたリソースタイプは、例えば、計算リソースタイプをプロビジョニングするための要求、またはストレージリソースタイプをプロビジョニングするための要求であってもよい。

【0211】

ステップ1030において、要求されたリソースに関連付けられる特権レベル分類が判断される。例示的实施形態によれば、リソースは、リソースにアクセスするために必要とされる特権レベルを反映する印に関連して記憶されてもよい。特権レベルは、例えば図8の851～854、861～864、871～874および図1の140a、16a、170aに示すような1つ以上の特権レベルタグ内に、またはそのような1つ以上の特権レベルタグとして、記憶することができる。判断されたリソースグループは、例えば、人事グループにグループ化されたリソースをプロビジョニングするための要求であってもよい。

10

【0212】

ステップ1040において、リソース要求911aを、判断された要求のグループに従って、特定のコンテナに割り当てることができる。この例では、リソース要求911aは、たとえば、この例に従って、第3のコンテナ946に割り当てられ得る。割り当てられたコンパートメントに対応するポリシーは、リソース要求に選択的に適用され得る。図示の例では、第3のポリシー926は、リソース要求911aに選択的に適用され得る。ステップ1040において、リソース要求911aの内容に従った追加のリソースのプロビジョニングが、コンパートメント946に割り当てられたポリシー926において指定される制限および／または割り当てを超えないと判断された場合、要求911aにおいて要求されたインスタンスは、コンパートメント946において作成されてもよい。

20

【0213】

ステップ1050において、要求911aの要求コンテキスト情報914aは、第1の特権レベル分類を有する、テナンシにおけるリソースの取り扱いを可能にするために、複数の必要とされるクレデンシャルゲートレベルのうちの第1の必要とされるクレデンシャルゲートレベルと比較される。

【0214】

ステップ1060において、要求コンテキスト情報が第1の必要とされるクレデンシャルゲートレベルと一致すると判断された場合、ステップ1070において、第1のリソースを扱う要求が許可され、例えば、要求されたリソースのインスタンスが作成され得る、要求されたリソースがプロビジョニングされ得る、要求されたリソースが終了され得る、または別様にプロビジョニング解除され得るなど、リソースが取り扱われ得る。

30

【0215】

ステップ1060において、要求コンテキスト情報が第1の必要とされるクレデンシャルゲートレベルと一致しないと判断された場合、ステップ1080において、第1のリソースを取り扱う要求はドロップされる。

【0216】

リソースタグベースの制限／割り当て

40

図11は、一実施形態による、クラウドインフラストラクチャ環境においてタグベースのリソース制限／割り当てを設けるシステム1100の機能概略図である。

【0217】

概して、クライアントデバイス810（図8）は、複数のタグ付けされたリソース1040の中で新たなリソースをプロビジョニングするための要求1111をクラウドインフラストラクチャ環境に提出することができる。複数のタグ付けされたリソース1140は、例えば、計算リソース層850のタグ付けされた計算リソース851～854、ネットワークリソース層860のタグ付けされたネットワークリソース861～864、および／またはストレージリソース層870のタグ付けされたストレージリソース871～874のいずれかであり得る。

50

【0218】

例示的な実施形態によれば、プロビジョニングされるリソースおよびサービスはタグ付け可能である。例示的な実施形態では、リソースは、1つ以上のタグと関連付けられる。加えて、リソースは、それらのタグ値に基づいてグループ化され得る。本質的に、例示的な実施形態では、各プロビジョニングされたリソースと関連付けられるリソースタグは、クラウドインフラストラクチャ環境においてプロビジョニングされたリソースにアタッチされ得るか、または別様にそれらに関連付けられ得る、キー値ペアである。タグキー値ペアは、例えば、様々な会計目的を含む多くの目的のために用いられ得る。ある例では、プロビジョニングされたリソースに関連付けられるリソースキー値ペアタグは、リソースをグループ化するために用いられ、リソースタグによって提供されるグループ化は、クラウドインフラストラクチャ環境における値のすべてのコスト管理および／またはリソース管理を可能にする。

10

【0219】

クラウドインフラストラクチャ環境においてプロビジョニングされるリソースは、各リソースに割り当てられるタグ値に基づいて、コンテナ1142、1144、1146にグループ化されてもよい。

【0220】

ある例に従うと、リソースインスタンスは、異なるコンテナ1142、1144、1146に論理的に配置され、それにより、別々のコストセンターを提供し、各コストセンターにはタグ値が割り当てられ、エンドユーザは、さまざまなコストセンターへのアクセスについて請求され得、コストセンターのタグは、コスト管理および課金のために用いられる。一部の顧客は、彼らのエンドグループ価格内で複数のコストセンターをモデル化し得る。各コストセンターに対して別個のタグが存在してもよく、クラウドは、各タグに対して、限定されたリソースのセットを割り当ててもよい。

20

【0221】

例示的な実施形態では、1つ以上のポリシー1120は、エンドユーザがアクセスについて標準契約で許可されるよりも多くのリソースにアクセスすることから自身を保護するための機構を提供し、実質的過剰は、エンドユーザが標準契約の標準契約条件下で許可されるよりも多くのリソースにアクセスすることによって生じ得る。例えば、顧客は、リソース制御プレーン1130を介して、例えば、100個の計算リソース等の複数の計算リソースのプロビジョニングをアクティブにする、リソースに対する要求を送信し得、契約条件は、標準レートで90個のコンピュータリソースのプロビジョニングのみを許可しており、過剰分が、この実施例では10が、顧客エンドユーザに対して追加費用を招く。

30

【0222】

上述のように、およびある実施形態に従うと、細かい粒度のアプローチは、タグ、特にリソースに関連付けられるタグに基づいて、リソース制限を設けることができる。リソースと関連付けられるタグは、リソース管理110（図1）において用いられ得る機構を提供し、クラウドプロバイダは、コスト管理のためにもそれらを使用し得る。システムおよび方法は、タグを通して、グループレベルを含むレベルでコストを制御するための機構を作成することができる。例として、ユーザは、以下のような細かい粒度のルール／ポリシーを指定することができる：

40

Set limits <resource type> to 10 in group A where target.resource.tag = "finance"
（制限<リソースタイプ>をグループAにおいて10に設定し、ターゲットリソースタグ＝「財務」である）

ある実施形態に従うと、タグは、リソースに関連付けることができ、上記アプローチを用いて、タグは、たとえばグループレベルなどの1つ以上の選択されたレベルで顧客をリソース過剰から保護することができる。上記の例では、タグ値がグループAにおいて「財務」である場合、のユーザメンバーは、<リソースタイプ>の10を超えるインスタンスを作成することはできないことになる。グループレベルでコストを制限するこのアプローチは、コストおよびリソース使用をより良く管理するために、細かい粒度の機構をクライ

50

アントに提供する。

【0223】

例示的な実施形態によれば、第1のポリシー1120aは、第1のタグに関連付けられ、コンテナ1142、1144、1146のいずれかにグループ化され得るリソースの過剰使用から顧客を保護する。同様に、第2のポリシー1120bは、第2のタグに関連付けられ、コンテナ1142、1144、1146のいずれかにグループ化され得るリソースの過剰使用から顧客を保護する。同様に、第3および第4のポリシー1120c、1120dは、第3および第4のタグに関連付けられ、コンテナ1142、1144、1146のいずれかにグループ化され得るリソースの過剰使用から顧客を保護する。

【0224】

ある例に従うと、リソース要求1111a~1111dの各々は、要求されているリソースインスタンスのタイプを表すデータ（リソースタイプ）と、要求されているリソースインスタンスのグループを表すデータ（リソースグループ）と、リソース要求の特性を表すデータ（リソース特性）と、リソース要求のコンテキストを表すデータ（コンテキストタグ）とを有するフィールドを含む。この点に関して、リソース要求1111a~1111dの各々は、要求されているリソースインスタンスのタイプを表すデータ（リソースタイプ）を有するリソースタイプフィールド1112a~1112dを含む。加えて、リソース要求1111a~1111dの各々は、要求されているリソースインスタンスのグループ（リソースグループ）を表すリソースグループフィールド1113a~1113dを含む。さらに加えて、リソース要求1111a~1111dの各々は、リソース要求のコンテキストを表す要求コンテキストデータ（コンテキストタグ）を含む要求コンテキストフィールド1114a~1114dを含む。さらに追加して、リソース要求1111a~1111dの各々は、リソース要求の特性を表す要求特性データ（特性タグ）を含む要求特性フィールド1115a~1115dを含む。要求特性フィールド1115a~1115dは、説明を容易にするために別途示され説明されるが、それは、リソースタイプ情報から、またはリソースグループ情報から、またはリソース要求を形成する任意の他の情報から導出され得ることを理解されたい。

【0225】

ある例に従うと、計算制御プレーンは、ユーザ701からの要求の一部であるタグに関連付けられるすべてのタグベースの制限／割り当て1150を制限サービスデータプレーン740（図7）からフェッチすることができる（代替的に、フェッチ動作は、リソース制御プレーン1130において実行され得る）。そのようなタグベースの割り当ては、例えば、テナンシ全体にわたって適用することができ、コンパートメント固有である必要はない。

【0226】

ある実施形態に従うと、計算制御プレーンは、要求された使用がメモリ1150において任意の割り当てまたは制限ルールについてタグベースの制限／割り当てのいずれかに違反するかどうかをチェックすることができる。要求された使用がいかなるリソースタグベースの割り当てにも違反しない場合、要求は、たとえばデータベースに対して処理され得る。要求された使用がコンパートメントツリーに沿ったリソースタグベースの制限／割り当てのいずれかに違反する場合、要求はドロップされ得、ユーザに通知すべくメッセージが送信され得る。

【0227】

例示的な実施形態によれば、リソースタグベースの制限／割り当ては、テナンシ内のコンパートメントに適用される。以下で説明する例示的な実施形態によれば、リソースタグベースの制限／割り当ては、たとえば、テナンシが有効にされる本質的に複数のコンパートメントに跨がるすべてのリージョンを含む、テナンシ全体にわたって適用される。要求されたインスタンスがリソースタグベースの制限／割り当てに違反するかどうかを判断するとき、計算制御プレーンは、新たな要求が、例えばサービス開発者キット（SDK）を介して、割り当てのいずれにも違反しないことを保証することができる。要求が割り当て

を超える場合、計算制御プレーンは要求を落とすことができる。

【0228】

ある実施形態に従うと、計算制御プレーンのSDKは、クラウドインフラストラクチャ環境のすべての制御プレーンに存在し得る。ある実施形態に従うと、計算制御プレーンは、制限サービスデータプレーンと連携して、新たな要求をリソースタグベースの制限／割り当てに対してチェックすることができる。

【0229】

ある実施形態に従うと、クライアントがクラウドリソースを作成する動作をトリガすると、要求はリソース制御プレーンに進む。リソース制御プレーンは、たとえばグループレベルなどの選択されたレベルで構成された制限を考慮して、リソースが安全にスピニングアップされ得るかどうかを知るべく、制限サービスから尋ねる。制限サーバがリソース制御プレーンに否定／失敗応答を返す場合、リソースは作成されず、要求はドロップされる。

【0230】

内部的に、制限サービスが要求を受信すると、制限サービスは、リソース作成に関連付けられるタグをチェックし、その特定のタグを有するリソースの現在の使用を見るために、ストアもしくはデータベースまたはメモリを参照する。リソースは、複数のタグに関連付けられてもよく、リソースは、複数の異なるタグに関連付けられてもよい。タグ値が、たとえばグループレベルなどの選択されたレベルで構成された制限を超える場合、それは、リソース作成が失敗するように、リソース制御プレーンに失敗／否定応答を送信する。

【0231】

ある実施形態に従うと、メモリデバイス1140は、テナンシ305（図3）におけるリソースプロビジョニングの、複数のタグベースの割り当てを表す、タグベースの割り当てデータ1150を記憶する。テナンシにおいてリソースをプロビジョニングする要求1111a～1111dが受信される。要求1111a～1111dは、要求の要求特性を表す要求特性データ1115a～1115dを含み得る。ある実施形態に従うと、要求の要求特性に対応するリソースタグ150a、160a、170a（図1）に関連付けられる、テナンシにおけるリソースの使用が判断され、複数のタグベースの割り当ておよび／または制限1150と比較される。リソースをプロビジョニングする要求は、判断された使用が複数のタグベースの割り当てのうちの1つを超えることに基づいてドロップされる。

【0232】

実施形態の例によれば、テナンシ305は、リソースを格納する複数のコンパートメント1142、1144、1146を備え、複数のコンパートメントの各コンパートメントは、他のコンパートメント内のリソースの1つ以上の他のセットに対する、各コンパートメント内のリソースのセットの隔離を提供する。要求の要求特性に対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用は、複数のコンパートメントにわたってまとめて判断され、複数のコンパートメントにわたってまとめて判断された使用は、テナンシの複数のタグベースの割り当てと比較される。リソースをプロビジョニングする要求1111a～1111dは、複数のコンパートメントにわたってまとめて判断された使用が複数のタグベースの割り当てのうちの1つを超えることに基づいてドロップされる。

【0233】

実施形態の例によれば、メモリデバイス1140に記憶されたタグベースの割り当てデータ1150は、テナンシの対応する複数のリソースタイプの、テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当てを表す。加えて、テナンシにおいてリソースをプロビジョニングする要求1111a～1111dの要求特性データ1115a～1115dは、要求されたリソースの第1のリソースタイプ1112a～1112dを表すリソースタイプデータを含む。例示的な実施形態では、第1のリソースタイプ1112aに対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用が判断され、第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て1120aと比較される。第1のリソースタイプ1112aのリソースをプロビジョニングする要求1111aは、第1のリソースタイプに対応するリソ

10

20

30

40

50

ースタグに関連付けられる、テナンシにおける判断されたリソースの使用が、第1のリソースタイプの、テナンシにおけるリソースプロビジョニングのたとえばポリシー1120aとして記憶される第1のタグベースの割り当てを超えることに基づいて、ドロップされる。

【0234】

実施形態の一例によれば、メモリデバイス1140に記憶されたタグベースの割り当てデータ1150は、テナンシの対応する複数のユーザグループに割り当てられた、テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当てを表す。テナンシにおいてリソースをプロビジョニングする要求1111a~1111dの要求特性データ1115a~1115dは、リソースを要求するシステムのユーザに割り当てられたユーザグループカテゴリを表すユーザグループデータ1113a~1113dを含む。ユーザグループカテゴリに対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用が判断され、ユーザグループカテゴリに割り当てられた、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当て1120bと比較される。リソースをプロビジョニングする要求は、ユーザグループカテゴリに対応するリソースタグに関連付けられる、テナンシにおける判断されたリソースの使用が、ユーザグループカテゴリに割り当てられた、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てを超えることに基づいて、ドロップされる。

【0235】

実施形態の一例によれば、メモリデバイスに記憶されたタグベースの割り当てデータは、テナンシの複数のユーザグループに割り当てられた、テナンシの複数のリソースタイプの、テナンシにおけるリソースプロビジョニングの、タグベースの割り当てを表す。テナンシにおいてリソースをプロビジョニングする要求の要求特性データは、たとえば、i) 要求されたリソースの第1のリソースタイプを表すリソースタイプデータ、および/またはii) リソースを要求するシステムのユーザに割り当てられたユーザグループカテゴリを表すユーザグループデータを含んでもよい。この例では、第1のユーザグループカテゴリにプロビジョニングされる第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用が判断され、第1のユーザグループカテゴリに割り当てられた第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てと比較される。加えて、リソースをプロビジョニングする要求は、第1のユーザグループカテゴリにプロビジョニングされる第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおける判断されたリソースの使用が、第1のユーザグループカテゴリに割り当てられた第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てを超えることに基づいて、ドロップされる。

【0236】

実施形態の一例によれば、メモリデバイス1140に記憶されたタグベースの割り当てデータ1150は、テナンシの複数のユーザグループに割り当てられた、テナンシの複数のリソースタイプの、テナンシにおけるリソースプロビジョニングの、タグベースの割り当てを表す。テナンシのリソース使用を追跡する第1の要求がユーザ701から受信され得、第1の要求は、第1のユーザグループカテゴリ1113a~1113dおよび第1のリソースタイプ1112a~1112dを表す要求特性データ1115a~1115dを含む。

【0237】

第1のユーザグループカテゴリによってプロビジョニングされる第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおけるリソースの第1の使用が判断され、リソース使用追跡データは、第1のユーザグループによってプロビジョニングされる第1のリソースタイプの、テナンシにおけるリソースの、判断された第1の使用に基づいて生成される。

【0238】

実施形態の一例によれば、リソースをプロビジョニングする要求は、判断された使用が複数のタグベースの割り当てのうちの1つを超えることに基づいてドロップされる。しかしながら、テナンシのリソースをプロビジョニングするオーバーライド要求が、ユーザ701から受信されてもよい。リソースは、実施形態の一例に従って、システムがオーバーライド要求を受信することに基づいて、選択的にプロビジョニングされる。加えて、システムがオーバーライド要求を受信したことに応答してリソースが選択的にプロビジョニングされることに基づいて、リソース使用過剰データが生成される。

【0239】

図12は、例示的な実施形態による、リソースタグに基づいてクラウドインフラストラクチャ環境においてリソースをプロビジョニングすることを制限するかまたはそれに割り当てを課すための方法1200を示す流れ図である。

10

【0240】

方法1200によれば、ステップ1210において、テナンシが提供され、タグベースの制限／割り当てデータがメモリに記憶される。その好ましい形態では、テナンシは、関連付けられるクラウドインフラストラクチャ環境において、1つ以上のプロセッサと、コンピュータに作動的に結合されるメモリデバイスとを含むコンピュータによって提供される。メモリデバイスは、関連付けられるクラウドインフラストラクチャ環境におけるリソース使用のタグベースの制御を提供するためにコンピュータによって実行可能なタグベースの制御論理を記憶する。例示的な実施形態では、メモリデバイスに記憶されたタグベースの割り当てデータは、テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当てを表す。

20

【0241】

ステップ1220において、テナンシにおいてリソースをプロビジョニングする要求が受信される。要求は、要求の要求特性を表す要求特性データを含む。

【0242】

ステップ1230において、要求されたリソースのリソースタイプが判断される。

ステップ1240において、要求の要求特性に対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用が、1つ以上のプロセッサがタグベースの制御論理を実行することにより、判断される。

【0243】

30

要求は、ステップ1250において、要求されたリソースのグループに基づいて、コンパートメントのうちの1つ以上に割り当てられる。

【0244】

タグベースの制御論理を実行する1つ以上のプロセッサは、タグに関連付けられるリソースの使用を判断し、判断された使用は、ステップ1260において、複数のタグベースの割り当てと比較される。

【0245】

リソース要求は、ステップ1290において、ステップ1270における、使用が複数のタグベースの割り当てのうちの1つを超えるという判断に基づいて、リソースをプロビジョニングする要求を、1つ以上のプロセッサがタグベースの制御論理を実行することによって、ドロップされる。

40

【0246】

要求されたリソースのインスタンスは、ステップ1280において、ステップ1270における、使用が複数のタグベースの割り当てのうちの1つを超えないという判断に基づいて、リソースをプロビジョニングする要求を、1つ以上のプロセッサがタグベースの制御論理を実行することによって、作成される。

【0247】

実施形態の例によれば、テナンシは、リソースを格納する複数のコンパートメントを提供することにより提供され、複数のコンパートメントの各コンパートメントは、他のコンパートメント内のリソースの1つ以上の他のセットに対する、各コンパートメント内のリ

50

ソースのセットの隔離を提供する。加えて、使用を判断することは、複数のコンパートメントにわたってまとめて、要求の要求特性に対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用を判断することを含み、比較することは、判断された使用を、複数のコンパートメントにわたってまとめて、テナンシの複数のタグベースの割り当てと比較することを含む。さらに加えて、要求をドロップすることは、複数のコンパートメントにわたってまとめて判断された使用が複数のタグベースの割り当てのうちの1つを超えることに基づいて、リソースをプロビジョニングする要求をドロップすることを含む。

【0248】

実施形態の例によれば、タグベースの割り当てデータを記憶することは、テナンシの対応する複数のリソースタイプの、テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当てを表す、タグベースの割り当てデータを、メモリデバイスに記憶することを含む。加えて、要求を受信することは、要求されたリソースの第1のリソースタイプを表すリソースタイプデータを含む要求を受信することを含み、判断することは、第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用が判断されることを判断することを含む。さらに加えて、比較することは、判断された使用を、第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てと比較することを含み、要求をドロップすることは、第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおける判断されたリソースの使用が、第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てを超えることに基づいて、要求をドロップすることを含む。

【0249】

実施形態の例によれば、タグベースの割り当てデータを記憶することは、テナンシの対応する複数のユーザグループに割り当てられた、テナンシにおけるリソースプロビジョニングの、複数のタグベースの割り当てを表す、タグベースの割り当てデータを、メモリデバイスに記憶することを含み、要求を受信することは、リソースを要求するシステムのユーザに割り当てられたユーザグループカテゴリを表すリソースタイプデータを含む要求を受信することを含む。加えて、判断することは、ユーザグループカテゴリに対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用を判断することを含み、比較することは、判断された使用を、ユーザグループカテゴリに割り当てられた、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てと比較することを含む。加えて、要求をドロップすることは、ユーザグループカテゴリに対応するリソースタグに関連付けられる、テナンシにおける判断されたリソースの使用が、ユーザグループカテゴリに割り当てられた、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てを超えることに基づいて、要求をドロップすることを含む。

【0250】

実施形態の例によれば、タグベースの割り当てデータを記憶することは、テナンシの複数のユーザグループに割り当てられた、テナンシの複数のリソースタイプの、テナンシにおけるリソースプロビジョニングの、タグベースの割り当てを表す、タグベースの割り当てデータを、メモリデバイスに記憶することを含み、要求を受信することは、i) 要求されたリソースの第1のリソースタイプを表すリソースタイプデータと、ii) リソースを要求するシステムのユーザに割り当てられたユーザグループカテゴリを表すユーザグループデータとを含むリソースタイプデータを含む要求を受信することを含む。加えて、判断することは、第1のユーザグループカテゴリにプロビジョニングされる第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用を判断することを含み、比較することは、判断された使用を、第1のユーザグループカテゴリに割り当てられた第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てと比較することを含む。さらに加えて、要求をドロップすることは、第1のユーザグループカテゴリにプロビジョニングされる第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおける判断されたリソースの使

用が、第1のユーザグループカテゴリに割り当てられた第1のリソースタイプの、テナンシにおけるリソースプロビジョニングの、第1のタグベースの割り当てを超えることに基
づいて、要求をドロップすることを含む。

【0251】

実施形態の一例によれば、テナンシの複数のユーザグループに割り当てられた、テナンシの複数のリソースタイプの、テナンシにおけるリソースプロビジョニングの、タグベースの割り当てを表す、タグベースの割り当てデータを、メモリデバイスに記憶する。本方法はさらに、テナンシのリソース使用を追跡する第1の要求を受信することを含み、第1の要求は、第1のユーザグループカテゴリおよび第1のリソースタイプを表す要求特性データを含む。加えて、第1のユーザグループカテゴリによってプロビジョニングされる第1のリソースタイプに対応するリソースタグに関連付けられる、テナンシにおけるリソースの第1の使用を判断し、第1のユーザグループによってプロビジョニングされる第1のリソースタイプの、テナンシにおける判断されたリソースの第1の使用に基づいて、リソース使用追跡データを生成する。

【0252】

本方法はさらに、テナンシのリソースをプロビジョニングするオーバーライド要求を受信することと、システムがオーバーライド要求を受信することに基づいてリソースを選択的にプロビジョニングすることと、システムがオーバーライド要求を受信したことに応答してリソースが選択的にプロビジョニングされることに基づいて、リソース使用過剰データを生成することを含む。

【0253】

様々な実施形態によれば、本明細書の教示は、本開示の教示に従ってプログラミングされた1つ以上のプロセッサ、メモリ、および／またはコンピュータ読取可能記憶媒体を含む、1つ以上の従来の汎用または専用デジタルコンピュータ、コンピューティングデバイス、マシン、またはマイクロプロセッサを使用して都合よく実現されてもよい。適切なソフトウェアコーディングは、ソフトウェア技術の当業者には明らかなように、本開示の教示に基づいて熟練したプログラマーによって容易に準備することができる。

【0254】

いくつかの実施形態では、本開示の教示は、コンピュータ可読媒体を用いて、1つ以上のプログラマブルプロセッサまたはコンピュータが本教示のプロセスのいずれかを実行するための命令を伝達する（たとえば、記憶するまたは搬送する）ことができるコンピュータプログラム製品を含むことができる。コンピュータ可読媒体の一例は、本教示のプロセスのいずれかを実行するようにコンピュータをプログラムするために用いられ得る命令が記憶された非一時的コンピュータ可読記憶媒体である。そのような記憶媒体の例は、ハードディスクドライブ、ハードディスク、ハードドライブ、固定ディスク、もしくは他の電気機械データストレージデバイス、フロッピー（登録商標）ディスク、光ディスク、DVD、CD-ROM、マイクロドライブ、および光磁気ディスク、ROM、RAM、EEPROM、DRAM、VRAM、フラッシュメモリデバイス、磁気もしくは光カード、ナノシステム、または命令および／もしくはデータの非一時的な格納に適した他のタイプの記憶媒体もしくはデバイスを含み得るが、それらに限定はされない。コンピュータ可読媒体の別の例は、コンピュータシステム間または所与のコンピュータシステムのコンポーネント間でそのような命令を伝達する過渡的媒体である。過渡媒体の例は、搬送波および伝送信号を含むことができるが、これらに限定されない。

【0255】

したがって、ある観点から、クラウドインフラストラクチャ環境においてタグベースのリソース制限または割り当てをサポートするシステムおよび方法が説明された。クラウド管理者は、概して、既存のクラウドにおいてリソース使用を制限する能力を有していない。ユーザにリソースを作成するための許可を与えることにより、ユーザは、事前定義されたアカウント限度まで任意の数のリソースを作成することが可能になる。タグは、微調整されたコスト制御を可能にすることによって、管理者がユーザのリソース使用を適切なレ

10

20

30

40

50

ベルに制限することを可能にするために、リソースと関連付けられる。リソースをプロビジョニングする要求の要求特性に対応するリソースタグに関連付けられる、テナンシにおけるリソースの使用が判断され、複数のタグベースの割り当てと比較され、リソースをプロビジョニングする要求は、判断された使用が複数のタグベースの割り当てのうちの1つを超えることに基づいてドロップされる。

【0256】

前述の説明は、例示および説明を目的として提供された。それは、網羅的であること、または保護の範囲を開示された厳密な形態に限定することを意図するものではない。多くの修正および変形が当業者には明らかであろう。例えば、本開示で提供される例のいくつかは、Oracle Fusion Applicationsなどの企業ソフトウェアアプリケーションコンポーネント、Oracle Cloud Infrastructureなどのクラウド環境、およびOracle Fusion Analyticsなどのクラウドサービスとの使用を例示するが、様々な実施形態によれば、本開示に記載のシステムおよび方法は、他のタイプの企業ソフトウェアアプリケーション、クラウド環境、クラウドサービス、クラウドコンピューティング、または他のコンピューティング環境とともに用いることができる。

【0257】

実施形態は、本教示の原理およびそれらの実際の適用を最もよく説明するために選択および記載されており、それにより、当業者は、企図される特定の使用に適した様々な実施形態および様々な修正を理解することができる。その範囲は、特許請求の範囲およびそれらの均等物によって規定されることが意図される。

10

20

30

40

50

【図面】

【図 1】

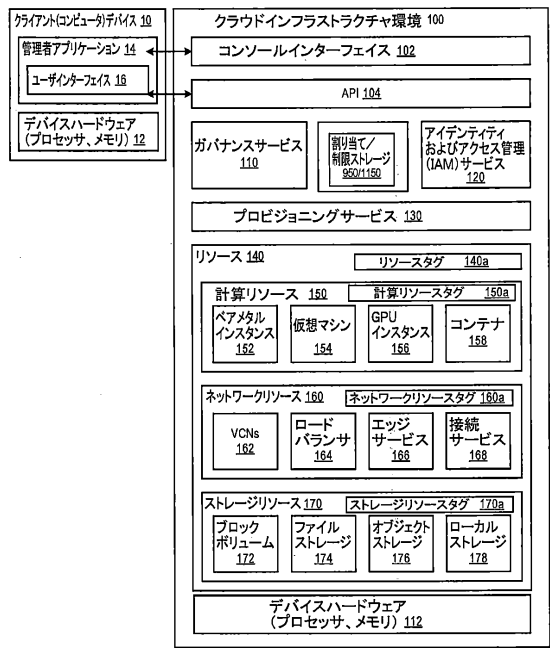


FIGURE 1

【図 2】

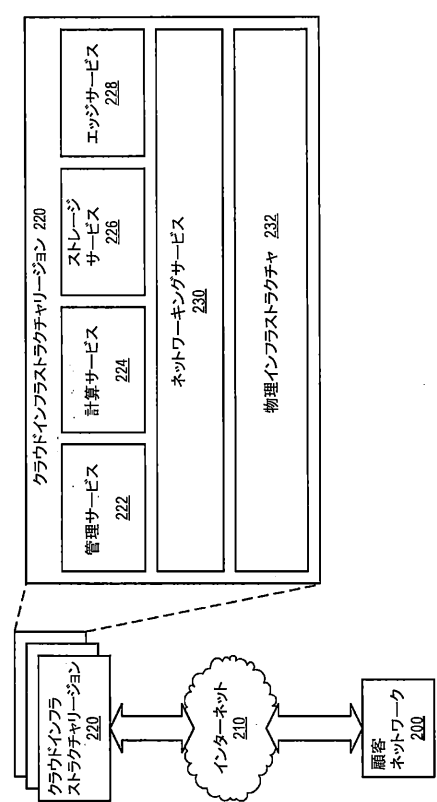


FIGURE 2

10

20

30

40

50

【図 3】

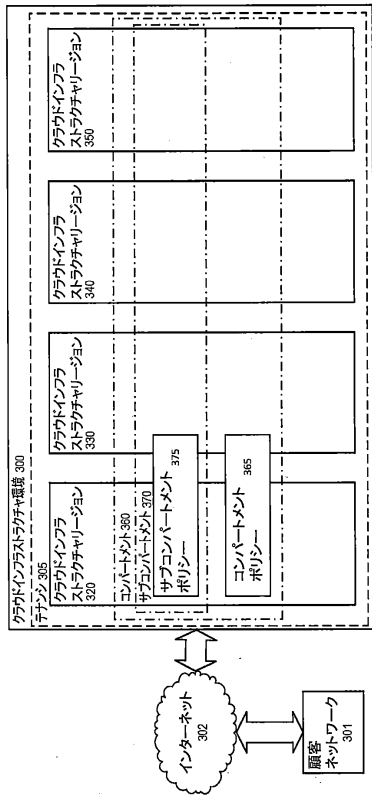


FIGURE 3

【図 4】

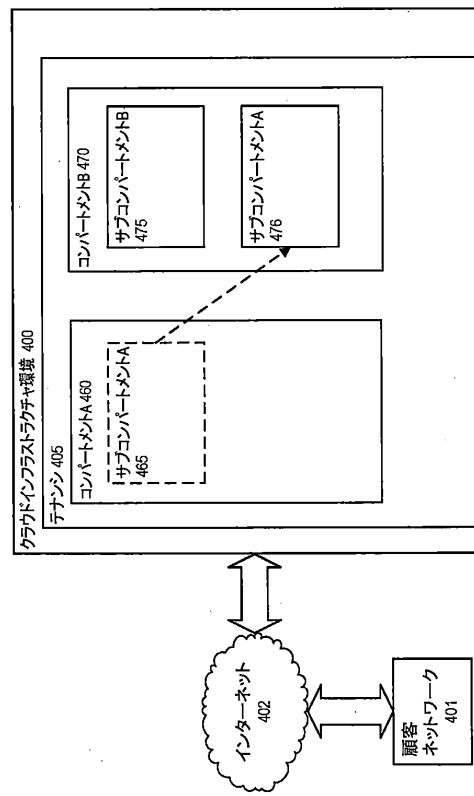


FIGURE 4

【図 5】

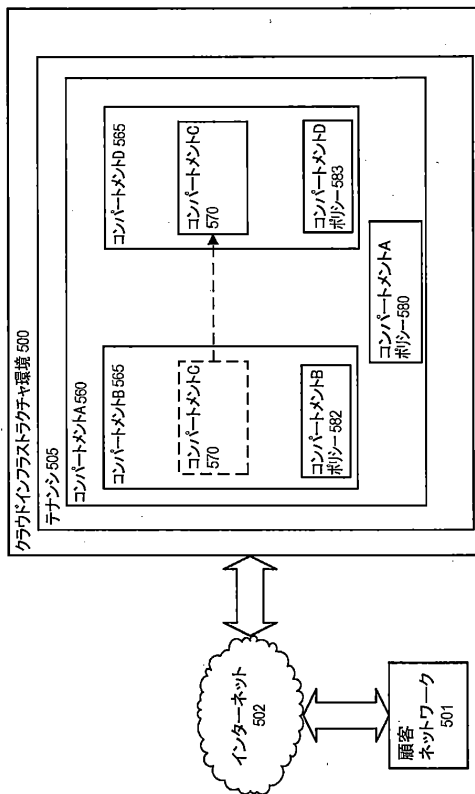


FIGURE 5

【図 6】

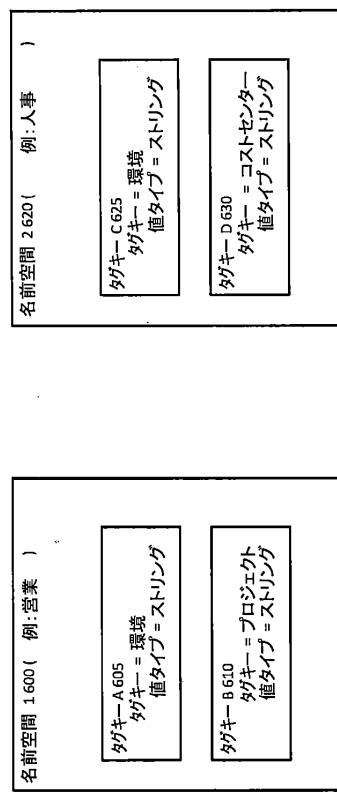


FIGURE 6

【図 7】

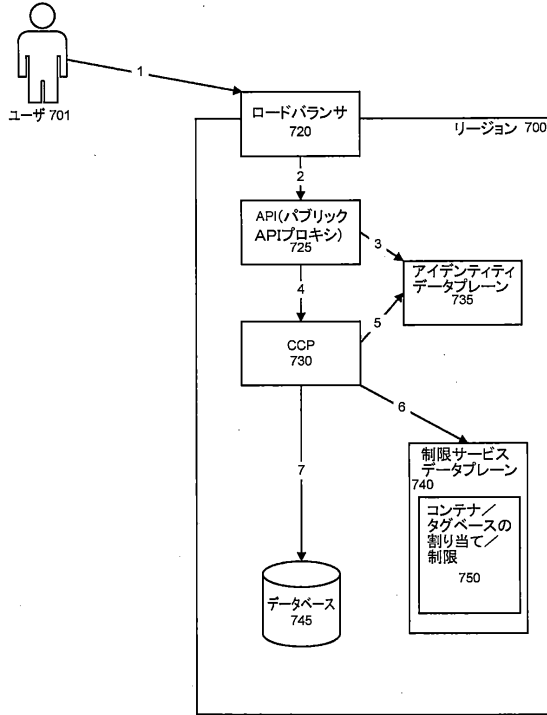


FIGURE 7

【図 8】

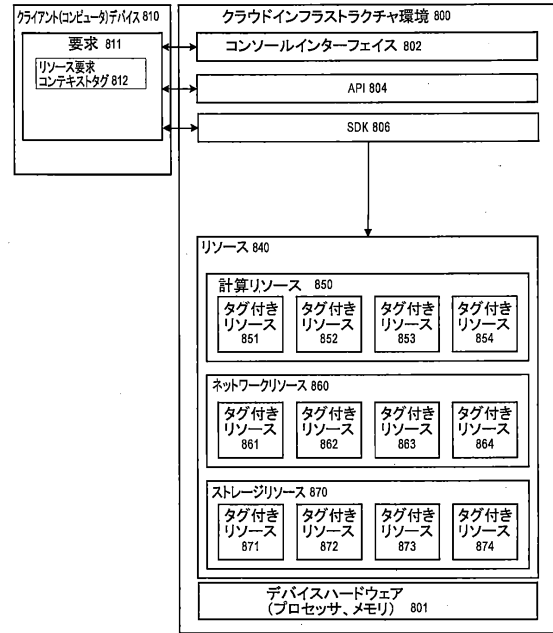


FIGURE 8

【図 9】

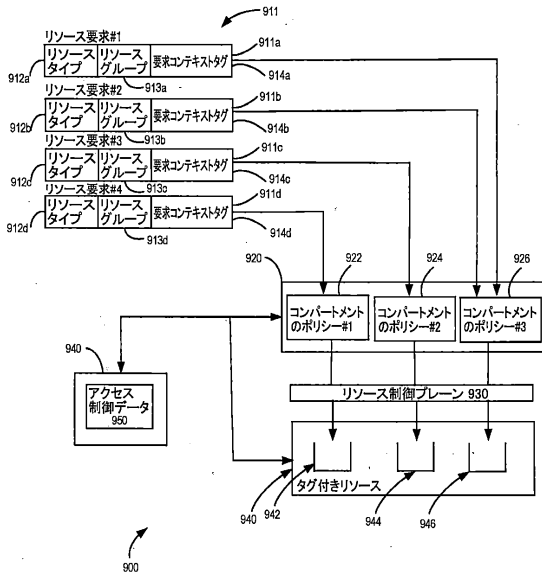


FIGURE 9

【図 10】

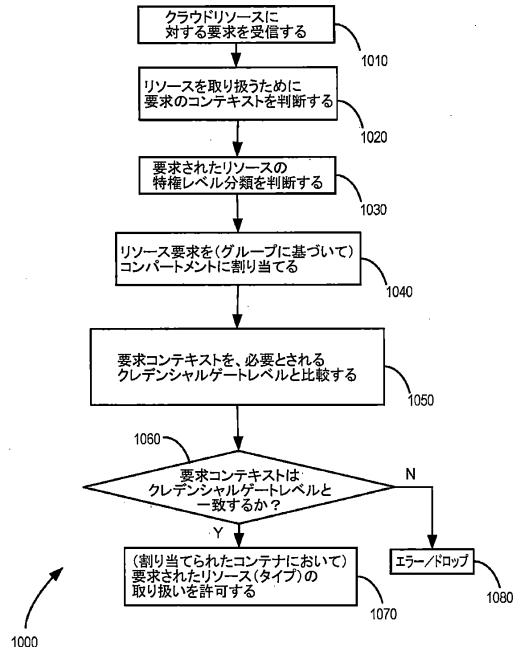


FIGURE 10

【図 11】

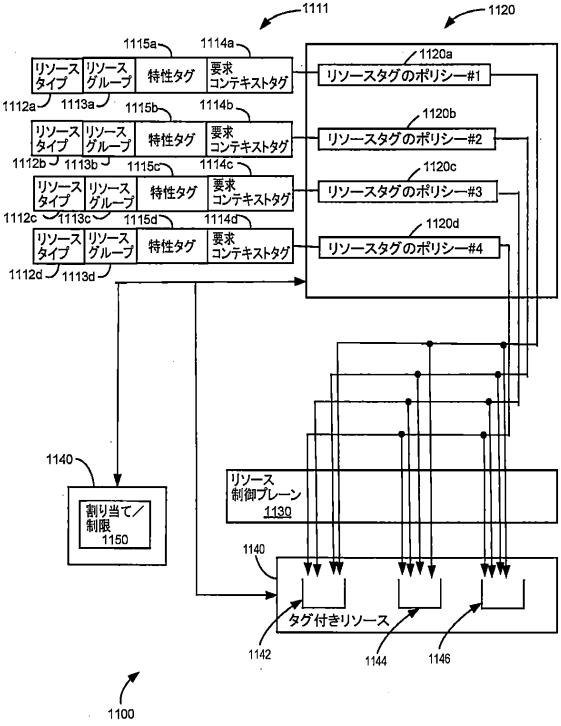


FIGURE 11

【図 12】

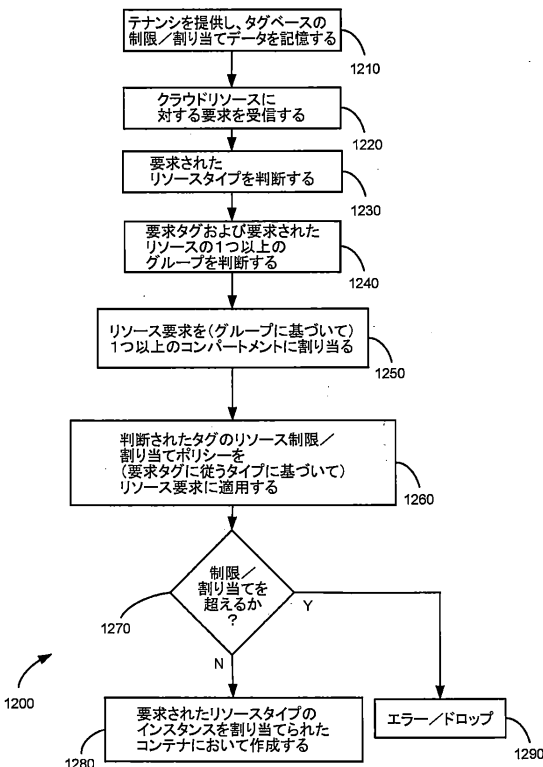


FIGURE 12

フロントページの続き

(33)優先権主張国・地域又は機関

米国(US)

(31)優先権主張番号 16/986,158

(32)優先日 令和2年8月5日(2020.8.5)

(33)優先権主張国・地域又は機関

米国(US)

(31)優先権主張番号 16/986,160

(32)優先日 令和2年8月5日(2020.8.5)

(33)優先権主張国・地域又は機関

米国(US)

審査官 田中 幸雄

(56)参考文献 特表2016-507839(JP, A)

米国特許第5341477(US, A)

(58)調査した分野(Int.Cl., DB名)

G06F 9/50