高度な概念

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Citrix ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Citrix は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Citrix 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Citrix とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Citrix は責任を負わないものとします。

Contents

設計 **3**

OpenShift 検証済みリファレンスデザインのルートを使用した **Citrix ADC** へのサービス移行 **5**

VRD ユースケース **— Kubernetes** での **Citrix ADC** 動的ルーティングの使用 **16**

Red Hat OpenShift 3.11 検証済みリファレンスデザイン用の **Citrix Cloud** ネイティブネットワーキング **23**

Citrix ADC ADC および **Microsoft Azure** 検証済みリファレンスデザイン **66**

Citrix ADC CPX、**Citrix Ingress Controller,**、および **Google** クラウドでの **Application Delivery Management** **113**

Citrix ADC クラスタリング検証済みリファレンスデザイン **131**

Citrix ADC プール容量検証済みリファレンス設計 **189**

Diamanti および **Nirmata** 検証済みリファレンスデザインにおける **Kubernetes** での **Citrix ADC CPX** **216**

Citrix ADC SSL プロファイル検証済みリファレンスデザイン **236**

Citrix ADC と **Amazon Web Services** 検証済みのリファレンスデザイン **244**

Citrix ADC 管理パーティション検証済みリファレンスデザイン **319**

Citrix Gateway SaaS および **O365** クラウド **Citrix** 検証済みリファレンスデザイン **333**

Access Control 付き **Citrix Gateway** サービス **SSO Citrix** 検証済みリファレンスデザイン **336**

Azure Load Balancer フロントエンド **IP** 検証済みリファレンスデザインを使用した **Citrix ADC** 高可用性 **342**

XenDesktop 7 のデータベースサイズ設定ツール **345**

実装と構成 **349**

Citrix ADC と **OpenShift 4** ソリューション概要 **349**

SC2S での **VPX Amazon** マシンイメージ（**AMI**）の作成 **354**

Citrix Gateway と **Microsoft Azure** の多要素認証 **377**

データベースの無停止アップグレードのためのローカルホストキャッシュの使用 **440**

AWS の **Linux** 踏み台ホスト経由で **RDP** 経由で **Citrix** インフラストラクチャに接続する **448**

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Azure DNS プライベートゾーンでの **Citrix ADC** 展開ガイド **452**

Citrix フェデレーション認証サービスのログオン証拠の概要 **472**

XenApp および **XenDesktop 7.6** 用の **HDX** ポリシーテンプレートを現在のバージョンにアップグレードする **477**

SQL Server と **Citrix** データベース **492**

XenApp および **XenDesktop** のグループポリシー管理テンプレートの更新 **497**

XenApp および **XenDesktop 7.11** から現在のバージョンまで：遅延および **SQL** ブロッキングクエリの改善 **501**

XenApp および **XenDesktop ktop** バージョン **7.6** のデータベースサイズ設定ガイダンス **504**

オーバーフローによる **PVS RAM** キャッシュの分析 **519**

Citrix Secure Browser で保護されたブラウザーを使用してレガシー **Web** アプリケーションの寿命を延ばす **525**

ローカルホストキャッシュのサイズ設定とスケーリング **552**

XenApp および **XenDesktop 7.9** での **Citrix** ユニバーサルプリントサーバーの負荷分散 **562**

SQL Server 高可用性ソリューションを使用するときにデータベース接続文字列を更新する **575**

Active Directory OU ベースの **Controller** 検出 **583**

© 1999–2021 Citrix Systems, Inc. All rights reserved.

設計

May 20, 2020

OpenShift 検証済みリファレンスデザインのルートを使用した Citrix ADC へのサービス移行

中断することなくサービスを移行します。

VRD ユースケース — Kubernetes での Citrix ADC 動的ルーティングの使用：Acme Inc. Kubernetes アプリケーションのためのルートヘルスインジェクションと BGP 統合

Citrix ADC でルートヘルスインジェクションを使用して、Acme Inc. と Citrix は、既存の BGP + ECMP ルーティングファブリック経由でアクセスされる Kubernetes サービスに冗長性を提供するソリューションを実装しました。Acme Inc. は、Citrix ADC の大規模なフットプリントを持つ長年のシトリックス顧客です。Citrix ADC は、重要な Kubernetes アプリケーションの主な負荷分散およびビジネス継続性ソリューションとして機能します。Acme Inc. は、現在、3 つの主要なデータセンターを持っています。

Red Hat OpenShift 3.11 検証済みリファレンスデザイン用の Citrix Cloud ネイティブネットワーキング

Citrix ADC Stack はアプリケーション可用性機能（ADC）、セキュリティ機能の分離（WAF）、アジャイルアプリケーショントポロジ（SSL と GSLB）のスケーリング、および積極的な観察性（サービスグラフ）の高度に調整された Cloud Native Era 環境での基本的な要件を満たします。この検証済みのリファレンスデザインは、Red Hat OpenShift 3.11 用の Citrix Cloud ネイティブネットワーキングの展開をガイドします。

Citrix ADC ADC および Microsoft Azure 検証済みリファレンスデザイン

Citrix ADC はオールインワンのアプリケーション配信 Controller で、アプリケーションを最大 5 倍に実行し、アプリケーションの所有コストを削減し、ユーザーエクスペリエンスを最適化し、アプリケーションを常に利用できるようにします。

Citrix ADC CPX、Citrix Ingress Controller,、および Google クラウドでの Application Delivery Management

Citrix ADC クラスタリング検証済みリファレンスデザイン

Citrix ADC クラスターは、単一のシステムイメージとして連携して動作する Citrix ADC nCore アプライアンスのグループです。クラスターの各アプライアンスは、ノードと呼ばれます。Citrix ADC クラスターには、ノードとして 2 台または 32 台までの Citrix ADC nCore ハードウェアまたは仮想アプライアンスを含めることができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クライアントトラフィックは、高可用性、高スループット、およびスケーラビリティを提供するために、ノード間で分散されます。

Citrix ADC プール容量検証済みリファレンス設計

Citrix ADC プール容量は、Citrix Application Delivery Management でホストされ、サービスされる帯域幅プールと仮想インスタンスプールで構成されるライセンスフレームワークです。

Diamanti および Nirmata 検証済みリファレンスデザインにおける Kubernetes での Citrix ADC CPX

Citrix ADC は、アプリケーション固有のトラフィック分析を実行し、Web アプリケーションのレイヤー 4 レイヤー 7（L4〜L7）ネットワークトラフィックをインテリジェントに分散、最適化、保護するアプリケーションデリバリーコントローラーです。この機能のセットは、スイッチング、セキュリティと保護、およびサーバファーム最適化機能で構成できます。

Citrix ADC SSL プロファイル検証済みリファレンスデザイン

SSL プロファイルを使用して、Citrix ADC が SSL トラフィックを処理する方法を指定します。このプロファイルは、仮想サーバ、サービス、サービスグループなどの SSL エンティティの SSL パラメータ設定の集まりであり、設定の容易さと柔軟性を提供します。グローバルパラメータのセットを 1 つだけ設定することに限定されません。グローバルパラメータの複数のセット（プロファイル）を作成し、異なる SSL エンティティに異なるセットを割り当てることができます。

Citrix ADC と Amazon Web Services 検証済みのリファレンスデザイン

Citrix Networking VPX は、AWS Marketplace に Amazon マシンイメージ（AMI）として表示されます。Citrix Networking VPX on AWS では、AWS クラウドコンピューティング機能を活用し、Citrix ADC の負荷分散機能とトラフィック管理機能をビジネスニーズに合わせて利用できます。Citrix ADC on AWS は、物理 Citrix ADC アプライアンスのすべてのトラフィック管理機能をサポートします。AWS で実行されている Citrix ADC インスタンスは、スタンドアロンインスタンスとして、または HA ペアで展開できます。

Citrix ADC 管理パーティション検証済みリファレンスデザイン

NetScaler 管理者パーティションでは、単一の NetScaler インスタンスでソフトウェアレベルでマルチテナント機能を使用できます。各パーティションには、独自のコントロールプレーンとネットワークプレーンがあります。このドキュメントでは、管理パーティションによって有効になっている一般的なユースケースと、お客様の環境で管理パーティションを使用するためのガイドラインを詳しく説明します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Gateway SaaS および O365 クラウド検証済みリファレンスデザイン

Software as a Service（SaaS）は、ソフトウェアを Web ベースのサービスとしてリモートで配信するためのソフトウェア配布モデルです。一般的に使用される SaaS アプリ (Microsoft Office 365 サブスクリプションを含む)。

Citrix Gateway サービスを使用して、Citrix Workspace で SaaS アプリにアクセスできるようになりました。Citrix Gateway サービスと Citrix Workspace を組み合わせることで、構成済みの SaaS アプリケーション、構成済みの仮想アプリケーション、またはその他のワークスペースリソースに対する統一されたユーザーエクスペリエンスが提供されます。

Citrix Gateway サービスを使用した SaaS アプリの配信は、アプリを管理するための簡単で安全で堅牢でスケーラブルなソリューションを提供します。

Access Control 検証済みのリファレンスデザイン付き Citrix Gateway サービス SSO

アクセス制御サービスを使用すると、管理者はシングルサインオン、リモートアクセス、コンテンツ検査を単一のソリューションに統合し、エンドツーエンドのアクセス制御を実現する一貫したエクスペリエンスを提供できます。IT 管理者は、承認された SaaS アプリへのアクセスを、シンプルなシングルサインオン環境で制御できます。アクセス制御サービスを使用すると、管理者は、特定の Web サイトや Web サイトカテゴリへのアクセスをフィルタリングすることで、マルウェアやデータ漏洩から組織のネットワークやエンドユーザーのデバイスを保護することもできます。アクセスに関するセキュリティの強化ポリシーを設定することで、SaaS アプリへのセキュアなアクセスが可能になります。一度認証されると、社内、自宅、または外出中のいずれの場合も、従業員は任意のデバイスから重要なすべてのアプリケーションにアクセスできます。

Azure Load Balancer フロントエンド IP 検証済みリファレンスデザインを使用した Citrix ADC 高可用性

Azure ロードバランサー（ALB）をフロントエンド（FE）ロードバランサーとして使用して、Microsoft Azure に NetScaler の高可用性展開を実装します。

OpenShift 検証済みリファレンスデザインのルートを使用した Citrix ADC へのサービス移行

May 18, 2020

OpenShift クラスター内の静的ルートと自動ルート

静的ルート（デフォルト）-静的ルートを介して **OpenShift HostSubnet** を外部 **ADC** にマッピングします

静的ルートは、HAProxy を使用するレガシー OpenShift の展開では一般的です。静的ルートは、あるサービスプロキシから別のサービスプロキシにサービスを移行する場合に、機能しているクラスターに展開された名前空間を中断

© 1999–2021 Citrix Systems, Inc. All rights reserved.

することなく、Citrix Node Controller（CNC）、Citrix Ingress Controller（CIC）、および CPX と並行して使用することができます。

Citrix ADC 静的ルート構成例：

```
    oc get hostsubnet (Openshift Cluster) snippet
        oc311-master.example.com 10.x.x.x 10.128.0.0/23
        oc311-node1.example.com 10.x.x.x 10.130.0.0/23
        oc311-node2.example.com 10.x.x.x 10.129.0.0/23

    show route (external Citrix VPX) snippet
        10.128.0.0 255.255.254.0 10.x.x.x STATIC
        10.129.0.0 255.255.254.0 10.x.x.x STATIC
        10.130.0.0 255.255.254.0 10.x.x.x STATIC
<!--NeedCopy-->
```

自動ルート**-CNC**（**Citrix** ノードコントローラ）を使用して、定義されたルートシャードへの外部ルートを自動化します

Citrix ADC を OpenShift と統合するには、2 つの方法があります。どちらの方法も OpenShift ルーターのシャーディングをサポートします。

ルートタイプ

- 非セキュア-CIC ルータへの外部ロードバランサ、HTTP トラフィックは暗号化されません。
- セキュアエッジ-TLS を終了する CIC ルータへの外部ロードバランサー。
- セキュアパススルー-TLS を終了する宛先への外部ロードバランサー
- セキュアな再暗号化-TLS を終了する CIC ルータへの外部ロードバランサー。TLS を使用して宛先に暗号化する CIC ルーター。

さまざまなルートタイプについて詳しくは、Citrix 入力 Controller 展開ソリューションを参照してください。

Citrix Ingress Controller の展開と **OpenShift** のルーターシャーディングのサポート

Citrix Ingress Controller（CIC）はルーターとして機能し、トラフィックをさまざまなポッドにリダイレクトして、使用可能なさまざまなポッド間で着信トラフィックを分散します。

この移行プロセスは、従来の OpenShift トポロジーから Citrix CNC、CIC、CPX コンポーネントを使用した自動展開へのクラスターアップグレードプロセスの一部でもあります。

このソリューションは、次の 2 つの方法で実現できます。

- CIC ルータープラグイン (Pod)
- OpenShift 内にある CPX ルーター (サイドカー)

© 1999–2021 Citrix Systems, Inc. All rights reserved.

どちらの方法も、移行例とともに以下で説明します。

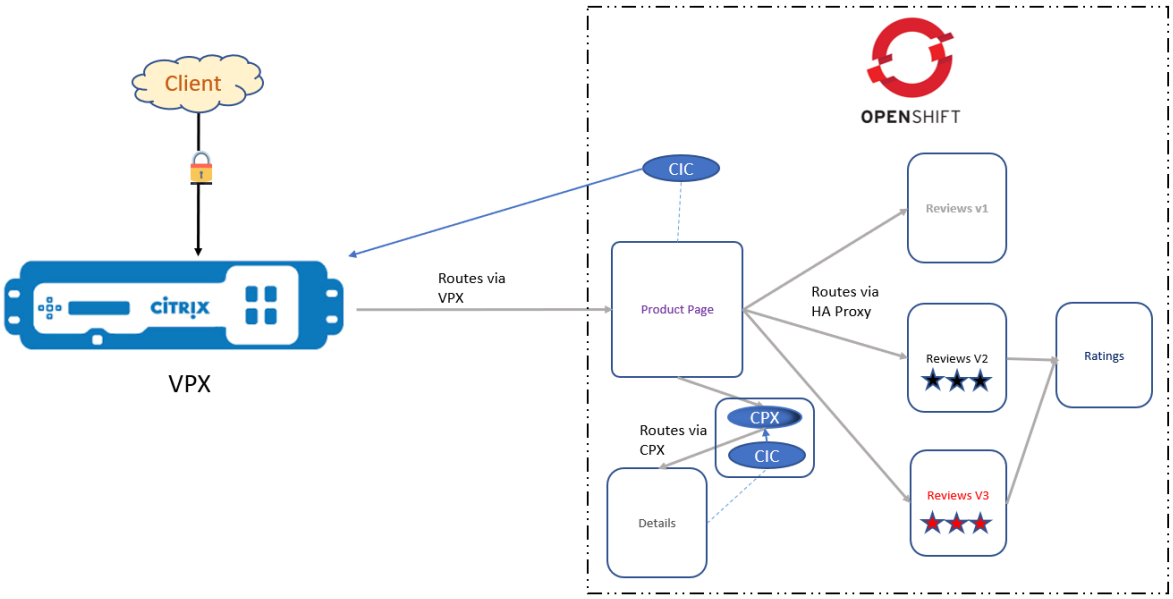
OpenShift ルーターのシャーディング では、複数の OpenShift ルーター間で一連のルートを配布できます。デフォルトでは、OpenShift ルーターはすべての名前空間からすべてのルートを選択します。ルーターシャーディングでは、ルートまたは名前空間にラベルが追加され、ルートをフィルタリングするためのラベルセレクタがルーターに追加されます。各ルーターシャードは、ラベル選択パラメータに一致する特定のラベルを持つルートだけを選択します。

OpenShift で Citrix ADC 展開のルーターシャーディングを構成するには、シャードごとに Citrix 入力 Controller インスタンスが必要です。Citrix Ingress Controller インスタンスは、シャーディングに必要な条件に応じて、ルートラベル、名前空間ラベル、またはその両方を環境変数として展開します。Citrix Ingress Controller はルートを処理するときに、ルートのラベルまたはルートの名前空間ラベルを、そのルートに設定された選択基準と比較します。ルートが基準を満たす場合、適切な構成が Citrix ADC に適用されます。そうでない場合、構成は適用されません。

ルーターシャーディングでは、ルートプール全体からルートのサブセットを選択することは、選択式に基づきます。選択式は、複数の値と演算の組み合わせです。式、値、および操作について詳しくは、こちら（Citrix ブログ）を参照してください。

Bookinfo の展開

Bookinfo アプリケーションのアーキテクチャは、下の図に示されています。CIC は OpenShift ルータープラグインとして第 1 層で展開され、Citrix ADC VPX が南北トラフィックを製品ページにルーティングするように構成されます。第 2 層では、Citrix ADC CPX が OpenShift ルーターとして展開され、詳細と製品ページのマイクロサービス間で東西のトラフィックをルーティングします。一方、製品ページ、レビュー、評価のマイクロサービス間の東西のトラフィックは、デフォルトの HAProxy ルーターを介してルーティングされます。



Citrix コンポーネント

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- VPX-DNS にクラスタサービスを提示する入力 ADC。
- CIC-CNC ルートを介して外部 Citrix ADC にルートラベルと名前空間のラベルを提供します。
- CPX-OpenShift クラスター内で OpenShift ルーティングを提供します。

展開手順

1. 展開の名前空間を作成します。`oc create ns sml`
2. Bookinfo アプリケーションを名前空間に展開します。`oc apply -f bookinfo.yaml`

```
##################################################################################

# Details service
##################################################################################

apiVersion: v1
kind: Service
metadata:
  name: details
  labels:
    app: details
    service: details
spec:
  ports:
  - port: 9080
    name: http
  selector:
    app: details
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: details-v1
  labels:
    app: details
    version: v1
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
      labels:
        app: details
        version: v1
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    spec:
      containers:
"bookinfo.yaml" 224L, 5120C

<!--NeedCopy-->
```

3. 製品ページサービスにマップするルートファイルを展開します。指定 `frontend-ip`（これはティア 1ADC のコンテンツスイッチング vip です）`oc apply -f routes-productpage.yaml`

```
apiVersion: v1
kind: Route
metadata:
   name: productpage-route
   namespace: sml
   annotations:
    ingress.citrix.com/frontend-ip: "X.X.X.X"
   labels:
    name: productpage
spec:
   host: bookinfo.com
   path: /
   port:
     targetPort: 80
   to:
     kind: Service
     name: productpage-service
<!--NeedCopy-->
```

4. 実行に必要なパーミッションを CIC に付与する sml 名前空間の RBAC ファイルを展開します。RBAC ファイルは既に名前空間になっています。`oc apply -f rbac.yaml`

```
 kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
rules:
  - apiGroups: [""]
    resources: ["endpoints", "ingresses", "services", "pods", "
       secrets", "nodes", "routes", "namespaces","tokenreviews","
       subjectaccessreview"]
    verbs: ["get", "list", "watch"]
  # services/status is needed to update the loadbalancer IP in
     service status for integrating
  # service of type LoadBalancer with external-dns
  - apiGroups: [""]
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
12      resources: ["services/status"]
13      verbs: ["patch"]
14    - apiGroups: ["extensions"]
15      resources: ["ingresses", "ingresses/status"]
16      verbs: ["get", "list", "watch"]
17    - apiGroups: ["apiextensions.k8s.io"]
18      resources: ["customresourcedefinitions"]
19      verbs: ["get", "list", "watch"]
20    - apiGroups: ["apps"]
21      resources: ["deployments"]
22      verbs: ["get", "list", "watch"]
23    - apiGroups: ["citrix.com"]
24      resources: ["rewritepolicies", "canarycrds", "authpolicies", "
            ratelimits"]
25      verbs: ["get", "list", "watch"]
26    - apiGroups: ["citrix.com"]
27      resources: ["vips"]
28      verbs: ["get", "list", "watch", "create", "delete"]
29    - apiGroups: ["route.openshift.io"]
30      resources: ["routes"]
31      verbs: ["get", "list", "watch"]
32
33  ---
34  kind: ClusterRoleBinding
35  apiVersion: rbac.authorization.k8s.io/v1beta1
36  metadata:
37    name: cpx
38  roleRef:
39    apiGroup: rbac.authorization.k8s.io
40    kind: ClusterRole
41    name: cpx
42  subjects:
43  - kind: ServiceAccount
44    name: cpx
45    namespace: sml
46  ---
47  apiVersion: v1
48  kind: ServiceAccount
49  metadata:
50  "rbac.yaml" 51L, 1513C
51   <!--NeedCopy-->
```

5. CIC を展開して、ルート設定を VPX にプッシュします。パラメータ ROUTE_LABELS を`route-productpage.yaml`で指定されたラベルに一致させます。ROUTE_LABERS の構文ついて詳しくは、

© 1999–2021 Citrix Systems, Inc. All rights reserved.

こちら（ブログ）を参照してください。`oc apply -f cic-productpage-v2.yaml`

```
apiVersion: v1
kind: Pod
metadata:
  name: cic
  labels:
    app: cic
spec:
  serviceAccount: cpx
  containers:
  - name: cic
    image: "quay.io/citrix/citrix-k8s-ingress-controller:1.7.6"
    securityContext:
       privileged: true
    env:
    - name: "EULA"
      value: "yes"
    # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has to be
       enabled)
    - name: "NS_IP"
      value: "X.X.X.X"
    # Set NetScaler VIP that receives the traffic
#    - name: "NS_VIP"
#      value: "X.X.X.X"
    - name: "NS_USER"
      value: "nsroot"
    - name: "NS_PASSWORD"
      value: "nsroot"
    - name: "NS_APPS_NAME_PREFIX"
      value: "BOOK"
    - name: "ROUTE_LABELS"
      value: "name in (productpage)"
#    - name: "NAMESPACE_LABELS"
#      value: "app=hellogalaxy"
    # Set username for Nitro
#    - name: "NS_USER"
#      valueFrom:
#       secretKeyRef:
#        name: nslogin
#        key: nsroot
#    # Set user password for Nitro
#    - name: "NS_PASSWORD"
#      valueFrom:
#       secretKeyRef:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
#         name: nslogin
#         key: nsroot
    args:
#    - --default-ssl-certificate
#      default/default-cert
    imagePullPolicy: Always
~
"cic-productpage-v2.yaml" 48L, 1165C
<!--NeedCopy-->
```

6. 次に、クラスターの DNS Pod を使用して CPX に詳細を探しているユーザーを指し示すヘッドレスサービスを作成する必要があります。`oc apply -f detailsheadless.yaml`

```
##################################################################################

# Details service
##################################################################################

apiVersion: v1
kind: Service
metadata:
  name: details
spec:
  ports:
  - port: 9080
    name: http
  selector:
    app: cpx
<!--NeedCopy-->
```

7. 新しいサービスをデプロイして、詳細コンテナを公開します。`oc apply -f detailsservice.yaml`

```
##################################################################################

# Details service
##################################################################################

apiVersion: v1
kind: Service
metadata:
  name: details-service
  labels:
    app: details-service
    service: details-service
spec:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
  clusterIP: None
  ports:
  - port: 9080
    name: http
  selector:
    app: details
<!--NeedCopy-->
```

8. 作成した詳細サービスの前にある新しいルート定義を展開します。ラベルが「名前：詳細」の形式になっていることに注意してください。`oc apply -f detailsroutes.yaml`

```
apiVersion: v1
kind: Route
metadata:
   name: details-route
   namespace: sml
   annotations:
    ingress.citrix.com/insecure-port: "9080"
   labels:
    name: details
spec:
   host: details
   path: /
   port:
      targetPort: 9080
   to:
     kind: Service
     name: details-service
<!--NeedCopy-->
```

9. E/W トラフィック用に CPX を展開します。CIC はサイドカーとして展開され、detailsroutes.yaml のラベルと一致するように ROUTE_LABEL パラメータが設定されます。`oc apply -f cpx.yaml`

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: cpx
  labels:
    app: cpx
    service: cpx
spec:
  replicas: 1
  template:
    metadata:
      name: cpx
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
13        labels:
14          app: cpx
15          service: cpx
16        annotations:
17          NETSCALER_AS_APP: "True"
18      spec:
19        serviceAccountName: cpx
20        containers:
21          - name: cpx
22            image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-36.28
                  "
23            securityContext:
24               privileged: true
25            env:
26            - name: "EULA"
27              value: "yes"
28            - name: "KUBERNETES_TASK_ID"
29              value: ""
30            - name: "MGMT_HTTP_PORT"
31              value: "9081"
32            ports:
33            - name: http
34              containerPort: 9080
35            - name: https
36              containerPort: 443
37            - name: nitro-http
38              containerPort: 9081
39            - name: nitro-https
40              containerPort: 9443
41  # readiness probe?
42            imagePullPolicy: Always
43          # Add cic as a sidecar
44          - name: cic
45            image: "quay.io/citrix/citrix-k8s-ingress-controller
                  :1.7.6"
46            env:
47            - name: "EULA"
48              value: "yes"
49            - name: "NS_IP"
50  "cpx.yaml" 75L, 1939C
51  <!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

マイクロサービス環境における継続的デリバリーの選択

継続的インテグレーション（CI）は、開発者が 1 日に数回コードを共有リポジトリに統合することを要求する開発慣行です。

継続的デリバリー（CD）は、継続的インテグレーションの自然な拡張です。チームが、システムへのすべての変更がリリース可能であることを確認し、ボタンを押すだけで任意のバージョンをリリースできるようにするアプローチです。

さまざまな CD の選択肢と、その長所と短所は次のとおりです。

- 再作成: バージョン 1 (V1) が終了し、バージョン 2 (V2) がロールアウトされます。
  - 長所
    - セットアップが簡単。
    - アプリケーションの状態は完全に更新されます。
  - 短所
    - ユーザーへの影響が大きい。シャットダウンと起動時間の両方に依存するダウンタイムが予想されます。
- 傾斜/ローリング更新 -V2 はゆっくりとロールアウトされ、V1 を置き換えます。
  - 長所
    - セットアップが簡単。
    - バージョンはインスタンス間でゆっくりとリリースされます。
    - データの再バランスを処理できるステートフルなアプリケーションに便利です。
  - 短所
    - ロールアウト/ロールバックには時間がかかる場合があります。
    - 複数の API をサポートするのは難しいです。
    - トラフィックの制御はほとんどありません。
- 青緑 -V2 は V1 とともに解放され、トラフィックは V2 に切り替わります。
  - 長所
    - インスタントロールアウト/ロールバック。
    - アプリケーション全体が一度に変更されるため、バージョンの問題を回避できます。
  - 短所
    - それは 2 倍のリソースを必要とするので、高価です。
    - プラットフォーム全体の適切なテストは、本番環境にリリースする前に行う必要があります。
    - 複数のステートフルなアプリケーションの処理は難しい場合があります。
- **Canary** -V2 はユーザのサブセットにリリースされ、完全なロールアウトに進みます。
  - 長所
    - ユーザーのサブセット用にリリースされたバージョン。
    - エラー率とパフォーマンス監視に便利です。
    - 高速ロールバック。
  - 短所
    - [遅い] ロールアウト。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

        * 複数のステートフルなアプリケーションの処理は難しい場合があります。
- **A/B** テスト -V2 は、特定の条件下でユーザーのサブセットにリリースされます。
    - 長所
        * いくつかのバージョンが並行して実行されます。
        * トラフィック分散を完全に制御します。
    - 短所
        * インテリジェントなロードバランサーが必要です。
        * 特定のセッションのエラーのトラブルシューティングが難しく、分散トレースが必須になります。
- **Shadow** -V2 は V11 とともに実世界のトラフィックを受信し、応答には影響しません。
    - 長所
        * 本番トラフィックを使用したアプリケーションのパフォーマンステスト。
        * ユーザーへの影響はありません。
        * アプリケーションの安定性とパフォーマンスが要件を満たさない限り、ロールアウトは行われません。
    - 短所
        * それは 2 倍のリソースを必要とするので、高価です。
        * 真のユーザーテストではなく、誤解を招く可能性があります。
        * セットアップが複雑です。
        * 特定のケースではモックサービスが必要です。

参考資料

Citrix GitHub:「OpenShift routes and ingress」

Citrix Developer Docs:「Deployment solutions」

Citrix ブログ:「Enable OpenShift router sharding support with Citrix ADC」

OpenShift ルートドキュメント:

VRD ユースケース **— Kubernetes** での **Citrix ADC** 動的ルーティングの使用

May 18, 2020

Acme Inc. Kubernetes アプリケーション向けルートヘルスインジェクションと **BGP** 統合

Acme Inc. は、Citrix ADC の大規模なフットプリントを持つ長年のシトリックス顧客です。Citrix ADC は、重要な Kubernetes アプリケーションの主な負荷分散およびビジネス継続性ソリューションとして機能します。Acme Inc. は、現在、3 つの主要なデータセンターを持っています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Acme Inc. は、重要な Kubernetes アプリケーションに冗長性と高可用性を提供したいと考えています。これにより、3 つのデータセンターのすべてのデプロイラックでフォールトトレランスを強化できます。

Citrix ADC でルートヘルス注入を使用すると、既存の BGP + ECMP ルーティングファブリックを介してアクセスされる Kubernetes サービスに冗長性を提供します。

ルートヘルスインジェクションに加えて、多くの Kubernetes アプリケーションは、実際のクライアント IP を受信するためにバックエンドサーバーを必要とします。Citrix ADC を使用した従来の負荷分散では、バックエンドサーバー宛てのパケットを ADC サブネット IP アドレスから送信します。ソースアドレスとして真のクライアント IP アドレスを必要とするアプリケーションでは、Citrix ADC は複数の方法を提供します。これらの方法には、USIP（送信元 IP モードを使用）と DSR（直接サーバーリターン）が含まれます。

Acme Inc. IT は、Kubernetes アプリケーションのテスト VIP とテスト Citrix ADC VPX インスタンスをプロビジョニングします。このテスト環境は、クライアント IP を使用してルートヘルスインジェクションソリューションを構築し、運用環境にロールアウトする前に完全にテストするために使用されます。

展開の要件

Acme Inc. と Citrix は、いくつかの異なる要件を特定しました。

- 各データセンター内の Citrix ADC VPX ユニット（動的ルーティングネットワーク接続）（3）
- Acme Inc. の動的ルーティングで /32 ルートとして構成される、最大 3 つの仮想サーバーの IP アドレス

環境:

クベルネテステスト VIP

- 各 Citrix ADC ユニットのルートヘルスインジェクション VIP のネクストホップとして使用される各データセンターの SNIP アドレスには、動的ルーティングが有効になっている独自の SNIP アドレスが必要です。これは、アドバタイズされたルートヘルスインジェクション VIP の Gateway です。

以下を含む Kubernetes の情報を特定します。

- バックエンド Kubernetes ポッドとテスト VIP
- 必要なポートとロードバランシングパラメーター
- SSL 証明書（該当する場合）

クライアント IP 構成

- バックエンドサーバーは、真のクライアント IP アドレスを受信する必要がある
- 使用可能な複数のオプションについては、「クライアント IP オプション」セクションで説明します。

ルートヘルスインジェクション（**RHI**）

Citrix ADC 動的ルーティング（ルートヘルスインジェクションあり）

Citrix ADC での動的ルーティングとルート正常性注入の主な目的は、VIP の状態または正常性をアップストリームルーターに伝達することです。VIP の状態は、それに関連付けられた仮想サーバーと、その VIP にバインドされている

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サービスによって異なります。ルートヘルスインジェクションによる VIP のアドバタイズメントは、仮想 IP アドレスに関連付けられた仮想サーバの状態に関連付けられます。

仮想 IP アドレスでアドバタイズメントが有効になっている必要があります。このためには、仮想 IP アドレスで-hostrouteオプションをenabledに設定します。デフォルトでは、-hostrouteオプションはdisabledに設定されています。-hostroute このオプションは、コマンドで IP アドレスを追加するとき、または add ns ip コマンドを使用して既存の IP アドレスを変更するときに有効にできます。set ns ip

ルートヘルスインジェクションのモニタリング

hostRoute このオプションを有効にすると、NetScaler カーネルは、仮想 IP アドレスに関連付けられた仮想サーバーの状態に基づいて、ホストルートを ZebOS NSM（ネットワークサービスモジュール）に挿入します。- vserverroute health injectionLevel スイッチは、仮想サーバの状態と Network Services Module（NSM; ネットワークサービスモジュール）に送信される仮想 IP ホストルートの関係を制御します。

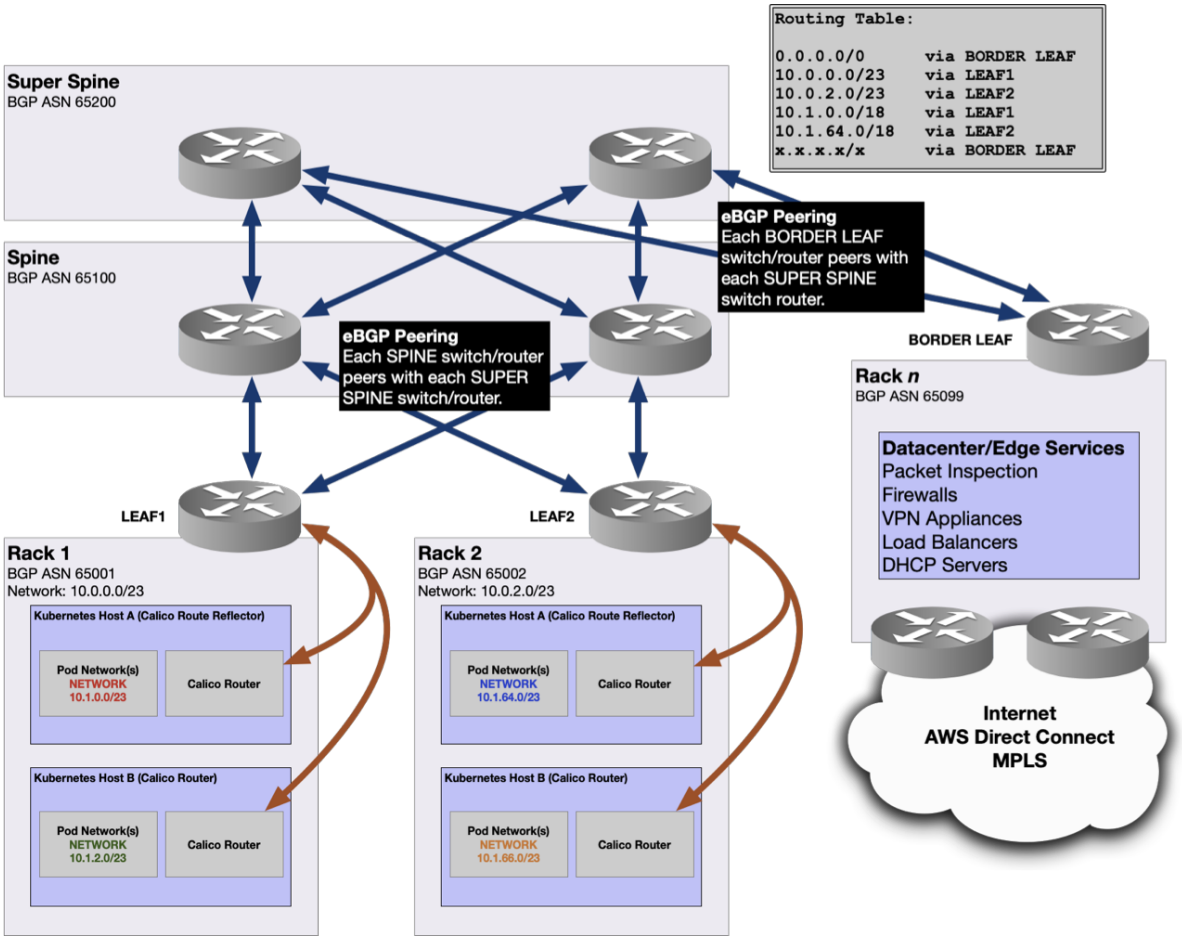
仮想サーバールートヘルスインジェクションレベルで使用できる次の 3 つのオプション。

- ALL_VSERVERS — ホストルートは、仮想 IP に関連付けられたすべての仮想サーバーが UP の場合のみ、NSM に注入されます。
- ONE_VSERVER — ホストルートは、仮想 IP に関連付けられた仮想サーバのいずれかが UP の場合のみ、NSM に注入されます。
- NONE — ホストルートは、仮想 IP に関連付けられた仮想サーバの状態に関係なく、NSM に注入されます。

> 注:
>
> デフォルトでは、—vServerRHilevel は ONE_VSERVER に設定されています。

次の図は、Citrix ADC 上の負荷分散仮想サーバーに関連付けられた仮想 IP アドレスの基本的なルートヘルス注入機能を示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



複数のデータセンターでのルートヘルスインジェクションオプション

次に、各アプリケーションの特定の要件に応じて、アプリケーションごとに選択されるルートヘルスインジェクション設定について説明します。以下の種類から選択できます。

Active：各クライアント（エニーキャストまたは ECMP）に対して最も効率的なルートを決定する BGP によるアクティブ

ルートヘルスインジェクションアクティブ ー アクティブ：エニーキャストまたは **ECMP**

ルートヘルスインジェクションがアクティブ/アクティブはエニーキャストまたは ECMP です。これは真のアクティブ-アクティブ代替手段です。このシナリオでは、ルートヘルスインジェクション VIP の /32 ルートがすべてのデータセンターでアドバタイズされ、コストやローカルプリファレンスが BGP に提示されることはありません。3 つのルートが、各 VIP にアクセスするための Gateway として機能する各データセンターに固有の Citrix ADC の SNIP アドレスを持つネットワークに提供されます。Acme Inc. の動的ルーティング環境では、トラフィック分散のために均等なコストでクライアント要求をデータセンターに送信します。3 つのデータセンターのいずれかでサービスに障害が発生した場合、負荷分散されたサービスにバインドされたモニターによって仮想サーバーが停止します。これによ

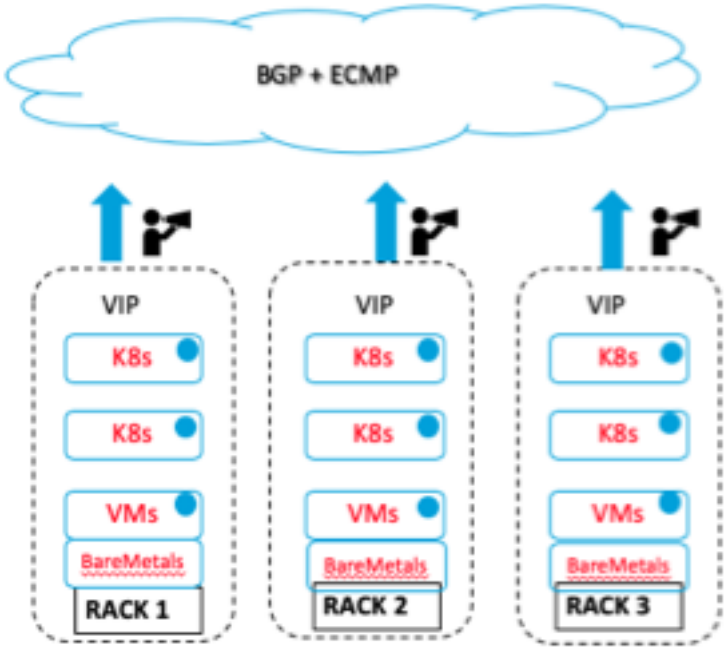
© 1999–2021 Citrix Systems, Inc. All rights reserved.

り、障害が発生したデータセンターのルートアドバタイズメントが削除されます。すべてのクライアント接続は、残りのデータセンターで引き続き動作します。

ルートヘルスインジェクションのアクティブ/アクティブ設定に関する重要な考慮事項:

1. ECMP を使用したルートヘルスインジェクションは、TCP および UDP ベースのサービスに対して推奨され、Acme Inc. ネットワークチームによる BGP 設定が必要です。ECMP を使用したルートヘルスインジェクションでは、アップストリームルータがサポートできるルートの数（64）に制限があります。
2. エニーキャストを使用したルートヘルスインジェクションは UDP ベースのサービスで動作しますが、TCP ベースのサービスにはお勧めしません。

次の図は、アクティブな ANYCast/ECMP シナリオを示しています。



Citrix ADC とクライアント **IP** のオプション

大量の Kubernetes アプリケーションに対して Acme Inc. が要求する重要な要件の 1 つは、バックエンドサーバーが Citrix ADC によって負荷分散されるサービスの真のクライアント IP アドレスを受信することです。Citrix ADC の一般的な負荷分散は、NetScaler が所有する SNIP（サブネット IP）アドレスからバックエンドサーバー宛てのすべてのトラフィックを処理します。一部のアプリケーションでは、実際のクライアント IP が必要です。ルートヘルスインジェクションを利用するアプリケーションのほとんどは、真のクライアント IP をバックエンドサーバーに送信する必要があります。

Citrix ADC には「Use Source IP」（USIP）と呼ばれる機能があり、グローバルにバインドすることも、バックエンドサーバーにクライアント IP を必要とする各サービスに個別にバインドすることもできます。この問題は、クライアントが異なる送信元 IP を持つパケットを受信すると、非対称ルーティングが発生し、パケットがドロップされること

© 1999–2021 Citrix Systems, Inc. All rights reserved.

です。このため、その他の考慮事項を評価する必要があり、USIP を適切に動作させるには、バックエンドサーバーに追加の設定が必要になります。

Citrix ADC でソース IP モードの使用を実装する際の重要な考慮事項は、Citrix ADC モードでサージ保護モードをオフにする必要があることです。サージ保護を使用した USIP モードの詳細については、Citrix の記事を参照してください ここ。

Citrix ADC では、これを実現するための複数の方法が用意されています。これらの方法については、次のセクションで説明します。使用可能なオプションは次のとおりです。

- Citrix ADC SNIP をデフォルト Gateway として使用した USIP モード
- ダイレクトサーバリターンレイヤ 3
  - IP トンネリング
  - TOS ヘッダーへのクライアント IP 挿入
- ダイレクトサーバリターンレイヤ 2
- TCP ヘッダーのクライアント IP 挿入

デフォルトのゲートウェイとして **Citrix ADC SNIP** を使用する **USIP** モード

Acme Inc. IT との複数の会議で、クライアントの IP を必要とする負荷分散サービスのほとんどでこの方式が好ましいと判断されました。この方法では、負荷分散される各バックエンドサーバーのデフォルト Gateway を変更し、負荷分散された VIP をホストする Citrix ADC ユニットの SNIP アドレスに設定します。このオプションは、Citrix ADC が受信クライアント要求のみを管理する、ダイレクトサーバーのリターンオプションとは対照的に、すべての Citrix ADC 機能をサポートします。また、このオプションでは、ADC ユニットの帯域幅が最も多く必要になります。この方法には、次の基本的な要件があります。

- Citrix ADC は、負荷分散されるすべてのバックエンドサーバーと同じ L2 サブネットに SNIP アドレスを設定する必要があります。
- SNIP アドレスは、すべてのバックエンドサーバーのデフォルト Gateway として構成されます。異なる L2 サブネットのバックエンドサーバーには、複数の SNIP アドレスを使用できます。
- バックエンドサーバーを指すサービスで USIP モードを有効にする必要があります。

> 注:
>
> USIP は Citrix ADC ユニットでもグローバルに有効化できますが、USIP は USIP モードを有効にした後に作成されたサービスにのみ適用されます。

バックエンドサーバーにネットワークインターフェイスを追加し、非クライアントトラフィックの静的ルートを構成することをお勧めします。

- 帯域幅を必要とするバックアップルーチンやその他のプロセスは、Citrix ADC ユニットをトラバースする必要はありません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サーバーへのダイレクトリターン**:** レイヤ **3** オプション

Citrix ADC によるサーバーダイレクトリターンは、負荷分散構成でバックエンドサーバー上のクライアント IP アドレスを取得するためのもう 1 つの構成オプションです。ダイレクトサーバリターンはレイヤ 3 モードで設定できるため、ADC からバックエンドサーバーへの L2 接続を必要とする USIP とは対照的に、他の L3 VLAN 上のバックエンドサーバの使用を許可します。レスポンストラフィックが Citrix ADC ユニットを通過しないため、ダイレクトサーバーリターン構成では特定の Citrix ADC 機能をサポートしていません。このオプションでは、Citrix ADC ユニットのスループットが最小になります。

ダイレクトサーバーリターンは、クライアント IP を抽出し、TCP ヘッダーを書き換えてクライアントに直接応答できるようにする必要があるため、バックエンドサーバーに必要なより複雑な構成を持っています。Citrix は現在、レイヤー 3 DSR を構成するための 2 つの異なる方法をサポートしています。

- IP トンネリング付き DSR モード（IP オーバー IP）
- TOS（タイプオブサービス TCP ヘッダーフィールド）を備えた DSR モードレイヤ 3

DSR には、次の基本的な要件があります。

- Citrix ADC は、サービス上で USIP で構成する必要があります。
- バックエンドサーバーには、Citrix ADC VIP アドレスで構成されたループバックアドレスがあります。
- バックエンドサーバーは、各方式に固有に設定する必要があります。
  - IP トンネリング: バックエンドサーバーは、ADC からのパケットをカプセル化解除し、クライアントへの直接応答のためにクライアント IP を抽出する必要があります。
  - TOS（Type of Service）: バックエンドサーバーが TCP パケットの TOS ヘッダーを読み取り、この情報を使用してクライアントに直接応答できる必要があります。
  - どちらの方法でも、バックエンドサーバーでのカスタム設定と、サードパーティ製アプリケーションの使用が必要になる場合があります。

レイヤ 3 DSR では、ファイアウォールとセキュリティデバイスの例外の設定が必要になる場合があります。

レイヤ 3 での直接サーバーリターンの詳細については、こちらを参照してください。

- TOS 付きの DSR
- IP トンネリングを使用した DSR

タイプ「ロードバランサー」のサービスを公開する

タイプ LoadBalancer のサービスは、AWS、GCP、Azure などのパブリッククラウド上の Kubernetes デプロイでネイティブにサポートされています。クラウドデプロイメントでは、LoadBalancer タイプのサービスを作成すると、クラウドで管理されるロードバランサーがそのサービスに割り当てられます。その後、ロードバランサーを使用してサービスが公開されます。

Kubernetes のオンプレミス、ベアメタル、またはパブリッククラウドの展開では、クラスター外の Citrix ADC を使用して、着信トラフィックの負荷分散を行うことができます。Citrix 入力 Controller は、Citrix ADC のマルチテナンシーを可能にする柔軟な IP アドレス管理を提供します。Citrix Ingress Controller を使用すると、単一の ADC

© 1999–2021 Citrix Systems, Inc. All rights reserved.

を使用して複数のサービスを負荷分散し、さまざまな Ingress 機能を組み合わせることができます。Citrix ADC を Citrix Ingress Controller とともに使用すると、パブリッククラウドのロードバランサーリソースを最大限に活用し、運用コストを大幅に削減できます。

Citrix ADC が Kubernetes クラスター (Tier-1) の外側にある場合、Citrix 入力 Controller は LoadBalancer タイプのサービスをサポートします。LoadBalancer タイプのサービスを作成、更新、または削除すると、Citrix 入力 Controller が Citrix ADC に負荷分散仮想サーバーを構成します。

負荷分散仮想サーバーには、次のいずれかの方法で取得される IP アドレス（仮想 IP アドレスまたは VIP）が設定されます。

1. Citrix が提供する IPAMController を使用して、サービスに仮想 IP アドレスを自動的に割り当てます。このソリューションは、Infoblox などの ExternalDNS プロバイダとソリューションを簡単に統合できるように設計されています。詳しくは、「外部 DNS との相互運用性」を参照してください。

2. サービス定義の Spec.LoadBalancerIP フィールドを使用して IP アドレスを指定します。Citrix 入力 Controller は、Spec.LoadBalancerIP フィールドで指定されている IP アドレスを、サービスに対応する負荷分散仮想サーバーの IP アドレスとして使用します。

```
apiVersion: v1
kind: Service
metadata:
    name: hello-world-service
spec:
    type: LoadBalancer
    loadBalancerIP: ""
ports:
- port: 80
    targetPort: 8080
selector:
    run: load-balancer-example
<!--NeedCopy-->
```

より詳細なリファレンスについては、ロードバランサー型のサービスを公開するを参照してください。

Red Hat OpenShift 3.11 検証済みリファレンスデザイン用の **Citrix Cloud** ネイティブネットワーキング

May 18, 2020

Citrix ADC Stack はアプリケーション可用性機能（ADC）、セキュリティ機能の分離（WAF）、アジャイルアプリケ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ーショントポロジ（SSL と GSLB）のスケーリング、および積極的な観察性（サービスグラフ）の高度に調整された Cloud Native Era 環境での基本的な要件を満たします。

デジタルトランスフォーメーションにより、最新のアプリケーション展開をマイクロサービスベースのアーキテクチャに移行する必要性が高まっています。これらのクラウドネイティブアーキテクチャは、アプリケーションコンテナ、マイクロサービス、Kubernetes を活用します。

最新のアプリケーションに対するクラウドネイティブのアプローチは、アジャイルなワークフロー、自動展開ツールセット、開発言語とプラットフォームなどの開発ライフサイクルも変革しました。

最新アプリケーション展開の新時代により、月次および年次ソフトウェアのリリースと契約、サイロコンピューティングリソースと予算、ベンダー消費モデルなど、従来のデータセンターのビジネスモデルの分野も変わりつつあります。

そして、このような近代化はすべてエコシステムで行われていますが、アプリケーション可用性機能（ADC）、セキュリティ機能の分離（WAF）、アジャイルアプリケーショントポロジ（SSL と GSLB）のスケーリング、および積極的な観察性（サービスグラフ）の高度に調整された環境で使用します。

最新のアプリケーション配信に **Citrix** が選ばれる理由

最新のアプリケーション展開に対する Citrix ソフトウェアアプローチでは、組織内の多くのチームでアジャイルなワークフローを組み込む必要があります。アジャイルアプリケーションの開発と配信の利点の 1 つは、CI/CD と呼ばれるフレームワークです。

CI/CD は、最新のアプリケーションのライフサイクルにスピード、安全性、信頼性を提供する手段です。

継続的インテグレーション（CI）は、1 日に数回リアルタイムで更新し、自動ビルドプラットフォームに統合できる共通のコードベースを可能にします。
継続的インテグレーションの 3 つのフェーズは、プッシュ、テスト、修正です。

Continuous Delivery (CD) は、展開パイプラインを CI 開発プロセスに直接統合し、最新のアプリケーション向けのソフトウェア提供モデルを最適化および改善します。

Citrix ADC は、自動カナリア分析のプログレッシブロールアウトを実装することで、継続的デリバリープロセスに結びついています。

すべてのステークホルダーのためのソリューション

Citrix は、最新のアプリケーションを展開する際のクロスファンクショナル要件に対応し、オブザーバビリティスタック、セキュリティフレームワーク、CI/CD インフラストラクチャのさまざまなコンポーネントを統合する、専用のソフトウェアベースのソリューションを開発しました。

最新のアプリケーションを導入するために CI/CD 技術を採用する従来の組織では、CI/CD に関わるすべてのメンバーに共通の配信と可用性フレームワークを提供する必要性を認識していました。これらのリソースは一般に、ビジネスユニット「利害関係者」として定義されています。一方、各ステークホルダーは組織の全体的な成功に投資し、各利害関係者は一般的に明確な要件と違いを持っています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

現代の配信活動における利害関係者の一般的な例としては、次のようなものがあります。

- プラットフォームチーム：IaaS、PaaS、SDN、ADC、WAF などのデータセンターインフラストラクチャの導入
- DevOps とエンジニアリングチーム：統一されたコードリポジトリ、自動化ツール、ソフトウェアアーキテクチャの開発と保守
- SRE（サービス信頼性エンジニアリング）チーム：組織のサイロ、エラー管理、導入の自動化、測定を削減
- セキュリティ運用チーム：プロアクティブなセキュリティポリシー、インシデント管理、パッチの展開、ポートフォリオの強化

Citrix ソフトウェアスタックの説明

シングルコードベース
- オンプレミスデプロイ、パブリッククラウドデプロイ、プライベートクラウドデプロイ、GOV クラウドデプロイ

- プラットフォームの選択-あらゆるアジャイル要件を満たすために、Citrix ADC モデルをお選びください。
  - CPX — Citrix ADC CPX は、コンテナとして提供される Citrix ADC です。
  - VPX — Citrix ADC VPX 製品は、さまざまな仮想化プラットフォームとクラウドプラットフォームでホストできる仮想アプライアンスで、10 Mb/秒から 100 Gb/秒までのパフォーマンスを提供します。
  - MPX — Citrix ADC MPX は、500Mb/秒から 200 Gb/秒までのパフォーマンスを提供するハードウェアベースのアプリケーションデリバリアプライアンスです。
  - SDX — Citrix ADC SDX アプライアンスは、複数の仮想 Citrix ADC マシン（インスタンス）をプロビジョニングおよび管理できるマルチテナントプラットフォームです。
  - BLX — Citrix ADC BLX アプライアンスは、Citrix ADC のソフトウェアフォームファクタです。市販の市販サーバ（COTS）上のベアメタル Linux 上でネイティブに動作するように設計されています。
    コンテナー化された環境-オーバーレイを作成し、Kubernetes Ingress を中心に構築された Citrix ADC を自動的に構成し、
  - Citrix Ingress Controller入力リソースの構成
  - Citrix Node Controller-Kubernetes ノードと入力 Citrix ADC の間に VXLAN ベースのオーバーレイネットワークを作成する
  - Citrix IPAM Controller-Citrix ADC 上の負荷分散仮想サーバーを IP アドレス（仮想 IP アドレスまたは VIP）で自動的に割り当てます。
    プール容量ライセンス — 1 つのグローバルライセンス
  - ユビキタスグローバルライセンスプールプラットフォームとライセンスを分離し、設計とパフォーマンスの完全な柔軟性を実現
    Application Delivery Manger（一元管理機能
  - フリートの管理、ポリシーとアプリケーションの調整、リアルタイムの
    柔軟なトポロジーでの監視とトラブルシューティング-従来のデータセンターまたはモダンクラウド
  - 単一層、2 層、サービスメッシュライト

© 1999–2021 Citrix Systems, Inc. All rights reserved.

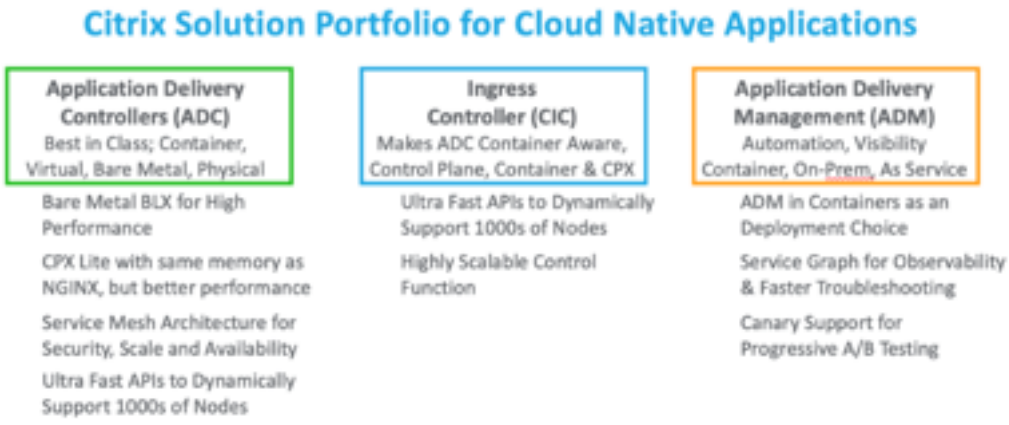
Citrix ADC ADC の価値

- Kubernetes と CNCF オープンソースツールの統合
- Perfect Proxy — 最新アプリケーション向けの定評のある Layer7 アプリケーションデリバリ Controller
  - ポッドまたはサイドカー展開での高性能 ADC コンテナ
  - 複数のオプションを使用した Kubernetes クラスターへの低遅延アクセス
- 豊富な機能を備えた API — セキュリティ機能を制限なく簡単に実装およびオーケストレーション
- CI/CD 用の高度なトラフィックステアリングとカナリア展開
- TLS/SSL、WAF、DoS、API 保護による実証済みのセキュリティ
- 豊富なレイヤー 7 機能
- レガシーおよびモダンアプリケーション展開の統合監視
- 可視化のための実用的なインサイトとサービスグラフ

Citrix ADC ADC のメリット

- レガシーアプリケーションを書き直さずに移動
- 開発者は、Kubernetes API を使用して Citrix ADC ポリシーでアプリケーションを保護できます (CRD を使用 — 開発者向け)。
- North-South およびサービスメッシュ向けの高性能マイクロサービスの展開
- すべてのマイクロサービスに 1 つのアプリケーションサービスグラフを使用
- TCP、UDP、HTTP/S、SSL でのマイクロサービスの問題のトラブルシューティングを高速化
- API を保護し、Kubernetes API を使用して設定する
- カナリア展開での CICD プロセスの強化

アーキテクチャコンポーネント



© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC ADC スイートの利点

Citrix は選択肢です。
従来のデータセンターやコンポーネントを使用する場合でも、新しいクラウドネイティブの最新アプリケーションを立ち上げた場合でも、Citrix ADC は、あらゆるプラットフォーム要件にシームレスに統合します。サブスクリプションベースのクラウドプラットフォームとツール用のクラウドネイティブ ADC 機能を提供し、簡単な IngressController オーケストレーションでオンプレミス Kubernetes クラスターへのトラフィックの転送とオーケストレーションを可能にし、サービスメッシュアーキテクチャをシンプルから複雑なものまで対応します。

Citrix は検証済みです。
検証済みの設計テンプレートとサンプルアプリケーションにより、望ましい状態とビジネス要件を簡単に参照でき、迅速かつ完全に対処できます。DevOps、SecOps、プラットフォームの各チームで参照しやすいように、設定例を文書化して一元的に公開しています。

Citrix はアジャイルでモダンです。
既存の ADC と新しいモジュール（CNC、IPAM など）を使用して、Citrix Cloud ネイティブスタックの新機能を利用するための基盤アーキテクチャを作成します。

Citrix はオープンです。
パートナーエコシステムとの統合についてお客様が理解できるよう支援します。このドキュメントでは、オープンソースの CNCF ツールと Citrix エンタープライズグレード製品の両方を使用しています.

パートナーエコシステム

このトピックでは、さまざまな Kubernetes プラットフォーム、展開トポロジ、機能、および Citrix ADC および Citrix Ingress Controller を含むクラウドネイティブ展開でサポートされる CNI について詳しく説明します。

Citrix Ingress Controller は、次のプラットフォームでサポートされています

- Kubernetes v1.10 をベアメタルで使用するか、AWS、GCP、Azure などのパブリッククラウドでセルフホストします。
- Google Kubernetes Engine (GKE)
- Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Red Hat OpenShift version 3.11 以降
- Pivotal Container Service (PKS)
- Diamanti Enterprise Kubernetes Platform

パートナーエコシステムには、次のものも含まれています。

- Prometheus — 指標、アラート、洞察のための監視ツール
- Grafana — 分析とモニタリングのためのプラットフォーム
- Spinnaker — マルチクラウドの継続的デリバリーとカナリア分析のためのツール
- Elasticsearch — アプリケーションまたはサイト検索サービス
- Kibana — 弾性検索データと弾性スタックナビゲーションツールのための視覚化ツール

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- Fluentd — データ収集ツール

次のセクションでは、OpenShift を使用した設計/アーキテクチャを中心に説明します。

OpenShift の概要

Red Hat OpenShift は Kubernetes プラットフォームで、マイクロサービスとコンテナーを使用してアプリケーションをより迅速に構築およびスケーリングすることに重点を置いています。OpenShift は、コンテナースタックの自動化、インストール、アップグレード、管理によって Kubernetes を合理化し、日々の DevOps タスクを容易にします。

- 開発者は、合理化されたワークフローを介して本番稼働にプッシュされる検証済みのソリューションおよびパートナーへのアクセスをアプリケーションにプロビジョニングします。
- 運用では、Web Console と組み込みのログと監視を使用して、環境を管理および拡張できます。

図 1-6：OpenShift の高レベルアーキテクチャ

OpenShift の利点とコンポーネントには、次のようなものがあります。

- インフラストラクチャの選択
- マスターノードとワーカーノード
- イメージレジストリ
- ルーティングとサービスレイヤ
- 開発者の操作（導入されていますが、このドキュメントの範囲を超えています）

Red Hat OpenShift と Citrix ネイティブスタックを統合するユースケースには、次のようなものがあります。

- レガシーアプリケーションのサポート
- API として展開されたリライト/レスポンダーポリシー
- マイクロサービスのトラブルシューティング
- セキュリティパッチと機能強化による日常的な運用

この文書では、Citrix ADC がルーティング/サービス層の堅牢な統合を提供する方法をカバーしています。

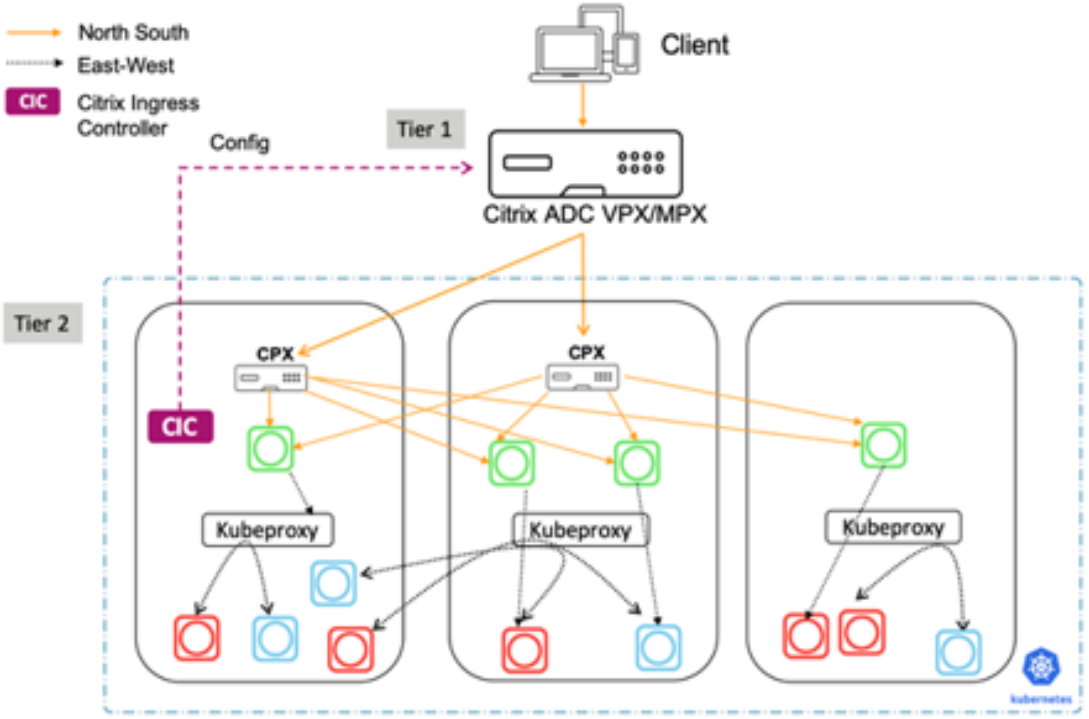
OpenShift プロジェクト

OpenShift で追加された最初の新しい概念は project です。プロジェクトによって制御される名前空間へのアクセスを持つ名前空間を効果的にラップします。アクセスは、ユーザーおよびグループに基づく認証および認可モデルによって制御されます。したがって、OpenShift のプロジェクトは、名前空間間の壁を提供し、ユーザーまたはアプリケーションは、許可されているもののみを表示およびアクセスできるようにします。

OpenShift 名前空間

Kubernetes のグループ化の主要な概念は名前空間です。名前空間は、クラスターリソースを複数の用途に分割する方法でもあります。つまり、Kubernetes の名前空間の間にセキュリティはありません。Kubernetes クラスター内の「ユーザー」であれば、すべての異なる名前空間とそれらで定義されているリソースを見ることができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



OpenShift Software Defined Networking (SDN)

OpenShift Container Platform は、ソフトウェア定義ネットワーキング (SDN) アプローチを使用して、OpenShift Container Platform クラスター全体でポッド間の通信を可能にする統合クラスターネットワークを提供します。このポッドネットワークは OpenShift SDN によって確立され、管理されます。OpenShift SDN は Open vSwitch (OVS) を使用してオーバーレイネットワークを設定します。

OpenShift SDN には、ポッドネットワークを設定するための 3 つの SDN プラグインが用意されています。

- ovs-subnet プラグインは元のプラグインで、すべてのポッドが他のすべてのポッドおよびサービスと通信できる「フラット」ポッドネットワークを提供します。
- ovs-multitenant プラグインは、ポッドとサービスのプロジェクトレベルの分離を提供します。各プロジェクトは、プロジェクトに割り当てられたポッドからトラフィックを識別する一意の仮想ネットワーク ID (VNID) を受け取ります。異なるプロジェクトのポッドは、異なるプロジェクトのポッドおよびサービスとの間でパケットを送信したり、ポッドおよびサービスからパケットを受信したりすることはできません。
- ただし、VNID 0 を受け取るプロジェクトは、他のすべてのポッドとの通信が許可され、その他のすべてのポッドがそれらと通信できるということで、より特権があります。OpenShift Container Platform クラスターでは、デフォルトのプロジェクトには VNID 0 があります。これにより、ロードバランサーなどの特定のサービスがクラスター内の他のすべてのポッドと通信しやすくなり、その逆も同様です。
- ovs-networkpolicy プラグインを使用すると、プロジェクト管理者は NetworkPolicy オブジェクトを使用して独自の分離ポリシーを設定できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

OpenShift ルーティングとプラグイン

OpenShift 管理者は、OpenShift クラスター内でルータの展開ができます。これにより、外部クライアントで使用するために開発者が作成したルートが有効になります。OpenShift のルーティングレイヤーはプラガブルで、デフォルトで 2 つの利用可能なルータープラグインが提供され、サポートされています。

OpenShift ルーターは、識別情報をルーターに直接渡すプロトコルに対して、外部ホスト名マッピングとservicesに対する負荷分散を提供します。ルータがどこに送信するかを決定するためにホスト名は必要です。

ルータプラグインは、ホストポート 80 および 443 にバインドできることを前提としています。これは、外部トラフィックがホストにルーティングされ、その後ルータを経由することを許可するためです。また、ルーターは、クラスター内のすべてのポッドにアクセスできるようにネットワーキングが設定されていることを前提としています。

OpenShiftルーターは、OpenShift インストールでservicesあてに送信されるすべての外部トラフィックの入力ポイントです。OpenShift は、次のルータープラグインを提供およびサポートします。

- HAProxy テンプレートルーターが既定のプラグインです。OpenShift3/ose-haproxy-routerimage を使用して、OpenShift のコンテナ内でテンプレートルータープラグインと共に HAProxy インスタンスを実行します。現在、HTTP (S) トラフィックと SNI 経由の TLS 対応トラフィックをサポートしています。ルーターのコンテナは、プライベート IP でのみリッスンするほとんどのコンテナとは異なり、ホストネットワークインターフェースでリッスンします。ルーターは、ルート名に対する外部要求を、ルートに関連付けられたサービスによって識別される実際のポッドの IP にプロキシします。
- Citrix Ingress Controller OpenShift クラスターにルータープラグインとして展開し、環境に展開された Citrix ADC と統合することができます。Citrix Ingress Controller を使用すると、OpenShift クラスターで Citrix ADC の高度な負荷分散機能とトラフィック管理機能を使用できます。「Citrix Ingress Controller ルータープラグインとして OpenShift クラスターに展開する」を参照してください。

OpenShift ルートと入力メソッド

OpenShift クラスターでは、外部クライアントはポッドが提供するサービスにアクセスする方法が必要です。OpenShift は、クラスターで実行されているサービスと通信するための 2 つのリソースを提供します：ルートおよびIngress。

ルート

OpenShift クラスターでは、ルートは指定されたドメイン名上のサービスを公開するか、ドメイン名をサービスに関連付けます。OpenShift ルーターは、ルートで指定されたルールに従って、OpenShift クラスター内のサービスに外部要求をルーティングします。OpenShift ルーターを使用する場合は、外部 DNS を設定して、トラフィックがルーターに着陸していることを確認する必要があります。

Citrix Ingress Controller OpenShift クラスターにルータープラグインとして展開し、環境に展開された Citrix ADC と統合することができます。Citrix Ingress Controller を使用すると、OpenShift クラスターで Citrix ADC の高度な負荷分散機能とトラフィック管理機能を使用できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

OpenShift ルートは、セキュアまたは非セキュアにできます。セキュアなルートは、ルートの TLS 終端を指定します。

Citrix Ingress Controller は、以下の OpenShift ルートをサポートしています。

- セキュリティで保護されていないルート: セキュリティで保護されていないルートの場合、HTTP トラフィックは暗号化されません。
- エッジ終端: エッジ終端の場合、TLS はルータで終端されます。内部ネットワーク経由でルータからエンドポイントへのトラフィックは暗号化されません。
- パススルー終了: パススルー終了では、ルータは TLS オフロードに関与せず、暗号化されたトラフィックは宛先に直接送信されます。
- 再暗号化の終了: 再暗号化の終了時に、ルーターは TLS 接続を終了しますが、エンドポイントへの別の TLS 接続を確立します。

Citrix ADC の使用方法に基づいて、Citrix Ingress Controller を OpenShift クラスターのルータープラグインとしてデプロイする方法には、クラスター内の Citrix ADC CPX として、またはクラスター外の Citrix ADC MPX/VPX としてデプロイする方法があります。

Citrix ADC CPX を **OpenShift** クラスター内でルーターとして展開する

Citrix IngressController は、同じポッド内の Citrix ADC CPX コンテナーとともにサイドカーとしてデプロイされます。このモードでは、Citrix 入力 Controller が Citrix ADC CPX を構成します。「Citrix ADC CPX を OpenShift クラスター内でルーターとして展開する」を参照してください。

Citrix ADC MPX/VPX を **OpenShift** クラスター外のルーターとして展開する

Citrix Ingress Controller は、スタンドアロンポッドとして展開され、OpenShift クラスターの外部から Citrix ADC MPX または VPX アプライアンスを制御できます。「Citrix ADC MPX/VPX を OpenShift クラスター外のルーターとして展開する」を参照してください。

Ingress

KubernetesIngressは、リクエストのホストまたはパスに基づいてリクエストをサービスにルーティングし、多数のサービスを単一のエントリポイントに集中させる方法を提供します。

Citrix Ingress Controller は Kubernetes 入力を中心に構築され、入力リソースに基づいて 1 つまたは複数の Citrix ADC アプライアンスを自動的に構成します。

入力によるルーティングは、次の方法で行うことができます。

- ホスト名ベースのルーティング
- パスベースのルーティング
- ワイルドカードベースのルーティング
- 完全パス一致

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- 非ホスト名ルーティング
- デフォルトのバックエンド

例と詳細については、Ingress 構成を参照してください。

Citrix Ingress Controller OpenShift ルータープラグインとして展開する

Citrix ADC の使用方法に基づいて、OpenShift クラスターにルータープラグインとして Citrix Ingress Controller を展開する方法は 2 つあります。

- 同じポッド内の Citrix ADC CPX とサイドカーコンテナとして：このモードでは、Citrix Ingress Controller が Citrix ADC CPX を構成します。「Citrix ADC CPX を OpenShift クラスター内でルーターとして展開する」を参照してください。
- OpenShift クラスターのスタンドアロンポッドとして：このモードでは、クラスター外に展開された Citrix ADC MPX または VPX アプライアンスを制御できます。「Citrix ADC MPX/VPX を OpenShift クラスター外のルーターとして展開する」を参照してください。

推奨アーキテクチャ

マイクロサービスアーキテクチャを設計する際には、次のアーキテクチャをお客様に推奨します。

- Citrix Unified Ingress
- Citrix 2-Tier Ingress
- Citrix Service Mesh Lite

図 1-2：アーキテクチャは、比較的単純なものから、より複雑で豊富な機能まで多岐にわたります。

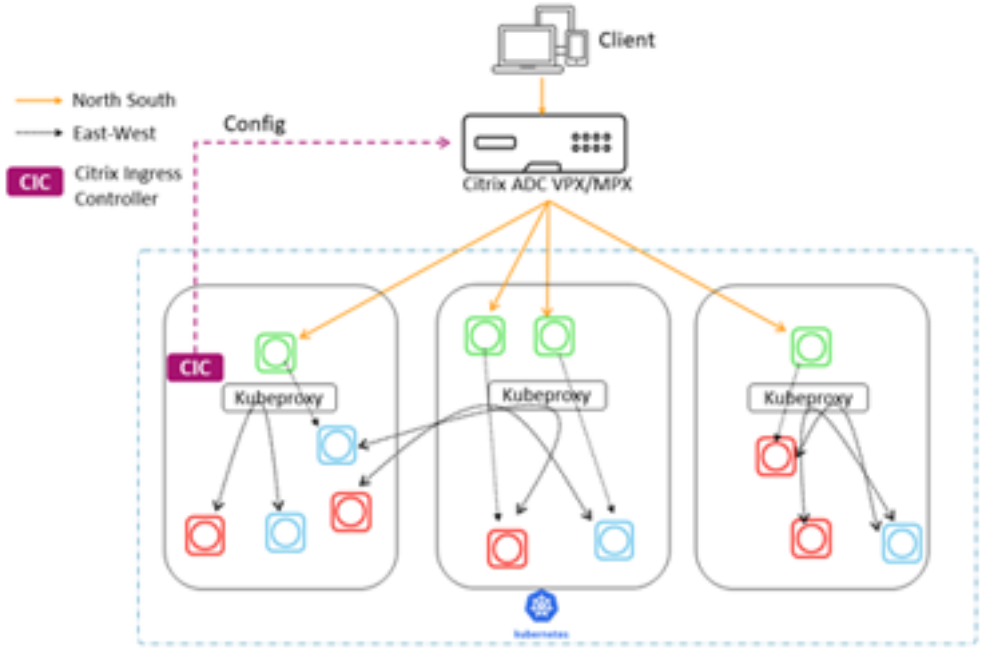
Citrix Unified Ingress

Unified Ingress 展開では、Citrix ADC MPX または VPX デバイスは、クライアントからクラスター内のマイクロサービスとして展開されたエンタープライズグレードのアプリケーションへの North-South トラフィックをプロキシします。Citrix Ingress Controller は、Kubernetes クラスターにポッドまたはサイドカーとして展開され、マイクロサービスまたは Ingress リソースへの変更に基づいて Citrix ADC デバイス（MPX または VPX）の構成を自動化します。

アプリケーションがモノリスである間は、Unified Ingress モデルの実装を開始できます。Citrix ADC をアプリケーションサーバーの前にリバースプロキシとして配置し、後で説明する機能を実装するだけです。その後、アプリケーションをマイクロサービスに変換する良い立場にあります。

マイクロサービス間の通信は、選択したメカニズム（kube-proxy、IPVS など）によって処理されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



さまざまなカテゴリで提供される機能

Unified Ingress アーキテクチャの機能は、3 つのグループに分類されます。

最初のグループの機能は、パフォーマンスを最適化します。

- 負荷分散
- 低遅延の接続
- 高可用性

2 番目のグループの機能は、セキュリティを向上させ、アプリケーション管理を容易にします。

- レート制限
- SSL/LS ターミネーション
- HTTP/2 のサポート
- ヘルスチェック

最後のグループの機能は、マイクロサービスに固有のものです。

- サービスの中央通信ポイント
- API Gateway 機能

概要

Unified Ingress モデルの機能には、サービスに対する堅牢な負荷分散、中央通信ポイント、動的サービス検出、低遅延接続、高可用性、レート制限、SSL/TLS 終了、HTTP/2 などが含まれます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Unified Ingress モデルを使用すると、トラフィックの管理、要求のロードバランシング、バックエンドマイクロサービスアプリケーションの変更への動的応答が容易になります。

次のようなメリットがあります。

- North-South のトラフィックフローはスケーラブルで、観察と監視のために可視であり、Spinnaker や Citrix ADM などのツールによる継続的な配信を提供します。
- 単一の階層により、ネットワークおよびプラットフォームサービスを管理するインフラストラクチャチームを統合し、ホップを短縮して遅延を短縮
- Web App Firewall と SSL オフロードを必要としないが、後で追加できる内部アプリケーションに適しています。

次のような欠点があります。

- kube-proxy では East-West セキュリティはありませんが、L4 セグメンテーションに Calico を追加することができます
- kube-proxy のスケーラビリティが不明です
- kube-proxy は可視性、制御、ログを提供しないため、East-West トラフィックの可視性に制限があり、オープンツールの統合と継続的な配信を緩和します。
- プラットフォームチームはネットワークに精通している必要があります

Citrix 2-Tier Ingress

2-Tier Ingress アーキテクチャモデルは、クラウドネイティブの初心者にとって最適なソリューションです。このモデルでは、Tier 1 の Citrix ADC は着信トラフィックを管理しますが、サービスインスタンスに直接ではなく、開発者が管理する 2 層 ADC にリクエストを送信します。Tier-2 Ingress モデルは、プラットフォームと開発者チームによって記述されたポリシーをインバウンドトラフィックにのみ適用し、クラウドのスケールとマルチテナントを可能にします。

図 1-4：階層 1 の Citrix ADC VPX/MPX および階層 2 の Citrix ADC CPX コンテナを使用した Citrix 2 層入力モデルの図

Tier-1 によって提供される機能

従来のネットワーキングチームによって管理される第 1 層 ADC は、L4 負荷分散、Citrix Web App Firewall、SSL オフロード、およびリバースプロキシサービスを提供します。Tier-1 の Citrix ADC MPX または VPX デバイスは、クライアントから Tier-2 の Citrix ADC CPX へのトラフィック（North-South）をプロキシします。

デフォルトでは、Citrix Ingress Controller は Tier-1 で次の構成をプログラムします。

- ユーザーへのアプリケーションのリバースプロキシ：
- コンテンツスイッチ仮想サーバー
- 仮想サーバ（フロントエンド、ユーザー向け）
- サービスグループ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- SSL オフロード
- NetScaler のログ/デバッグ
- サービスの健全性モニタリング

Tier-2 によって提供される機能

第 1 層 ADC はリバースプロキシサービスを提供しますが、第 2 層 ADC はプラットフォームチームによって管理され、マイクロサービスへの通信ポイントとして機能し、以下を提供します。

- 動的サービス検出
- 負荷分散
- 可視性と豊富な指標

Tier-2 Citrix ADC CPX は、トラフィックを Kubernetes クラスター内のマイクロサービスにルーティングします。スタンドアロンポッドとして展開された Citrix Ingress Controller は、Tier-1 デバイスを構成します。また、1 つ以上の Citrix ADC CPX ポッドのサイドカー Controller は、関連付けられた Citrix ADC CPX を同じポッド内で構成します。

概要

2 層モデルのマイクロサービスのネットワーキングアーキテクチャでは、異なる役割用に構成された 2 つの ADC を使用しています。Tier-1 ADC は、ユーザー側のプロキシサーバーとして機能し、Tier-2 ADC はマイクロサービスのプロキシとして機能します。

異なるタイプの機能を 2 つの異なる階層に分割すると、速度、制御、およびセキュリティを最適化する機会が提供されます。第 2 層では、ロードバランシングは高速、堅牢で、構成可能です。

このモデルでは、ADC の管理者と開発者の間で明確な分離があります。これは、開発者のための BYOL です。

次のようなメリットがあります。

- North-South のトラフィックフローはスケーラブルで、観察と監視のために可視であり、Spinnaker や Citrix ADM などのツールによる継続的な配信を提供します。
- ネットワークチームとプラットフォームチームの学習が制限されたクラウドネイティブの初心者向けのシンプルかつ迅速な展開

次のような欠点があります。

- kube-proxy では East-West セキュリティはありませんが、L4 セグメンテーションに Calico を追加することができます
- kube-proxy のスケーラビリティが不明です
- kube-proxy は可視性、制御、ログを与えず、オープンツールの統合と継続的な配信を緩和するため、East-West トラフィックの可視性に制限があります。

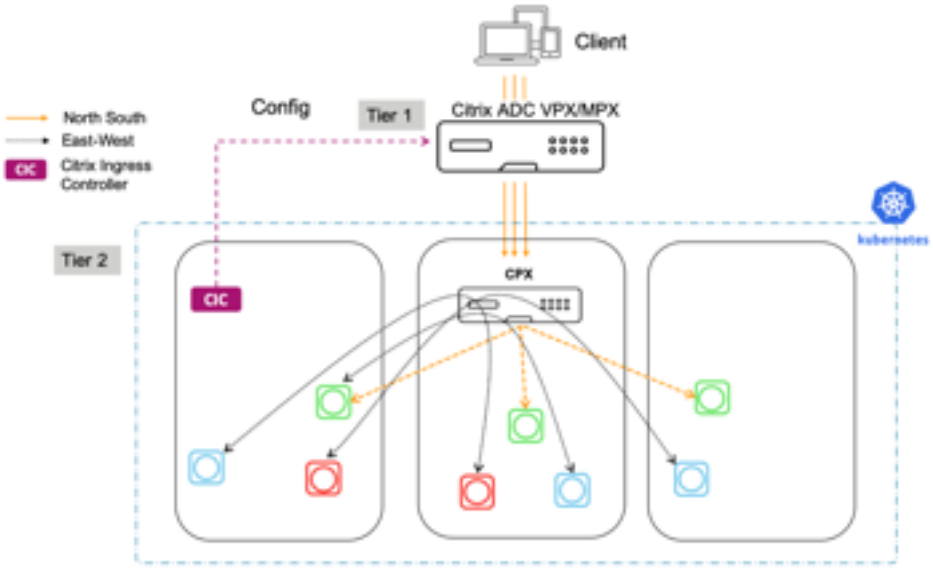
© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Service Mesh Lite

Service Mesh Lite は、3 つのモデルの中で最も豊富な機能です。内部的に安全で、高速、効率的で、耐障害性があり、インバウンドおよびコンテナ間のトラフィックにポリシーを適用するために使用できます。

Service Mesh Lite モデルは、次のようないくつかのユースケースに適しています。

- 医療および金融アプリ — 規制およびユーザー要件では、金融および医療アプリのセキュリティと速度の組み合わせが義務付けられています。財務および評判の価値は数十億ドルにも及んでいます。
- E コマースアプリ — ユーザーの信頼は e コマースにとって大きな問題であり、スピードは競争上の重要な差別化要因です。だから、スピードとセキュリティを組み合わせることが重要です。



概要

次のようなメリットがあります。

- ロードバランサー
  CPX がインバウンドおよびコンテナ間のトラフィックにポリシーを適用し、完全な L7 ポリシーをデプロイする、ネットワークに対するより堅牢なアプローチ
- North-South および East-West トラフィックに対するより高度な観察性、分析、継続的配信、およびセキュリティ
- 組み込み Citrix ADC を搭載した各コンテナのカナリア
- 単一の階層により、ネットワークおよびプラットフォームサービスを管理するインフラストラクチャチームを統合し、ホップを短縮して遅延を短縮

次のような欠点があります。

- 複雑なモデルの展開
- プラットフォームチームはネットワークに精通している必要があります

© 1999–2021 Citrix Systems, Inc. All rights reserved.

アーキテクチャの選択の概要

Citrix Unified Ingress

- **North-South**（**NS**）アプリケーショントラフィック - 1 つの Citrix ADC が、K8s クラスター外の L4 および L7 NS トラフィック、セキュリティ、外部負荷分散を担当します。
- **East-West(EW)** アプリケーショントラフィック - kube-proxy は L4 EW トラフィックを処理します。
- セキュリティ：ADC は、NS トラフィックの保護とユーザーの認証を担当します。kube-proxy は、L4 EW トラフィックを担当しています。
- スケーラビリティとパフォーマンス：NS トラフィックは拡張性に優れ、クラスタリングはオプションです。EW トラフィックと kube-proxy のスケーラビリティは不明です。
- 観測性：ADC は NS トラフィックに対して優れた観測性を提供しますが、EW トラフィックには観測性はありません。

Citrix 2-Tier Ingress

- **North-South**（**NS**）アプリケーショントラフィック - Tier-1 ADC は、SSL オフロード、Web App Firewall、および L4 NS トラフィックを処理します。モノリスと CN の両方のアプリケーションに使用されます。Tier-2 CPX は、k8 および L7 NS トラフィックの迅速な変更を管理します。
- **East-West(EW)** アプリケーショントラフィック - kube-proxy は L4 EW トラフィックを処理します。
- セキュリティ：Tier-1 ADC は、NS トラフィックの保護を担当します。認証は、どちらの ADC でも実行できます。EW トラフィックは、kube-proxy で保護されていません。L4 セグメンテーションのための Calico を追加します。
- スケーラビリティとパフォーマンス：NS トラフィックは拡張性に優れ、クラスタリングはオプションです。EW トラフィックと kube-proxy のスケーラビリティは不明です。
- 観測性：Tier-1 ADC は、NS トラフィックに対して優れた観測性を提供しますが、EW トラフィックに対する観測性はありません。

Citrix Service Mesh Lite

- **North-South**（**NS**）アプリケーショントラフィック - Tier-1 ADC は、SSL オフロード、Web App Firewall、および L4 NS トラフィックを処理します。モノリスと CN の両方のアプリケーションに使用されます。Tier-2 CPX は、k8 および L7 NS トラフィックの迅速な変更を管理します。
- **East-West**（**EW**）アプリケーショントラフィック - Tier-2 CPX またはオープンソースプロキシは、L4 EW トラフィックを処理します。CPX を使用するアプリケーションと、kube-proxy を使用するアプリケーションを選択できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- セキュリティ：Tier-1 ADC は、NS トラフィックの保護を担当します。認証は、どちらの ADC でも実行できます。Citrix CPX は、認証、SSL オフロード、EW トラフィックのセキュリティ保護を担当します。暗号化は、アプリケーションレベルで適用できます。
- 拡張性とパフォーマンス：NS および EW トラフィックは拡張性に優れていますが、インラインホップが 1 つ追加されます。
- 観測性：Tier-1 ADC は、NS トラフィックの優れた観測性を提供します。Tier-2 の CPX は EW トラフィックを監視できますが、無効にして CPX メモリまたは CPU フットプリントを減らすことができます。

展開方法

Citrix Unified Ingress

OpenShift を使用して Citrix Unified Ingress 展開を検証するには、Citrix ADC VPX または MPX でサンプルの「hello-world」アプリケーションを使用します。OpenShift のデフォルトの名前空間「default」がこの展開に使用されます。

1. Citrix ADC インスタンスは、手で構築され、NSIP/SNIP を使用して構成されています。ここで XenServer 上の Citrix ADC のインストールを見つけることができます。
2. 次の YAML ファイルの例を OpenShift ディレクトリにコピーし、application.yaml という名前を付けます。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-world
spec:
  selector:
    matchLabels:
      run: load-balancer-example
  replicas: 2
  template:
    metadata:
      labels:
        run: load-balancer-example
    spec:
      containers:
        -  name: hello-world
          image: gcr.io/google-samples/node-hello:1.0
          ports:
            -  containerPort: 8080
              protocol: TCP
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

3. アプリケーションを展開します。
   ```
   oc apply -f application.yaml
   ```
4. ポッドが実行されていることを確認します。
   ```
   oc get pods
   ```
5. 次の YAML ファイルの例を OpenShift ディレクトリにコピーし、service.yaml という名前を付けます。

```
apiVersion: v1
kind: Service
metadata:
  name: hello-world-service
spec:
  type: NodePort
  ports:
  -  port: 80
    targetPort: 8080
  selector:
    run: load-balancer-example
<!--NeedCopy-->
```

6. サービスを使って NodePort 経由でアプリケーションを公開します。
   ```
   oc apply -f service.yaml
   ```
7. サービスが作成されたことを確認します。
   ```
   oc get service
   ```
8. 次の YAML ファイルの例を OpenShift ディレクトリにコピーし、.yaml という名前を付けます。「ingress.citrix.com/frontend-ip」という注釈を、Citrix ADC の VIP として使用するフリーの IP アドレスに変更する必要があります。

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: hello-world-ingress
  annotations:
   kubernetes.io/ingress.class: "vpx"
   ingress.citrix.com/insecure-termination: "redirect"
   ingress.citrix.com/frontend-ip: "10.217.101.183"
spec:
  rules:
  -  host:  helloworld.com
    http:
      paths:
      -  path:
        backend:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
            serviceName: hello-world-service
            servicePort: 80
<!--NeedCopy-->
```

9. Ingress YAML ファイルを展開します。
   `oc apply -f ingress.yaml`
10. 現在、サービスを使用して公開したアプリケーションポッドがあり、Ingress を使用してトラフィックをルーティングできます。Citrix 入力コントローラをインストールします (CIC) 私たちの層にこれらの構成をプッシュします 1 ADC VPx.CIC を展開する前に, CIC に実行するための正しい権限を与える RBAC ファイルを展開します.

> 注:
>
> rbac yaml ファイルは、名前空間を指定し、それは名前空間が使用されている保留中、変更する必要があります。

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
rules:
  -  apiGroups: [""]
    resources: ["services", "endpoints", "ingresses", "pods", "
       secrets", "nodes", "routes", "routes/status", "tokenreviews
       ", "subjectaccessreviews"]
    verbs: ["\*"]
  -  apiGroups: ["extensions"]
    resources: ["ingresses", "ingresses/status"]
    verbs: ["\*"]
  -  apiGroups: ["citrix.com"]
    resources: ["rewritepolicies"]
    verbs: ["\*"]
  -  apiGroups: ["apps"]
    resources: ["deployments"]
    verbs: ["\*"]

<!--NeedCopy-->
```

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
roleRef:
  apiGroup: rbac.authorization.k8s.io
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
  kind: ClusterRole
  name: cpx
subjects:
-  kind: ServiceAccount
  name: cpx
  namespace: default

<!--NeedCopy-->
```

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cpx
  namespace: default
<!--NeedCopy-->
```

11. RBAC ファイルを配備します。
    `oc apply -f rbac.yaml`

12. CIC を展開する前に、YAML ファイルを編集します。仕様の下で、Tier 1 の ADC の SNIP で管理が有効になっている限り、NSIP または SNIP のいずれかを追加します。引数「ingress-classes」は、Ingress YAML ファイルで指定された入力クラス注釈と同じであることに注意してください。

```
apiVersion: v1
kind: Pod
metadata:
  name: hello-world-cic
  labels:
    app: hello-world-cic
spec:
  serviceAccountName: cpx
  containers:
  -  name: hello-world-cic
    image: "quay.io/citrix/citrix-k8s-ingress-controller:1.1.3"
    env:
     # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has to be
         enabled)
     -  name: "NS_IP"
       value: "10.217.101.193"
     # Set username for Nitro
     # Set log level
     -  name: "NS_ENABLE_MONITORING"
       value: "NO"
     -  name: "NS_USER"
       value: "nsroot"
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
      -  name: "NS_PASSWORD"
         value: "nsroot"
      -  name: "EULA"
         value: "yes"
      -  name: "LOGLEVEL"
         value: "DEBUG"
    args:
      -  --ingress-classes
         vpx
      -  --feature-node-watch
         false
    imagePullPolicy: IfNotPresent
<!--NeedCopy-->
```

13. CIC を展開します。
    `oc apply -f cic.yaml`
14. すべてのポッドが実行されていることを確認します。
    `oc get pods`
15. ローカルマシン上の hosts ファイルを編集します。helloworld.com のエントリと、入力 YAML ファイルで指定された Citrix ADC 上の VIP を使用します。
16. ブラウザーで helloworld.com に移動します。「Hello Kubernetes!」が表示されます。

> 注：以下は、削除コマンドです
>
> - `oc delete pods (pod name)-n (namespace name)`
> - `oc delete deployment (deployment name)-n (namespace name)`
> - `oc delete service (service name)-n (namespace name)`
> - `oc delete ingress (ingress name)-n (namespace name)`
> - `oc delete serviceaccounts (serviceaccounts name)-n (namespace name)`

Citrix 2-Tier Ingress

OpenShift を使用して Citrix 2-Tier Ingress 展開を検証するには、Citrix ADC VPX または MPX でサンプルの「hello-world」アプリケーションを使用します。この展開には、既定の名前空間「tier-2-adc」が使用されます。** 注:Pod、サービス、および Ingress をデプロイする場合、名前空間は「-n (名前空間名)」パラメーターを使用して指定する必要があります。

1. Citrix ADC インスタンスは、手で構築され、NSIP/SNIP を使用して構成されています。XenServer 上の Citrix ADC をインストールすることは見つけることができます [ここ. インスタンスがすでに設定されている場合は、ロードバランシングまたはコンテンツスイッチングで、Unified Ingress として hello-world を展開して ADC にプッシュされた仮想サーバーをすべてクリアします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

2. 「tier-2-adc」という名前の名前空間を作成します。
   `oc create namespace tier-2-adc`

3. 次の YAML ファイルの例を OpenShift ディレクトリにコピーし、`application-2t.yaml`という名前を付けます。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-world
spec:
  selector:
    matchLabels:
      run: load-balancer-example
  replicas: 2
  template:
    metadata:
      labels:
        run: load-balancer-example
    spec:
      containers:
        -  name: hello-world
          image: gcr.io/google-samples/node-hello:1.0
          ports:
            -  containerPort: 8080
              protocol: TCP

<!--NeedCopy-->
```

4. 名前空間にアプリケーションを展開します。
   `oc apply -f application-2t.yaml -n tier-2-adc`

5. ポッドが実行されていることを確認します。
   `oc get pods`

6. 次の YAML ファイルの例を OpenShift ディレクトリにコピーし、`service-2t.yaml`という名前を付けます。

```
apiVersion: v1
kind: Service
metadata:
  name: hello-world-service-2
spec:
  type: NodePort
  ports:

```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
  -port: 80
    targetPort: 8080
  selector:
    run: load-balancer-example

<!--NeedCopy-->
```

7. サービスを使って NodePort 経由でアプリケーションを公開します。
   `oc apply -f service-2t.yaml -n tier-2-adc`
8. サービスが作成されたことを確認します。
   `oc get service -n tier-2-adc`
9. 次の YAML ファイルの例を OpenShift ディレクトリにコピーし、`ingress-2t.yaml`という名前を付けます。

```
    apiVersion: extensions/v1beta1
    kind: Ingress
    metadata:
      name: hello-world-ingress-2
      annotations:
       kubernetes.io/ingress.class: "cpx"
    spec:
      backend:
        serviceName: hello-world-service-2
        servicePort: 80

<!--NeedCopy-->
```

10. Ingress YAML ファイルを展開します。
    `oc apply -f ingress-2t.yaml -n tier-2-adc`
11. CIC および CPX に適切な実行権限を付与する RBAC ファイルを展開します。

> 注:
>
> rbac yaml ファイルは名前空間を指定し、どの名前空間が使用されているかを保留中に変更する必要があります。

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
rules:
  -apiGroups: [""]
    resources: ["services", "endpoints", "ingresses", "pods", "
       secrets", "nodes", "routes", "routes/status", "tokenreviews
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
          ", "subjectaccessreviews"]
    verbs: ["\*"]
  -apiGroups: ["extensions"]
    resources: ["ingresses", "ingresses/status"]
    verbs: ["\*"]
  -apiGroups: ["citrix.com"]
    resources: ["rewritepolicies"]
    verbs: ["\*"]
  -apiGroups: ["apps"]
    resources: ["deployments"]
    verbs: ["\*"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cpx
subjects:
-  kind: ServiceAccount
  name: cpx
  namespace: tier-2-adc
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cpx
  namespace: tier-2-adc
<!--NeedCopy-->
```

12. RBAC ファイルを配備します。
    `oc apply -f rbac-2t.yaml`

13. CPX を作成するには、サービスアカウントに昇格したアクセス許可が必要です。
    `oc adm policy add-scc-to-user privileged system:serviceaccount:tier-2-adc:cpx`

14. CPX YAML ファイルを編集して`cpx-2t.yaml`という名前を付けます。これにより、CPX とそれを公開するサービスが展開されます。Ingress クラスの引数が、`ingress-2t.yaml`ファイル内の注釈と一致していることに注目してください。

```
    apiVersion: extensions/v1beta1
    kind: Deployment
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
3     metadata:
4       name: hello-world-cpx-2
5     spec:
6       replicas: 1
7       template:
8         metadata:
9           name: hello-world-cpx-2
10          labels:
11            app: hello-world-cpx-2
12            app1: exporter
13          annotations:
14            NETSCALER_AS_APP: "True"
15        spec:
16          serviceAccountName: cpx
17          containers:
18            -  name: hello-world-cpx-2
19              image: "quay.io/citrix/citrix-k8s-cpx-ingress
                    :13.0-36.28"
20              securityContext:
21                 privileged: true
22              env:
23              -  name: "EULA"
24              value: "yes"
25              -  name: "KUBERNETES_TASK_ID"
26                value: ""
27              imagePullPolicy: Always
28        # Add cic as a sidecar
29            -  name: cic
30              image: "quay.io/citrix/citrix-k8s-ingress-controller
                    :1.1.3"
31              env:
32              -  name: "EULA"
33                value: "yes"
34              -  name: "NS_IP"
35                value: "127.0.0.1"
36              -  name: "NS_PROTOCOL"
37                value: "HTTP"
38              -  name: "NS_PORT"
39                value: "80"
40              -  name: "NS_DEPLOYMENT_MODE"
41                value: "SIDECAR"
42              -  name: "NS_ENABLE_MONITORING"
43                value: "YES"
44              -  name: POD_NAME
45                valueFrom:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
46                    fieldRef:
47                      apiVersion: v1
48                      fieldPath: metadata.name
49                -  name: POD_NAMESPACE
50                  valueFrom:
51                    fieldRef:
52                      apiVersion: v1
53                      fieldPath: metadata.namespace
54                args:
55                  -  --ingress-classes
56                    cpx
57                imagePullPolicy: Always
58          apiVersion: v1
59          kind: Service
60          metadata:
61            name: lb-service-cpx
62            labels:
63              app: lb-service-cpx
64          spec:
65            type: NodePort
66            ports:
67            -  port: 80
68              protocol: TCP
69              name: http
70              targetPort: 80
71            selector:
72              app: hello-world-cpx-2
73
74  <!--NeedCopy-->
```

15. CPX を展開します。

    ```
    oc apply -f cpx-2t.yaml -n tier-2-adc
    ```

16. ポッドが実行中で、サービスが作成されたことを確認します。

    ```
    oc get pods -n tier-2-adc
    oc get service -n tier-2-adc
    ```

17. VPX から CPX にルーティングする入力を作成します。フロントエンド IP は、ADC 上のフリー IP でなければなりません。ファイルに`ingress-cpx-2t.yaml`という名前を付けます。

    ```
    1  apiVersion: extensions/v1beta1
    2  kind: Ingress
    3  metadata:
    4    name: hello-world-ingress-vpx-2
    5    annotations:
    ```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    kubernetes.io/ingress.class: "helloworld"
    ingress.citrix.com/insecure-termination: "redirect"
    ingress.citrix.com/frontend-ip: "10.217.101.183"
spec:
  rules:
    -  host:  helloworld.com

    http:
      paths:
      -  path:
        backend:
          serviceName: lb-service-cpx
          servicePort: 80
<!--NeedCopy-->
```

18. 入力を展開します。

    ```
    oc apply -f ingress-cpx-2t.yaml -n tier-2-adc
    ```

19. CIC を展開する前に、YAML ファイルを編集します。仕様の下で、Tier 1 の ADC の SNIP で管理が有効になっている限り、NSIP または SNIP のいずれかを追加します。

```
apiVersion: v1
kind: Pod
metadata:
  name: hello-world-cic
  labels:
    app: hello-world-cic
spec:
      serviceAccountName: cpx
      containers:
      -  name: hello-world-cic
        image: "quay.io/citrix/citrix-k8s-ingress-controller:1.1.3
           "
        env:
         # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has
            to be enabled)
         -  name: "NS_IP"
       value: "10.217.101.176"
     # Set username for Nitro
     # Set log level
     -  name: "NS_ENABLE_MONITORING"
       value: "NO"
     -  name: "NS_USER"
       value: "nsroot"
     -  name: "NS_PASSWORD"
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
23          value: "nsroot"
24        -  name: "EULA"
25          value: "yes"
26        -  name: "LOGLEVEL"
27          value: "DEBUG"
28      args:
29        -  --ingress-classes
30          helloworld
31        -  --feature-node-watch
32          false
33      imagePullPolicy: IfNotPresent
34  <!--NeedCopy-->
```

20. CIC を展開します。
    `oc apply -f cic-2t.yaml -n tier-2-adc`
21. すべてのポッドが実行されていることを確認します。
    `oc get pods -n tier-2-adc`
22. ローカルマシン上の hosts ファイルを編集します。helloworld.com のエントリと、VPX から CPX にルーティングする入力 YAML ファイルで指定された Citrix ADC VIP を使用します。
23. ブラウザーで helloworld.com に移動します。「Hello Kubernetes!」が表示されます。

Citrix Service Mesh Lite

Service Mesh Lite は、組み込みの HAProxy 機能の代わりに、CPX（または他の Citrix ADC アプライアンス）を展開することができます。これにより、Kubernetes の N/S 機能を拡張し、E/W トラフィックのロードバランシング、ルーティング、および監視機能も提供することができます。
Citrix ADC（MPX、VPX、または CPX）は、E-W トラフィックに次のような利点があります。

- 相互 TLS または SSL オフロード
- HTTP または HTTPS ヘッダーパラメータに基づいてトラフィックを許可またはブロックするコンテンツベースのルーティング
- 高度なロードバランシングアルゴリズム（最小接続数、最小応答時間など）。
- ゴールデンシグナル（エラー、レイテンシー、飽和、トラフィック量）の測定による東西方向のトラフィックの観測性。Citrix ADM のサービスグラフは、マイクロサービスを監視およびデバッグするための監視ソリューションです。
- この展開シナリオでは、Bookinfo アプリケーションを展開し、デフォルトでどのように機能するかを観察します。次に、デフォルトの Kubernetes サービスをリッピングして置き換え、CPX と VPX を使用して E/W トラフィックをプロキシします。

CPX を使用した Citrix Service Mesh Lite

© 1999–2021 Citrix Systems, Inc. All rights reserved.

OpenShift を使用して Citrix Unified Ingress 展開を検証するには、Citrix ADC VPX または MPX でサンプルの「hello-world」アプリケーションを使用します。OpenShift のデフォルトの名前空間「default」がこの展開に使用されます。

1. Citrix ADC インスタンスは、手で構築され、NSIP/SNIP を使用して構成されています。ここで XenServer 上の Citrix ADC のインストールを見つけることができます。
2. この展開の名前空間を作成します。この例では、`sml` が使用されます。
   `oc create namespace sml`
3. 以下の YAML をコピーして、Bookinfo の展開とサービスを作成します。それに、bookinfo.yaml という名前を付けます。

```
##################################################################################################

# Details service
##################################################################################################

apiVersion: v1
kind: Service
metadata:
  name: details
  labels:
    app: details
    service: details
spec:
  ports:
  -  port: 9080
    name: http
  selector:
    app: details
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: details-v1
  labels:
    app: details
    version: v1
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
      labels:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
32          app: details
33          version: v1
34      spec:
35        containers:
36        -  name: details
37          image: docker.io/maistra/examples-bookinfo-details-v1:0.12.0
38          imagePullPolicy: IfNotPresent
39          ports:
40          -  containerPort: 9080
41  ---
42  ##################################################################################
43  # Ratings service
44  ##################################################################################
45  apiVersion: v1
46  kind: Service
47  metadata:
48    name: ratings
49    labels:
50      app: ratings
51      service: ratings
52  spec:
53    ports:
54    -  port: 9080
55      name: http
56    selector:
57      app: ratings
58  ---
59  apiVersion: extensions/v1beta1
60  kind: Deployment
61  metadata:
62    name: ratings-v1
63    labels:
64      app: ratings
65      version: v1
66  spec:
67    replicas: 1
68    template:
69      metadata:
70        annotations:
71          sidecar.istio.io/inject: "false"
72        labels:
73          app: ratings
74          version: v1
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
75      spec:
76        containers:
77        -  name: ratings
78          image: docker.io/maistra/examples-bookinfo-ratings-v1:0.12.0
79          imagePullPolicy: IfNotPresent
80          ports:
81          -  containerPort: 9080
82  ---
83  ##################################################################################
84  # Reviews service
85  ##################################################################################
86  apiVersion: v1
87  kind: Service
88  metadata:
89    name: reviews
90    labels:
91      app: reviews
92      service: reviews
93  spec:
94    ports:
95    -  port: 9080
96      name: http
97    selector:
98      app: reviews
99  ---
100 apiVersion: extensions/v1beta1
101 kind: Deployment
102 metadata:
103   name: reviews-v1
104   labels:
105     app: reviews
106     version: v1
107 spec:
108   replicas: 1
109   template:
110     metadata:
111       annotations:
112         sidecar.istio.io/inject: "false"
113       labels:
114         app: reviews
115         version: v1
116     spec:
117       containers:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
118         -  name: reviews
119           image: docker.io/maistra/examples-bookinfo-reviews-v1:0.12.0
120           imagePullPolicy: IfNotPresent
121           ports:
122           -  containerPort: 9080
123   ---
124     apiVersion: extensions/v1beta1
125     kind: Deployment
126     metadata:
127       name: reviews-v2
128       labels:
129         app: reviews
130         version: v2
131     spec:
132       replicas: 1
133       template:
134         metadata:
135           annotations:
136             sidecar.istio.io/inject: "false"
137           labels:
138             app: reviews
139             version: v2
140         spec:
141           containers:
142           -  name: reviews
143             image: docker.io/maistra/examples-bookinfo-reviews-v2
                  :0.12.0
144             imagePullPolicy: IfNotPresent
145             ports:
146             -  containerPort: 9080
147   ---
148     apiVersion: extensions/v1beta1
149     kind: Deployment
150     metadata:
151       name: reviews-v3
152       labels:
153         app: reviews
154         version: v3
155     spec:
156       replicas: 1
157       template:
158         metadata:
159           annotations:
160             sidecar.istio.io/inject: "false"
161           labels:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
162             app: reviews
163             version: v3
164         spec:
165           containers:
166           -  name: reviews
167             image: docker.io/maistra/examples-bookinfo-reviews-v3
                   :0.12.0
168             imagePullPolicy: IfNotPresent
169             ports:
170             -  containerPort: 9080
171     ---
172     ##################################################################################
173     # Productpage services
174     ##################################################################################
175     apiVersion: v1
176     kind: Service
177     metadata:
178       name: productpage-service
179     spec:
180       type: NodePort
181       ports:
182       -  port: 80
183         targetPort: 9080
184       selector:
185         app: productpage
186     ---
187     apiVersion: extensions/v1beta1
188     kind: Deployment
189     metadata:
190       name: productpage-v1
191       labels:
192         app: productpage
193         version: v1
194     spec:
195       replicas: 1
196       template:
197         metadata:
198           annotations:
199             sidecar.istio.io/inject: "false"
200           labels:
201             app: productpage
202             version: v1
203         spec:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
204             containers:
205             -  name: productpage
206               image: docker.io/maistra/examples-bookinfo-productpage-v1
                     :0.12.0
207               imagePullPolicy: IfNotPresent
208               ports:
209               -  containerPort: 9080
210       ---
211   <!--NeedCopy-->
```

1. sml 名前空間に bookinfo.yaml を展開します。
   `oc apply -f bookinfo.yaml -n sml`
2. 製品ページサービスにマップされる Ingress ファイルをコピーして展開します。このファイルには`ingress-productpage.yaml`という名前を付けることができます。フロントエンド IP は、Citrix ADC VPX/MPX 上の無料の VIP である必要があります。

```
1  apiVersion: extensions/v1beta1
2  kind: Ingress
3  metadata:
4    name: productpage-ingress
5    annotations:
6     kubernetes.io/ingress.class: "bookinfo"
7     ingress.citrix.com/insecure-termination: "redirect"
8     ingress.citrix.com/frontend-ip: "10.217.101.182"
9  spec:
10   rules:
11   -  host: bookinfo.com
12     http:
13       paths:
14       -  path:
15         backend:
16           serviceName: productpage-service
17           servicePort: 80
18 <!--NeedCopy-->
```

`oc apply -f ingress-productpage.yaml -n sml`

1. sml 名前空間の RBAC ファイルの次の YAML をコピーし、展開します。製品ページのマイクロサービスの前で、CIC に使用されるファイルの名前を`rbac-cic-pp.yaml`に指定します。

```
1  kind: ClusterRole
2  apiVersion: rbac.authorization.k8s.io/v1beta1
3  metadata:
4    name: cpx
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
rules:
  -  apiGroups: [""]
    resources: ["services", "endpoints", "ingresses", "pods", "
       secrets", "routes", "routes/status", "nodes", "namespaces"]
    verbs: ["\*"]
  -  apiGroups: ["extensions"]
    resources: ["ingresses", "ingresses/status"]
    verbs: ["\*"]
  -  apiGroups: ["citrix.com"]
    resources: ["rewritepolicies", "vips"]
    verbs: ["\*"]
  -  apiGroups: ["apps"]
    resources: ["deployments"]
    verbs: ["\*"]
  -  apiGroups: ["apiextensions.k8s.io"]
    resources: ["customresourcedefinitions"]
    verbs: ["get", "list", "watch"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cpx
subjects:
-  kind: ServiceAccount
  name: cpx
  namespace: sml
apiVersion: rbac.authorization.k8s.io/v1
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cpx
  namespace: sml
<!--NeedCopy-->
```

```
oc apply -f rbac-cic-pp.yaml -n sml
```

1. サービスアカウント権限を昇格して、CIC および CPX を展開します。
   `oc adm policy add-scc-to-user privileged system:serviceaccount:sml:cpx`
2. `ingress-productpage.yaml`で指定されているフロントエンド IP に bookinfo.com がマッピングさ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

れているローカルマシンの hosts ファイルを編集します。

3. CIC を使用して製品ページをコピーして展開します。ファイルにcic-productpage.yamlという名前を付けます。NS_IP は、Tier-1 の ADC の NS_IP である必要があります。

```
apiVersion: v1
kind: Pod
metadata:
  name: productpage-cic
  labels:
    app: productpage-cic
spec:
      serviceAccountName: cpx
      containers:
      -  name: productpage-cic
        image: "quay.io/citrix/citrix-k8s-ingress-controller:1.1.3
           "
        env:
         # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has
            to be enabled)
         -  name: "NS_IP"
           value: "10.217.101.176"
         # Set username for Nitro
         # Set log level
         -  name: "NS_ENABLE_MONITORING"
           value: "NO"
         -  name: "NS_USER"
           value: "nsroot"
         -  name: "NS_PASSWORD"
           value: "nsroot"
         -  name: "EULA"
           value: "yes"
         -  name: "LOGLEVEL"
           value: "DEBUG"
         -  name: "NS_APPS_NAME_PREFIX"
           value: "BI-"
        args:
          -  --ingress-classes
            bookinfo
          -  --feature-node-watch
            false
        imagePullPolicy: IfNotPresent
<!--NeedCopy-->
```

```
oc apply -f cic-productpage.yaml -n sml
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

1. bookinfo.com に移動し、通常のユーザーをクリックします。製品ページには、その他のマイクロサービスである詳細、レビュー、評価が表示されます。HAProxy は、マイクロサービス（East-West）間のトラフィックをルーティングする責任があります。

2. 詳細の前にサービスを削除します。Bookinfo Web ページを更新し、製品ページで詳細情報についてマイクロサービスをプルできなかったことに注目してください。

   ```
   oc delete service details -n sml
   ```

3. 製品ページから詳細へのトラフィックが CPX を通過するように、ヘッドレスサービスをコピーして展開します。このファイルに detailsheadless.yaml という名前を付けます。

   ```
   apiVersion: v1
   kind: Service
   metadata:
     name: details
   spec:
     ports:
     -  port: 9080
       name: http
     selector:
       app: cpx
   <!--NeedCopy-->
   ```

```
oc apply -f detailsheadless.yaml -n sml
```

1. detailsservice.yaml という名前の新しい詳細サービスをコピーして展開し詳細マイクロサービスの前に配置します。

   ```
   apiVersion: v1
   kind: Service
   metadata:
     name: details-service
     labels:
       app: details-service
       service: details-service
   spec:
     clusterIP: None
     ports:
     -  port: 9080
       name: http
     selector:
       app: details
   <!--NeedCopy-->
   ```

```
oc apply -f detailsservice.yaml -n sml
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

1. 詳細サービスを入力とともに公開し、展開します。detailsingress.yaml という名前を付けます。

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: details-ingress
  annotations:
   kubernetes.io/ingress.class: "cpx"
   ingress.citrix.com/insecure-port: "9080"
spec:
  rules:
  -  host: details
    http:
      paths:
      -  path:
        backend:
          serviceName: details-service
          servicePort: 9080
<!--NeedCopy-->
```

```
oc apply -f detailsingress.yaml -n sml
```

1. CPXEastWest.yaml ファイルをコピーして展開します。

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: cpx
  labels:
    app: cpx
    service: cpx
spec:
  replicas: 1
  template:
    metadata:
      name: cpx
      labels:
        app: cpx
        service: cpx
      annotations:
        NETSCALER_AS_APP: "True"
    spec:
      serviceAccountName: cpx
      containers:
        -  name: reviews-cpx
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-36.28
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
                "
23            securityContext:
24               privileged: true
25            env:
26            -  name: "EULA"
27              value: "yes"
28            -  name: "KUBERNETES_TASK_ID"
29              value: ""
30            -  name: "MGMT_HTTP_PORT"
31              value: "9081"
32            ports:
33            -  name: http
34              containerPort: 9080
35            -  name: https
36              containerPort: 443
37            -  name: nitro-http
38              containerPort: 9081
39            -  name: nitro-https
40              containerPort: 9443
41            imagePullPolicy: Always
42          # Add cic as a sidecar
43          -  name: cic
44            image: "quay.io/citrix/citrix-k8s-ingress-controller
                 :1.2.0"
45            env:
46            -  name: "EULA"
47              value: "yes"
48            -  name: "NS_IP"
49              value: "127.0.0.1"
50            -  name: "NS_PROTOCOL"
51              value: "HTTP"
52            -  name: "NS_PORT"
53              value: "80"
54            -  name: "NS_DEPLOYMENT_MODE"
55              value: "SIDECAR"
56            -  name: "NS_ENABLE_MONITORING"
57              value: "YES"
58            -  name: POD_NAME
59              valueFrom:
60                fieldRef:
61                  apiVersion: v1
62                  fieldPath: metadata.name
63            -  name: POD_NAMESPACE
64              valueFrom:
65                fieldRef:
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
                apiVersion: v1
                fieldPath: metadata.namespace
          args:
            -  --ingress-classes
               cpx
          imagePullPolicy: Always
<!--NeedCopy-->
```

```
oc apply -f CPXEastWest.yaml -n sml
```

1. bookinfo.com を更新し、詳細マイクロサービスから詳細をプルする必要があります。CPX はプロキシ EW トラフィックに正常に展開されました。

VPX/MPX を使用した Citrix Service Mesh Lite

1. 次のコマンドを実行して、EW プロキシとして使用されている CPX を削除します。新しいファイルが展開され、製品ページと詳細マイクロサービス間の EW プロキシとして VPX を構成します。

   ```
   oc delete -f detailsheadless.yaml -n sml
   oc delete -f detailsservice.yaml -n sml
   oc delete -f detailsingress.yaml -n sml
   oc delete -f CPXEastWest.yaml -n sml
   ```

2. サービスをコピーして展開し、detailstoVPX.yaml という名前を付けて、製品ページから VPX にトラフィックを送信します。IP パラメーターは、Citrix ADC VPX/MPX 上の無料の VIP である必要があります。

```
---
kind: "Service"
apiVersion: "v1"
metadata:
  name: "details"
spec:
  ports:
    -
      name: "details"
      protocol: "TCP"
      port: 9080
---
kind: "Endpoints"
apiVersion: "v1"
metadata:
  name: "details"
subsets:
  -
    addresses:
      -
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
          ip: "10.217.101.182" # Ingress IP in MPX
      ports:
        -
          port: 9080
          name: "details"
<!--NeedCopy-->
```

```
oc apply -f detailstoVPX.yaml -n sml
```

1. 詳細マイクロサービスの前に detailsservice.yaml を再展開します。
   ```
   oc apply -f detailsservice.yaml -n sml
   ```
2. Ingress をコピーして展開し、詳細マイクロサービスを VPX に公開します。これは`detailsVPXingress.yaml`という名前です。フロントエンド IP は、Tier 1 の ADC 上の VIP と一致する必要があります。

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: details-ingress
  annotations:
   kubernetes.io/ingress.class: "vpx"
   ingress.citrix.com/insecure-port: "9080"
   ingress.citrix.com/frontend-ip: "10.217.101.182"
spec:
  rules:
  -  host: details
    http:
      paths:
      -  path:
        backend:
          serviceName: details-service
          servicePort: 9080
<!--NeedCopy-->
```

```
oc apply -f detailsVPXingress.yaml
```

1. bookinfo.com を更新し、詳細は、詳細マイクロサービスから引き出す必要があります。VPX はプロキシ EW トラフィックに正常に展開されました。

Openshift でルートまたは入力クラスを使用した **Citrix ADC** へのサービス移行

ルートシャーディングによるサービスの移行

Citrix Ingress Controller（CIC）はルーターとして機能し、トラフィックをさまざまなポッドにリダイレクトして、使用可能なさまざまなポッド間で着信トラフィックを分散します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

この移行プロセスは、従来の Openshift トポロジーから Citrix CNC、CIC、CPX コンポーネントを使用した自動展開へのクラスターアップグレードプロセスの一部でもあります。

このソリューションは、次の 2 つの方法で実現できます。

- プラグインによる CIC ルーター (Pod)
- OpenShift 内 CPX ルーター（サイドカー）

どちらの方法も、移行例とともに以下で説明します。

静的ルート（デフォルト）-静的ルートを介して Openshift HostSubnet を外部 ADC にマッピングします。

静的ルートは、HAProxy を使用するレガシー Openshift の展開では一般的です。静的ルートは、あるサービスプロキシから別のサービスプロキシにサービスを移行する場合に、機能しているクラスターに展開された名前空間を中断することなく、Citrix CNC、CIC、および CPX と並行して使用することができます。

Citrix ADC 静的ルート構成例:

```
1 oc ホストサブネット (Openshift クラスター) スニペットの取得
2 oc311-master.example.com 10.x.x.x 10.128.0.0/23
3 oc311-node1.example.com 10.x.x.x 10.130.0.0/23
4 oc311-node2.example.com 10.x.x.x 10.129.0.0/23
5
6 ルート（外部Citrix VPX）スニペットを表示する
7 10.128.0.0 255.255.254.0 10.x.x.x 静的
8 10.129.0.0 255.255.254.0 10.x.x.x 静的
9 10.130.0.0 255.255.254.0 10.x.x.x 静的
```

自動ルート -CNC（Citrix ノードコントローラ）を使用して、定義されたルートシャードへの外部ルートを自動化します。

Citrix ADC を OpenShift と統合するには、2 つの方法があります。どちらの方法も OpenShift ルーターのシャーディングをサポートします。

ルートタイプ

- 非セキュア-CIC ルータへの外部ロードバランサ、HTTP トラフィックは暗号化されません。
- セキュアエッジ-TLS を終了する CIC ルータへの外部ロードバランサ。
- セキュアパススルー-TLS を終了する宛先への外部ロードバランサー
- セキュアな再暗号化-TLS を終了する CIC ルータへの外部ロードバランサ。TLS で宛先に対して暗号化する CIC ルータ。

デプロイの例 **#1: OpenShift** ルータープラグインとしてデプロイされた **CIC**

ルートについては、ルートシャーディングの概念を使用します。ここで、CIC はルーターとして機能し、トラフィックをさまざまな Pod にリダイレクトして、さまざまな利用可能な Pod 間で着信トラフィックを分散します。CIC は、

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC MPX または VPX のルータープラグインとしてインストールされ、クラスターの外部に展開されます。

Citrix コンポーネント:

- VPX-DNS にクラスターサービスを提示する入力 ADC。
- CIC-CNC ルートを介して外部 Citrix ADC にルートラベルと名前空間のラベルを提供します。

ルートシャードの **YAML** ファイルパラメータの例**:**

Citrix の Openshift ソースファイルは、ここ Github にあります

1. 次の環境変数 ROUTE_LABELS と NAMESPACE_LABELS を kubernetes ラベル形式で追加します。CIC の NAMESPACE_LABELS のルートシャーディング式は、オプションのフィールドです。使用する場合は、route.yaml ファイルに記載されている名前空間ラベルと一致する必要があります。

```
        env:
         - name: "ROUTE_LABELS"
           value: "name=apache-web"
         - name: "NAMESPACE_LABELS"
           value: "app=hellogalaxy"

<!--NeedCopy-->
```

1. route.yaml を介して作成されたルートには、CIC 内のルートシャーディング式と一致するラベルが設定されます。

```
        metadata:
            name: apache-route
            namespace: hellogalaxy
            labels:
                name: apache-web
<!--NeedCopy-->
```

1. service.yaml でサービスを公開します。

```
        metadata:
            name: apache-service
        spec:
        type: NodePort
        #type=LoadBalancer
        ports:
            - port: 80
        targetPort: 80
        selector:
            app: apache
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

1. service.yaml 内のセレクタラベルと一致する単純な Web アプリケーションをデプロイします。

デプロイの例 **#2: OpenShift** ルーターとしてデプロイされた **Citrix ADC CPX**

Citrix ADC CPX は、クラスター内の Citrix Ingress Controller とともに、OpenShift ルーターとして展開できます。クラスター内のルーターとして CPX または CIC を展開する手順については、Citrix ADC で OpenShift ルーティングシャーディングサポートを有効にするを参照してください。

Citrix コンポーネント:

- VPX-DNS にクラスターサービスを提示する入力 ADC。
- CIC-ルートシャードを定義するために、外部 Citrix ADC にルートラベルとネームスペースラベルを提供します。
- CNC-シャードの自動ルート設定を外部ロードバランサーに提供します。
- CPX-Openshift クラスター内で Openshift ルーティングを提供します。

入力クラスアノテーションを使用したサービス移行

入力クラスアノテーションは、入力クラスアノテーションの概念を使用して、入力クラス情報を持つ入力にアノテーションを追加します。これは、外部 ADC から特定の POD/ノードにトラフィックをリダイレクトするのに役立ちます。

入力クラスの **YAML** ファイルパラメータの例**:****

Citrix Ingress のソースファイルは、ここにある Github にあります

```
    env:
        args:
          - --ingress-classes
            vpx
<!--NeedCopy-->
```

入力設定ファイルには、メタデータ内に kubernetes.io/ingress.class アノテーションフィールドも必要です。このフィールドは、作成時に CIC 入力クラス args フィールドと照合されます。

「**ingress.classes**」の例を含む入力 **VPX** 展開の例 **

```
        kind: Ingress
            metadata:
                name: ingress-vpx
                annotations:
                    kubernetes.io/ingress.class: "vpx"
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix メトリックスエクスポータ

Citrix ADC メトリックスエクスポーターと Prometheus-Operator を使用して、Citrix ADC VPX または CPX 入力デバイスおよび Citrix ADC CPX（East-West）デバイスを監視できます。「Prometheus と Grafana を使用した Citrix ADC のメトリックの表示」を参照してください。

Citrix ADC ADC および Microsoft Azure 検証済みリファレンスデザイン

May 18, 2020

Citrix ADC on Microsoft Azure は、組織がクラウドに展開された安全で最適化されたアプリケーションや資産にアクセスできるようにし、変化する環境のニーズに合わせて調整するネットワーク基盤を確立するための柔軟性を提供します。この検証済みの設計は、Azure でフロントエンド自動スケールを構成し、信頼性とコスト効率に優れた方法でアプリケーションを提供する方法を組織にガイドします。

概要：Citrix ADC VPX

Citrix ADC は、内部および外部の Web アプリケーションのパフォーマンスを加速するオールインワンのアプリケーション配信 Controller です。アプライアンスは、アプリケーション所有コストを削減し、ユーザーエクスペリエンスを最適化し、次の機能を使用してアプリケーションを常に使用できるようにします。

- 高度な Layer4-7 ロードバランシングとトラフィック管理
- 実証済みのアプリケーションアクセラレーション（HTTP 圧縮やキャッシュなど）
- アプリケーションセキュリティのための統合されたアプリケーションファイアウォール
- サーバのオフロードにより、コストを大幅に削減し、サーバーを統合

Citrix ADC は、サービスとアプリケーションデリバリのリーダーとして、世界中の何千ものネットワークに展開されています。Citrix ADC は、エンタープライズおよびクラウドサービスの提供を最適化、セキュリティ保護、制御するために活用されています。アプライアンスは、Web サーバーとデータベースサーバーの前に直接展開されます。Citrix ADC は、高速負荷分散とコンテンツスイッチ、HTTP 圧縮、コンテンツキャッシュ、SSL アクセラレーション、アプリケーションフローの可視性、強力なアプリケーションファイアウォールを組み合わせて、使いやすい統合プラットフォームにします。ネットワークデータを実用的なビジネスインテリジェンスに変換するエンドツーエンドの監視によって SLA を満たす方がはるかに簡単です。Citrix ADC では、プログラミングの専門知識を必要とせずに、シンプルな宣言型ポリシーエンジンを使用してポリシーを定義および管理できます。

Microsoft Azure での Citrix ADC 概要

Citrix ADC VPX 仮想アプライアンスは、Microsoft Azure Marketplace でイメージとして使用することができます。Microsoft Azure Resource Manager（ARM）上の Citrix ADC VPX を使用すると、Azure クラウドコンピューティング機能を使用し、Citrix ADC 負荷分散機能とトラフィック管理機能をビジネスニーズに適用できます。Citrix

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ADC VPX インスタンスは、スタンドアロンインスタンスとして、またはアクティブ/アクティブ/スタンバイモードの高可用性ペアとして、ARM 上に展開できます。

制限事項と使用上のガイドライン

- Azure アーキテクチャは、次の機能のサポートに対応していません。
  - クラスタリング
  - IPv6
  - グラチュイタス ARP（GARP）
  - L2 モード
  - タグ付き VLAN
  - 動的ルーティング
  - 仮想 MAC（仮想 MAC）
  - USIP
  - CloudBridge Connector
- Azure にはこの機能に必要な IP アドレスのプールが用意されていないため、イントラネット IP（IIP）機能はサポートされません。IIP は、VOIP、SIP、またはサーバーによって開始される接続の展開で頻繁に使用されます。
- Citrix ADC VPX 仮想マシンをシャットダウンして一時的に割り当て解除しなければならないことが予想される場合は、仮想マシンの作成中に静的な内部 IP アドレスを割り当てます。静的内部 IP アドレスを割り当てないと、Azure が再起動のたびに異なる IP アドレスを仮想マシンに割り当てる可能性があり、仮想マシンにアクセスできなくなる場合があります。
- Azure 展開では、以下の Citrix ADC VPX モデルのみがサポートされます：VPX 10、VPX 200、および VPX 1000 です。これらの仮想アプライアンスは、コアが 2 つ以上あり、2GB 超のメモリを持つインスタンスであればどの種類にも展開できます。「Citrix ADC VPX のデータシート」を参照してください。
- Azure が仮想マシンのプロビジョニング中に生成する 展開 **ID** は、ARM ではユーザーには表示されません。展開 ID を使用して Citrix ADC VPX アプライアンスを ARM に展開することはできません。

使用例

各サービスを個別の仮想アプライアンスとして展開する必要がある代替ソリューションと比較して、Citrix ADC on Azure は、1 つの VPX インスタンスに不可欠なアプリケーション配信機能を組み合わせています。これには、L4 負荷分散、L7 トラフィック管理、サーバーオフロード、アプリケーションアクセラレーション、アプリケーションセキュリティ、および Azure Marketplace 経由で便利なその他のサービスが含まれます。さらに、単一のポリシーフレームワークがすべてを統括します。Citrix ADC は、オンプレミスの Citrix ADC 展開を管理するのと同じ強力なツールセットで管理されます。その結果、Azure の Citrix ADC では、いくつかの説得力のあるユースケースが有効になります。Citrix ADC は、今日の企業の緊迫したニーズだけでなく、レガシーコンピューティングインフラストラクチャからエンタープライズクラウドデータセンターへの継続的な進化をサポートします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

プロダクションデリバリー

多くの企業では、Azure をサービスとしてのインフラストラクチャ (IaaS) 製品として積極的に採用しています。現在、企業は、世界最大のウェブサイトやクラウドサービスプロバイダーが使用しているのと同じクラウドネットワーキングプラットフォームを使用して、これらのアプリケーションをフロントエンドできます。広範なオフロード、アクセラレーション、セキュリティ機能を活用して、パフォーマンスを向上させ、コストを削減できます。

ハイブリッドクラウド設計

Citrix ADC on Azure を使用すると、エンタープライズデータセンターにまたがり、Azure に拡張されるハイブリッドクラウドは、同じ Citrix ADC クラウドネットワーキングプラットフォームの恩恵を受けることができます。これにより、プライベートデータセンターと Azure 間のアプリケーションとワークロードの移行が大幅に容易になります。Citrix ADC on Azure では、データストリームによるインテリジェントなデータベース負荷分散から、AppFlow® による前例のないアプリケーションの可視化、およびアクション分析によるリアルタイム監視と応答に至るまで、Citrix ADC の全機能を利用できます。

ビジネス継続性

災害復旧およびビジネス継続性計画の一環として Azure を使用することを検討している企業は、オンプレミスと Azure の両方で実行されている Citrix ADC グローバルサーバーの負荷分散を利用して、エンタープライズデータセンターと Azure 環境の両方の可用性とパフォーマンスを継続的に監視し、ユーザーは常に最適な場所に送信されます。

開発とテスト

本番配信をオンプレミスで実行しているが、開発とテストに Azure を使用している企業は、Azure テスト環境に Citrix ADC を含めることができるようになりました。これにより、テスト環境内での本番実装の模倣性が向上するため、本番稼働までの時間が短縮されます。各ユースケースにおいて、ネットワークアーキテクトは、スタンドアロンインスタンスまたは Citrix ADC プラチナエディションインスタンスの機能として構成された Citrix CloudBridge を活用して、エンタープライズデータセンターと Azure クラウド間の接続を安全かつ最適化し、データ転送速度を向上させ、同期とネットワークコストの最小化

ネットワークアーキテクチャ

ARM では、Citrix ADC VPX 仮想マシン（VM）が仮想ネットワーク内に存在します。デフォルトでは、Azure でプロビジョニングされた Citrix ADC VPX は、次のセクションで説明するシングル IP モードで動作します。

各 Citrix ADC 仮想マシンに仮想 NIC が作成されます。仮想ネットワークで構成されたネットワークセキュリティグループは、NIC にバインドされます。これらのトラフィックは、仮想マシンに流入するトラフィックと VM から流出するトラフィックを制御します。

ネットワークセキュリティグループは Citrix ADC VPX インスタンスに要求を転送し、VPX インスタンスはそれらをサーバーに送信します。サーバーからの応答は同じパスを逆にたどります。ネットワークセキュリティグループを構

© 1999–2021 Citrix Systems, Inc. All rights reserved.

成して、単一の VPX VM を制御するか、サブネットと仮想ネットワークを使用して複数の VPX VM 展開でトラフィックを制御できます。

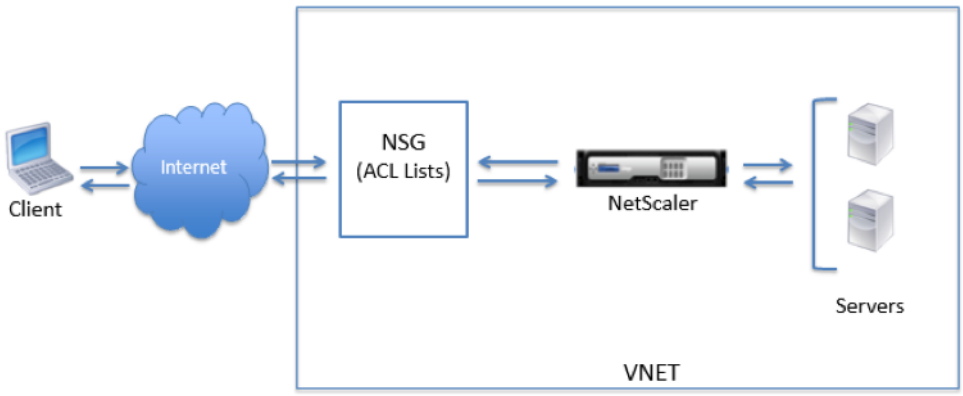
NIC には、ネットワーク構成の詳細（仮想ネットワーク、サブネット、内部 IP アドレス、パブリック IP アドレスなど）が含まれます。

ARM 上では、VM にアクセスするために使用される次の IP アドレスを理解しておくと便利です。

- パブリック IP（PIP）アドレスは、Citrix ADC VM の仮想 NIC 上で直接構成されるインターネット側 IP アドレスです。PIP を使用すると、ネットワークセキュリティグループのインバウンドルールとアウトバウンドルールを設定しなくても、外部ネットワークから VM に直接アクセスできます。
- Citrix ADC IP（NSIP）アドレスは、仮想マシン上で構成された内部 IP アドレスです。これはルーティング不可能です。
- 仮想 IP アドレス（VIP）は、NSIP とポート番号を使用して構成されます。クライアントは PIP アドレスを介して Citrix ADC サービスにアクセスします。要求が Citrix ADC VPX VM または Azure ロードバランサーの NIC に到達すると、VIP は内部 IP（NSIP）と内部ポート番号に変換されます。
- 内部 IP アドレスは、仮想ネットワークのアドレス空間プールからの VM のプライベート内部 IP アドレスです。この IP アドレスは、外部ネットワークから到達できません。この IP アドレスは、静的に設定しない限り、デフォルトで動的です。インターネットからのトラフィックは、ネットワークセキュリティグループで作成されたルールに従って、このアドレスにルーティングされます。ネットワークセキュリティグループと NIC は、NIC の適切なポートに適切なタイプのトラフィックを選択的に送信します。これは、VM に設定されているサービスによって異なります。

> 注:
>
> このドキュメントでは、PIP、VIP、およびインスタンスレベル PIP（ILPIP）は同じものを意味し、置き換え可能です。

次の図は、ARM でプロビジョニングされた Citrix ADC VPX インスタンスを介して、クライアントからサーバーにトラフィックがどのように流れるかを示しています。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

Azure 上での Citrix ADC VPX の動作

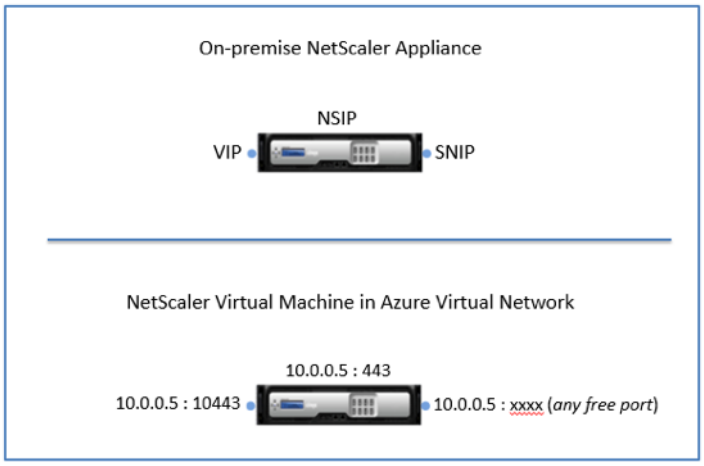
オンプレミス展開では、Citarix ADC VPX インスタンスは、少なくとも次の 3 つの IP アドレスを必要とします。

- Citrix ADC IP（NSIP）アドレスと呼ばれる管理 IP アドレス
- サーバーファームとやり取りするためのサブネット IP（SNIP）アドレス
- クライアント要求を受け付ける仮想サーバー IP（VIP）アドレス

Azure 展開では、DHCP による Provisioning 中に 1 つの IP アドレス (プライベート (内部) アドレス) のみがインスタンスに割り当てられます。

この制限を回避するには、単一の IP アーキテクチャを使用して Azure に Citrix ADC VPX インスタンスを展開します。これにより、Citrix ADC アプライアンスの 3 つの IP 機能が 1 つの IP アドレスに多重化されます。この単一 IP アドレスは、異なるポート番号を使用して、NSIP、SNIP、および VIP として機能します。

次の図は、単一の IP アドレスを使用して NSIP、SNIP、VIP の機能を実行する方法を示しています。



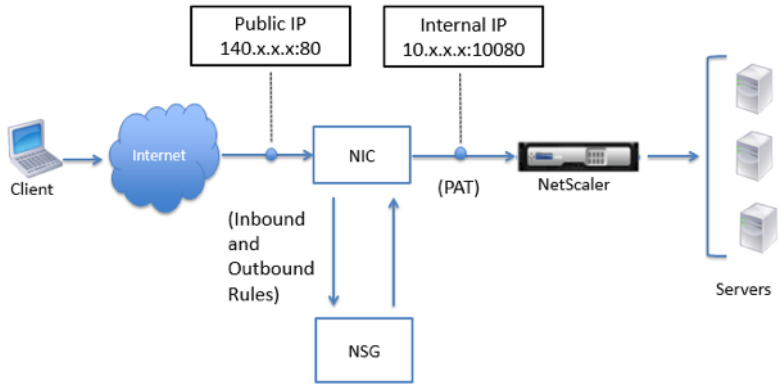
ポートアドレス変換によるトラフィックフロー

Azure 展開では、Citrix ADC VPX インスタンスを仮想マシン（VM）としてプロビジョニングすると、パブリック IP アドレスと内部 IP アドレス（ルーティング不可能）が Citrix ADC 仮想マシンに割り当てられます。受信ルールと送信ルールは、Citrix ADC インスタンスのネットワークセキュリティグループで、定義された各ルールのパブリックポートとプライベートポートとともに定義されます。Citrix ADC インスタンスは、内部 IP アドレスとプライベートポートをリッスンします。

すべての外部要求は、Citrix ADC VPX 仮想マシンの仮想 NIC で受信されます。NIC はネットワークセキュリティグループにバインドされます。ネットワークセキュリティグループでは、要求の宛先アドレスとポート (パブリック IP アドレスとポート) を変換するプライベート IP とプライベートポートの組み合わせを指定します。ARM はポートアドレス変換（PAT）を実行して、パブリック IP アドレスとポートを Citrix ADC 仮想マシンの内部 IP アドレスとプライベートポートにマッピングします。最後に、ARM は VM にトラフィックを転送します。

次の図は、Azure が PAT を実行して、トラフィックを Citrix ADC 内部 IP アドレスとプライベートポートに転送する方法を示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



この例では、パブリック IP アドレスは仮想マシンに 140.x.x.x が割り当てられ、内部 IP アドレスは 10.x.x.x です。インバウンドルールとアウトバウンドルールが定義されている場合、パブリック HTTP ポート 80 は、クライアント要求を受信するポートとして定義されます。対応するプライベートポート 10080 は、Citrix ADC VM がリッスンするポートとして定義されます。クライアント要求はポート 80 のパブリック IP アドレス 140.x.x.x で受信されます。Azure は PAT を実行して、このアドレスとポートをプライベートポート 10080 の内部 IP アドレス 10.x.x.x にマッピングし、クライアント要求を転送します。

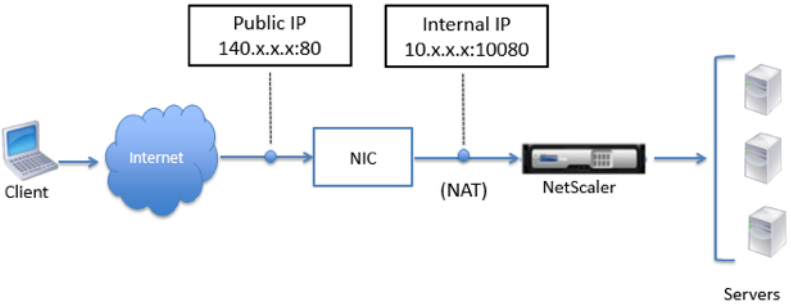
ポートの使用に関する注意事項については、ポート使用のガイドラインを参照してください。

ネットワークセキュリティグループとアクセス制御リストの詳細については、ここをクリックしてください。

ネットワークアドレス変換によるトラフィックフロー

Citrix ADC VM（インスタンスレベル）のパブリック IP（PIP）アドレスをリクエストすることもできます。VM レベルでこの Direct PIP を使用する場合、ネットワークトラフィックを代行受信するためにインバウンドおよびアウトバウンドのルールを定義する必要はありません。インターネットからの着信要求が VM で直接受信されます。Azure はネットワークアドレス変換（NAT）を実行し、Citrix ADC インスタンスの内部 IP アドレスにトラフィックを転送します。

次の図は、Azure がネットワークアドレス変換を実行して Citrix ADC 内部 IP アドレスをマッピングする方法を示しています。



この例では、ネットワークセキュリティグループに割り当てられたパブリック IP は 140.x.x.x で、内部 IP アドレスは 10.x.x.x です。インバウンドルールとアウトバウンドルールが定義されている場合、パブリック HTTP ポート 80

© 1999–2021 Citrix Systems, Inc. All rights reserved.

は、クライアント要求を受信するポートとして定義されます。対応するプライベートポート 10080 は、Citrix ADC 仮想マシンがリッスンするポートとして定義されます。クライアント要求はパブリック IP アドレス 140.x.x.x で受信されます。Azure がネットワークアドレス変換を実行して、PIP を内部 IP アドレス 10.x.x.x（ポート 10080）にマップし、クライアント要求を転送します。

> 注:
>
> 高可用性の Citrix ADC VPX VM は、外部または内部のロードバランサーによって制御されます。これらのロードバランサーには、ロードバランシングトラフィックを制御するためのインバウンドルールが定義されています。まず、外部トラフィックはこれらのロードバランサーによって傍受されます。次に、設定されたロードバランシングルールに従ってトラフィックが迂回されます。これには、ロードバランサーで定義されたバックエンドプール、NAT ルール、およびヘルスプローブが含まれます。

複数の **IP** アドレスを割り当てる

Azure 仮想マシン (VM) には、1 つ以上のネットワークインターフェイス (NIC) がアタッチされています。すべての NIC には、1 つ以上の静的または動的なパブリック IP アドレスとプライベート IP アドレスを割り当てることができます。複数の IP アドレスを仮想マシンに割り当てると、次の機能が有効になります。

- 異なる IP アドレスと SSL 証明書を持つ複数の Web サイトまたはサービスを 1 つのサーバー上でホストする。
- ファイアウォールやロードバランサなどのネットワーク仮想アプライアンスとして機能します。
- Azure Load Balancer バックエンドプールに任意の NIC のプライベート IP アドレスを追加できます。以前は、プライマリ NIC のプライマリ IP アドレスのみをバックエンドプールに追加できました。複数の IP 設定のロードバランシング方法の詳細については、複数の IP 構成の負荷分散に関する記事を参照してください。

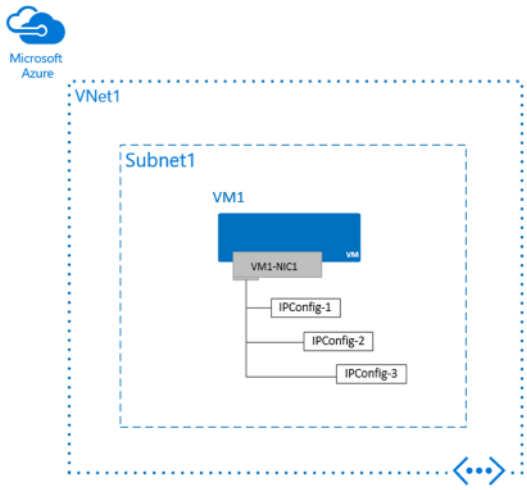
シナリオ

単一の NIC を持つ仮想マシンが作成され、仮想ネットワークに接続されます。VM には、3 つの異なるプライベート IP アドレスと 2 つのパブリック IP アドレスが必要です。

IP アドレスは、次の IP 設定に割り当てられます。

- IPConfig-1: 動的プライベート IP アドレス（デフォルト）と静的パブリック IP アドレスを割り当てます。
- IPConfig-2: 静的プライベート IP アドレスと静的パブリック IP アドレスを割り当てます。
- IPConfig-3: 動的プライベート IP アドレスを割り当てます。パブリック IP アドレスは割り当てません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



仮想マシンに接続されているすべての NIC には、1 つ以上の IP 構成が関連付けられています。各設定には、スタティックプライベート IP アドレスまたはダイナミックプライベート IP アドレスが 1 つ割り当てられます。各構成には、1 つのパブリック IP アドレスリソースが関連付けられている場合もあります。パブリック IP アドレスリソースには、動的または静的なパブリック IP アドレスが割り当てられています。Azure の IP アドレスの詳細については、Azure の記事の IP アドレスをお読みください。各 NIC には最大 250 個のプライベート IP アドレスを割り当てることができます。各 NIC に複数のパブリック IP アドレスを割り当てることができますが、Azure サブスクリプションで使用できるパブリック IP アドレスの数には制限があります。詳しくは、Azure の制限に関する記事を参照してください。

> 注:
>
> クラシック展開モデルで作成されたリソースには、複数の IP アドレスを割り当てることはできません。

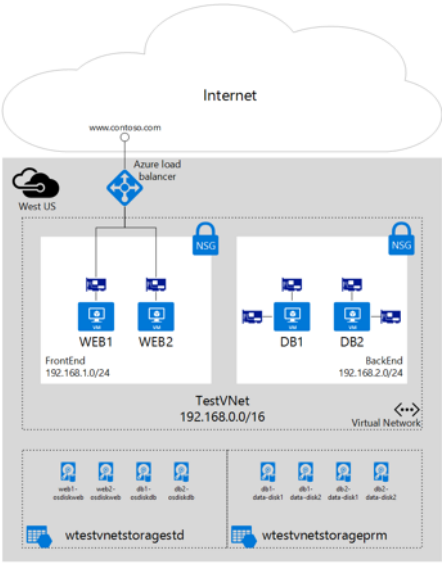
複数の **NIC** インターフェイスを持つ仮想マシンを作成する

Azure で仮想マシン (VM) を作成し、各 VM に複数のネットワークインターフェイス (NIC) をアタッチできます。マルチ NIC は、アプリケーション配信や WAN 最適化ソリューションなど、多くのネットワーク仮想アプライアンスの要件です。マルチ NIC は、より多くのネットワークトラフィック管理機能を提供します。たとえば、フロントエンド NIC とバックエンド NIC 間のトラフィックの分離、管理プレーントラフィックからのデータプレーントラフィックの分離などがあります。

シナリオ

このドキュメントでは、特定のシナリオで VM で複数の NIC を使用する展開について説明します。このシナリオでは、Azure でホストされている 2 層の IaaS ワークロードがあります。各層は、仮想ネットワーク (VNet) 内の独自のサブネットに展開されます。フロントエンド層は、複数の Web サーバーで構成され、高可用性を実現するロードバランサーセットにグループ化されます。バックエンド層は、複数のデータベースサーバーで構成されます。これらのデータベースサーバーには、それぞれ 2 つの NIC があり、1 つはデータベースアクセス用、もう 1 つは管理用です。このシナリオには、各サブネットに許可されるトラフィックを制御するネットワークセキュリティグループと、展開内の NIC も含まれます。次の図は、このシナリオの基本的なアーキテクチャを示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ポートの使用に関する注意事項

Citrix ADC VM を作成するとき、または VM のプロビジョニング後に、ネットワークセキュリティグループに追加のインバウンドルールとアウトバウンドルールを設定できます。各受信および送信規則は、パブリックポートおよびプライベートポートに関連付けられています。

ネットワークセキュリティグループルールを設定する前に、使用できるポート番号に関する次のガイドラインに注意してください。

1. 以下のポートは、Citrix ADC 仮想マシンによって予約されています。パブリック IP アドレスを使用してインターネットからの要求に対応する場合、これらのポートをプライベートポートとして定義することはできません。

   ポート 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   ただし、VIP などのインターネットに直接接続するサービスに標準ポート (ポート 443 など) を使用する場合は、ネットワークセキュリティグループを使用してポートマッピングを作成する必要があります。標準ポートは、この VIP サービス用に Citrix ADC 上で構成されている別のポートにマッピングされます。

   たとえば、VIP サービスが Citrix ADC インスタンスのポート 8443 で実行されているが、パブリックポート 443 にマッピングされているとします。したがって、ユーザーがパブリック IP を介してポート 443 にアクセスすると、要求はプライベートポート 8443 に送信されます。

2. パブリック IP アドレスでは、ポートマッピングが動的に解放される、パッシブ FTP や ALG のようなプロトコルをサポートしていません。

3. Azure ロードバランサーはパブリック IP アドレスとは連動しません。高可用性は、ロードバランサー上に構成された PIP でなく、VPX インスタンスに関連付けられた PIP を使用するトラフィックでは機能しません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ARM で Citrix ADC VPX HA を構成する方法については、「Azure の高可用性モードで Citrix ADC VPX を構成する」を参照してください。

4. Citrix ADC Gateway 環境では、SNIP を構成する必要がありません。これは、SNIP を構成していないときに SNIP を SNIP として使用できるためです。

> 注: NSIP アドレスといくつかの非標準ポート番号を使用して、VIP アドレスを構成する必要があります。バックエンドサーバのコールバック設定では、VIP ポート番号を VIP URL とともに指定する必要があります（たとえば、url: port)。
> 注: ARM では、Citrix ADC VPX 仮想マシンは 2 つの IP アドレスに関連付けられています。パブリック IP アドレスと内部 IP アドレスです。外部トラフィックは PIP に接続しますが、内部 IP アドレスまたは NSIP はルーティング不可能です。VPX で VIP を構成するには、内部 IP アドレスとポート番号のこの組み合わせを使用します。
> 例:VPN 仮想サーバーの完全修飾ドメイン名が vip.test.com で、VPN 仮想サーバーがポート 8443 で実行している場合、コールバック URL はとなりますhttps://vip.test.com:8443。

構成の手順

次の手順では、ADC を機能させるために必要なリソースグループ、セキュリティグループ、仮想ネットワーク、および変換設定を設定する方法の概要を示します。

リソースグループのプロビジョニング

Microsoft Azure ポータルページで、ユーザー名とパスワードを入力して Azure Resource Manager ポータルにログオンします。(ARM ポータルで、1 つのペインでオプションをクリックすると、右側に新しいペインが開きます。あるペインから別のペインに移動して、デバイスを設定します)。

すべてのリソースのコンテナとして機能するリソースグループを作成します。リソースグループを使用して、リソースをグループとして展開、管理、および監視します。

ネットワークセキュリティグループの作成

仮想ネットワーク内の着信トラフィックと発信トラフィックを制御するインバウンドルールとアウトバウンドルールを割り当てるネットワークセキュリティグループを作成します。ネットワークセキュリティグループを使用すると、1 つの仮想マシンのセキュリティルールを定義したり、仮想ネットワークサブネットのセキュリティルールを定義したりできます。

仮想ネットワークとサブネットの設定

ARM の仮想ネットワークは、サービスのセキュリティを強化し、隔離するものです。同じ仮想ネットワークに属する VM およびサービスは、互いにアクセスできます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

たとえば、予約済 CIDR ブロックが 192.168.0.0/16 の仮想ネットワークと、CIDR ブロックがそれぞれ 192.168.1.0/24 および 192.168.2.0/24 の 2 つのサブネットを作成します。

1. 仮想ネットワークの作成ウィンドウで、次の値を入力し、作成をクリックします。
    - 仮想ネットワークの名前
    - Address space - 仮想ネットワークの予約済 IP アドレスブロックを入力します
    - Subnet — 最初のサブネットの名前を入力します (この手順の後半で 2 番目のサブネットを作成します)。
    - Subnet address range - サブネットの予約済 IP アドレスブロックを入力します
    - Resource group - 以前に作成したボックスの一覧からリソースグループを選択します

2 番目のサブネットの構成

1. すべてのリソースペインから新しく作成した仮想ネットワークを選択し、設定ペインで サブネットをクリックします。
2. **+Subnet** をクリックし、次の詳細を入力して 2 番目のサブネットを作成します。
    - 2 番目のサブネットの名前
    - Address range - サブネットの予約済 IP アドレスブロックを入力します
    - ネットワークセキュリティグループ — ドロップダウンリストからネットワークセキュリティグループを選択します。

ストレージアカウントを構成する

ARM IaaS インフラストラクチャストレージには、BLOB、表、キューおよびファイルの形式でデータを保存できるすべてのサービスが含まれます。ARM では、これらの形式のストレージデータを使用してアプリケーションを作成することもできます。

すべてのデータを格納するストレージアカウントを作成する

1. **+** 新規**] >** ストレージ **>** ストレージアカウント] をクリックします。
2. ストレージアカウントの作成ウィンドウで、次の詳細を入力します。
    - アカウントの名前
    - 展開モード — リソースマネージャを選択します。
    - [アカウントの種類] — ドロップダウンリストから [汎用] を選択します。
    - レプリケーション：ドロップダウンリストから [ローカル冗長ストレージ] を選択します。
    - Resource group - ボックスの一覧から新しく作成したリソースグループを選択します
3. ［作成］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

可用性セットの構成

可用性セットを使用すると、計画済みメンテナンスまたは計画外メンテナンスの場合に、少なくとも 1 つの VM が確実に稼働しています。冗長サービスを実現するために、同じ「可用性セット」の下にある 2 つ以上の仮想マシンを異なる障害ドメインに配置します。

1. [+ 新規] をクリックして、可用性セットを検索します。
2. リストから [可用性セットエンティティ] を選択します。［作成］をクリックします。
3. [可用性セットの作成] ペインで、次の詳細を入力します。
   - セットの名前
   - Resource group - ボックスの一覧から新しく作成したリソースグループを選択します
4. [作成] をクリックします。

Citrix ADC インスタンスのプロビジョニング

仮想ネットワーク内に Citrix ADC VPX インスタンスを作成します。次に、Azure マーケットプレイスから Citrix ADC VPX イメージを取得します。Azure Resource Manager ポータルを使用して、Citrix ADC VPX インスタンスを作成します。

Citrix ADC VPX インスタンスの作成を開始する前に、必要なサブネットを持つ仮想ネットワークが作成されていることを確認します。仮想マシンのプロビジョニング時に仮想ネットワークを作成することもできますが、柔軟性に欠けるため別のサブネットを作成することはできません。詳しくは、Azure ポータルを使用して仮想ネットワークを作成するの記事を参照してください。

オプション:VM がインターネットリソースにアクセスできるように、DNS サーバーと VPN 接続を構成します。

> 注： Citrix ADC VPX VM をプロビジョニングする前に、リソースグループ、ネットワークセキュリティグループ、仮想ネットワークなどのエンティティを作成することをお勧めします。これにより、Provisioning 中にネットワーク情報が利用可能になります。

1. [** + 新規] > [ネットワーク]** をクリックします。
2. ［すべて表示］をクリックし、［ネットワーク］ペインで ［**Citrix ADC VPX Bring Your Own License**］をクリックします。
3. ［作成］をクリックします。

   > 注： ARM ポータル上で任意のエンティティをすばやく検出する方法として、Azure Marketplace 検索ボックスにエンティティの名前を入力して、<Enter>キーを押す方法もあります。検索ボックスに「**Citrix ADC** 」と入力して、Citrix ADC イメージを検索します。

4. ［**Citrix ADC 12.0 VPX** 自分のライセンスを持参］を選択します。
5. 詳細情報を入力します。
6. 検証に合格した後、私の Citrix ADC を購入して展開します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

7. IP アドレスを [静的] に設定することをお勧めします。

> 注**:** 必ず最新のイメージを選択してください。Citrix ADC イメージの名前にリリース番号が含まれている場合があります。

PowerShell を使用して複数の **IP** アドレスを持つ仮想マシンを作成する

次の手順では、シナリオで説明されているように、複数の IP アドレスを持つサンプルの VM を作成する方法について説明します。実装に必要な変数名と IP アドレスの種類を変更します。

ここで説明する設定手順は次のとおりです。

1. 複数の IP アドレスを持つ仮想マシンを作成する
2. 仮想マシンへの IP アドレスの追加
3. VM オペレーティングシステムへの IP アドレスの追加
4. 検証（Windows）
5. 検証（Linux）

次の Microsoft Azure のドキュメントを参照してください：PowerShell を使用して仮想マシンに複数の IP アドレスを割り当てる。

Citrix ADC ポート変換の構成

1. VM、Citrix ADC ネットワークインターフェースをクリックします。
2. ネットワークセキュリティグループをクリックします。
3. [受信セキュリティルール] をクリックします。
4. インバウンド接続のセキュリティグループで **SSH** と **HTTP** を許可します。

この時点で、Citrix ADC インスタンスにログインして、Azure 環境に必要な機能と設定を構成できます。

> 注： Citrix ADC に初めてログインするときに、ウィザードでサブネット IP アドレスを要求することがあります。Citrix ADC Azure インスタンスでは、すべての機能に対して 1 つの IP アドレスしか使用しないため、これは必須ではありません。プロンプトが表示されたらこの手順をスキップし、デフォルトの構成ログインページに進みます。

Microsoft Azure Resource Manager ポータル

アプリケーションのインフラストラクチャは、通常、仮想マシン、ストレージアカウント、仮想ネットワーク、Web アプリ、データベース、データベースサーバー、およびサードパーティのサービスなど、多くのコンポーネントで構成されます。これらのコンポーネントは、個別のエンティティとして表示されません。代わりに、単一のエンティティの関連部分と相互依存部分として表示されます。グループとして展開、管理、および監視する場合。Azure Resource Manager を使用すると、ソリューション内のリソースをグループとして操作できます。1 回の調整操作

© 1999–2021 Citrix Systems, Inc. All rights reserved.

で、ソリューションのすべてのリソースを展開、更新、または削除できます。展開にはテンプレートを使用し、そのテンプレートはテスト、ステージング、本番環境などのさまざまな環境で使用できます。Resource Manager には、セキュリティ機能、監査、タグ付け機能があり、展開後のリソース管理に役立ちます。

用語

Azure Resource Manager ーを初めて使用する場合は、慣れていない用語がいくつかあります。

- リソース -Azure を通じて利用可能な管理可能なアイテム。一般的なリソースには、仮想マシン、ストレージアカウント、Web アプリ、データベース、仮想ネットワークなどがあります。
- リソースグループ -Azure ソリューションに関連するリソースを保持するコンテナー。リソースグループには、ソリューションのすべてのリソースを含めることも、グループとして管理するリソースのみを含めることもできます。組織にとって最も意味のあるものに基づいて、リソースグループにリソースを割り当てる方法を決定します。「リソースグループ」を参照してください。
- リソースプロバイダ -リソースマネージャを使用して展開および管理できるリソースを提供するサービス。各リソースプロバイダーは、展開されたリソースを操作するための操作を提供します。一般的なリソースプロバイダは、仮想マシンリソースを提供するリソース`Microsoft.Compute`、ストレージアカウントリソースを提供するリソース`Microsoft.Storage`、Web アプリに関連したリソースを提供するリソース`Microsoft.Web`です。「リソースプロバイダ」を参照してください。
- リソースマネージャテンプレート -リソースグループに展開する 1 つ以上のリソースを定義する JavaScript オブジェクト記法（JSON）ファイル。また、展開されたリソース間の依存関係も定義します。テンプレートを使用して、リソースを一貫して繰り返し展開できます。「テンプレートの展開」を参照してください。
- 宣言型構文 -作成するためのプログラミングコマンドのシーケンスを記述することなく、「ここで作成する予定です」と記述できる構文。リソースマネージャテンプレートは、宣言構文の例です。ファイルで、Azure に展開するインフラストラクチャのプロパティを定義します。

参考資料：Azure Resource Manager 概要

Citrix ADC マルチ NIC の概要

Azure プラットフォーム上で実行されている Citrix ADC 仮想インスタンスは、スタンドアロンの仮想 Citrix ADC アプライアンスに複数の仮想 NIC を接続できます。

これは、アプリケーション層やデータベース層など、Azure で分散アーキテクチャが必要な場合の一般的なシナリオです。

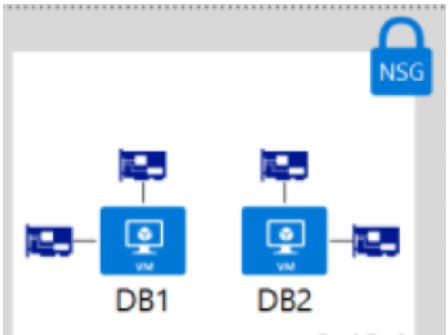
複数の NIC の 2 つ目の一般的な Citrix ADC の使用例として、Azure 環境でネットワークゾーンを分離したいということが挙げられます。分離の例としては、インターネットから発信されたトラフィックを 1 つのインターフェイス（DMZ または Public）で終端させ、内部 Web サービスおよびアプリケーションサービスをプライベートにすることができます。

この 2 アームネットワークシナリオでは、Citrix ADC 仮想アプライアンスでは、少なくとも 2 つの仮想 NIC が必要です。パブリックネットワーク用の仮想 NIC 1 つ、プライベートネットワーク用の仮想 NIC 1 つ。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

さらに、Azure のマルチ NIC 構成では、分離された NIC に対応するために複数のサブネットワークを使用する必要があります。このコンポーネントは、Azure ポータルの VNET コンポーネントを使用して構成されます。

例:Azure VM に接続された複数の vNIC



> 注**:** VM のサイズが異なると、さまざまな NIC 数がサポートされるため、それに応じて仮想マシンのサイズを設定します。https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes

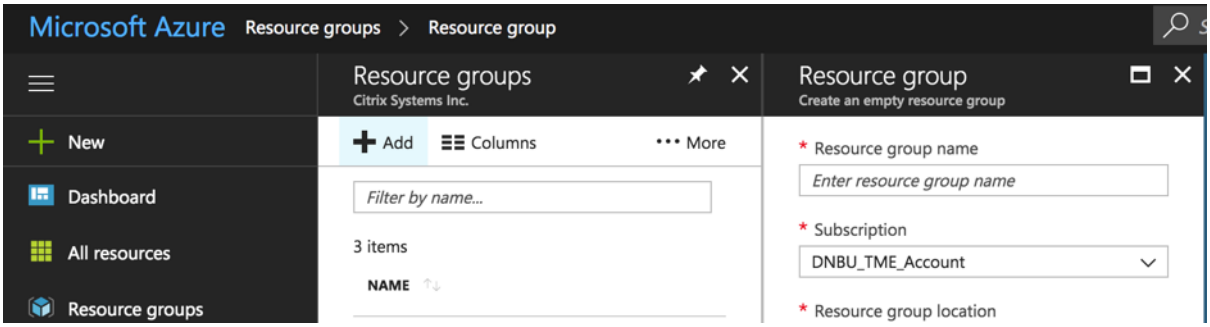
Citrix ADC マルチ **NIC** 構成

次の構成では、ADC でマルチ NIC 構成を行うために必要なサブネットと仮想ネットワークを簡単に作成する方法を説明します。

リソースグループの作成

PowerShellCopy

```
1 New-AzureRmResourceGroup -Name "myResourceGroup" -Location "EastUS"
2 <!--NeedCopy-->
```



VNET とサブネットの作成

一般的なシナリオは、仮想ネットワークに 2 つ以上のサブネットがある場合です。1 つのサブネットはフロントエンドトラフィック用で、もう 1 つのサブネットはバックエンドトラフィック用です。両方のサブネットに接続するには、VM で複数の NIC を使用します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

New-AzureRmVirtualNetworkSubnetConfigを使用して、2 つの仮想ネットワークサブネットを定義します。次の例では、mySubnetFrontEndおよびmySubnetBackEndのサブネットを定義します:

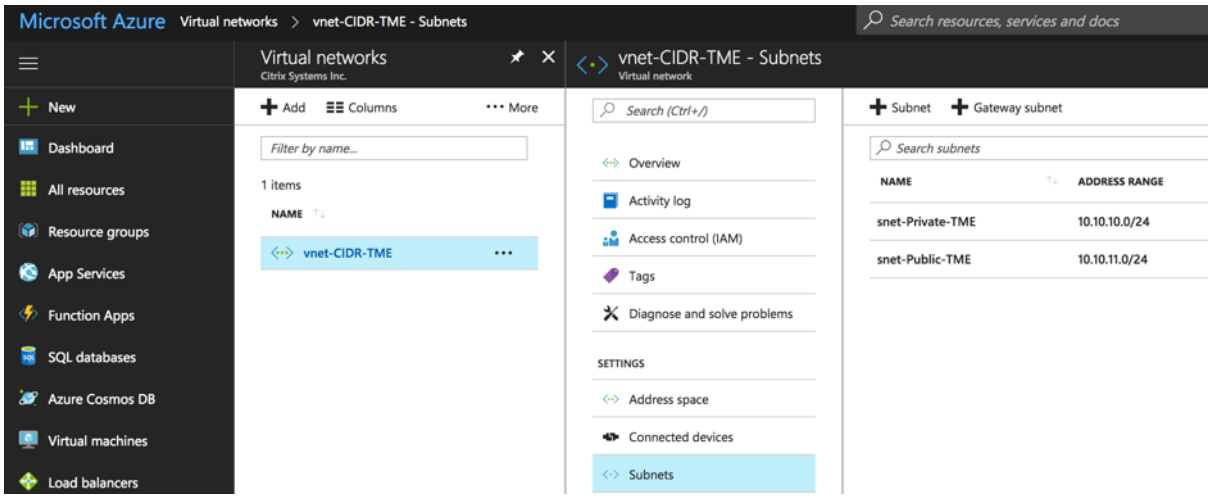
PowerShellCopy

```
$mySubnetFrontEnd = New-AzureRmVirtualNetworkSubnetConfig -Name "
    mySubnetFrontEnd" `
 -AddressPrefix "192.168.1.0/24"
$mySubnetBackEnd = New-AzureRmVirtualNetworkSubnetConfig -Name "
    mySubnetBackEnd" `
 -AddressPrefix "192.168.2.0/24"
 <!--NeedCopy-->
```

New-AzureRmVirtualNetworkを使用して仮想ネットワークとサブネットを作成します。次の例では、myVnetという名前の仮想ネットワークを作成します。

PowerShellCopy

```
$myVnet = New-AzureRmVirtualNetwork -ResourceGroupName "myResourceGroup
    " `
 -Location "EastUs" `
 -Name "myVnet" `
 -AddressPrefix "192.168.0.0/16" `
 -Subnet $mySubnetFrontEnd,$mySubnetBackEnd
 <!--NeedCopy-->
```



ネットワークセキュリティグループの作成

通常、仮想マシンへのネットワークトラフィックをフィルタリングするネットワークセキュリティグループと、複数の仮想マシンにトラフィックを分散するロードバランサーも作成します。

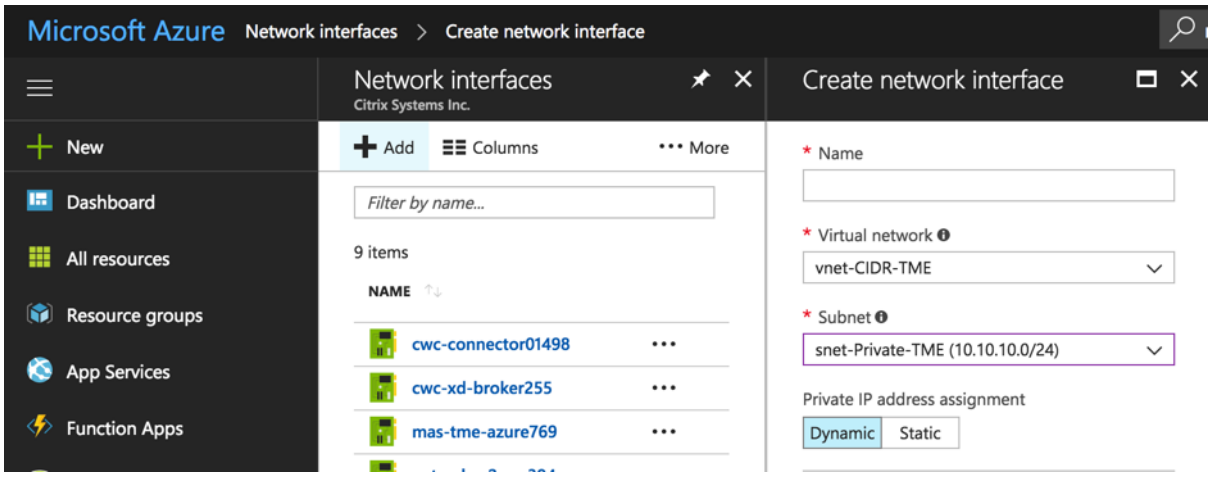
© 1999–2021 Citrix Systems, Inc. All rights reserved.

vNIC の作成と設定

New-AzureRmNetworkInterfaceを使用して 2 つの NIC を作成します。フロントエンドサブネットに 1 つの NIC を、バックエンドサブネットに 1 つの NIC を接続します。次の例では、myNic1 および myNic2 という名前の NIC を作成します。

PowerShellCopy

```
$frontEnd = $myVnet.Subnets|?{
 $\_.Name -eq 'mySubnetFrontEnd' }

$myNic1 = New-AzureRmNetworkInterface -ResourceGroupName "
    myResourceGroup" `
 -Name "myNic1" `
 -Location "EastUs" `
 -SubnetId $frontEnd.Id
$backEnd = $myVnet.Subnets|?{
 $\_.Name -eq 'mySubnetBackEnd' }

$myNic2 = New-AzureRmNetworkInterface -ResourceGroupName "
    myResourceGroup" `
 -Name "myNic2" `
 -Location "EastUs" `
 -SubnetId $backEnd.Id
 <!--NeedCopy-->
```



仮想マシンの作成と **vNIC** の接続

次に、VM 構成の構築を開始します。各 VM サイズには、VM に追加できる NIC の合計数に制限があります。詳しくは、「Windows 仮想マシンのサイズ」を参照してください。

Add-AzureRmVMNetworkInterfaceを使用して以前に作成した 2 つの NIC を接続します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

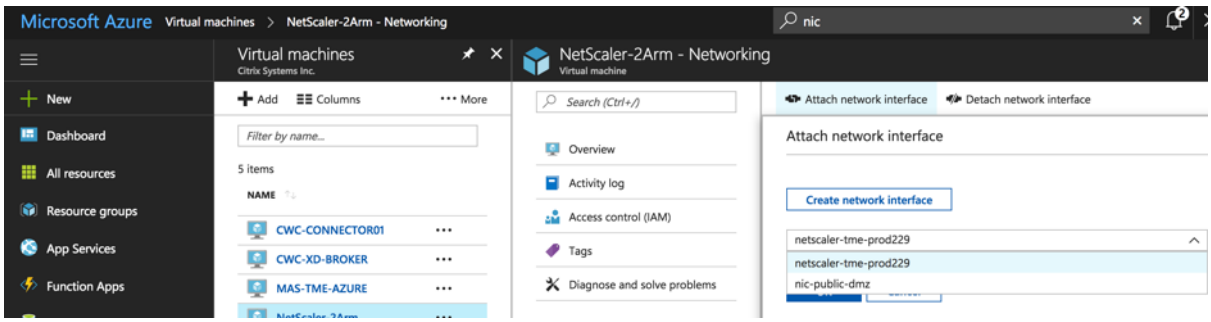
PowerShellCopy

```
$vmConfig = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $myNic1.Id
    -Primary
$vmConfig = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $myNic2.Id
<!--NeedCopy-->
```

最後に、`New-AzureRmVM`を使用して VM を作成します。

PowerShellCopy

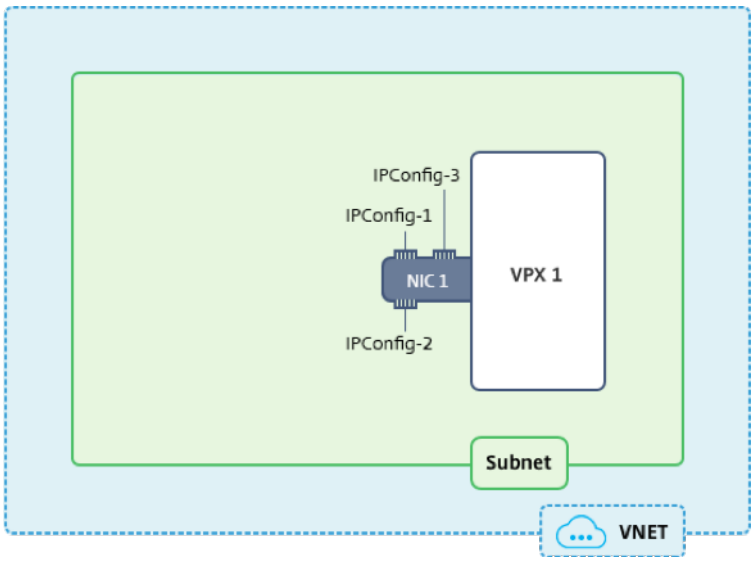
```
New-AzureRmVM -VM $vmConfig -ResourceGroupName "myResourceGroup" -
    Location "EastUs"
<!--NeedCopy-->
```



Citrix ADC の複数の IP アドレスの概要

このユースケースでは、スタンドアロン Citrix ADC VPX アプライアンスは、仮想ネットワーク（VNET）に接続された単一または複数の vNIC で構成できます。vNIC は 3 つの IP 構成（ipconfig）に関連付けられ、それぞれが異なる目的で使用されます。

例：複数の VIP が 1 つの vNIC にアタッチされている場合



© 1999–2021 Citrix Systems, Inc. All rights reserved.

複数の IP 構成を NIC に割り当てる場合は、1 つの構成を-Primary として割り当てる必要があります。

```
$MyNIC.IpConfigurations | Format-Table Name, PrivateIPAddress,
    PublicIPAddress, Primary
<!--NeedCopy-->
```

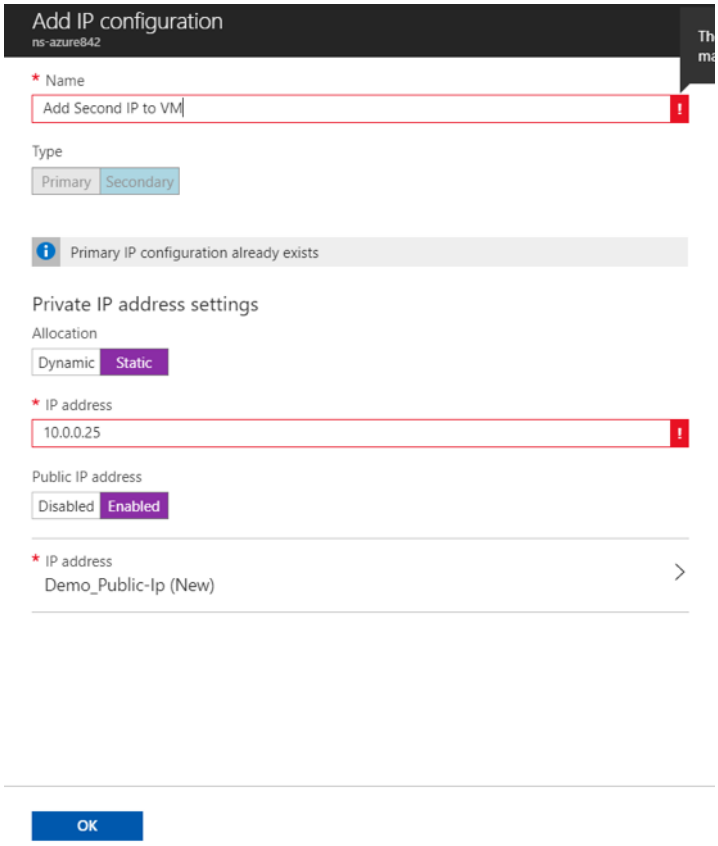
> 注:
>
> パブリック IP アドレスにはわずかな料金がかかります。IP アドレスの価格設定の詳細については、IP アドレスの価格設定ページを参照してください。サブスクリプションで使用できるパブリック IP アドレスの数には制限があります。制限の詳細については、Azure の制限に関する記事を参照してください。

プライベート **IP** アドレスを追加する

NIC にプライベート IP アドレスを追加するには、IP 構成を作成する必要があります。次のコマンドは、10.0.0.7 のスタティック IP アドレスで設定を作成します。静的 IP アドレスを指定する場合は、サブネットの未使用のアドレスである必要があります。最初にアドレスをテストして、`Test-AzureRmPrivateIPAddressAvailability -IPAddress 10.0.0.7 -VirtualNetwork $myVnet`コマンドを入力してアドレスが使用可能であることを確認することをお勧めします。IP アドレスが使用可能な場合は、出力が`True`を返します。アドレスが使用できない場合は、出力が`False`を返し、使用可能なアドレスのリストが含まれます。

```
Add-AzureRmNetworkInterfaceIpConfig -Name IPConfig-4 -NetworkInterface
    `
$MyNIC -Subnet $Subnet -PrivateIpAddress 10.0.0.7
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

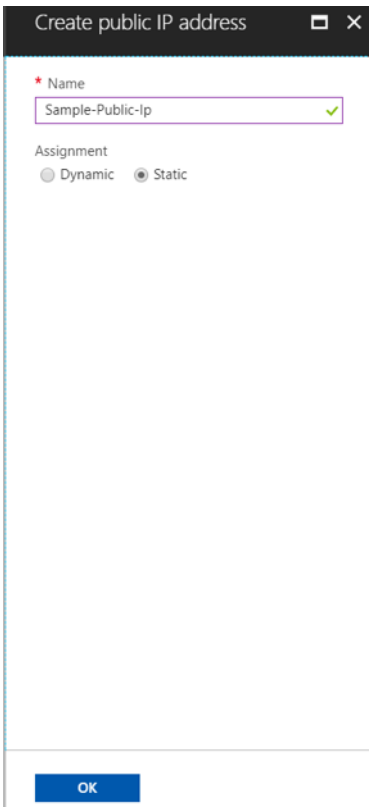


パブリック **IP** アドレスを追加する

パブリック IP アドレスは、パブリック IP アドレスリソースを新しい IP 設定または既存の IP 設定に関連付けることによって追加されます。必要に応じて、以下のいずれかのセクションの手順を実行します。

```
$MyPublicIp3 = New-AzureRmPublicIpAddress `
 -Name "MyPublicIp3" `
 -ResourceGroupName $RgName `
 -Location $Location -AllocationMethod Static
 <!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

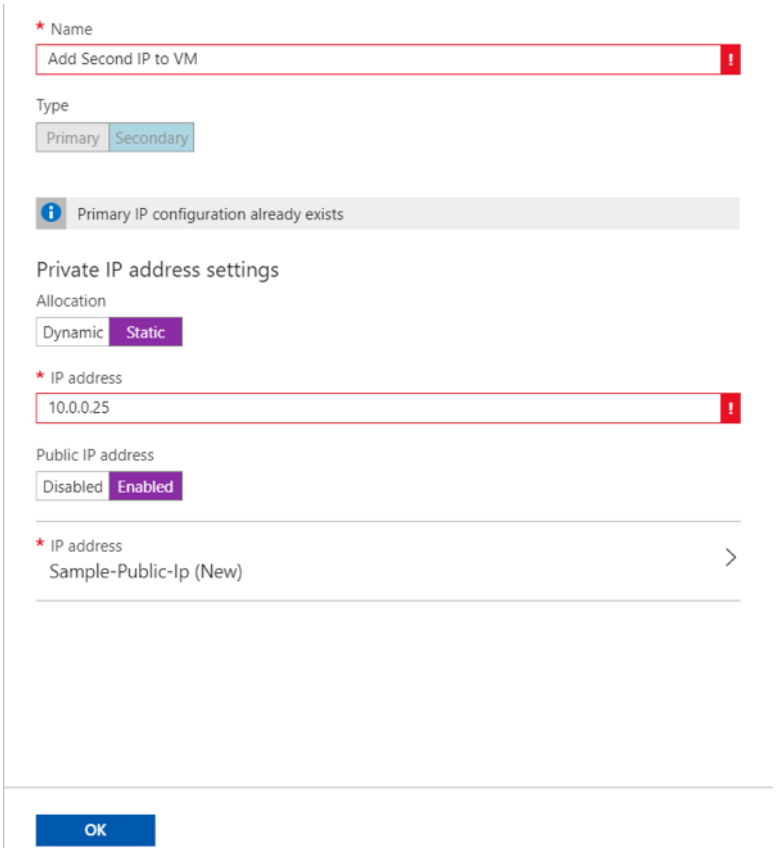


パブリック **IP** アドレスリソースを既存の仮想マシンに関連付ける

パブリック IP アドレスリソースは、関連付けられている IP 設定にのみ、関連付けられている IP 設定に関連付けることができます。

```
Set-AzureRmNetworkInterfaceIpConfig `
 -Name IpConfig-3 `
 -NetworkInterface $mynic `
 -Subnet $Subnet `
 -PublicIpAddress $myPublicIp3
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.



Citrix ADC 高可用性の概要

Azure のアクティブ-パッシブ高可用性 (HA) セットアップで、複数の NIC を持つ一対の Citrix ADC 仮想アプライアンスを展開できます。各 NIC に複数の IP アドレスを設定できます。アクティブ/パッシブ展開では以下が必要です。

- HA Independent Network Configuration（INC）構成
- Direct Server Return（DSR）モードの Azure Load Balancer（ALB）

すべてのトラフィックはプライマリノードを通過します。セカンダリノードは、プライマリノードが失敗するまでスタンバイモードを維持します。

アクティブ/パッシブ展開では、ALB フローティングパブリック IP（PIP）アドレスが各 Citrix ADC ノードの VIP アドレスとして追加されます。HA-INC 構成では、これらの VIP アドレスはフローティングされ、SNIP アドレスはインスタンス固有のアドレスとなります。ALB は、5 秒ごとにヘルスプローブを送信することにより、各 Citrix ADC インスタンスを監視します。ADC は、ヘルスプローブ応答を定期的に送信するインスタンスにだけトラフィックをリダイレクトします。そのため、HA セットアップでは、プライマリノードがヘルスプローブに応答し、セカンダリノードは応答しません。プライマリインスタンスで連続した 2 つのヘルスプローブが見つからない場合、ALB はそのインスタンスにトラフィックをリダイレクトしません。フェイルオーバー時は、新しいプライマリがヘルスプローブへの応答を開始し、ALB はそのプライマリにトラフィックをリダイレクトします。標準の Citrix ADC HA フェイルオーバー時間は 3 秒です。トラフィック切り替えにかかる合計フェイルオーバー時間は、最大で 13 秒になる可能性があります。

Citrix ADC ペアをアクティブ-パッシブ HA モードで展開するには、次の 2 つの方法があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- Citrix ADC 標準 HA テンプレート：3 つのサブネットと 6 つの NIC のデフォルトオプションを使用して HA ペアを構成するには、このオプションを使用します。
- Windows PowerShell コマンド：独自のサブネットおよび NIC 要件に応じて HA ペアを構成する場合にこのオプションを使用します。

Citrix ADC ADC HA 構成-PowerShell

PowerShell コマンドを使用した、複数の IP アドレスおよび NIC を使用した HA セットアップの構成で Azure PowerShell コマンドを確認します。

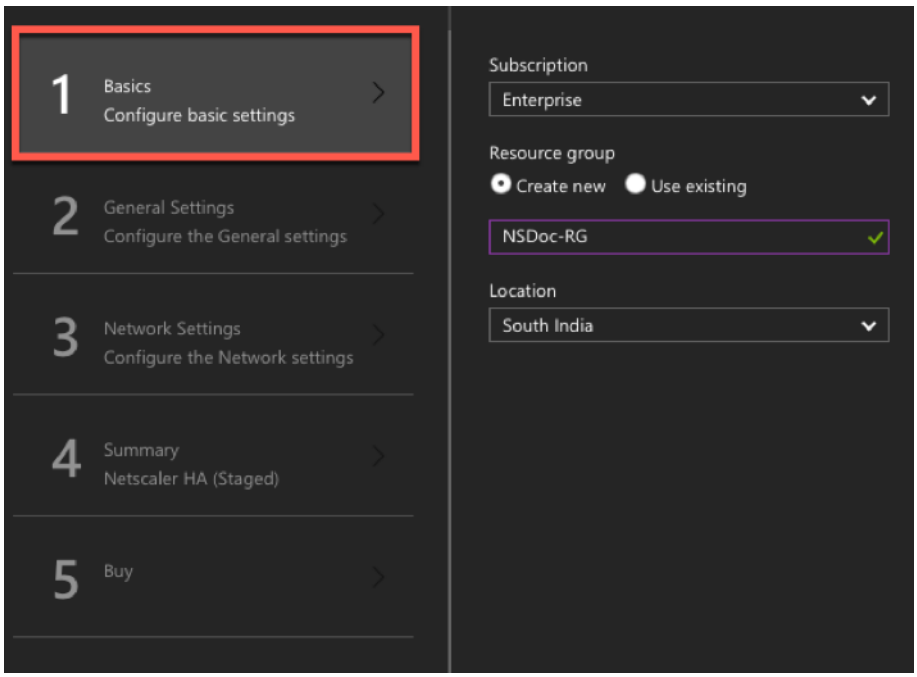
Citrix ADC ADC HA 構成-Azure ポータル

標準テンプレートを使用すると、一対の Citrix ADC インスタンスを HA-INC モードで迅速かつ効率的に展開できます。テンプレートは、3 つのサブネットと 6 つの NIC を持つ 2 つのノードを作成します。サブネットは管理、クライアント、サーバー側のトラフィック用です。各サブネットには、両方の VPX インスタンスに対して 2 つの NIC があります。

Citrix ADC ADC 12.0 HA ペアテンプレートは、Azure Marketplace で入手できます。

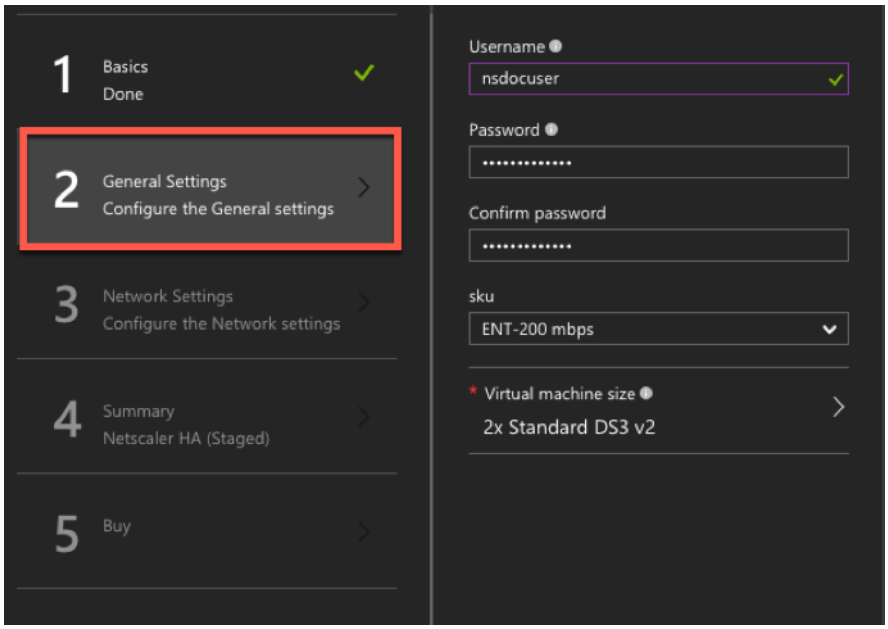
テンプレートを使用するには:

1. Azure Marketplace から、Citrix ソリューションテンプレートを選択して開始します。テンプレートが表示されます。
2. 展開の種類が 「リソースマネージャー」であることを確認し、「作成」を選択します。
3. [基本] ページが開きます。リソースグループを作成し、「**OK** 」を選択します。

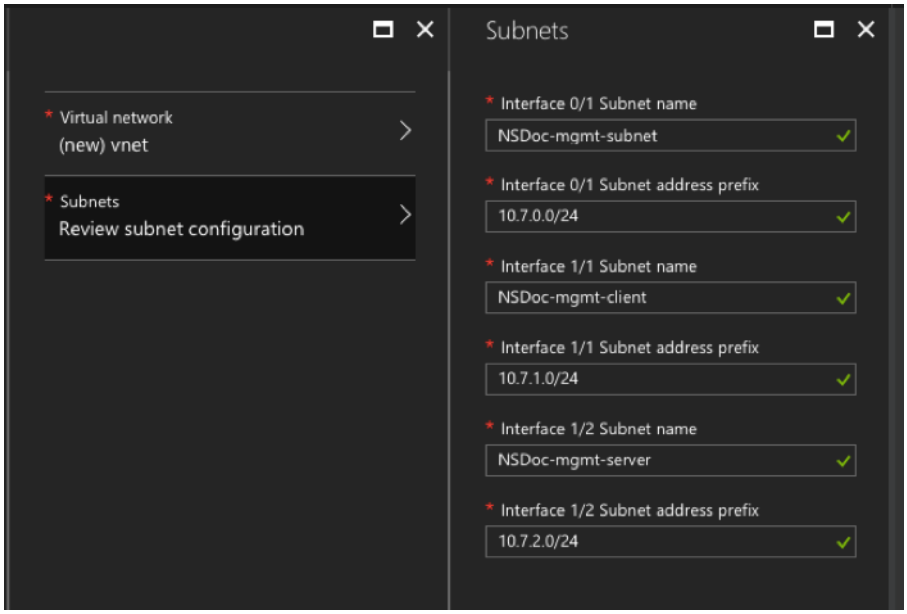


© 1999–2021 Citrix Systems, Inc. All rights reserved.

4. [一般設定] ページが表示されます。詳細を入力し、[**OK**] を選択します。



5. [ネットワーク設定] ページが表示されます。vnet とサブネットの構成を確認し、必要な設定を編集して、[**OK]** を選択します。



6. [概要] ページが開きます。構成を確認し、適宜編集します。[**OK**] を選択して確定します。

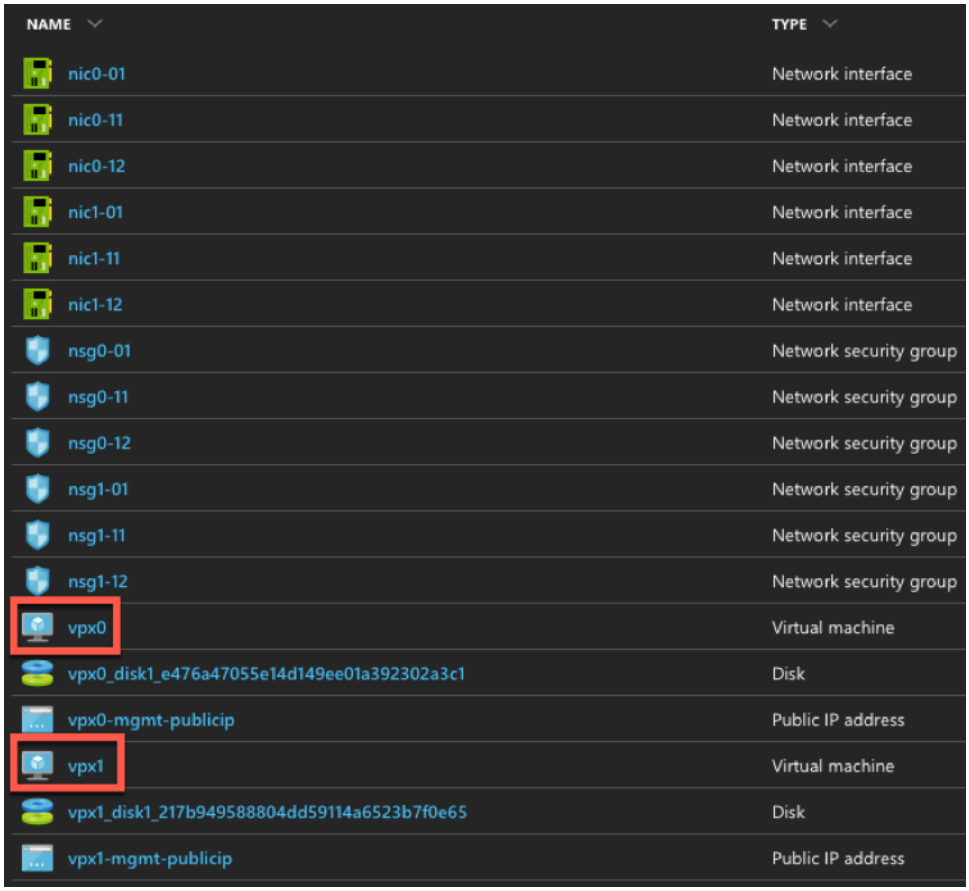
7. 「購入」ページが表示されます。[購入] を選択して、展開を完了します。

必要な構成で Azure リソースグループが作成されるまで時間がかかることがあります。完了後、リソースグループを選択して構成の詳細を表示します。これには、Azure Portal の LB ルール、バックエンドプール、正常性プローブなどが含まれます。HA ペアが VPX0 および VPX1 として表示されます。

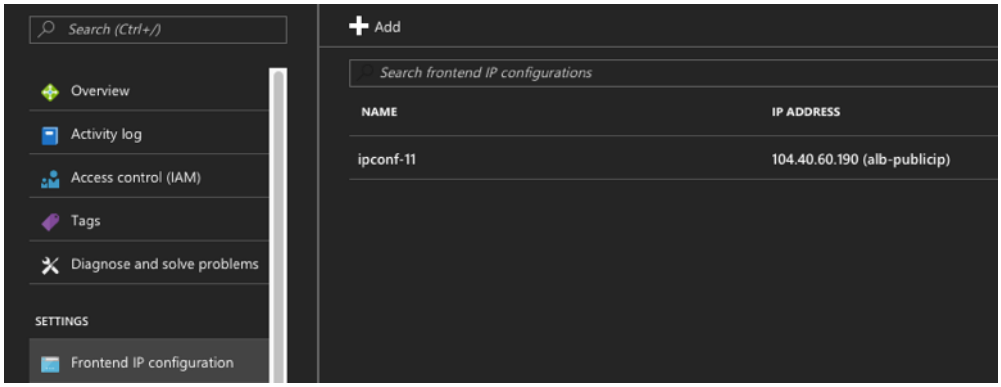
追加のセキュリティルールやポートを作成するなど、HA セットアップでさらに変更が必要な場合は、Azure Portal

© 1999–2021 Citrix Systems, Inc. All rights reserved.

から実行できます。



次に、各ノードで、負荷分散 vserver に ALB パブリック IP（PIP）アドレスを構成する必要があります。ALB PIP を検索するには、[** ALB] > [フロントエンド IP 構成 **] を選択します。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラウドロードバランサーを使用した **Citrix ADC GSLB** およびドメインベースのサービスのバックエンド自動スケール

GSLB および **DBS** の概要

Citrix ADC GSLB は、クラウドロードバランサー用の DBS（ドメインベースのサービス）の使用をサポートしています。これにより、クラウドロードバランサソリューションを使用して、動的なクラウドサービスを自動検出できます。この構成により、Citrix ADC はアクティブ/アクティブ環境でグローバルサーバー負荷分散ドメイン名ベースのサービス（GSLB DBS）を実装できます。DBS を使用すると、Amazon Web Services（AWS）および Microsoft Azure 環境のバックエンドリソースを DNS 検出からスケーリングできます。このセクションでは、AWS 環境と Azure Auto Scaling 環境における Citrix ADC 間の統合について説明します。ドキュメントの最後のセクションでは、AWS または Azure リージョンに固有の 2 つの異なるアベイラビリティーゾーン (AZ) にまたがる Citrix ADC の HA ペアをセットアップする機能について詳しく説明します。

必須要件:

Citrix ADC GSLB サービスグループの前提条件には、セキュリティグループ、Linux ウェブサーバー、AWS 内の Citrix ADC、Elastic IP、およびエラスティックロードバランサーを設定する知識と能力を持つ、機能する Amazon Web Services/Microsoft Azure 環境が含まれます。

GSLB DBS サービスの統合には、AWS ELB および Microsoft Azure ALB
ロードバランサーインスタンス用に、Citrix ADC バージョン 12.0.57 が必要です。

Citrix ADC GSLB サービスグループ機能の拡張

GSLB サービスグループエンティティ:Citrix ADC バージョン 12.0.57

DBS 動的検出を使用した自動スケーリングをサポートする GSLB サービスグループが導入されました。

DBS 機能コンポーネント（ドメインベースのサービス）は、GSLB サービスグループにバインドする必要があります

例:

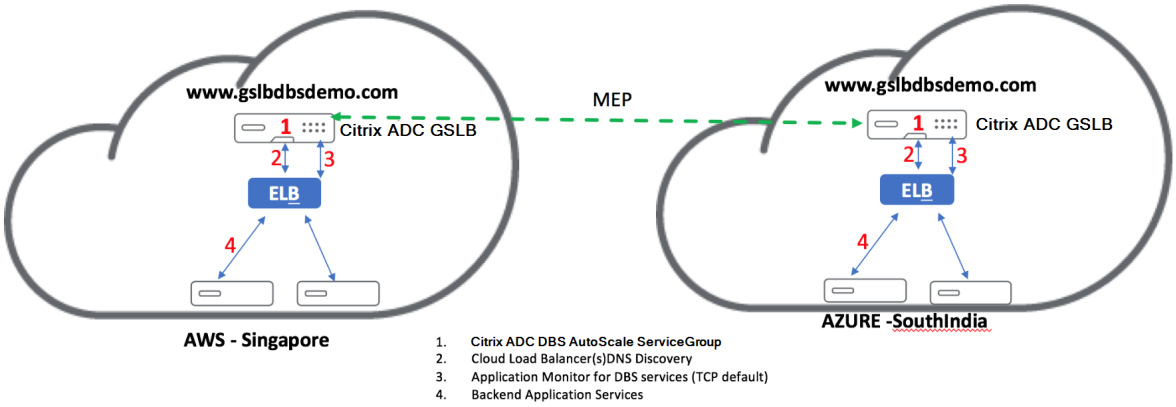
```
1  > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
     amazonaws.com
2  > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney
3  > bind gslb serviceGroup sydney_sg sydney_server 80
4 <!--NeedCopy-->
```

ドメイン名ベースのサービス **— Azure ALB**

GLSB DBS は、Azure ロードバランサーの FQDN を使用して、Azure 内で作成および削除されるバックエンドサーバーを含めるように GSLB サービスグループを動的に更新します。この機能を設定するには, 私たちは、動的に Azure 内の異なるサーバーにルーティングするために私たちの Azure のロードバランサーに Citrix ADC を指します. 私たちは、手動で Citrix ADC を更新することなく、インスタンスが作成され、Azure 内で削除されるたびにこれを行うことができます. GSLB サービスグループ用の Citrix ADC DBS 機能は、DNS 対応のサービス検出を使用して、autoscaler グループで識別される DBS 名前空間のメンバーサービスリソースを判別します。

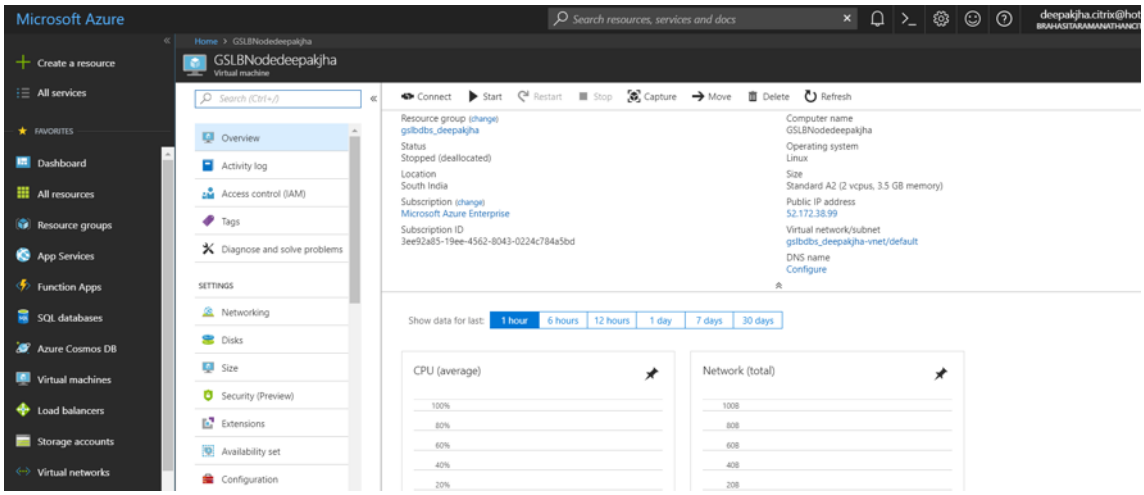
© 1999–2021 Citrix Systems, Inc. All rights reserved.

図：クラウドロードバランサーを使用した **Citrix ADC GSLB DBA** 自動スケーリングコンポーネント



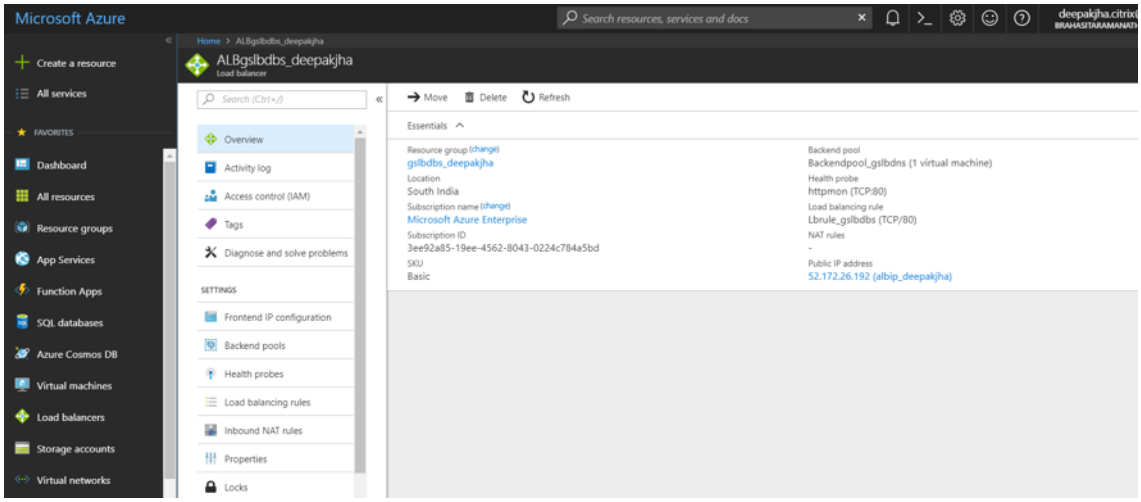
Azure コンポーネントを構成する

1. Azure ポータルにログインし、Citrix ADC テンプレートから新しい仮想マシンを作成します。

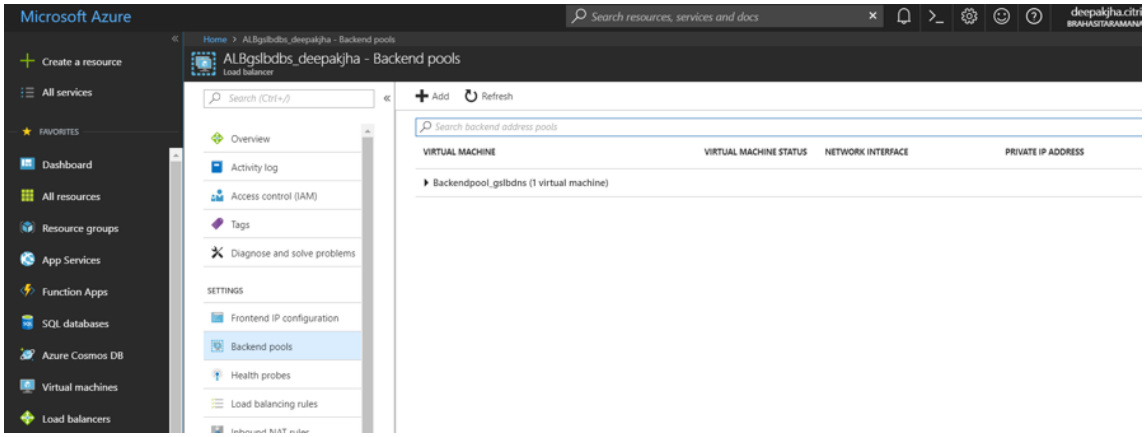


2. Azure ロードバランサーを作成する

© 1999–2021 Citrix Systems, Inc. All rights reserved.



3. 作成した Citrix ADC バックエンドプールの追加

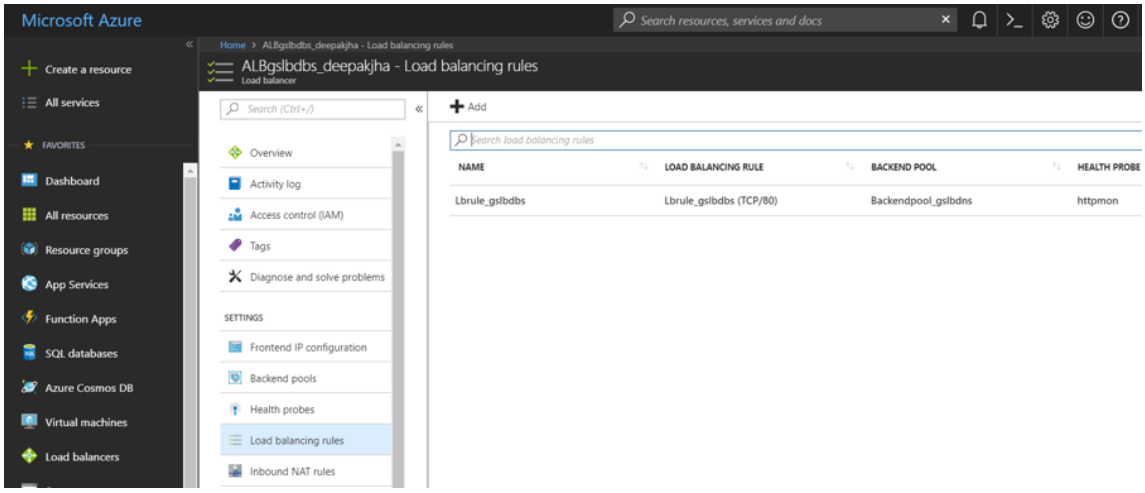


4. ポート 80 のヘルスプローブを作成します。

   ロードバランサから作成されたフロントエンド IP を使用して、ロードバランシングルールを作成します。

   a) プロトコル:TCP
   b) バックエンドポート:80
   c) バックエンドプール: 手順 1 で作成した Citrix ADC
   d) ヘルスプローブ: 手順 4 で作成した
   e) セッションの永続性: なし

© 1999–2021 Citrix Systems, Inc. All rights reserved.



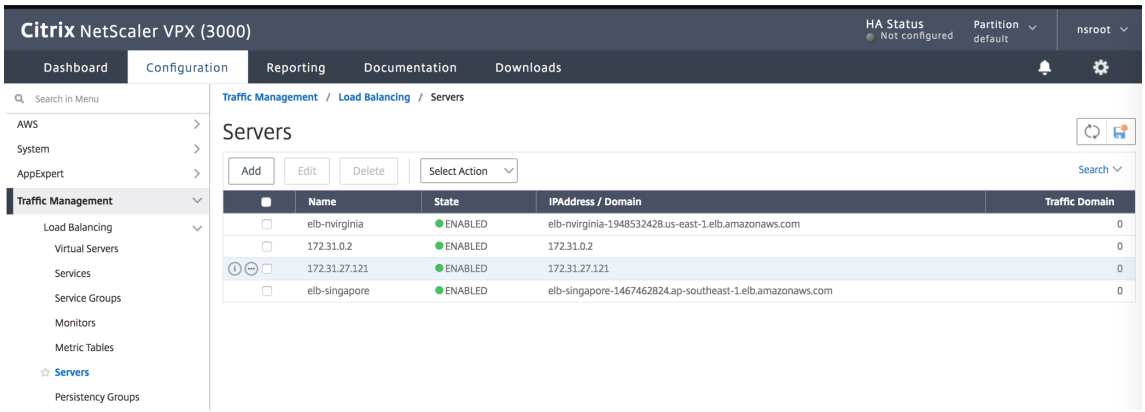
Citrix ADC GSLB ドメインベースのサービスを構成する

以下の構成は、GSLB 対応環境でオートスケーリング ADC のドメインベースのサービスを有効にするために必要なものをまとめたものです。

トラフィック管理の設定

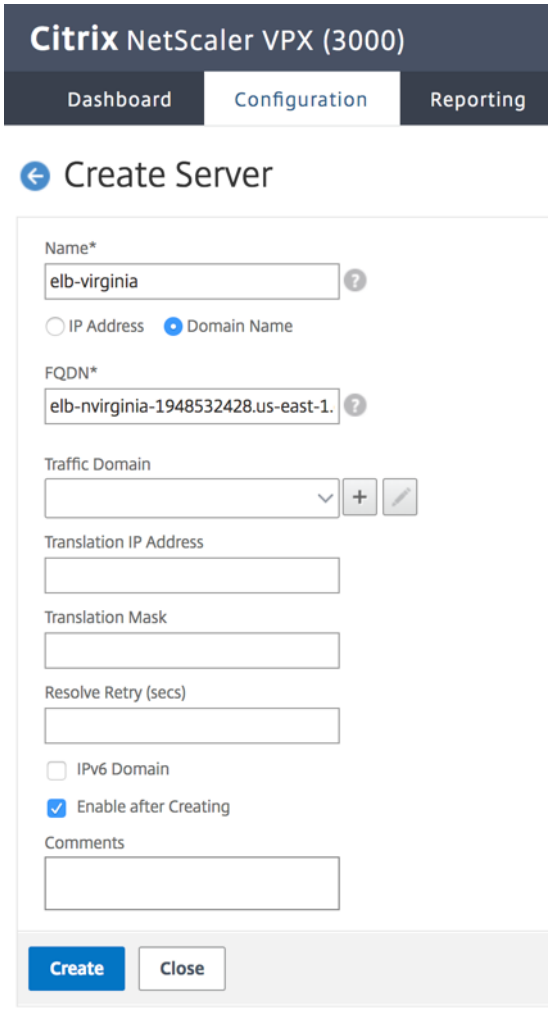
> 注: Citrix ADC には、DBS サービスグループに対して ELB/ALB ドメインが解決されるネームサーバーまたは DNS 仮想サーバーのいずれかを設定する必要があります。

1. 「トラフィック管理」**->**「ロードバランシング」**->**「サーバー」に移動します。



2. [追加] をクリックしてサーバーを作成し、Azure の Azure ロードバランサー (ALB) 用の A レコード (ドメイン名) に対応する名前と FQDN を指定します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



3. 手順 2 を繰り返して、Azure の 2 番目のリソースから 2 番目の ALB を追加します。

GSLB 構成

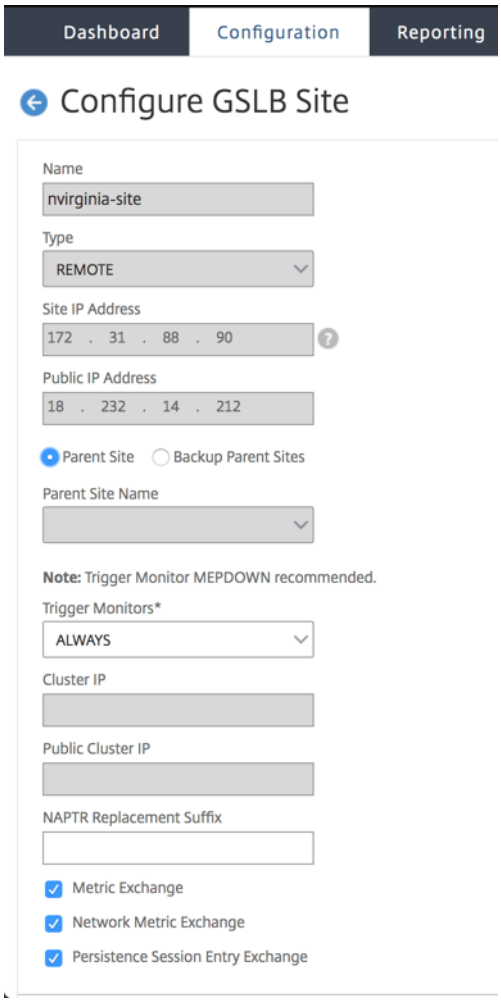
1. [追加] ボタンをクリックして、GSLB サイトを設定します。
2. 「サイト」に名前を付けます。

   [種類] は、サイトを構成している Citrix ADC に基づいて、[リモート] または [ローカル] として構成されます。サイトの IP アドレスは、GSLB サイトの IP アドレスです。GSLB サイトは、この IP アドレスを使用して、他の GSLB サイトと通信します。パブリック IP アドレスは、特定の IP が外部のファイアウォールまたは NAT デバイスでホストされているクラウドサービスを使用する場合に必要です。サイトは親サイトとして構成する必要があります。[トリガーモニター] が [常に] に設定されていることを確認します。また、「メトリック交換」、「ネットワークメトリック交換」、および「持続性セッションエントリ交換」の最下部にある 3 つのチェックボックスをオフにしてください。

   トリガモニタの設定を MEPDOWN に設定することを推奨しています。GSLB サービスグループの設定を参照してください。

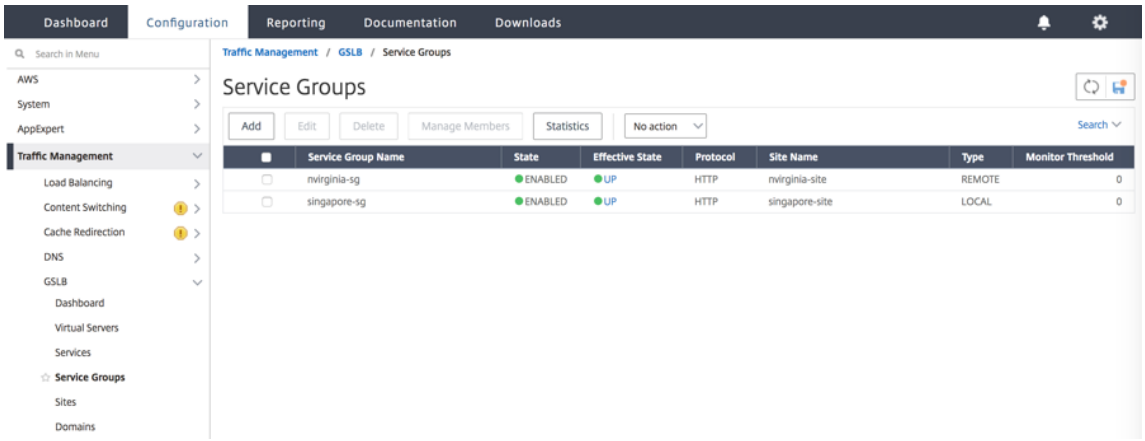
© 1999–2021 Citrix Systems, Inc. All rights reserved.

![image-citrix-adc-and-microsoft-azure-28]/ja-jp/advanced-concepts/media/image-citrix-adc-and-microsoft-azure-28.png)



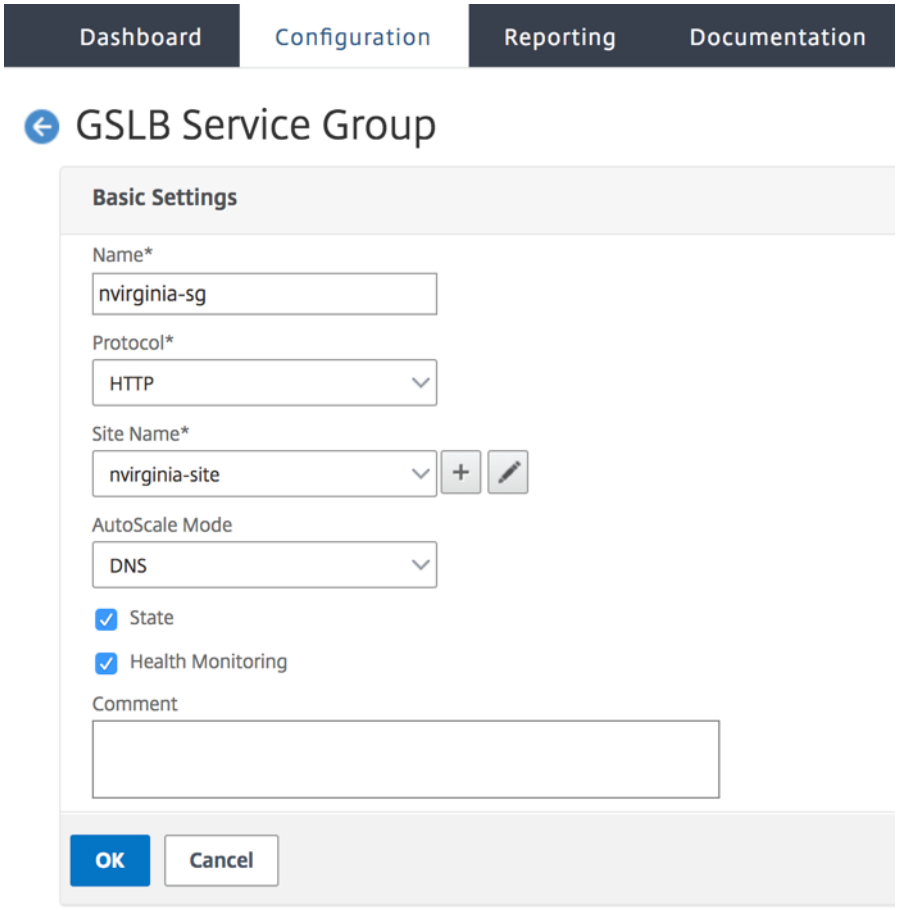
3. [作成] をクリックし、手順 3 と 4 を繰り返して、Azure 内の他のリソースの場所に GSLB サイトを構成します（これは同じ Citrix ADC 上で構成できます）。

4. [トラフィック管理]**-> [GSLB]-> [**サービスグループ] に移動します。



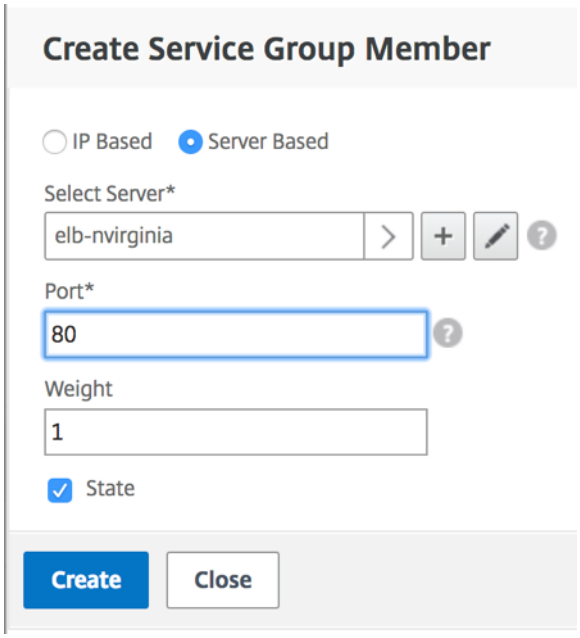
© 1999–2021 Citrix Systems, Inc. All rights reserved.

[**Add**] をクリックして、新しいサービスグループを追加します。サービスグループに名前を付け、HTTP プロトコルを使用し、[サイト名] で、前の手順で作成した各サイトを選択します。必ず自動スケールモードを DNS として設定し、状態およびヘルスモニタリングのチェックボックスをオフにします。[**OK**] をクリックしてサービスグループを作成します。

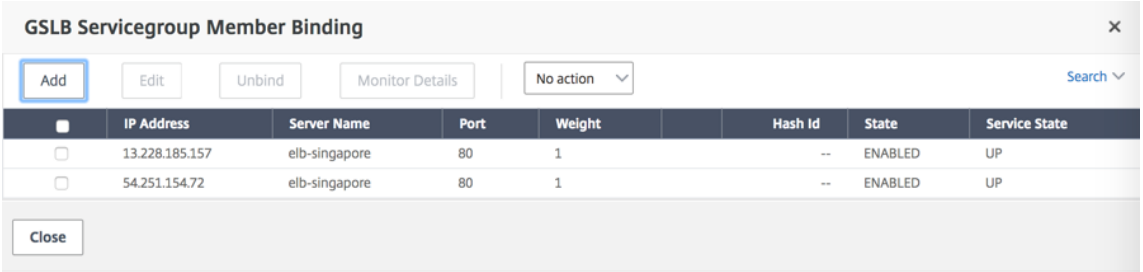


5. **[サービスグループメンバー]** をクリックし、**[サーバーベース]** を選択します。実行ガイドの冒頭で設定した Elastic Load Balancing Server を選択します。トラフィックがポート 80 を通過するように設定します。[作成] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



6. サービスグループメンバーバインディングには、Elastic Load Balancer から受信する 2 つのインスタンスが設定されます。

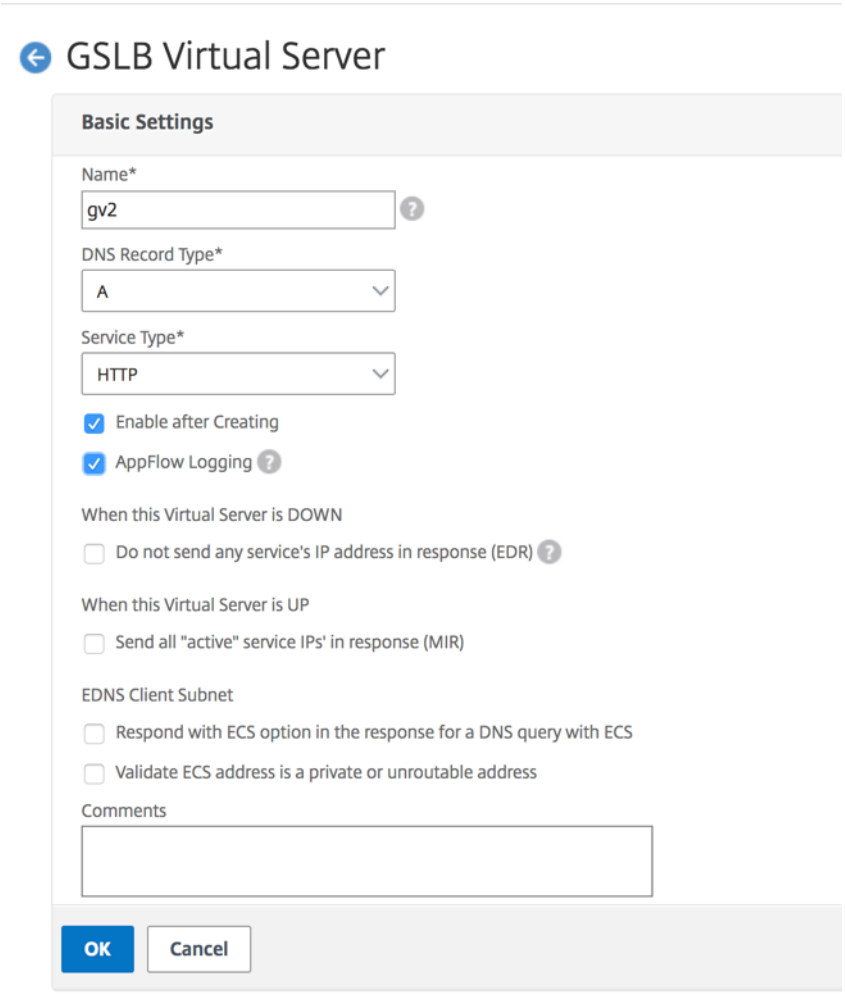


7. 手順 5 と 6 を繰り返して、Azure の 2 番目のリソースの場所にサービスグループを構成します。（これは、同じ Citrix ADC GUI から行うことができます）。

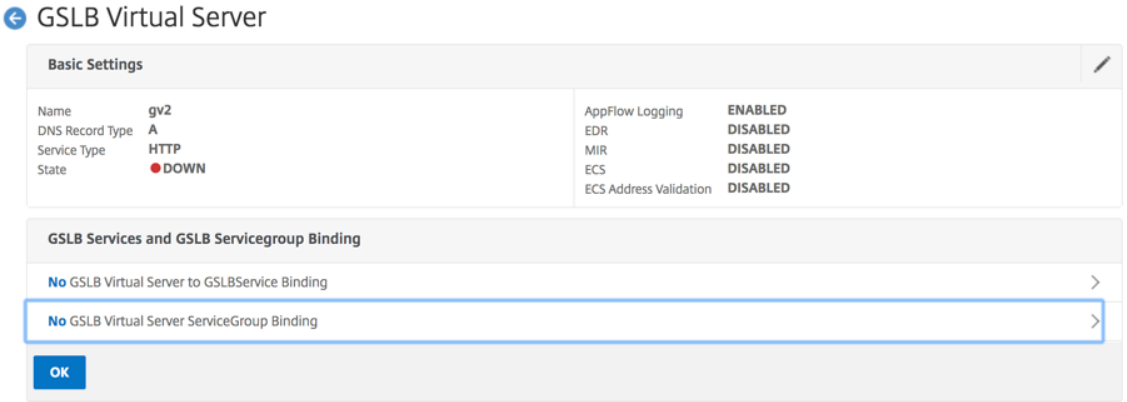
8. 最後のステップは、GSLB 仮想サーバーをセットアップすることです。[トラフィック管理]**-> [GSLB]-> [**仮想サーバー] に移動します。

9. [追加] をクリックして、仮想サーバーを作成します。サーバーの名前を指定し、DNS レコードタイプが A に設定され、サービスタイプが HTTP に設定され、AppFlow ロギングの作成後に有効にするチェックボックスをオンにします。[**OK**] をクリックして、GSLB 仮想サーバーを作成します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

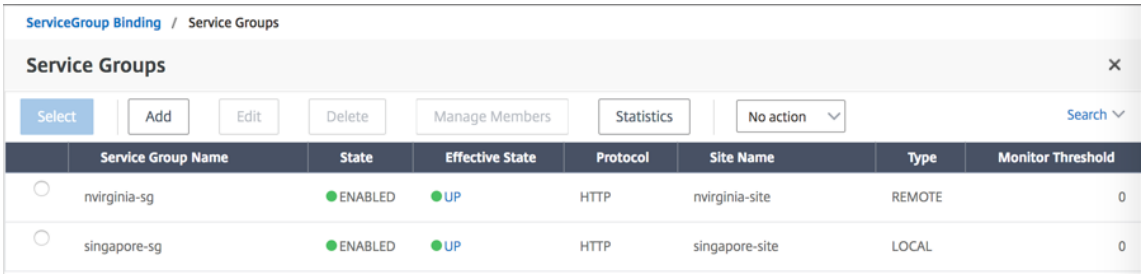


10. GSLB 仮想サーバーが作成されたら、[**GSLB** 仮想サーバーサービスグループバインドなし] をクリックします。

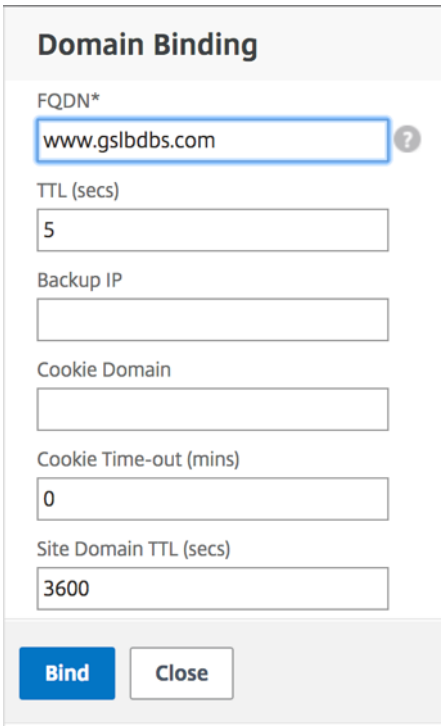


11. [ServiceGroup Binding] で、**[**サービスグループ名の選択**]** を使用して、前の手順で作成したサービスグループを選択して追加します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

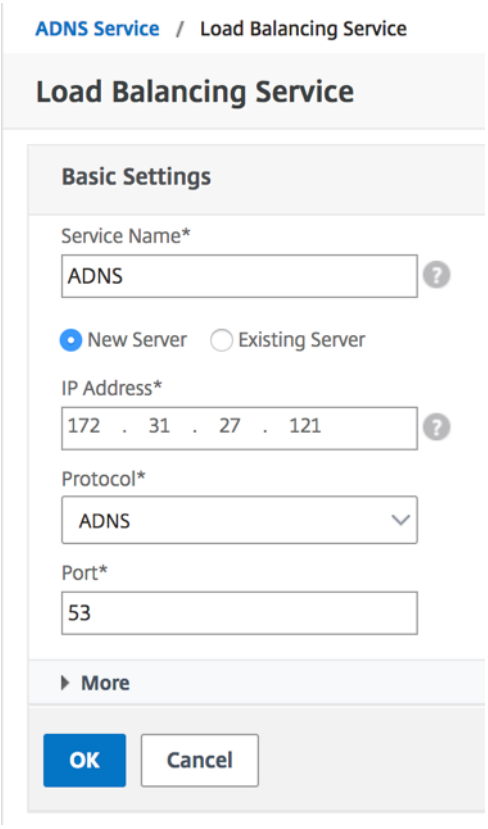


12. 次に、**[GSLB** 仮想サーバードメインバインディングなし**]** をクリックして、GSLB 仮想サーバードメインバインディングを設定します。FQDN とバインドを構成し、残りの設定をデフォルトのままにしておくことができます。

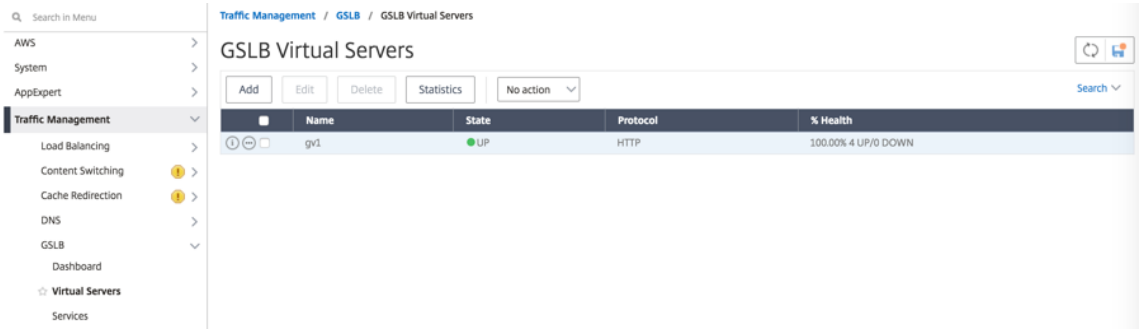


13. [サービスなし] をクリックして、ADNS サービスを構成します。サービス名を追加し、[新しいサーバー] をクリックして、ADNS サーバーの IP アドレスを入力します。さらに、ADNS がすでに構成されている場合は、[既存のサーバー] を選択し、ドロップダウンメニューから ADNS を選択できます。プロトコルが ADNS で、トラフィックがポート 53 経由であることを確認します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



14. 方式を「LEASTONNECTION」、バックアップ方式を「ROUNDROBIN」に設定します。
15. 「完了」をクリックし、GSLB 仮想サーバーが「アップ」と表示されていることを確認します。



Citrix Application Delivery Management 自動スケールグループを使用した **VPX** による **Azure** のフロントエンド自動スケール

オートスケーリングは、実際の使用状況に応じて自動的にリソースを追加または削除するクラウドコンピューティング方法です。自動スケーリングは、クライアント要求または処理ジョブの変動数を満たすために、サイトまたはアプリケーションがオンデマンドのリソース割り当てを必要とする場合に便利です。

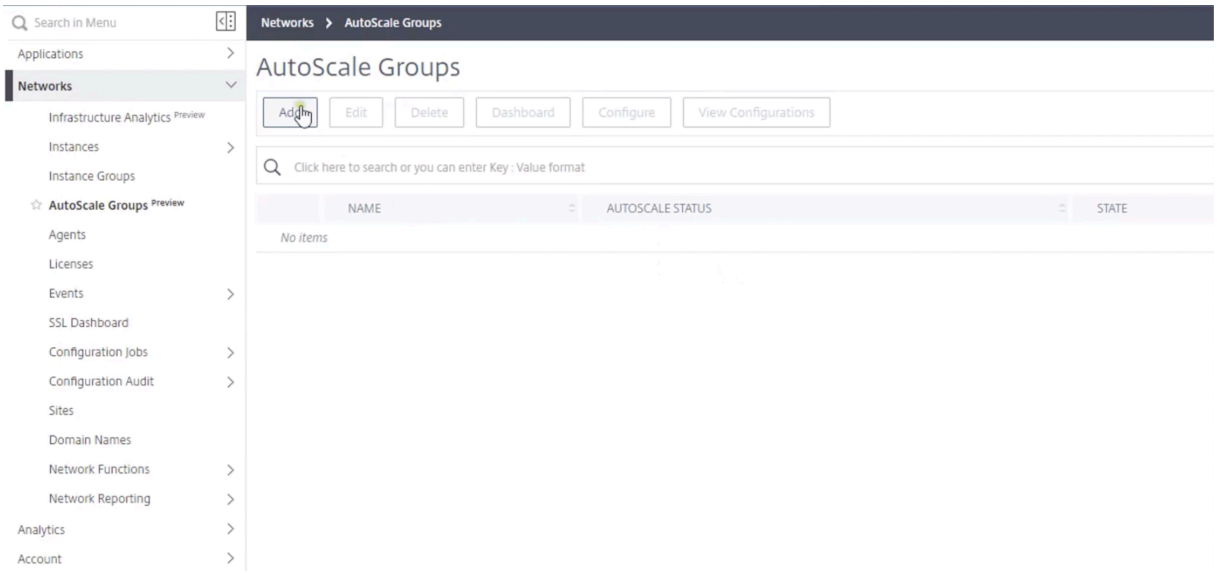
Web アプリケーションやサービスの需要は大きく異なる場合があります。さまざまなトラフィックニーズに合わせて正しい数の Citrix ADC インスタンスを維持することが重要です。需要に応じて、Microsoft Azure のネットワークリソースを増減できます。したがって、パフォーマンスを損なうことなく、コストの最適化を提供します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Application Delivery Management（ADM）オートスケーリングでは、リソースの消費量が変動するため、Citrix ADC インスタンスの正確な数が維持されます。Citrix ADM は、変動するリソース消費量に基づいてトラフィックフローを決定し、Citrix ADC インスタンスを動的にスケールアウトまたはスケールインします。

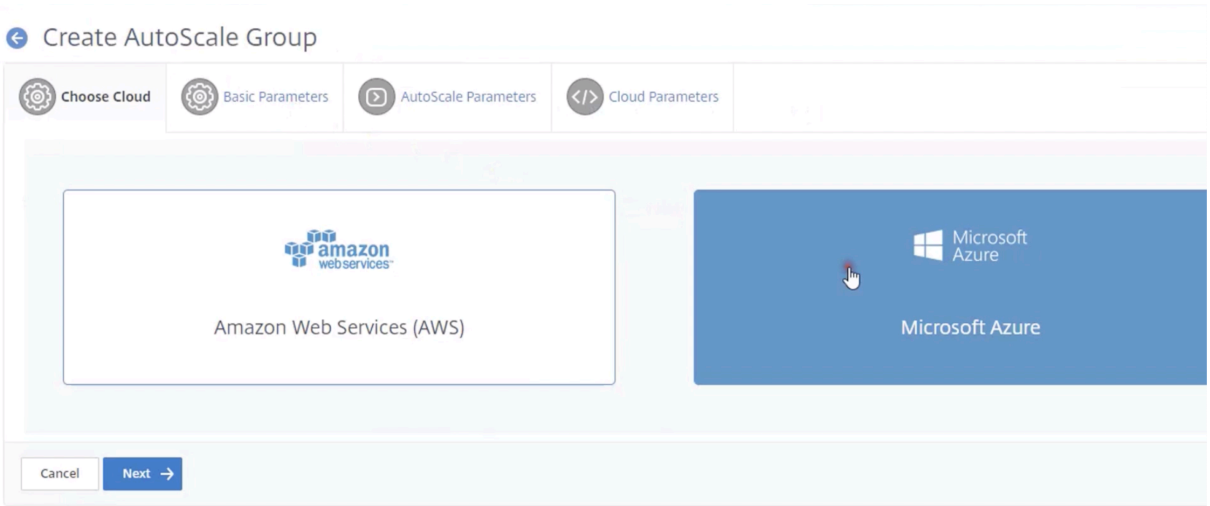
自動スケールグループの作成

- ADC 管理コンソールユーティリティで、**[ネットワーク] > [autoscale]** に移動します。
- ［追加］を選択します。



クラウドの選択

[自動スケールグループの作成] タブで、[**Microsoft Azure**] をクリックし、[追加] をクリックします。

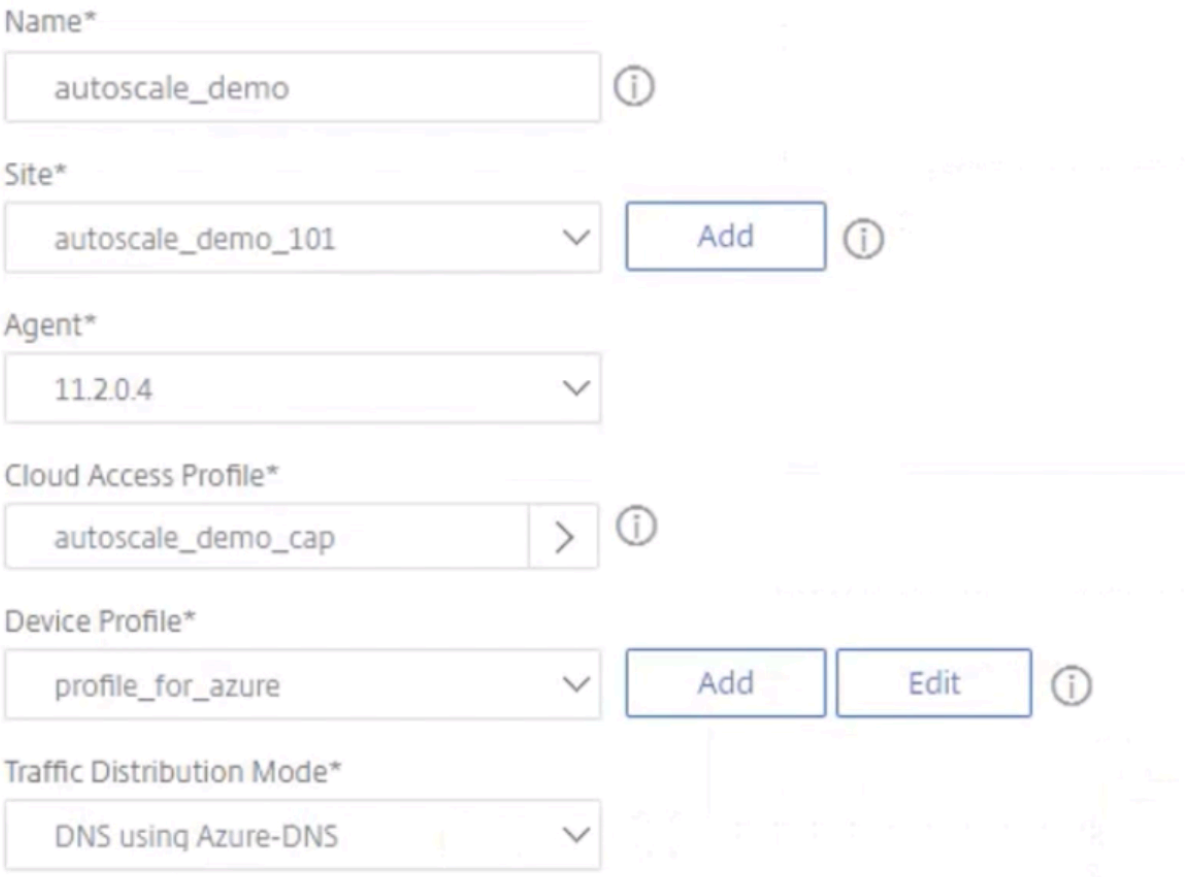


基本パラメータ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

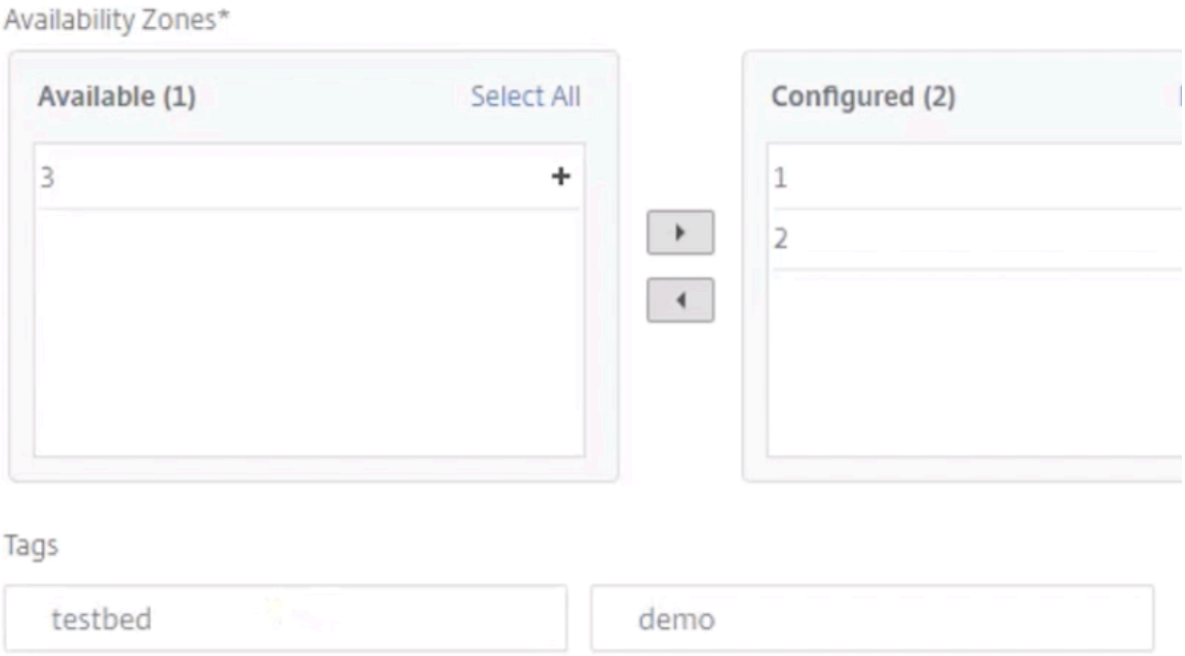
自動スケールグループの基本パラメータを設定します。

1. 名前: autoscale_demo
2. サイト: 自動スケールデモ _101
3. エージェント: 11.2.0.4
4. クラウドアクセスプロファイル: autoscale_demp_cap
5. デバイス: azure のプロファイル
6. トラフィック分散モード： Azure-DNS を使用した DNS



[次へ] は選択しないでください。プラス記号をクリックしてアベイラビリティーゾーン 1 と 2 を追加し、タグを [**Testbed**] に設定します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



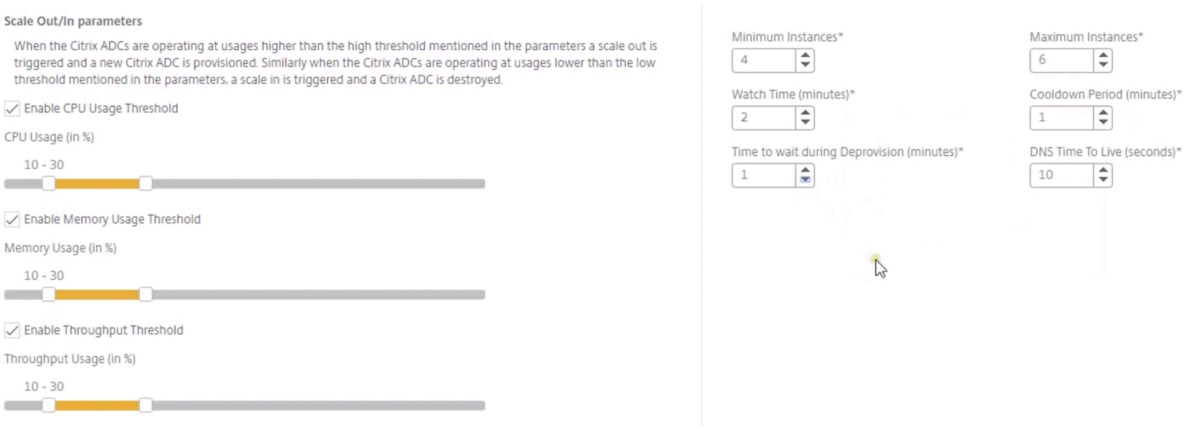
［次へ］をクリックします。

自動スケールパラメータ

自動スケールグループの自動スケールパラメータを構成します。

1. CPU 使用率:10 ～30
2. メモリ使用量:10 ～30
3. スループットの使用量:10 ～30
4. 最小インスタンス:4
5. 最大インスタンス:6
6. 総再生時間:2
7. クールダウン期間:1
8. プロビジョニング解除中の待機時間:1
9. DNS の生存時間:10

© 1999–2021 Citrix Systems, Inc. All rights reserved.



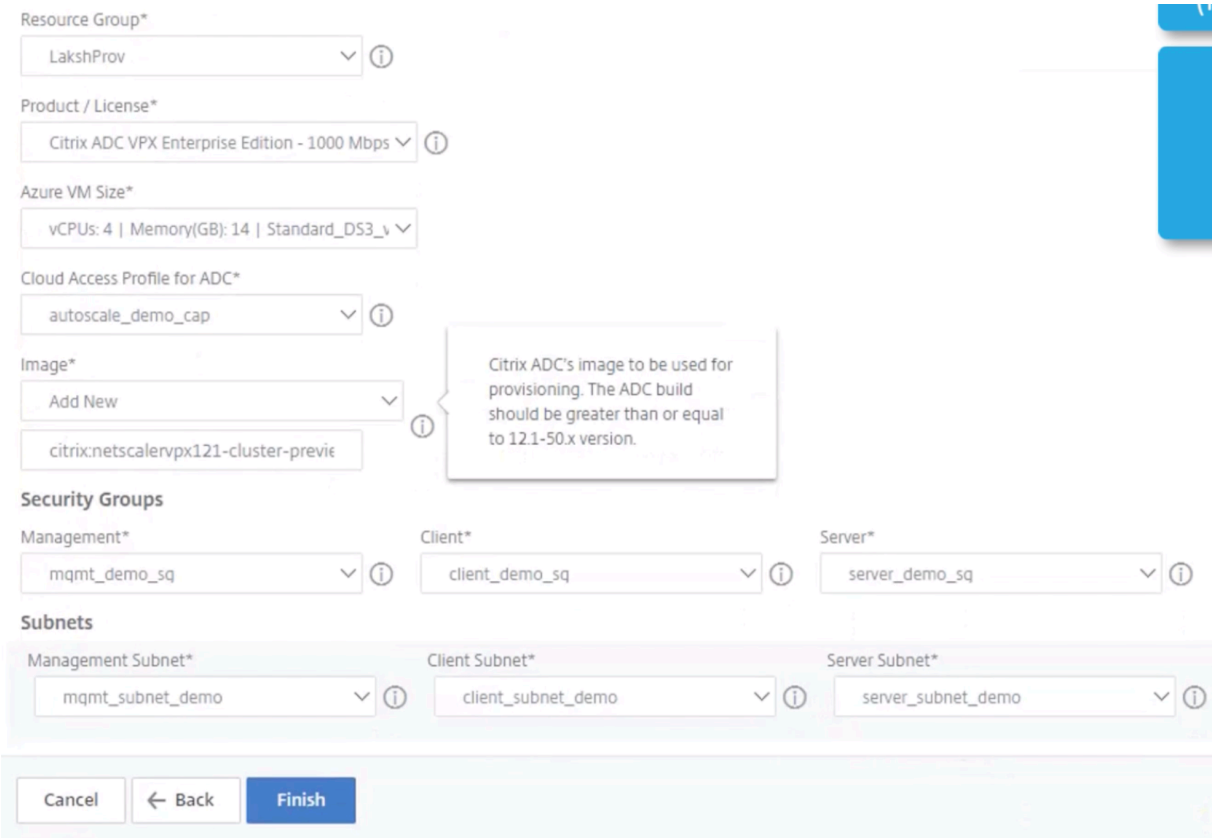
［次へ］をクリックします。

雲のパラメータ

自動スケールグループのクラウドパラメータを設定します。

1. リソースグループ: ラクシュプロブ
2. 製品/ライセンス： シトリックス Citrix ADC VPX エンタープライズエディション-1000 メガビット/秒
3. Azure 仮想マシンサイズ: 仮想 CPU: 4 | メモリ (ギガバイト): 14 | スタンダード DS3_V2
4. ADC のクラウドアクセスプロファイル: 自動スケールデモキャップ
5. イメージ: デフォルト
6. 管理: デモ方程式
7. クライアント: クライアントデモ平方
8. サーバ: サーバデモ平方
9. 管理サブネット:mgmt_subnet_demo
10. クライアントサブネット: クライアントサブネット
11. サーバサブネット： サーバサブネットデモ

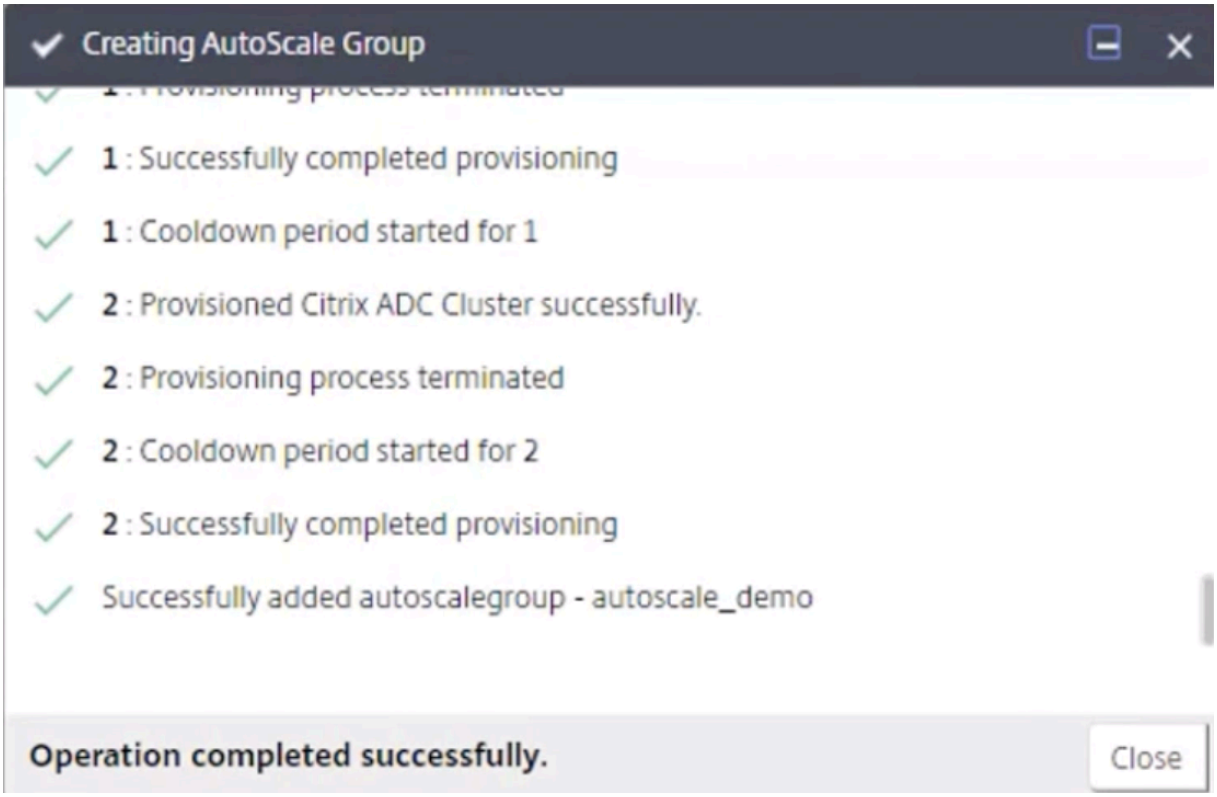
© 1999–2021 Citrix Systems, Inc. All rights reserved.



［次へ］をクリックします。

ダイアログボックスが表示されます。自動スケールグループが正常に作成されていることを確認します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



自動スケールグループの構成

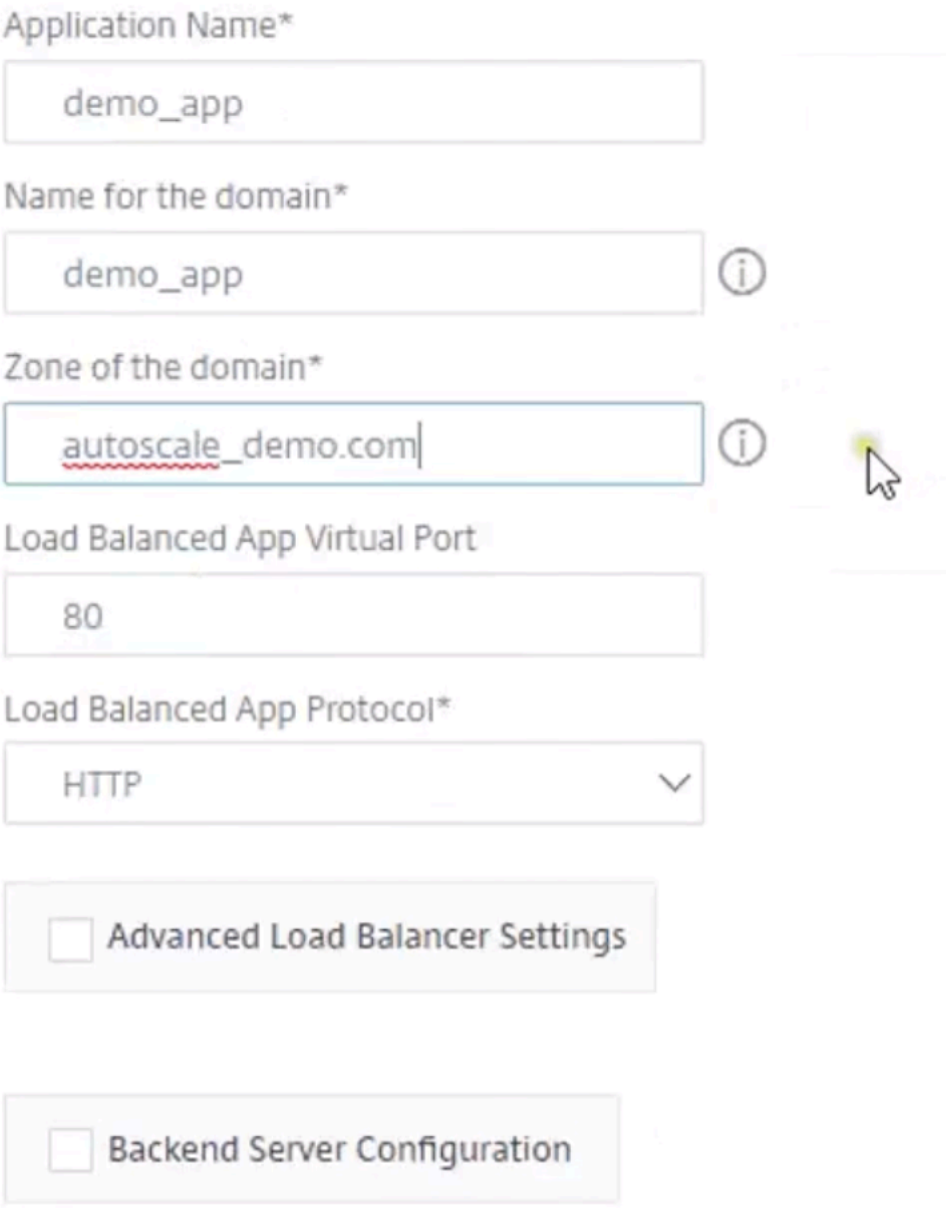
1. ADC 管理コンソールユーティリティで、**[ネットワーク] > [autoscale]** に移動します。
2. 作成した自動スケールを選択し、有効になっていることを確認します。
3. [環境設定] をクリックします。
4.「スタイルブックの選択」ページで、`HTTP/SSL LoadBalancing StyleBook`を選択します。

構成の詳細

StyleBook で作成する構成の詳細を入力します。

1. アプリケーション名:demo_app
2. ドメインの名前:demo_app
3. ドメインのゾーン:
4. 負荷分散アプリケーション仮想ポート:80
5. 負荷分散アプリケーションプロトコル:HTTP

© 1999–2021 Citrix Systems, Inc. All rights reserved.

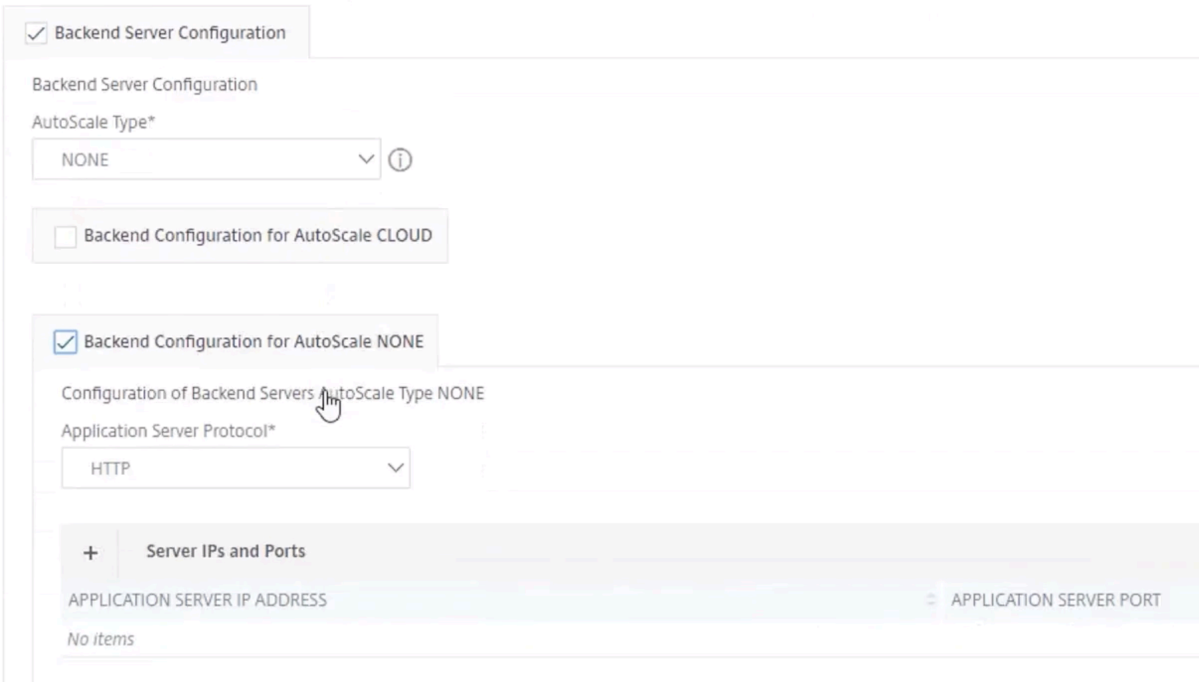


バックエンドサーバの設定をチェックします。

1. 自動スケールタイプ: なし

自動スケーリング **NONE** のバックエンド構成をチェックする

© 1999–2021 Citrix Systems, Inc. All rights reserved.

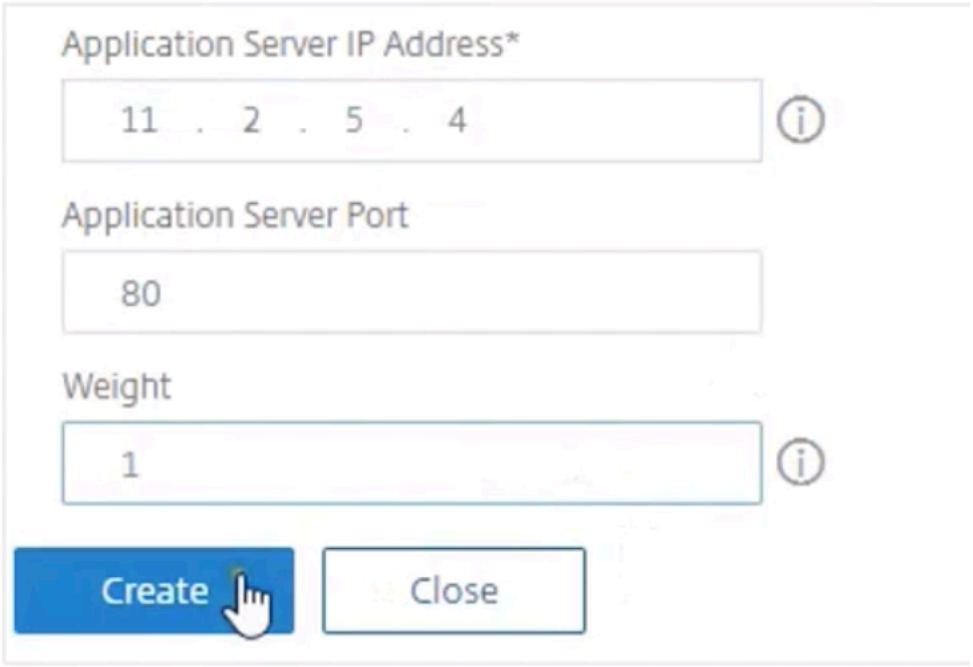


[サーバーの **IP** とポート**]** の横のプラス記号をクリックします。

1. アプリケーションサーバーの IP アドレス:11.2.5.4
2. アプリケーションサーバーポート:80
3. Weight: 1

［作成］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

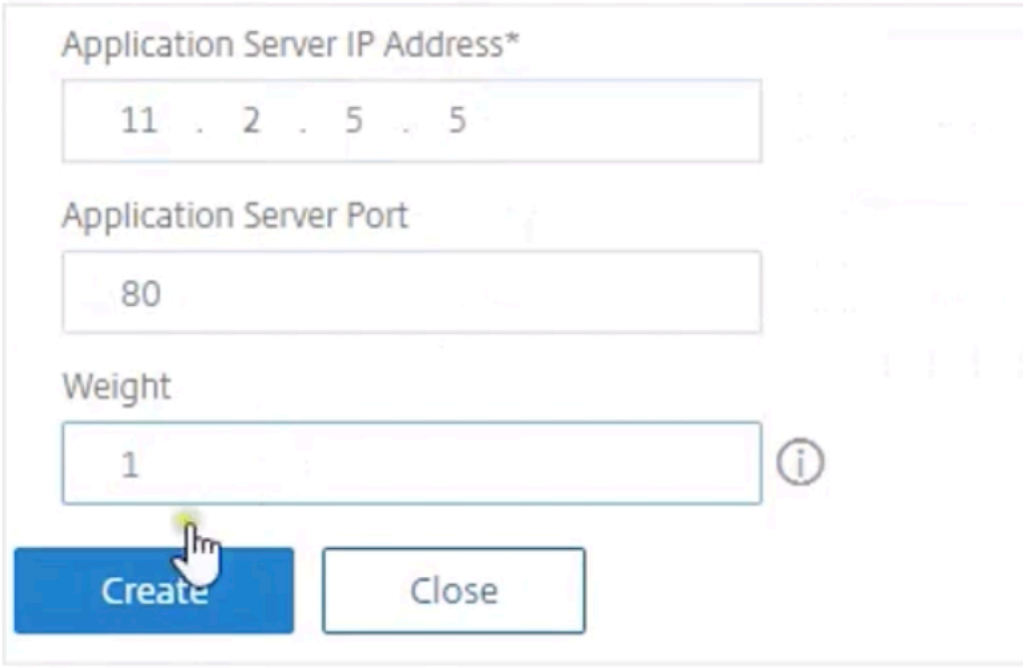


前の手順を繰り返します。

1. アプリケーションサーバーの IP アドレス:11.2.5.5
2. アプリケーションサーバーポート:80
3. Weight: 1

［作成］をクリックします。

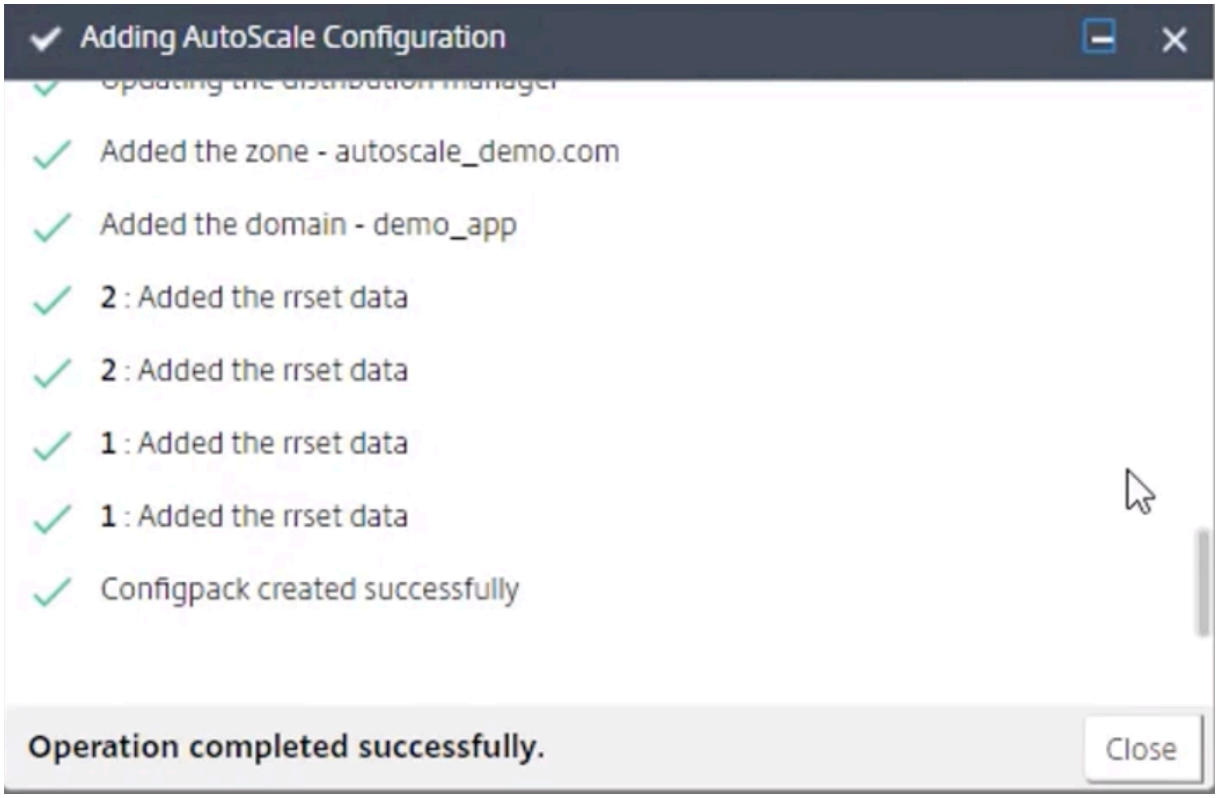
© 1999–2021 Citrix Systems, Inc. All rights reserved.



StyleBook のメイン構成ページで、「作成」をクリックします。

ダイアログボックスが表示されます。StyleBook 構成が正常に作成されていることを確認します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



その他の参考資料

Microsoft Azure で Citrix ADC VPC インスタンスを展開する

Microsoft Azure ドキュメント

PowerShell を使用して仮想マシンに複数の IP アドレスを割り当てる

PowerShell を使用して複数の NIC を持つ仮想マシンを作成する

Azure パブリッククラウドで Citrix ADC VPX を使用してバックエンドサービス仮想マシンを自動スケールする

Citrix 製品マニュアル

Citrix ADC VPX スタンドアロンインスタンスの複数の IP アドレスを構成する

PowerShell コマンドを使用して、スタンドアロンモードで Citrix ADC VPX インスタンスの複数の IP アドレスを構成する

スタンドアロン VPX インスタンス用に複数の Azure VIP を構成する

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC CPX、Citrix Ingress Controller,、および Google クラウドでの Application Delivery Management

March 2, 2021

GCP K8 のアーキテクチャとコンポーネントに関する Citrix 製品の概要

GCP の 5 つの主要な Citrix コンポーネント

1. 入力ベースのインターネットクライアントトラフィック用の **Tier-1ADC** としての **Citrix ADC VPX** です。

   GCP の VPX インスタンスを使用すると、GCP コンピューティング機能を活用し、ビジネスニーズに合わせて Citrix の負荷分散機能とトラフィック管理機能を使用できます。GCP で VPX をスタンドアロンインスタンスとして展開できます。単一および複数のネットワークインターフェイスカード (NIC) 構成がサポートされています。

2. **Google Kubernetes** エンジン **(GKE)** を使用してコンテナプラットフォームを形成する **Kubernetes** クラスターです。

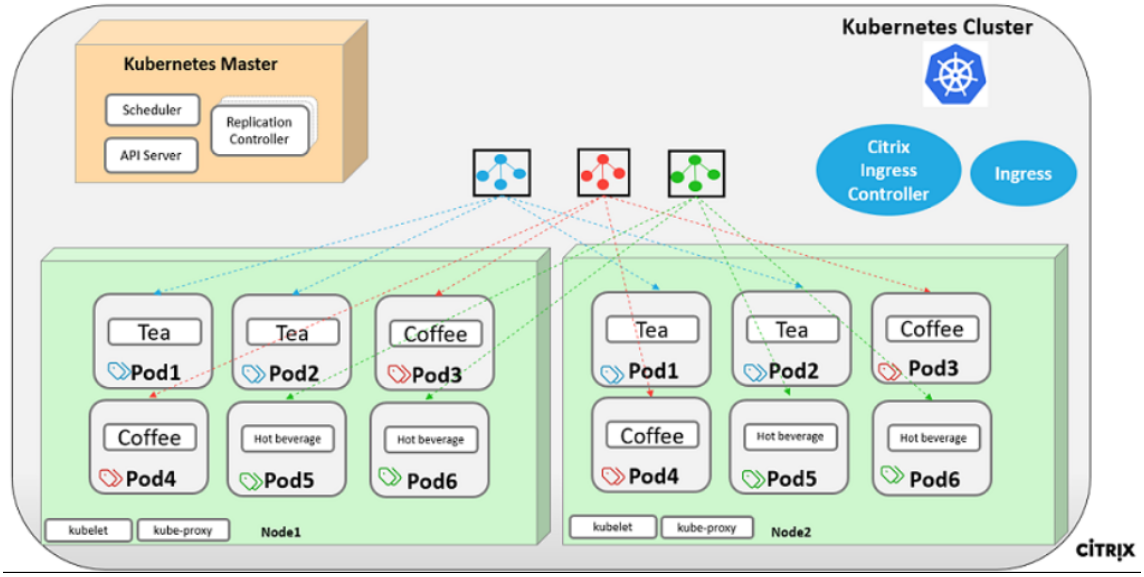
   Kubernetes Engine は、コンテナ化されたアプリケーションを展開するための、マネージド型の実稼働対応環境です。これにより、アプリケーションとサービスの迅速な展開と管理が可能になります。

3. **YAML** ファイルライブラリを使用して、サンプルの **Citrix Web** アプリケーションを展開します。

   Citrix は、GCP で 2 層アプリケーショントポロジをテストするためのサンプルマイクロサービス Web アプリケーションを提供しています。また、概念実証のために、サンプルファイルには次のコンポーネントも含まれています。

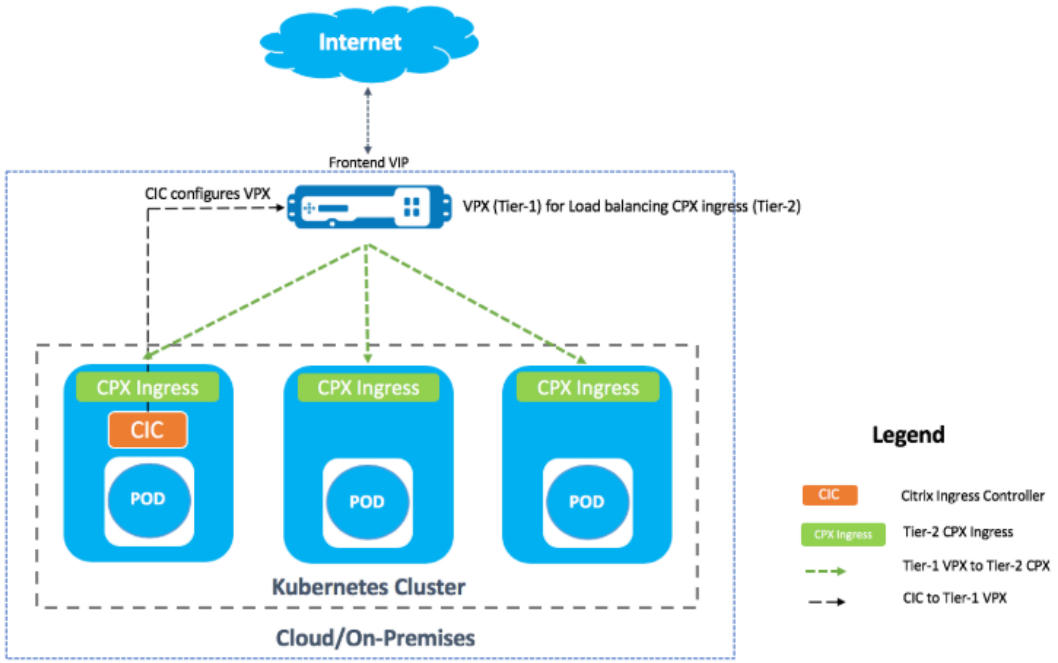
   - Kubernetes YAML ファイルのホットドリンク Web サービスのサンプル
   - クベルネスの YAML ファイル内のコールドドリンク Web サービスの例
   - Kubernetes YAML ファイルのゲストブックウェブサービスの例
   - Kubernetes YAML ファイルの Grafana チャートサービスの例
   - Kubernetes YAML ファイルの Prometheus のログサービスのサンプル

© 1999–2021 Citrix Systems, Inc. All rights reserved.



4. **Tier1 Citrix ADC** オートメーション用の **Citrix Ingress Controller** を **GKE** クラスターに展開します。

   Kubernetes を中心に構築された Citrix Ingress Controller は、入力リソース構成に基づいて 1 つまたは複数の Citrix ADC を自動的に構成します。Ingress Controller は、Kubernetes API サーバーが入力リソースの更新を監視し、それに応じて入力ロードバランサーを再設定するコントローラーです。Citrix Ingress Controller は、YAML ファイルを使用して直接展開することも、Helm チャートを使用して展開することもできます。



   Citrix は、Tier 1 の VPX インスタンスの Citrix Ingress Controller 自動化のためのサンプル YAML ファイルを提供しています。これらのファイルは、Tier 1 VPX 上の以下の構成を自動化します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- ポリシーとアクションの書き換え
- レスポンダーのポリシーとアクション
- コンテンツスイッチ URL ルール
- CPX ロードバランシングサービスの追加/削除

GCP 用の Citrix ingress Controller YAML ファイルは、次の場所にあります: https://github.com/citrix/example-cpx-vpx-for-kubernetes-2-tier-microservices/tree/master/gcp

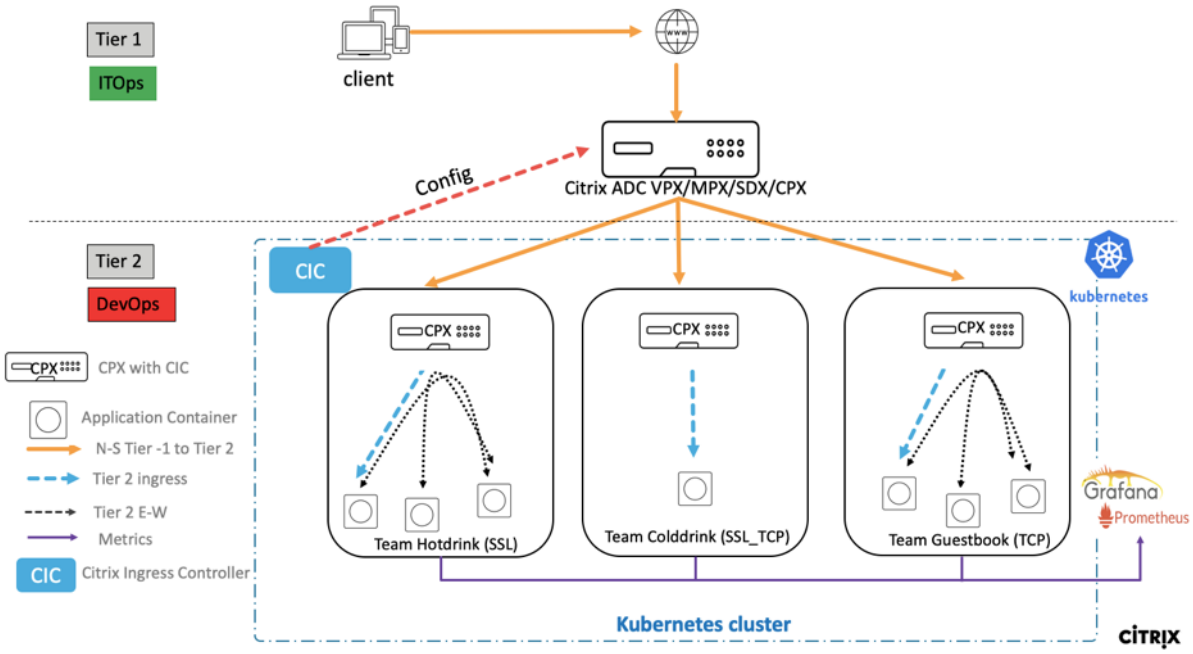
GCP での 2 層入力展開

デュアルティアの入力環境では、Citrix ADC VPX/MPX を Kubernetes クラスター（Tier 1）の外側に配置し、Citrix ADC CPX を Kubernetes クラスター（Tier 2）内に展開します。

Tier 1 の VPX/MPX は、Kubernetes クラスター内の Tier 2 の CPX を負荷分散します。これは、Google クラウド、Amazon Web Services、Azure、オンプレミスの展開のいずれであっても、プラットフォームに広く従う汎用展開モデルです。

Tier 1 の VPX/MPX の自動化

Tier 1 VPX/MPX は、Tier 2 CPX を自動的にロードバランシングします。Citrix Ingress Controller は、Kubernetes クラスター内でポッドとして実行することで、自動化構成を完了します。構成が他の入力リソースと重複しないように、Tier 1 VPX/MPX に対して個別の入力クラスを設定します。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix 展開の概要

GCP での Tier 1 の Citrix ADC のインストールと構成

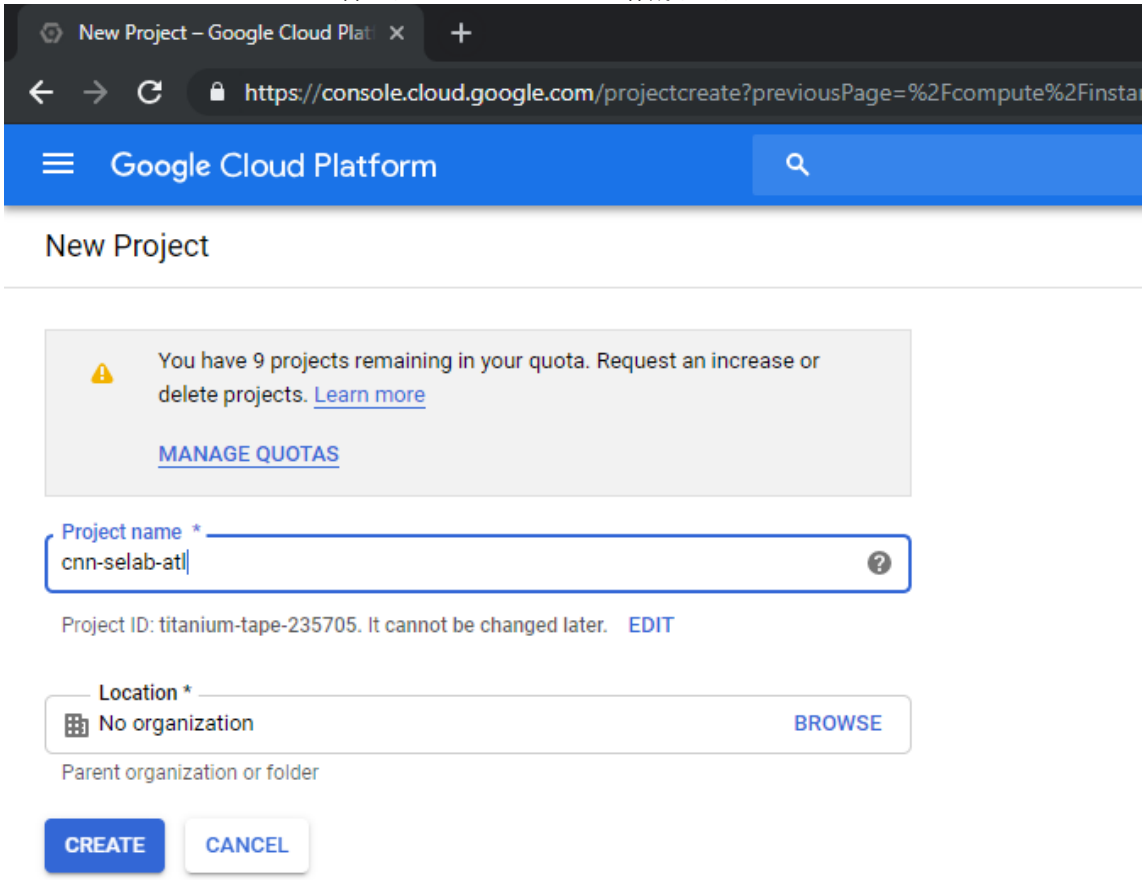
以下のいずれかを使用して、Citrix ADC を展開できます。

- **Google Cloud Platform GUI:** GUI を使用して Google Cloud Platform 上の階層 1 の Citrix ADC を構成する方法については、「Citrix ADC VPX インスタンスの展開」を参照してください。
- **Google Deployment Manager:** GDM テンプレートを使用して Google Cloud Platform 上の階層 1 の Citrix ADC を設定する方法については、「GDM テンプレートを使用して Citrix ADC VPX インスタンスを展開する」を参照してください。

これで、3-NIC GDM テンプレートを使用して Citrix VPX（teir-1-adc）を展開する必要があります。

前提条件（必須）:

1. Citrix メール ID のみを使用して GCP アカウントを作成する。http://console.cloud.google.com
2. GCP コンソールでプロジェクト名として cnn-selab-atl を作成します:



3. デバイスにgcloudユーティリティをインストールします。次のリンクをクリックして、ユーティリティを見つけます：https://cloud.google.com/sdk/install。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

4. gcloud API の gcloud 認証 ログインを使用して、**Google** アカウントに認証します.
5. クライアントに kubectl をインストールします: https://kubernetes.io/docs/tasks/tools/install-kubectl/
6. gcloudユーティリティで次のコマンドを実行して、イメージを作成します。

```
gcloud compute images create netscaler12-1 --source-uri=gs://tme-cpx-storage/NSVPX-GCP-12.1-50.28_nc.tar.gz --guest-os-features=MULTI_IP_SUBNET
<!--NeedCopy-->
```

イメージが作成されるまで少し時間がかかる場合があります。イメージが作成されると、GCP コンソールの [** コンピューティング] > [コンピュートエンジン **] の下に表示されます。

GCP に Citrix VPX（tier-1-adc）を展開する

1. **GCP VPC** インスタンス**:**
   セキュリティ上の目的で、外部、内部、および DMZ ネットワークの分離に対処します。次の表に示すように、3 つの NIC を作成する必要があります。

ネットワーク	コメント
192.168.10.0/24	管理ネットワーク（vpx-snet-管理）
172.16.10.0/24	クライアントネットワーク（vpx-snet-vip）
10.10.10.0/24	サーバネットワーク（vpx-snet-snip）

> 注:
>
> VM インスタンスを展開する前に、3 アームネットワーク VPC を構築します。

VPC は、gcloud API を使用して SDK で作成することも、gcloud API によって Google Cloud Platform コンソール VPC を使用して作成することもできます

VPC by gcloud API

管理トラフィックまたは NSIP トラフィック用の VPC を作成する

```
gcloud compute --project=cnn-selab-atl networks create vpx-snet-mgmt --subnet-mode=custom
gcloud compute --project=cnn-selab-atl networks subnets create vpx-snet-mgmt --network=vpx-snet-mgmt --region=us-east1 --range=192.168.10.0/24
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クライアントまたは VIP トラフィック用の VPC を作成する

```
gcloud compute --project=cnn-selab-atl networks create vpx-snet-vip --subnet-mode=custom
gcloud compute --project=cnn-selab-atl networks subnets create vpx-snet-vip --network=vpx-snet-vip --region=us-east1 --range=172.16.10.0/24
<!--NeedCopy-->
```

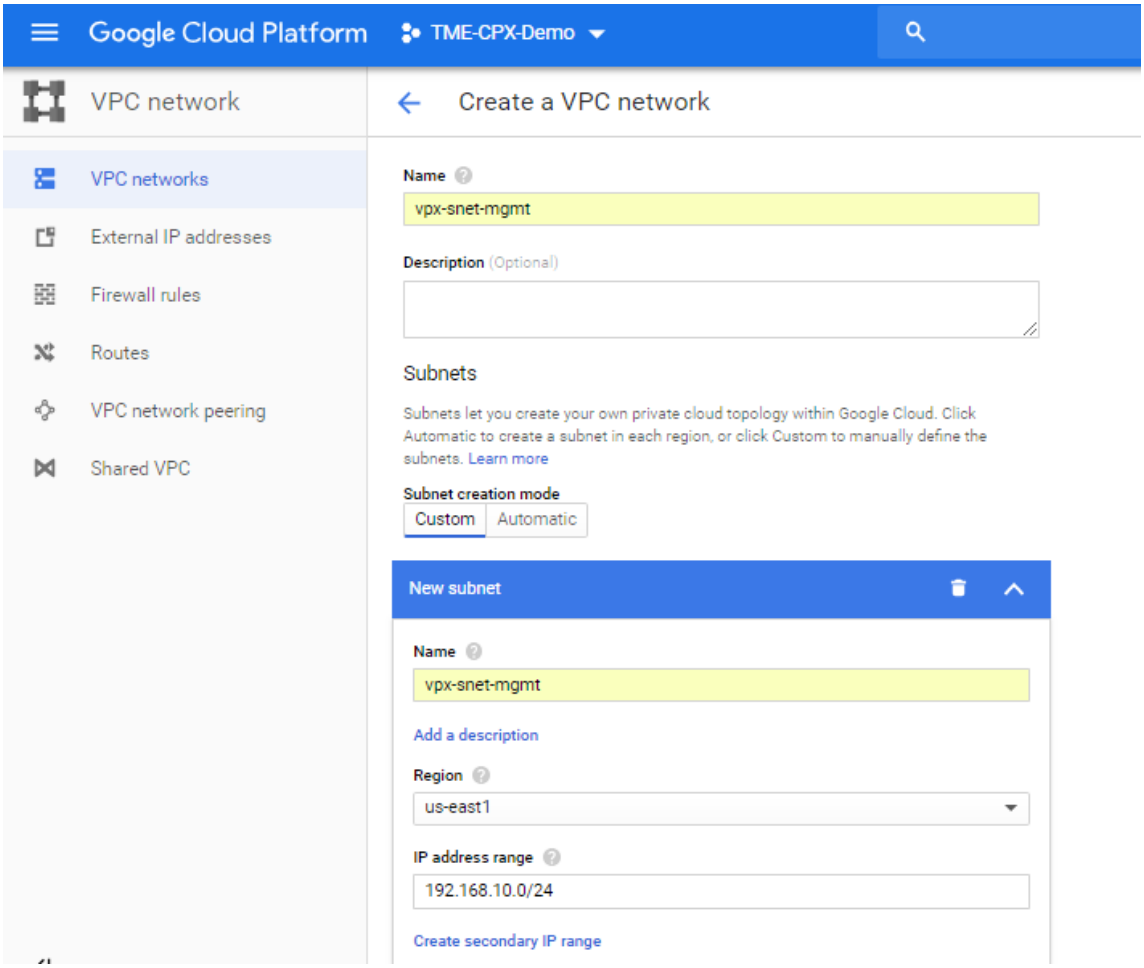
kubernetes クラスターをホストするサーバーまたは SNIP トラフィック用の VPC を作成する

```
gcloud compute --project=cnn-selab-atl networks create vpx-snet-snip --subnet-mode=custom
gcloud compute --project=cnn-selab-atl networks subnets create vpx-snet-snip --network=vpx-snet-snip --region=us-east1 --range=10.10.10.0/24
<!--NeedCopy-->
```

GCP GUI コンソールによる ***VPC***

Google コンソールから、**[**ネットワーク**] > [VPC** ネットワーク**] > [VPC** ネットワークを作成**]** を選択し、次に示すように必須フィールドを入力します。次に、[作成] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



同様に、クライアント側とサーバー側の NIC 用の VPC ネットワークを作成して、3 つのサブネットを作成します。

> 注:
>
> 3 つの VPC ネットワークはすべて同じリージョンに存在する必要があります。このシナリオでは us-east1 です。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

VPC networks　CREATE VPC NETWORK　REFRESH

Name	Region	Subnets	Mode	IP addresses ranges	Gateways
vpx-snet-vip		1	Custom		
	us-east1	vpx-snet-vip		172.16.10.0/24	172.16.10.1
vpx-snet-snip		1	Custom		
	us-east1	vpx-snet-snip		10.10.10.0/24	10.10.10.1
vpx-snet-mgmt		1	Custom		
	us-east1	vpx-snet-mgmt		192.168.10.0/24	192.168.10.1

2. **VPC** ネットワークで 3 つのネットワークと 3 つのサブネットを作成したら、GDM テンプレートを使用して Citrix ADC VPX インスタンスを展開します。**configuration.yml** と **template.py** の両方が同じフォルダまたはディレクトリにあることを確認してください。Google SDK から次のコマンドを使用して、インスタンスを展開します。

```
1  gcloud deployment-manager deployments create tier1-vpx --config
       configuration.yml
2  <!--NeedCopy-->
```

3. 展開が正常に完了したら、コンピュートエンジンに移動して **citrix-adc-tier1-vpx** セクションを確認し、内部 IP を検証します。

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	vpx-snet-mgmt	vpx-snet-mgmt	192.168.10.20	—	static-external-mgmt-ip-tier1-vpx (35.196.91.86)
nic1	vpx-snet-vip	vpx-snet-vip	172.16.10.20	—	static-external-traffic-ip-tier1-vpx (34.73.141.54)
nic2	vpx-snet-snip	vpx-snet-snip	10.10.10.20	—	None

Citrix Ingress Controller は、Tier 1 VPX の静的ルート設定を自動化できます。Kubernetes クラスターと同じサ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ブネット/仮想プライベートクラウドのサブネット IP (SNIP) アドレスを設定します。

> 注:
>
> 展開された Tier 1 VPX/MPX は、Kubernetes クラスター内の CPX の負荷分散を行います。Tier 1 VPX で SNIP を構成します。

Tier 1 VPX 上の PuTTY セッションから次のコマンドを実行して、SNIP を追加し、SNIP への管理アクセスを有効にします。

```
clear config -force full
add ns ip 10.10.10.20 255.255.255.0 -type snip -mgmt enabled
enable ns mode mbf
<!--NeedCopy-->
```

GKE を使用して **Kubernetes** クラスターを展開する

一つは、***Google*** クラウド ***SDK*** または ***Google Cloud Platform GUI*** コンソールを介してのいずれか Kubernetes クラスターを展開することができます。

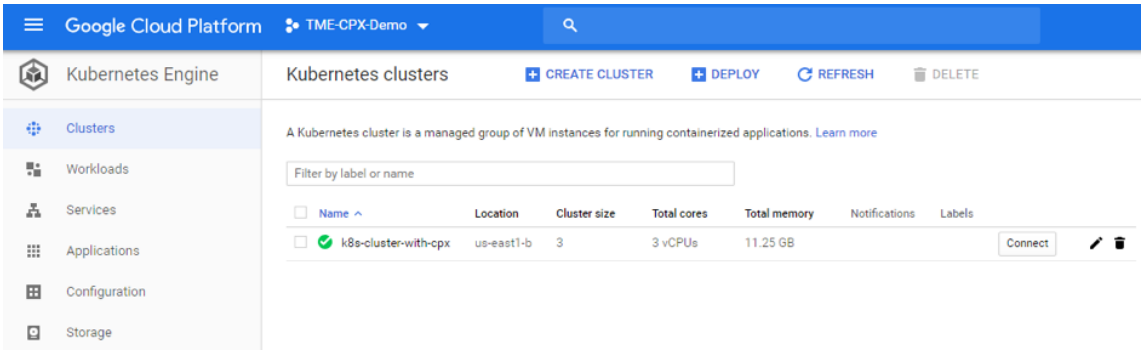
K8s クラスターを作成するための **Gcloud API** コマンド

```
gcloud beta container --project "cnn-selab-atl" clusters create "k8s-
    cluster-with-cpx" --zone "us-east1-b" --username "admin" --cluster-
    version "1.11.7-gke.12" --machine-type "n1-standard-1" --image-type
    "COS" --disk-type "pd-standard" --disk-size "100" --scopes "https://
    www.googleapis.com/auth/devstorage.read_only","https://www.
    googleapis.com/auth/logging.write","https://www.googleapis.com/auth/
    monitoring","https://www.googleapis.com/auth/servicecontrol","https
    ://www.googleapis.com/auth/service.management.readonly","https://www
    .googleapis.com/auth/trace.append" --num-nodes "3" --enable-cloud-
    logging --enable-cloud-monitoring --no-enable-ip-alias --network "
    projects/cnn-selab-atl/global/networks/vpx-snet-snip" --subnetwork "
    projects/cnn-selab-atl/regions/us-east1/subnetworks/vpx-snet-snip"
    --addons HorizontalPodAutoscaling,HttpLoadBalancing --enable-
    autoupgrade --enable-autorepair
<!--NeedCopy-->
```

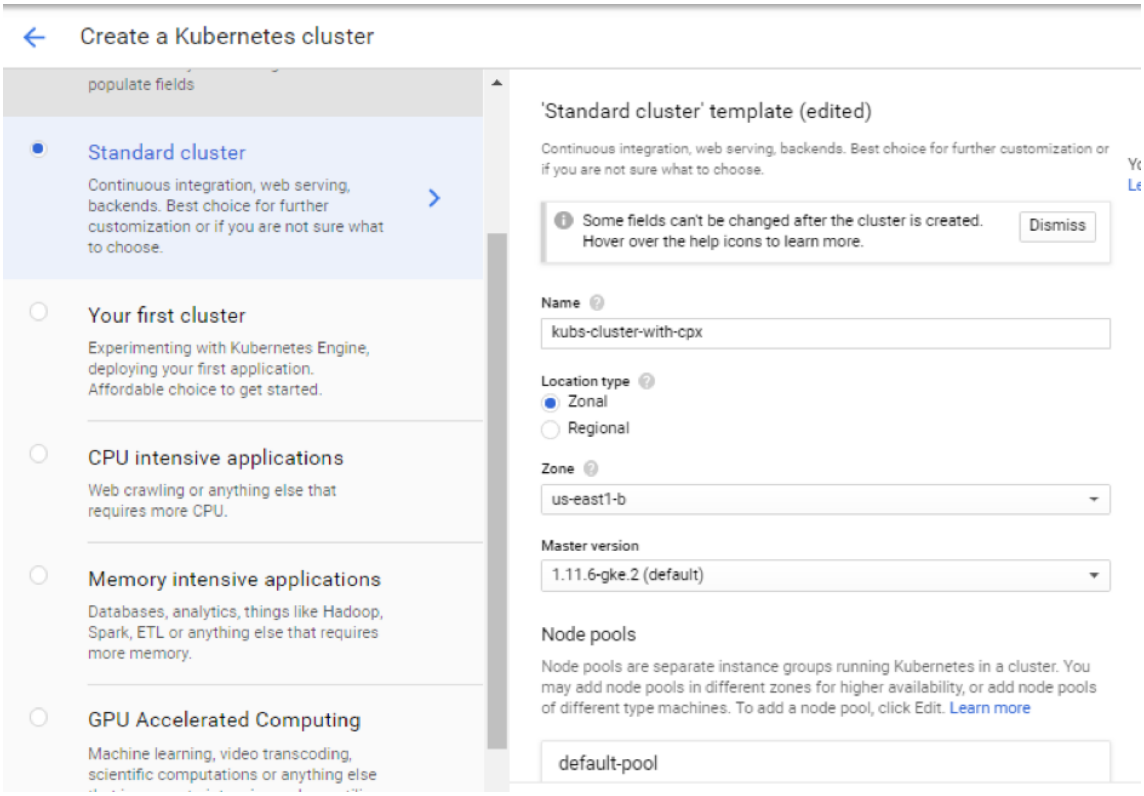
Google Cloud Platform GUI コンソールの手順

1. GCP コンソールで Kubernetes エンジンを検索し、[クラスターの作成] をクリックします。

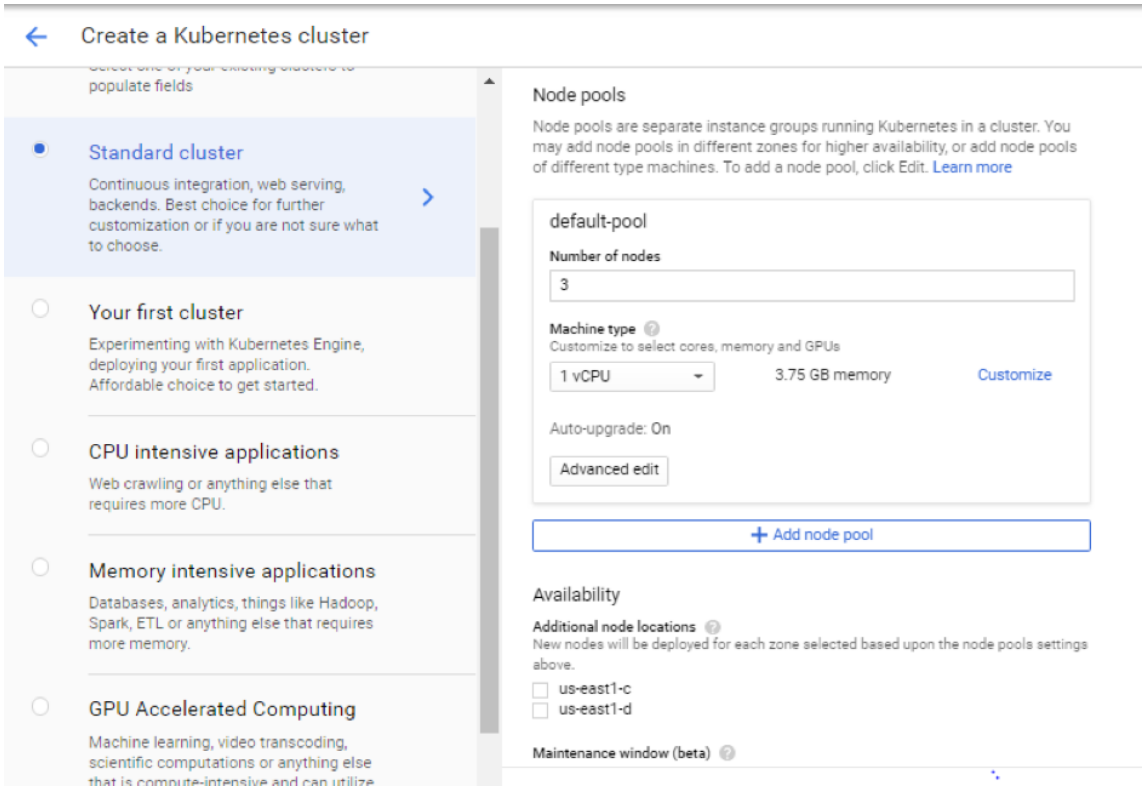
© 1999–2021 Citrix Systems, Inc. All rights reserved.



2. VPX SNIP と同じサブネットにクラスターを作成します（vpx-snet-snip）。このクラスターは、K8s クラスター内の Citrix Ingress Controller から Tier 1 の ADC への構成のプッシュを自動化します。

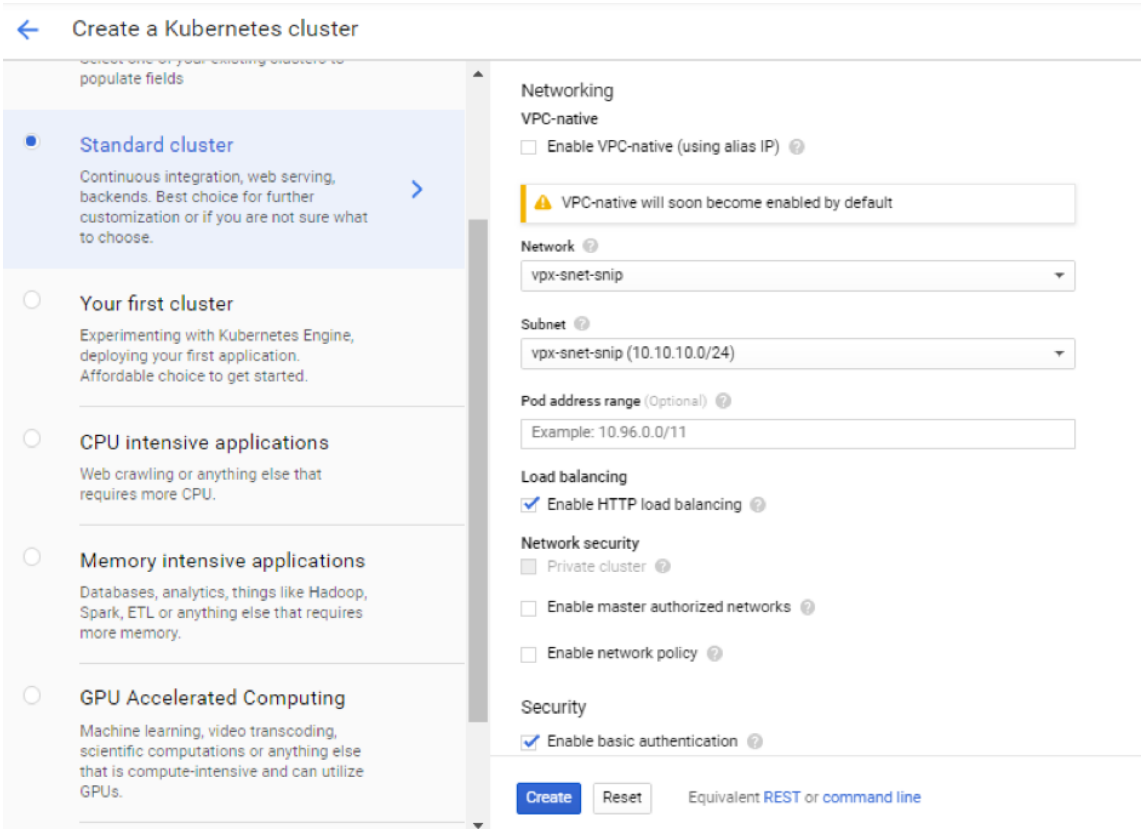


© 1999–2021 Citrix Systems, Inc. All rights reserved.



3. **[Advanced options]** をクリックしてサブネットを`vpx-snet-snip`に変更し、次のフィールドを選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



4. クラウド SDK からこのクラスターにアクセスするには、Kubernetes クラスターに接続ボタンをクリックし、コマンドをクラウド SDK に貼り付けます。

5. 次のコマンドを実行して、GKE クラスターの展開を検証します。

```
kubectl get nodes
<!--NeedCopy-->
```

```
C:\Program Files (x86)\Google\Cloud SDK\GCP_SE_2019\Multitier-Hairpin>kubectl get nodes
NAME                                                STATUS    ROLES     AGE       VERSION
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-l15t   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xbvf   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xs47   Ready     <none>    2d        v1.11.6-gke.2
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サンプル **YAML** ファイルライブラリを使用したサンプルアプリケーションの展開

Citrix ADC は、マイクロサービスで展開され、インターネット経由でアクセスされるエンタープライズグレードのアプリケーションを負荷分散する、2 層アーキテクチャの展開ソリューションを提供します。Tier 1 には、VPX/SDX/MPX などの負荷分散機能があり、North-South トラフィックの負荷分散を行います。Tier 2 は、マイクロサービスを管理し、East-West トラフィックの負荷分散を行うための CPX 展開を備えています。

1. GKE でクラスターを実行している場合は、クラスタロールバインディングを使用して cluster-admin を設定していることを確認します。次のコマンドを使用してこれを行うことができます。

```
kubectl create clusterrolebinding citrix-cluster-admin --
    clusterrole=cluster-admin --user=<email-id of your google
    account>.
<!--NeedCopy-->
```

2. 展開 YAML ファイルがある現在のディレクトリにアクセスします。ノードステータスを取得するには、次のコマンドを実行します。

```
kubectl get nodes
<!--NeedCopy-->
```

```
C:\Program Files (x86)\Google\Cloud SDK\GCP_SE_2019\Multitier-Hairpin>kubectl get nodes
NAME                                                STATUS    ROLES     AGE       VERSION
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-l15t   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xbvf   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xs47   Ready     <none>    2d        v1.11.6-gke.2
```

3. 名前空間を作成します。

```
kubectl create -f namespace.yaml
<!--NeedCopy-->
```

名前空間コマンドを確認します。

```
kubectl get namespaces
<!--NeedCopy-->
```

```
C:\Program Files (x86)\Google\Cloud SDK\GCP_SE_2019\Multitier-Hairpin>kubectl get namespaces
NAME              STATUS    AGE
default           Active    2d
kube-public       Active    2d
kube-system       Active    2d
monitoring        Active    10h
team-colddrink    Active    10h
team-guestbook    Active    10h
team-hotdrink     Active    10h
tier-2-adc        Active    10h
```

4. rbac.yaml をデフォルトの名前空間に展開します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
kubectl create -f rbac.yaml
<!--NeedCopy-->
```

5. 次のコマンドを使用して、ホットドリンク、コールドドリンク、ゲストブックのマイクロサービス用に CPX を展開します。

```
kubectl create -f cpx.yaml -n tier-2-adc
kubectl create -f hotdrink-secret.yaml -n tier-2-adc
<!--NeedCopy-->
```

6. 3 種類のホットドリンクマイクロサービス（ヘアピンアーキテクチャを備えた SSL タイプのマイクロサービス）を展開します。

```
kubectl create -f team_hotdrink.yaml -n team-hotdrink
kubectl create -f hotdrink-secret.yaml -n team-hotdrink
<!--NeedCopy-->
```

7. コールドドリンク用マイクロサービス（SSL_TCP タイプのマイクロサービス）を展開します。

```
kubectl create -f team_colddrink.yaml -n team-colddrink
kubectl create -f colddrink-secret.yaml -n team-colddrink
<!--NeedCopy-->
```

8. ゲストブック（NoSQL タイプのマイクロサービス）を展開します。

```
kubectl create -f team_guestbook.yaml -n team-guestbook
<!--NeedCopy-->
```

9. 上記の 3 つのアプリケーション用に展開された CPX を検証します。まず、階層 2-adc として展開された CPX ポッドを取得し、CPX への CLI アクセスを取得します。

   “‘

   tier-2-adc 名前空間で CPX ポッドを取得するには、次を入力します：kubectl get pods -n tier-2-adc

   CPX ポッド（hotdrinks-cpx pod）への CLI アクセス（bash）を取得するには、次のように入力します：`kubectl exec -it "copy and paste hotdrink CPX pod name from the above step"bash -n tier-2-adc`。

   例：

   `kubectl exec -it cpx-ingress-hotdrinks-768b674f76-pcnw4 bash -n tier-2-adc`

   CS vserver が hotdrink-cpx で実行されているかどうかを確認するには、CPX へのルートアクセスの後に次のコマンドを入力します：`cli-script"sh csvs"`。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

例:

```
root@cpx-ingress-hotdrinks-768b674f76-pcnw4:/## cli_script.sh "sh csvs"
```

10. VPX 入力および Ingress Controller を Tier 2 名前空間に展開し、VPX が自動的に構成されます。Citrix Ingress Controller（CIC）は、Tier 1ADC（VPX）を自動化します。

```
kubectl create -f ingress_vpx.yaml -n tier-2-adc
kubectl create -f cic_vpx.yaml -n tier-2-adc
<!--NeedCopy-->
```

11. インターネット経由でマイクロサービスにアクセスするための DNS エントリをローカルマシンのホストファイルに追加します。

    Windows クライアントの場合は、次に移動します：**C:\Windows\System32\drivers\etc\hosts**

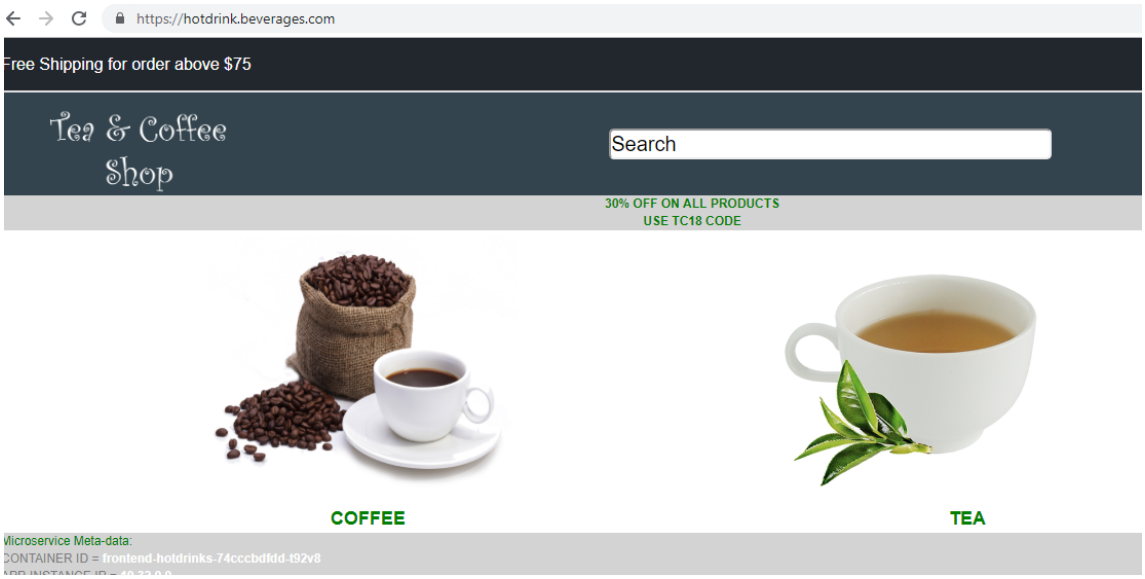
    macOS クライアントの場合は、ターミナルで次を入力します：**sudo nano /etc/hosts‘**

    ホストのファイルに次のエントリを追加し、ファイルを保存します。

```
hotdrink.beverages.com   xxx.xxx.xxx.xxx (static-external-traffic-ip-tier1-vpx)
colddrink.beverages.com  xxx.xxx.xxx.xxx (static-external-traffic-ip-tier1-vpx)
guestbook.beverages.com  xxx.xxx.xxx.xxx (static-external-traffic-ip-tier1-vpx)
grafana.beverages.com    xxx.xxx.xxx.xxx (static-external-traffic-ip-tier1-vpx)
prometheus.beverages.com xxx.xxx.xxx.xxx (static-external-traffic-ip-tier1-vpx)
<!--NeedCopy-->
```

12. これで、インターネット経由で各アプリケーションにアクセスできます。たとえば、https://hotdrink.beverages.comのようになります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



サンプルアプリケーションの書き換えポリシーとレスポンダーポリシーの有効化

次に、カスタムリソース定義（CRD）を使用して、VPX の書き換えポリシーとレスポンダーポリシーをプッシュします。

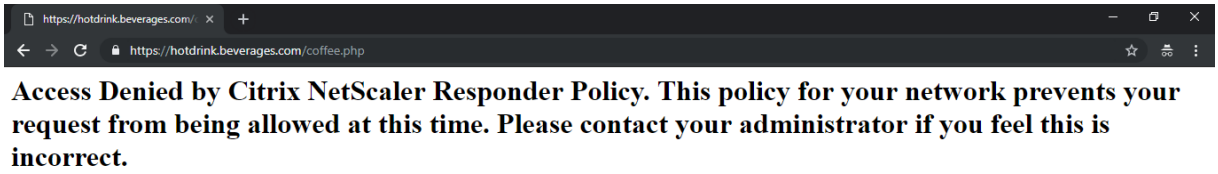
1. CRD を展開して、書き換えポリシーとレスポンダーポリシーを既定の名前空間の tier-1-adc にプッシュします。

```
kubectl create -f crd_rewrite_responder.yaml
<!--NeedCopy-->
```

1. ブラックリスト **URL** hotdrink.beverages.comでコーヒーページへのアクセスをブロックするように、レスポンダーポリシーを設定します。

```
kubectl create -f responderpolicy_hotdrink.yaml -n tier-2-adc
<!--NeedCopy-->
```

レスポンダーポリシーを展開したら、hotdrink.beverages.comのコーヒーページにアクセスします。次に、次のメッセージが表示されます。

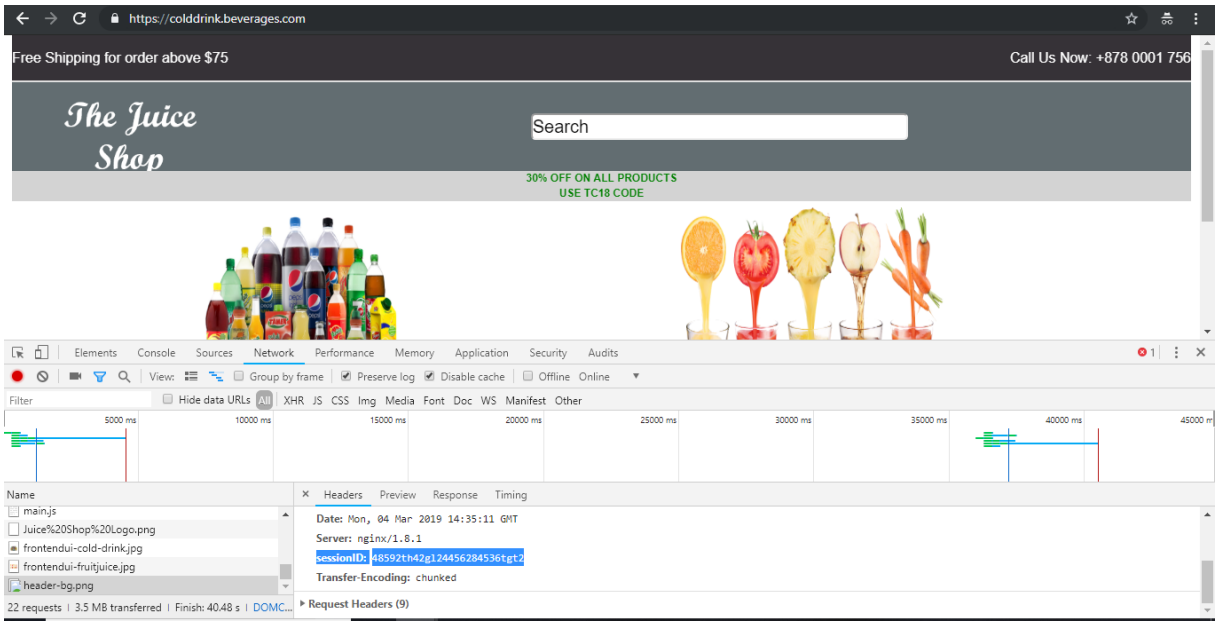


© 1999–2021 Citrix Systems, Inc. All rights reserved.

1. ヘッダー挿入：ヘッダーにセッション ID を挿入するように、colddrink.beverages.comで書き換えポリシーを設定します。

```
kubectl create -f rewritepolicy_colddrink.yaml -n tier-2-adc
<!--NeedCopy-->
```

書き換えポリシーを展開した後、ブラウザーで開発者モードを有効にしてcolddrink.beverages.comにアクセスします。Chrome で、F12 を押し、ネットワークカテゴリのログを保存して、セッション ID を確認します。セッション ID は、ティア 1-adc（VPX）の書き換えポリシーによって挿入されます。



オープンソースツールセット

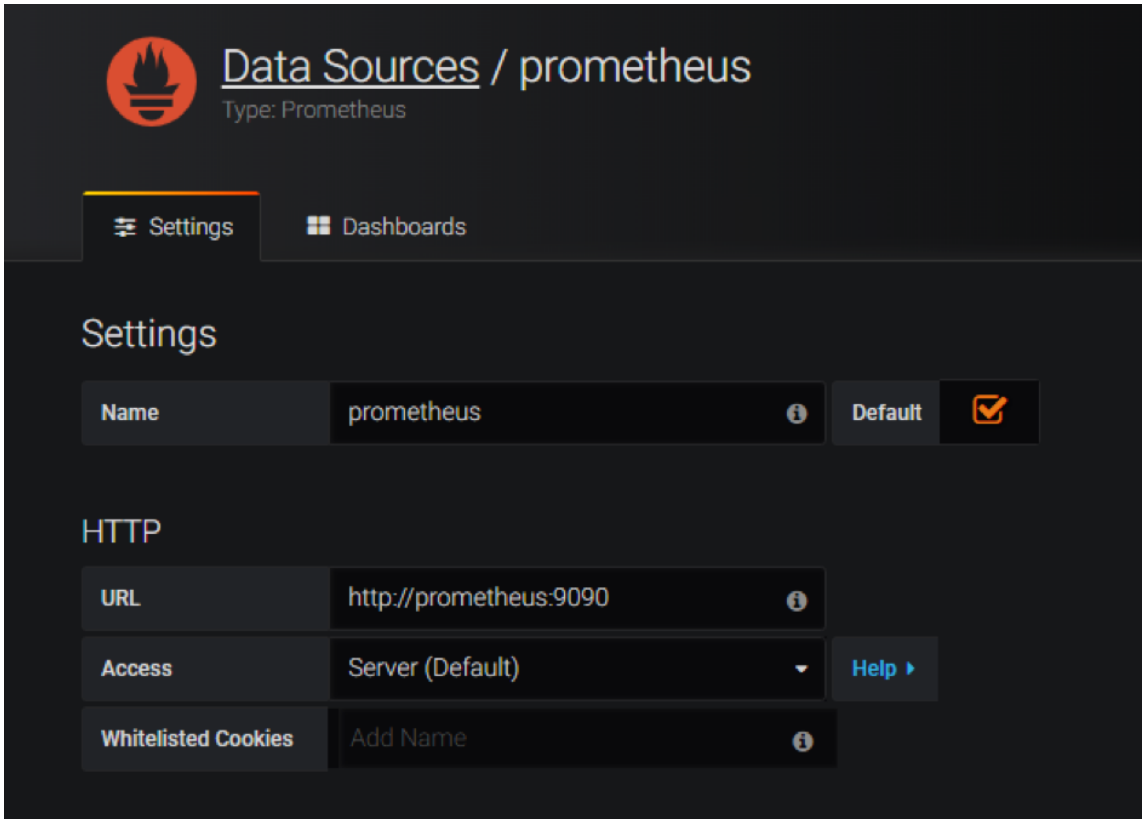
1. Prometheus や Grafana などの Deploy Cloud Native Computing Foundation (CNCF) 監視ツールを展開して、ADC プロキシの統計情報を収集します。

```
kubectl create -f monitoring.yaml -n monitoring
kubectl create -f ingress_vpx_monitoring.yaml -n monitoring
<!--NeedCopy-->
```

Prometheus ログアグリゲータ

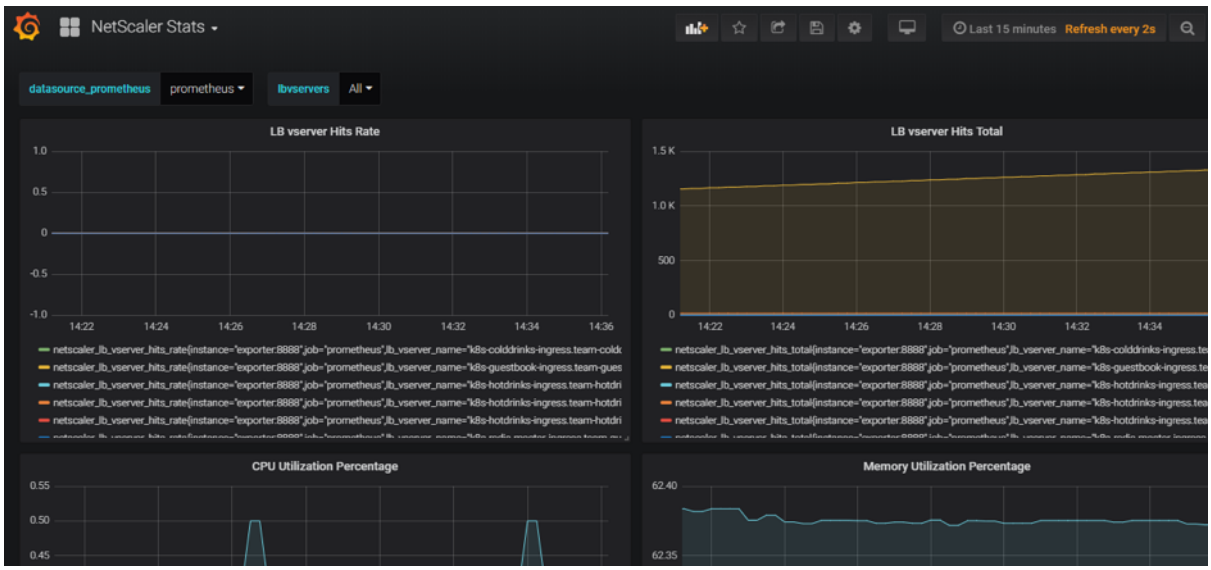
1. http://grafana.beverages.comにログインし、次の 1 回限りのセットアップを完了します。
   a) 管理者の認証情報を使用してポータルにログインします。
   b) [データソースを追加] をクリックし、**Prometheus** データソースを選択します。
   c) 次の設定を行い、[保存してテスト] ボタンをクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



Grafana ビジュアルダッシュボード

1. 左側のパネルで、[インポート] オプションを選択し、`yamlFiles`フォルダーで提供されている`grafana_config.json`ファイルをアップロードします。これで、基本的な ADC 統計がリストされた Grafana ダッシュボードを見ることができます。



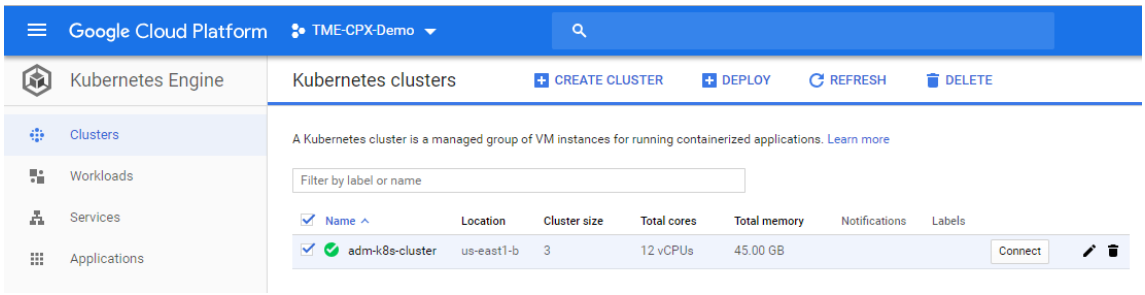
© 1999–2021 Citrix Systems, Inc. All rights reserved.

配置の削除

1. Citrix VPX（tier-1-adc）展開を削除するには、Google SDK CLI コンソールにアクセスしてインスタンスを削除します。

```
gcloud deployment-manager deployments delete tier1-vpx
<!--NeedCopy-->
```

2. GKE Kubernetes クラスターを削除するには、GCP コンソールで kubernetes クラスターを選択し、[削除] をクリックしてクラスターを消去します。



Citrix ADC クラスタリング検証済みリファレンスデザイン

May 18, 2020

Citrix ADC クラスターは、単一のシステムイメージとして連携して動作する Citrix ADC nCore アプライアンスのグループです。クラスターの各アプライアンスは、ノードと呼ばれます。Citrix ADC クラスターには、ノードとして 2 台または 32 台までの Citrix ADC nCore ハードウェアまたは仮想アプライアンスを含めることができます。

クライアントトラフィックは、高可用性、高スループット、およびスケーラビリティを提供するために、ノード間で分散されます。

クラスターを作成するには、必要な Citrix ADC アプライアンスをクラスターノードとして追加し、ノード間の通信をセットアップし、クライアントとサーバーネットワークへのリンクを設定し、Citrix ADC アプライアンスを構成し、クライアントとサーバーのトラフィックの分散を構成します。

クラスターでサポートされる Citrix ADC 機能

次の表は、クラスターで完全にサポートされ、個々のクラスターノードでのみ機能し、クラスターではサポートされていない Citrix ADC の機能の一覧です。

Citrix ADC 機能サポートマトリックス:

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サポートされる機能	ノードレベルでサポートされる機能	サポートされていない機能
負荷分散	サージ保護	DNS ロードバランシング
ロードバランシングの永続性	Sure Connect	FTP ロードバランシング
SIP	プライオリティキューイング	広域サーバー負荷分散（Global Server Load Balancing：GSLB）
最大クライアント	HTTP サービス拒否保護 (HTTP DoSP)	Citrix ADC ADC プッシュ配信
スピルオーバー	統合キャッシュ	RTSP
SSL PI ポリシー	Call Home	ステートフル接続のフェイルオーバー
コンテンツスイッチ		グレースフルシャットダウン
キャッシュのリダイレクト		DBS Auto Scaling
圧縮制御		TOS を使用した DSR
コンテンツフィルタリング		帯域幅に基づくスピルオーバー
OSPF（IPv4 および IPv6）		より細かいスタートアップ RR 制御
リファクシミリ		レート制限
BGP（IPv4 および IPv6）		ストリーム分析
HTML インジェクション		ネットプロファイル
TCP バッファリング		DNS キャッシュ
分散サービス拒否 (DDoS)		SSL-VPN
ベーシックネットワーク (IPv4 および IPv6)		SSL CPE ポリシー
VLAN		アプリケーションファイアウォール
ICMP		ああー
フラグメンテーション		クラウドブリッジングトンネリング
MAC ベースフォワーディング (MBF)		レイヤ 2 モード
RNAT		FIPS

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サポートされる機能	ノードレベルでサポートされる機能	サポートされていない機能
INAT		XML XSM
KRPC		AAA-TM
アクラシス		VMAC/VRRP
単純な ACL		リンク負荷分散
PBR		IP-IP トンネリング
SNMP 取得/セット、ウォーク		DHCP RA
SNMP トラップ		ブリッジグループ
ポリシーインフラストラクチャ (PE/PI)		ネットワークブリッジ
NITRO API		Citrix ADC 上の Web インターフェイス
AppExpert		EdgeSight Monitoring
書き換え		ポンド
レスポンダー		ISIS ルーティング
送信元 IP (USIP) を使用		FIS（フェイルオーバーインターフェイスセット）
ウォーターフォールチャート付きの AppFlow エクスポータと Appflow コレクタ（クライアント）		
DataStream		
MSR		
ポリシーベースの RNAT		
Web ログ		
監査 (syslog および nsauditlog)		
パス MTU ディスカバリ		
クライアントのキープアライブ		

ハードウェアとソフトウェアの要件

Citrix ADC クラスターに追加するアプライアンスは、次の要件を満たしている必要があります。

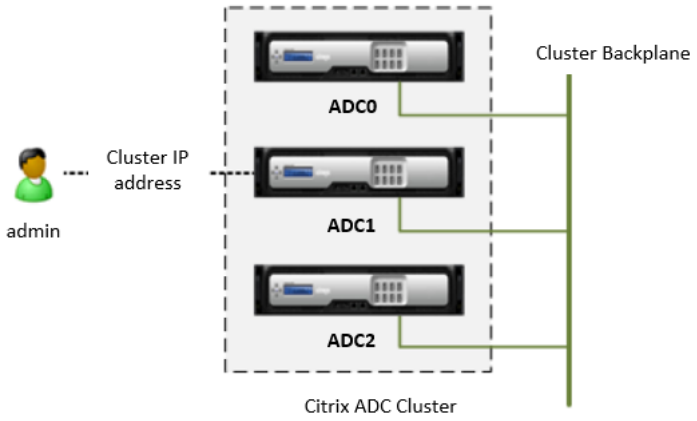
© 1999–2021 Citrix Systems, Inc. All rights reserved.

- Citrix ADC の nCore アプライアンスであること. Citrix ADC Classic アプライアンスのクラスタリングはサポートされていません。
- 同じプラットフォームタイプ（物理アプライアンスまたは VPX インスタンス）であること。
- 同じハードウェアタイプ（物理アプライアンスの場合）であること。
- 同じサブネット上に存在する。
- クラスターライセンスファイルを持っている。
- 同じライセンス（スタンダード、エンタープライズ、プラチナ、および任意のアドオンライセンス）を持っている。
- 同じソフトウェアバージョンとビルドであること。
- 最初に構成され、共通のクライアント側およびサーバー側のネットワークに接続されている。

クラスタリングのしくみ

Citrix ADC クラスターは、ハードウェアおよびソフトウェアの要件で指定された要件を満たす Citrix ADC アプライアンスをグループ化することによって形成されます。クラスターノードの 1 つは、構成コーディネーター (CCO) として指定されています。名前が示すように、CCO は、クラスターの管理 IP アドレス（クラスター IP アドレス）を使用して、すべてのクラスター設定を調整します。

クラスターは、次の図に示すように、クラスター IP アドレスを使用して CCO にアクセスして設定する必要があります。



> 注:
>
> Citrix ADC IP（ADCIP）アドレスを介してノードにアクセスして個々のノードを構成することはできません。ADCIP アドレスを介してアクセスされるノードは、読み取り専用モードで使用できます。つまり、表示できるのは設定と統計情報だけです。ただし、個々のノードで実行できるコマンドがいくつかあります。詳しくは、「個々のノードでサポートされる操作」を参照してください。

クラスターで定義した VIP アドレスは、クラスターのすべてのノード (ストライプアドレス) で使用できます。SNIP アドレスは、すべてのノード（ストライプアドレス）または単一ノード（スポッティングアドレス）でしか使用できないように定義できます。クラスター内のトラフィック分散の詳細は、使用されるアルゴリズムによって異なりますが、それぞれの場合に同じ論理エンティティがトラフィックを処理します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラスターの同期

ノードがクラスターに追加されると、Citrix ADC の構成と、CCO で使用できるファイル（SSL 証明書、ライセンス、DNS など）が、新しく追加されたクラスターノードで同期されます。これにより、構成とファイルが常にクラスターのすべてのノードで同期されます。

既存のクラスターノードがクラスターに再参加すると (障害が発生したか、意図的に無効になった後)、クラスターはノードで使用可能な構成をチェックします。再結合されたノードと CCO で使用可能な設定に不一致がある場合、ノードは次の方法のいずれかを使用して同期されます。

- 完全同期。設定間の差が 255 コマンドを超えると、CCO に実装されたすべての設定が、クラスターに再加入するノードに適用されます。同期の間、ノードは運用上使用できないままです。
- 差分同期。構成間の差が 255 コマンド以下の場合は、使用できない構成のみがクラスターに再参加するノードに適用されます。ノードの動作状態は影響を受けません。

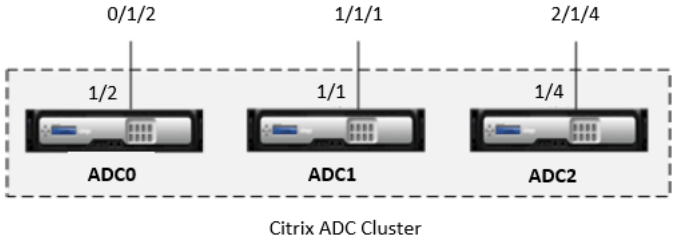
クラスター IP アドレスを介して CCO で実行される設定は、自動的にクラスターノードに伝播されます。クラスター構成は使用可能なノードの定足数に基づいているため、コマンド (クラスター IP アドレスで実行される) を他のクラスターノードに伝達できるのは、大半のノードが同期している場合のみです。ほとんどのノードが同期していないか、同期処理中である場合、新しいコマンドを受け入れないため、コマンドは同期が完了するまで伝播されません。

クラスター接続

インターフェイスが属するノードを識別するために、Citrix ADC 標準のインターフェイス命名規則の先頭にノード ID が付きます。つまり、インターフェイス識別子 **c/u**（**c** は Controller 番号、**u** はユニット番号）は **n/c/u** になります（**n** はノード ID です)。

たとえば、次の図では、ノード 0 のインターフェイス **1/2** は **0/1/2** 、ノード **1** のインターフェイス **1/** 1 は **1/1/1** 、ノード 2 のインターフェイス **1/4** は **2/1/4** と表されます。

ネットワークインターフェイスクラスター内の命名規則

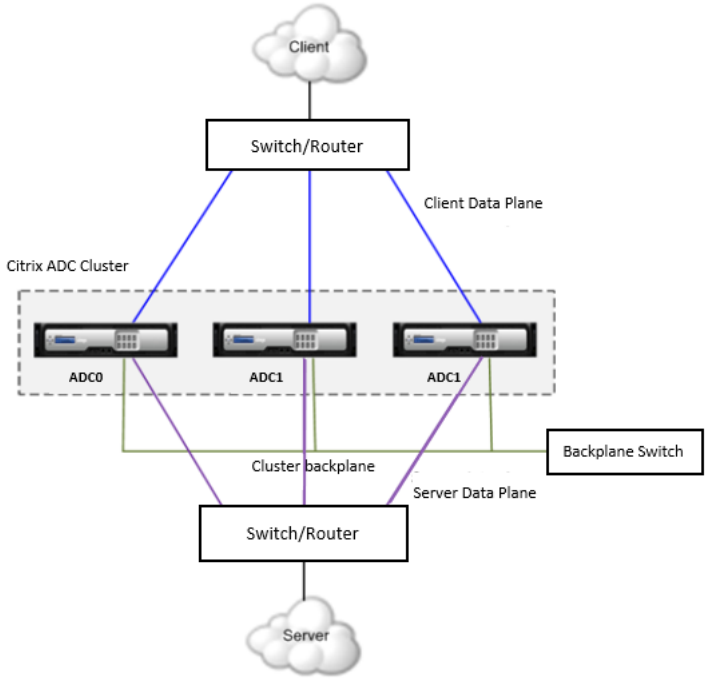


クラスターは、クラスターノードとクライアント側の接続デバイス間の物理接続を介してクライアントと通信します。これらの物理接続の論理的なグループ化は、クライアントデータプレーンと呼ばれます。同様に、クラスターは、クラスターノードとサーバー側の接続デバイス間の物理接続を介してサーバーと通信します。これらの物理接続の論理的なグループ化は、サーバーデータプレーンと呼ばれます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クライアントデータプレーンとサーバーデータプレーンを介してクライアントとサーバーとの通信に加えて、クラスターノードは クラスターバックプレーンを使用して相互に通信します。バックプレーンは、各クラスターノードとバックプレーンスイッチからの物理接続を含み、クラスターシステムのバックボーンです。

クラスタ通信インターフェイス



上の図は、クライアントデータプレーン、サーバーデータプレーン、およびクラスターバックプレーンを形成するための物理接続の論理的なグループを示しています。

ストライピングされた **IP** アドレスとスポッティング **IP** アドレス

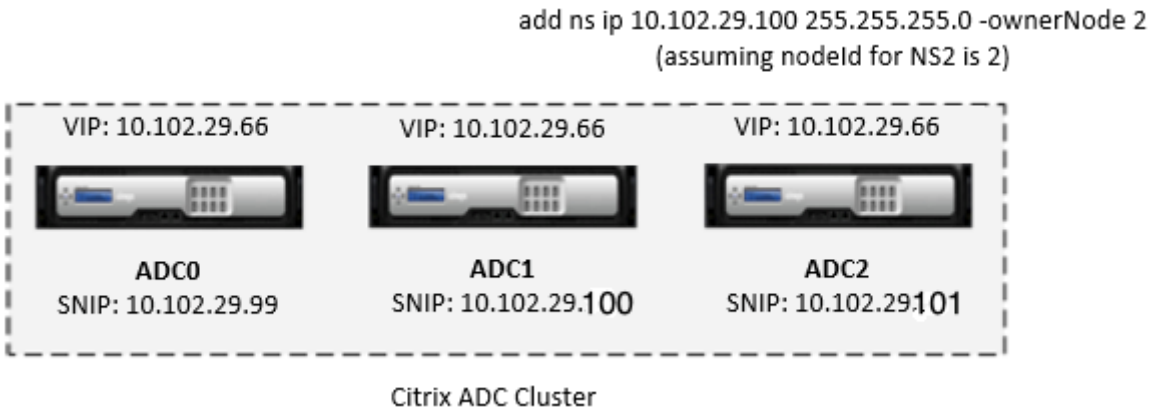
クラスタ配置では、VIP および SNIP アドレスをストライピングまたはスポッティングできます。

- ストライプ *IP* アドレスは、クラスターのすべてのノードでアクティブです。所有者ノードを指定せずにクラスタ上に構成された IP アドレスは、すべてのクラスターノードでアクティブになります。
- スポッティング *IP* アドレスは、1 つのノードでアクティブであり、1 つのノードによって排他的に所有されています。所有者ノードを指定してクラスタ上に構成された IP アドレスは、所有者として指定されたノード上でのみアクティブになります。

次の図は、3 ノードクラスター内のストライプおよびスポットされた IP アドレスを示しています。

ストライピングされた **IP** アドレスおよびスポッティング **IP** アドレスを持った **3** ノードクラスター

© 1999–2021 Citrix Systems, Inc. All rights reserved.



上の図では、VIP アドレス 10.102.29.66 がすべてのクラスターノードでストライピングされ、SNIP アドレス 10.102.29.99 が ADC0 と ADC1 でストライピングされます。ADC2 には、スポッティング SNIP アドレスがあります。

次の表に、ストライプ化またはスポットの指定が可能な Citrix ADC が所有する IP アドレスを示します。

ストライピングされた **IP** アドレスとスポッティング **IP** アドレス

Citrix ADC が所有する IP アドレス	ストライピング IP アドレス	スポッティング IP アドレス
ADCIP	いいえ	はい
クラスター IP アドレス	いいえ	いいえ
VIP	はい	いいえ
SNIP	はい	はい (推奨)

> 注:
>
> - クラスター IP アドレスは、ストライピングされた IP アドレスまたはスポッティング IP アドレスではありません。固定ノードではない CCO が所有するフローティング IP アドレスです。
> - スポッティング IP アドレスだけの使用をお勧めします。ストライプ化された IP アドレスは、IP アドレスが不足している場合にのみ使用できます。ストライプ IP アドレスを使用すると、ARP フラックスの問題が発生する可能性があります。

トラフィック分散

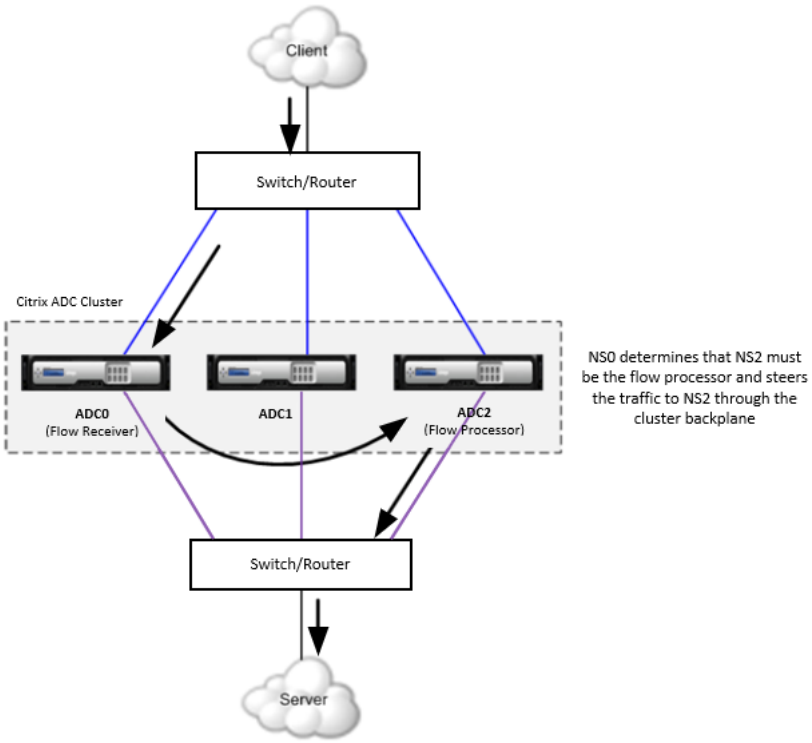
Citrix ADC クラスターは、等価コストマルチパス (ECMP) またはクラスタリンクアグリゲーショングループ (CLAG) のトラフィック分散メカニズムを使用して、外部接続デバイスからトラフィックを受信するノード（フローレシーバ）を決定します。これらのメカニズムはそれぞれ、異なるアルゴリズムを使用してフローレシーバを決定します。次に、

© 1999–2021 Citrix Systems, Inc. All rights reserved.

フローレシーバは内部クラスタロジックを使用して、トラフィックを処理するノード（フロープロセッサ）を決定します。

> 注:
>
> フローレシーバとフロープロセッサは、トラフィックを処理できるノードである必要があります。

クラスター内のトラフィック分散



上の図は、クラスターを流れるクライアント要求を示しています。クライアントは、ストライピングされた仮想 IP (VIP) アドレスに要求を送信します。クライアントデータプレーンに設定されたトラフィック分散メカニズムは、クラスターノードの 1 つをフローレシーバとして選択します。フローレシーバは、トラフィックを受信し、トラフィックを処理する必要があるノードを特定し、クラスターバックプレーンを介してそのノードへの要求を操縦します（フローレシーバがフロープロセッサとして自身を選択した場合を除く）。

フロープロセッサは、サーバーとの接続を確立します。サーバーは要求を処理し、要求をサーバーに送信したサブネット IP（SNIP）アドレスに応答を送信します。

- SNIP アドレスがストライピング IP アドレスの場合、サーバーデータプレーンに設定されたトラフィック分散メカニズムによって、（SNIP アドレスを所有する）クラスターノードの 1 つがフローレシーバとして選択されます。フローレシーバは、トラフィックを受信し、フロープロセッサを決定し、クラスターバックプレーンを介してフロープロセッサに要求を誘導します。
- SNIP アドレスがスポッティング IP アドレスの場合、SNIP アドレスを所有するノードはサーバーからの応答を受信します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

非対称クラスタトポロジ（すべてのクラスターノードが外部スイッチに接続されていない）では、リンクセットを排他的に使用するか、ECMP または CLAG と組み合わせて使用する必要があります。詳しくは、「リンクセットの使用」を参照してください。

クラスターとノードの状態

クラスターノードの分類には、管理状態、動作状態、および正常性の 3 種類の状態が含まれます。

- 管理者の状態。ノードをクラスターに追加すると、管理状態が設定されます。これは、ノードの目的を示します。これは、次のいずれかの状態になります。
  - アクティブ。この状態のノードは、動作可能で正常な場合にトラフィックを処理します。
  - パッシブ。この状態のノードはトラフィックを処理しませんが、クラスターと同期しています。これらのノードは、クラスターからノードを削除せずにアップグレードできるため、メンテナンス作業中に便利です。
  - スペア。この状態のノードはトラフィックを処理しませんが、クラスターと同期しています。スペアノードは、クラスターのバックアップノードとして機能します。ACTIVE ノードの 1 つが使用できなくなると、スペアノードの 1 つの動作状態が ACTIVE になり、そのノードはトラフィックの処理を開始します。
- 動作状態。ノードがクラスターの一部である場合、その動作状態は ACTIVE、INACTIVE、または UNKNOWN に変わります。ノードが INACTIVE 状態または UNKNOWN 状態になっている理由はいくつかあります。`ns.log`ファイルカウンタまたはエラーカウンタを確認して、正確な理由を特定します。
- 健全性状態。ノードの健全性に応じて、ノードは UP または NOT UP のいずれかになります。ノードが UP 状態になっていない理由を表示するには、クラスター IP アドレスからそのノードの **show cluster node** コマンドを実行します。

管理状態が ACTIVE、動作状態が ACTIVE、正常性ステータスが UP であるノードだけがトラフィックを処理できます。クラスタが機能するのは、最小（n/2 +1）ノード（n はクラスターノード数）がトラフィックを処理できる場合だけです。

Citrix ADC クラスターをセットアップする

Citrix ADC クラスターをセットアップするには、まずクラスターバックプレーンを設定します。次に、最初のノードをクラスターに追加し、これが初期構成コーディネータ (CCO) になり、そのノードにクラスター IP アドレスを割り当てることによって、クラスターを作成します。CCO でクラスター IP アドレスを定義したら、クラスターにさらにノードを追加できます。

クラスターに追加するアプライアンスは、次のことを行う必要があります。

- Citrix ADC の nCore アプライアンスであること. Citrix ADC Classic アプライアンスのクラスタリングはサポートされていません。
- 同じプラットフォームタイプ（物理アプライアンスまたは VPX インスタンス）であること。
- 同じハードウェアタイプ（物理アプライアンスの場合）であること。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- 同じサブネット上に存在する。
- クラスタライセンスファイルを持っている。
- 同じライセンス（スタンダード、エンタープライズ、プラチナ、および任意のアドオンライセンス）を持っている。
- 同じソフトウェアバージョンとビルドであること。
- 最初に構成され、共通のクライアント側およびサーバー側のネットワークに接続されている。

上記の条件をすべて満たすアプライアンスのみを Citrix ADC クラスターに含めることができます。

クラスターバックプレーンの設定

クラスター内のノードは、クラスターバックプレーンを介して相互に通信します。バックプレーンは、各ノードの 1 つのインターフェイスが共通のスイッチ（クラスターバックプレーンスイッチ）に接続される一連の接続です。クラスターの各ノードは、特別な MAC アドレスを使用して、クラスターバックプレーンを介して他のノードと通信します。

> 注:
>
> （MAC スプーフィングが有効になっている）XenServer 上に展開されている VPX アプライアンスのクラスターでは、NIC（XenServer Vswitch）がバックプレーン上で送信されたパケットをドロップできます。そのため、XenServer で MAC スプーフィングが無効になっていることを確認する必要があります。
> クラスターバックプレーンスイッチが 1,500 バイトを超えるパケットをサポートしていることを確認する必要があります。

確認事項:

- アプライアンスの管理インターフェイス（0/1）をバックプレーンインターフェイスとして使用しないでください。
- バックプレーンに使用するインターフェイスは、クライアントデータプレーンまたはサーバーデータプレーンに使用しないでください。
- クラスターのすべてのノードのバックプレーンインターフェイスは、同じスイッチに接続され、同じ L2 VLAN にバインドされている必要があります。デフォルトでは、バックプレーンインターフェイスは、クラスターに設定されているすべての L3 VLAN 上に存在しています。
- 同じクラスターインスタンス ID を持つ複数の Citrix ADC クラスタがある場合は、各クラスターのバックプレーンインターフェイスが異なる VLAN にバインドされていることを確認してください。
- 大量のトラフィックがシームレスに処理されるように、バックプレーン専用のスイッチを使用することをお勧めします。
- バックプレーンインターフェイスは、そのインターフェイスの HA モニタリング設定に関係なく、常にモニタされます。

クラスターバックプレーンを設定するには、各ノードで次の操作を行います。

1. バックプレーンに使用するネットワークインターフェイスを特定します。
2. 選択したネットワークインターフェイスからクラスターバックプレーンスイッチに、イーサネットケーブルまたは光ケーブルを接続します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

たとえば、ノード 4 のバックプレーンインターフェイスとしてインターフェイス 1/2 を使用するには、ノード 4 の 1/2 インターフェイスからバックプレーンスイッチにケーブルを接続します。

> 注:
>
> リンクアグリゲート（LA）チャネルを設定して、クラスターバックプレーンのスループットを最適化できます。

Citrix ADC クラスターを作成する

クラスターを作成するには、クラスターインスタンスを作成し、クラスターに追加する最初のアプライアンスでクラスタ IP アドレスを構成する必要があります。このノードは、構成コーディネータ (CCO) と呼ばれます。すべてのクラスター構成は、クラスター IP アドレスを通じてこのノードにアクセス
することによって実行されます。CCO は、特定の 1 つのクラスターノードに固定されていません。時間の経過とともに変化する可能性があります。たとえば、CCO がダウンした場合、クラスターは他のノードの 1 つを新しい CCO として選択し、クラスターの IP アドレスを所有します。

クラスターインスタンスを追加すると、**clear ns config** 拡張コマンドがそのノードで内部的に実行されます。さらに、SNIP アドレスとすべての VLAN 設定（デフォルト VLAN および ADCVLAN を除く）がノードから消去されます。

> 注:
>
> クラスターを作成する前に、そのノードのバックプレーン
> インターフェイスを設定していることを確認してください。

Citrix ADC コマンドラインを使用してクラスターを作成するには

> 注:
>
> 次のコマンドには、必須パラメータのみが含まれます。CLI コマンドについて詳しくは、各コマンドで使用できる **man** ページを参照してください。「`man <command syntax>`」と入力します。たとえば、add cluster instance コマンドの **man** ページを取得するには、`man add cluster instance`と入力します。

1. クラスターに追加する Citrix ADC アプライアンス（たとえば、ADCIP アドレスが 10.102.29.60 のアプライアンス）にログオンします。
2. クラスターインスタンスを追加します。クラスターインスタンスは、クラスターを識別するエンティティです。`add cluster instance <clId>`を入力します。ここで、**clId** はクラスターを識別する一意の番号です。最小値：1。最大値：16。

> 注:
>
> クラスターインスタンス ID が LAN 内で一意であることを確認します。

1. Citrix ADC アプライアンスをクラスターに追加します。`add cluster node <nodeId> <IPAddress> [-state <state>] [-backplane <interface_name>]`を入力します。各項目の意味は次のとおりです。
   - **nodeId** は、クラスタ上のアプライアンスを識別する一意の番号です。各ノードは、異なるノード ID を持つ必要があります。最小値：0。最大値：31。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- **IP** アドレスは、Citrix ADC アプライアンスの IP アドレスです。IPv4 アドレスのみがサポートされます。
- **state** は、クラスターノードの設定済みの状態です。有効な値:ACTIVE、PASSIVE、SPARE。デフォルト：PASSIVE。

> 注:
>
> スポッティング IP アドレスの追加など、ノード固有の構成を実行する場合は、ノードがトラフィックを処理する前に、状態を PASSIVE (デフォルトの状態) に設定します。ノード固有の構成を実行した後、**set cluster node** コマンドを使用してノードの状態を ACTIVE に変更します。

- バックプレーンは、ノードのバックプレーンインターフェイスです。たとえば、ノード 0 がインターフェイス 1/1 を使用する場合、このパラメータの値は 0/1/1 になります。

例:

```
1 add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
2 <!--NeedCopy-->
```

2. このノードでクラスター IP アドレス (10.102.29.61 など) を追加します。`add ns ip <IPAddress> <netmask> -type clip`を入力します。各項目の意味は次のとおりです。
   - **IP** アドレスは、Citrix ADC クラスターのクラスタ IP アドレスです。IPv4 アドレスのみがサポートされます。
   - **netmask** は、クラスター IP アドレスのサブネットマスクです。値は 255.255.255.255 でなければなりません。

   例:

```
1 add ns ip 10.102.29.61 255.255.255.255 -type clip
2 <!--NeedCopy-->
```

3. クラスターインスタンスを有効にしてクラスターを作成します。`enable cluster instance <clId>`を入力します。ここで、**clId** は、有効化する必要があるクラスターインスタンスを識別する番号です。
4. 構成を保存します。`save ns config`を入力します。
5. アプライアンスをウォーム再起動します。`reboot -warm`を入力します。

show cluster instance コマンドを使用して、クラスタ設定を確認します。このコマンドの出力には、クラスターのノードとして CCO の ADCIP アドレスが表示されている必要があります。

構成ユーティリティを使用してクラスターを作成するには

1. クラスターに追加する Citrix ADC アプライアンス（たとえば、ADCIP アドレスが 10.102.29.60 のアプライアンス）にログオンします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ペインの **[**はじめに**]** で、**[**クラスターの管理**]** をクリックします。
4. [クラスター構成] ダイアログボックスで、次のパラメータを設定します。
   - クラスターインスタンス **ID** -クラスターを識別する一意の番号。最小値：1。最大値：16。
   - クラスタ **IP** アドレス -Citrix ADC クラスターの IP アドレス。IPv4 アドレスのみがサポートされます。
   - バックプレーン -ノードのバックプレーンインターフェイス。たとえば、ノード 0 がインターフェイス 1/1 を使用する場合、このパラメータの値は 1/1 になります。
5. ［作成］をクリックします。
6. [クラスターインスタンスの構成] ダイアログボックスで、[クラスターインスタンスの有効化] チェックボックスがオンになっていることを確認します。
7. [クラスターノード] ペインで、ノードを選択し、[開く] をクリックします。
8. [クラスターノードの構成] ダイアログボックスで、テートを設定します。
9. [**OK]** をクリックし、[保存] をクリックします。
10. アプライアンスをウォーム再起動します。

クラスターへのノードの追加

クラスターのサイズをシームレスにスケーリングして、最大 32 個のノードを含めることができます。クラスターにアプライアンスを追加すると、そのアプライアンスのライセンスが CCO で使用可能なライセンスと照合されます。ライセンスが一致すると、アプライアンスが
クラスターに追加されます。ノードの既存の構成がクリアされ、クラスター構成がノードと同期されます。同期の進行中に、トラフィックが断続的にドロップされる可能性があります。

クラスターにノードを追加するには、まずクラスタ上でノードを構成し (ノードを追加する)、次にノード上でクラスターを構成する (クラスターに参加する) 必要があります。

Citrix ADC コマンドラインを使用する場合は、まずクラスタ IP アドレスにログオンしてノードを追加します。次に、そのノードにログオンし、ノードをクラスターに参加させます。構成ユーティリティを使用する場合は、ノードを追加するためにクラスター IP アドレスにのみログオンする必要があります。新しく追加されたノードは、自動的にクラスターに参加します。または、コマンドラインからノードを追加し、構成ユーティリティを使用してノードをクラスターに参加させることもできます。

> 注:
>
> - ノードを追加する前に、そのノードのバックプレーンインターフェイスを設定していることを確認してください。
> - スポットされた IP のみを持つクラスターに新しいノードを追加すると、スポットされた IP アドレスがそのノードに割り当てられる前に同期が実行されます。このような場合、L3 VLAN バインディングとスタティックルートが失われる可能性があります。この損失を回避するには、ストライピング IP を追加するか、新しく追加されたノードの ADCIP に L3 VLAN バインディングとスタティックルートを追加します。
> - 構成済みのリンクアグリゲート（LA）チャネルを持つ Citrix ADC アプライアンスをクラスターに追加しても、LA チャネルはクラスタ環境に存在し続けます。LA チャネルの名前は LA/x から nodeId/LA/x に

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 変更されます。ここで、LA/x は LA チャネル識別子です。

Citrix ADC コマンドラインを使用してクラスターにノードを追加するには

1. クラスターの IP アドレスにログオンし、次の操作を行います。
   - Citrix ADC アプライアンス (10.102.29.70 など) をクラスターに追加します。`add cluster node <nodeId> <IPAddress> [-state <state>] [-backplane <interface_name>]`を入力します。各項目の意味は次のとおりです。
     - **nodeId** は、クラスタ上のアプライアンスを識別する一意の整数です。各ノードは、異なるノード ID を持つ必要があります。最小値：0。最大値：31。
     - **IP** アドレスは、Citrix ADC アプライアンスの IP アドレスです。IPv4 アドレスのみがサポートされます。
     - **state** は、クラスターノードの設定済みの状態です。有効な値：ACTIVE、PASSIVE、SPARE。デフォルト：PASSIVE。

     > 注：
     > スポッティング IP アドレスの追加など、ノード固有の構成を実行する場合は、ノードがトラフィックを処理する前に、状態を PASSIVE（デフォルトの状態）に設定します。ノード固有の設定を実行した後、**set cluster node** コマンドを使用して、ノードの状態を ACTIVE に変更します。
     > - **interface_name** は、ノードのバックプレーンインターフェイスです。たとえば、ノード 1 がインターフェイス 1/1 を使用する場合、このパラメータの値は 1/1/1 になります。

     例：

     ```
     1 クラスターノードを追加 1 10.102.29.70-状態パッシブ-バックプレーン 1/1/1
     2 <!--NeedCopy-->
     ```

   - `save ns config`を入力して構成を保存します。
2. 新しく追加したノード (10.102.29.70 など) にログオンし、次の操作を実行します。
   - ノードをクラスターに参加させます。`join cluster -clip <ip_addr> -password <password>`を入力します。各項目の意味は次のとおりです。
     - クリップは、Citrix ADC クラスターの IP アドレスです。IPv4 アドレスのみがサポートされます。
     - パスワードは、CCO の nsroot パスワードです。

     例：

     ```
     1 join cluster -clip 10.102.29.61 -password nsroot
     2 <!--NeedCopy-->
     ```

   - `save ns config`を入力して構成を保存します。
   - `reboot -warm`と入力して、アプライアンスをウォームリブートします。

構成ユーティリティを使用してクラスターにノードを追加するには

© 1999–2021 Citrix Systems, Inc. All rights reserved.

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ペインの **[**はじめに**]** で、**[**クラスターの管理**]** をクリックします。
4. [追加] をクリックして、新しいノード (10.102.29.70 など) を追加します。
5. [クラスターノードの作成] ダイアログボックスで、次のパラメータを設定します。
   - ノード **ID** -クラスタ上のアプライアンスを識別する一意の整数。各ノードは、異なるノード ID を持つ必要があります。最小値：0。最大値：31。
   - **IP** アドレス -Citrix ADC アプライアンスの IP アドレス。IPv4 アドレスのみがサポートされます。
   - バックプレーン -ノードのバックプレーンインターフェイス。たとえば、ノード 1 がインターフェイス 1/1 を使用する場合、このパラメータの値は 1/1 になります。
   - 状態 - クラスターノードの構成済み状態。有効な値: ACTIVE、PASSIVE、SPARE。デフォルト: PASSIVE。

     > 注:
     > スポッティング IP アドレスの追加など、ノード固有の構成を実行する場合は、ノードがトラフィックを処理する前に、状態を PASSIVE (デフォルトの状態) に設定します。ノード固有の設定を実行した後、ノードの状態を ACTIVE に変更します。
6. **[** 作成**]** をクリックします。アプライアンスがウォームリブートされることを示すダイアログボックスが表示されます。［はい］をクリックして確定します。

構成ユーティリティを使用して、以前に追加したノードをクラスターに参加させるには

Citrix ADC コマンドラインを使用してノードをクラスターに追加したが、ノードをクラスターに参加させていない場合は、以下の手順に従ってノードをクラスターに参加させることができます。

1. クラスターに参加させるノード (10.102.29.70 など) にログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ペインの [はじめに] で、[クラスターに参加] をクリックします。
4. [既存のクラスターに参加] ダイアログボックスで、次のパラメータを設定します。
   - クラスタ **IP** -Citrix ADC クラスターの IP アドレス。IPv4 アドレスのみがサポートされます。
   - パスワード： CCO の`nsroot` パスワード。
5. ［**OK**］をクリックします。

クラスターノードの削除

クラスターからのノードの削除は、次の 2 つの手順で行います。

1. ノードからクラスターインスタンスへの参照を削除します。このコマンドは、そのノード上で **clear ns config** 拡張コマンドを内部的に実行します。さらに、SNIP アドレスとすべての VLAN 設定（デフォルト VLAN および ADCVLAN を除く）がノードから消去されます。
2. クラスターからノードを削除します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> - CCO であるノードを削除すると、現在のクラスター IP アドレスセッションはすべて無効になります。別のクラスターノードが CCO になり、クラスター IP アドレスがそのノードに割り当てられます。クラスター IP アドレスを使用して新しいセッションを開始する必要があります。
> - クラスター (およびすべてのノード) を削除するには、各ノードを個別に削除する必要があります。最後のノードを削除すると、クラスタ IP アドレスが削除されます。

Citrix ADC コマンドラインを使用してクラスターノードを削除するには

1. クラスターから削除するノードにログオンし、次の操作を行います。
   - クラスターインスタンスへの参照を削除します。`rm cluster instance <clId>`を入力します。ここで、**clId** は、ノードを削除するクラスターを識別する整数です。
   - `save ns config`を入力して構成を保存します。

   > 注:
   >
   > クラスターの最後のノードを削除するには、そのノードからクラスターインスタンスを削除するだけです。ノードはクラスターから自動的に削除されます。
2. クラスターの IP アドレスにログオンし、次の操作を行います。
   - クラスターインスタンスを削除したノードを削除します。`rm cluster node <nodeId>`を入力します。ここで、**nodeId** は、削除するノードを識別する整数です。
   - `save ns config`を入力して構成を保存します。

   > 注:
   >
   > **rm cluster node** コマンドをローカルノードから実行しないでください。この結果、CCO とノード間の設定に矛盾が生じるためです。

構成ユーティリティを使用してクラスターノードを削除するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ウィンドウの [はじめに] で、[**Cluste r** の管理] をクリックします。
4. クラスターから削除するノードを選択し、[削除] をクリックします。
5. [**OK**] をクリックします。

クラスターの詳細の表示

クラスター IP アドレスから、クラスターインスタンスとクラスターノードの詳細を表示できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC コマンドラインを使用してクラスターインスタンスの詳細を表示するには

クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します: `sh cluster instance <clId>`。**clId** は、詳細を表示するクラスターインスタンスを識別する整数です。

```
> show cluster instance 1
1)Cluster ID: 1
  Dead Interval: 3 secs
  Hello Interval: 200 msecs
  Preemption: DISABLED
  Propagation: ENABLED
  Cluster Status: ENABLED(admin), ENABLED(operational), UP
  Member Nodes:
  Node ID    Node IP    Health Admin State Operation State
  -------     -------     ------  -----------  ---------------
1)   0    10.102.29.60*   UP      ACTIVE      ACTIVE(CCO)
2)   1    10.102.29.70    UP      ACTIVE      ACTIVE
Done
<!--NeedCopy-->
```

> 注: 非 CCO ノードの ADCIP アドレスからこのコマンドを実行すると、このノード上のクラスターのステータスが表示されます。

Citrix ADC コマンドラインを使用してクラスターノードの詳細を表示するには

クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します: `sh cluster node <nodeId>`。**nodeId** は、詳細を表示するノードを識別する整数です。

```
>show cluster node 1
Node ID: 1
IP: 10.102.29.70
Backplane: 1/1/1
Health: UP
Admin state: ACTIVE
Operational State: ACTIVE
Sync State: ENABLED
<!--NeedCopy-->
```

構成ユーティリティを使用してクラスターインスタンスの詳細を表示するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ペインの **[はじめに]** で、**[クラスターの管理]** をクリックします。
4. [クラスターインスタンスの構成] ダイアログボックスで、クラスターの詳細を表示します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

構成ユーティリティを使用してクラスターノードの詳細を表示するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、**[**システム**]** を展開し、**[**クラスター**]** をクリックし、**[**ノード**]** をクリックします。
3. [クラスターノード**]** の一覧で、ノードの詳細を表示します。ノードの詳細を表示するには、ノードをクリックします。

クラスターノード間でのトラフィックの分散

Citrix ADC クラスターを作成し、必要な構成を実行したら、クライアントデータプレーン（クライアントトラフィック用）またはサーバーデータプレーン（サーバートラフィック用）に等価コストマルチパス（ECMP）またはクラスタリンクアグリゲーショングループ（CLAG）を展開する必要があります。これらのメカニズムは、外部トラフィックをクラスターノード全体に分散します。

等価コストのマルチパスの使用

等コストマルチパスメカニズムを使用すると、ルータは VIP アドレスへの等価コストルートを持ち、ネクストホップがクラスターのアクティブノードになります。ルータは、ステートレスハッシュベースのメカニズムを使用して、ルート全体にトラフィックを分散します。

> 注:
>
> ルートは、アップストリームルータでサポートされる ECMP ルートの最大数に制限されます。

ECMP を使用するには、まずクラスター IP アドレスで必要なルーティングプロトコル（OSPF、RIP、または BGP）を有効にする必要があります。インターフェイスおよびスポッティング IP アドレス（ダイナミックルーティングが有効の場合）を VLAN にバインドする必要があります。vtysh シェルを使用して、選択したルーティングプロトコルを設定し、ZebOS 上でカーネルルートを再配布します。

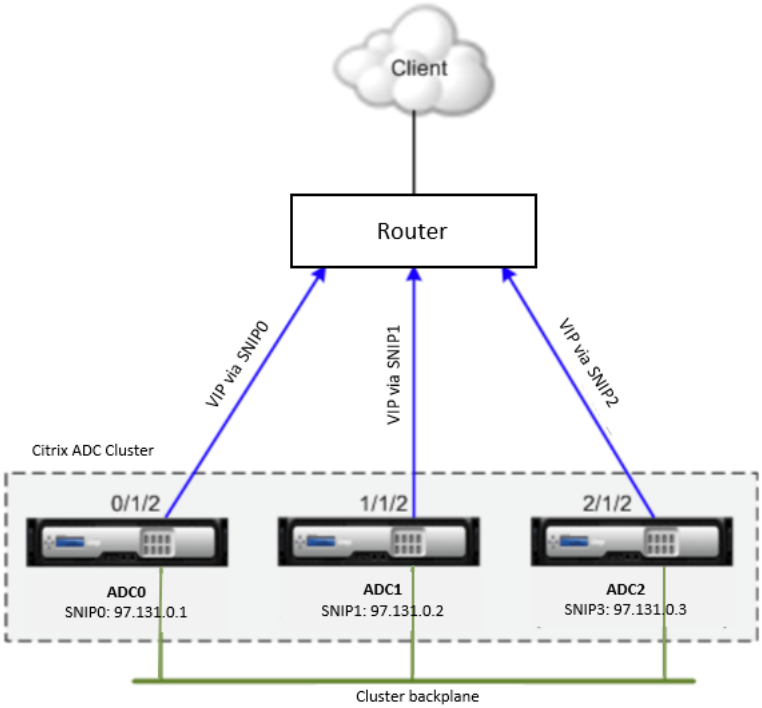
クラスター IP アドレスと外部接続デバイスでも同様の設定を行う必要があります。

ECMP を使用するには、ルーティングプロトコルに関する詳細な知識が必要です。詳しくは、「動的ルートの構成」を参照してください (/en-us/advanced-concepts/downloads/citrix-Citrix ADC-clustering-guide-v2 copy.pdf)。

> 注:
>
> クラスターのライセンスがダイナミックルーティングをサポートしていることを確認します。サポートされていない場合は、ECMP トラフィックの分散が機能しません。たとえば、標準の Citrix ADC ライセンスは、動的ルーティングをサポートしていません。

ECMP トポロジ

© 1999–2021 Citrix Systems, Inc. All rights reserved.



上の図に示すように、ECMP ルーターは、SNIP0、SNIP1、または SNIP2 を介して VIP アドレスに到達することができます。

Citrix ADC コマンドラインを使用して、**Citrix ADC** クラスターで **ECMP** を構成するには

1. クラスター IP アドレスにログオンします。
2. ルーティングプロトコル（OSPF、RIP、または BGP）を有効にします。

   ```
   enable ns feature <routing protocol>
   ```

   例:

   ```
   1 enable ns feature ospf
   2 <!--NeedCopy-->
   ```

3. VLAN を追加します。

   ```
   add vlan <vlan id>
   ```

   例:

   ```
   1 add vlan 97
   2 <!--NeedCopy-->
   ```

4. クラスターノードのインターフェイスを VLAN にバインドします。

   ```
   bind vlan <vlan id> -ifnum <interface_name>
   ```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

例:

```
bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
<!--NeedCopy-->
```

5. 各ノードにスポッティング SNIP アドレスを追加し、そのノードで動的ルーティングを有効にします。

   ```
   add ns ip <SNIP> <netmask> -ownerNode <node id> -dynamicRouting ENABLED
   ```

   例:

   ```
   add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
   ENABLED -type SNIP
   add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
   ENABLED -type SNIP
   add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
   ENABLED -type SNIP
   <!--NeedCopy-->
   ```

6. スポットのある SNIP アドレスの 1 つを VLAN にバインドします。スポッティング SNIP アドレスを 1 つの VLAN にバインドすると、そのサブネット内のクラスターで定義されている他のすべてのスポッティング SNIP アドレスは、自動的に VLAN にバインドされます。

   ```
   bind vlan <vlan id> -ipAddress <SNIP> <netmask>
   ```

   例:

   ```
   bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
   <!--NeedCopy-->
   ```

   > 注:
   >
   > SNIP アドレスを追加する代わりに、クラスターノードの ADCIP アドレスを使用できます。その場合は、手順 3 ～6 を実行する必要はありません。

7. vtysh シェルを使用して ZebOS 上でルーティングプロトコルを設定します。ノード ID 0、1、および 2 で OSPF ルーティングプロトコルを設定します。

   ```
   !
   interface vlan97
   !
   router ospf
   owner-node 0
   ospf router-id 97.131.0.1
   exit-owner-node
   owner-node 1
   ospf router-id 97.131.0.2
   exit-owner-node
   ```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
owner-node 2
ospf router-id 97.131.0.3
exit-owner-node
redistribute kernel
network 97.0.0.0/8 area 0
!
<!--NeedCopy-->
```

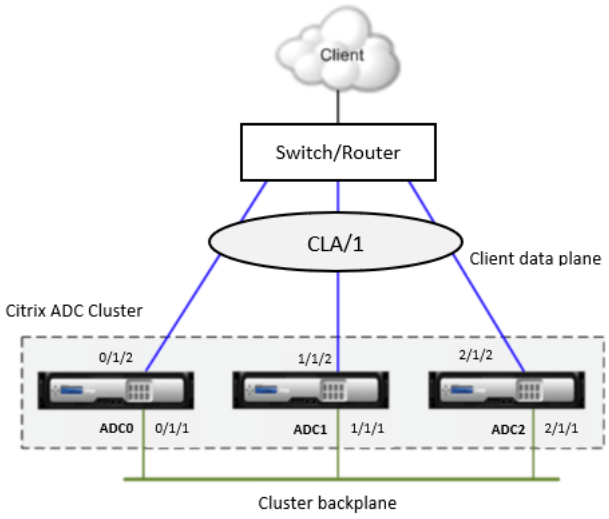
クラスターリンク集約グループ **(CLAG)** の使用

クラスタリンク集約グループは、名前が示すように、クラスターノードのインターフェイスのグループです。これは、Citrix ADC リンクアグリゲーションを拡張したものです。唯一の違いは、リンクアグリゲーションでは、同じデバイスからのインターフェイスが必要ですが、CLAG では、インターフェイスはクラスターの異なるノードからのものであることです。

リンク集約について詳しくは、「リンク集約の設定」を参照してください。

CLAG は、静的または動的のいずれかになります。たとえば、3 つのノードすべてがアップストリームスイッチに接続されている 3 ノードのクラスターを考えてみます。CLAG チャネル（CLA/1）は、インターフェイス 0/1/2、1/1/2、および 2/1/2 のバインディングによって形成されます。

クラスタリンク集約グループトポロジ



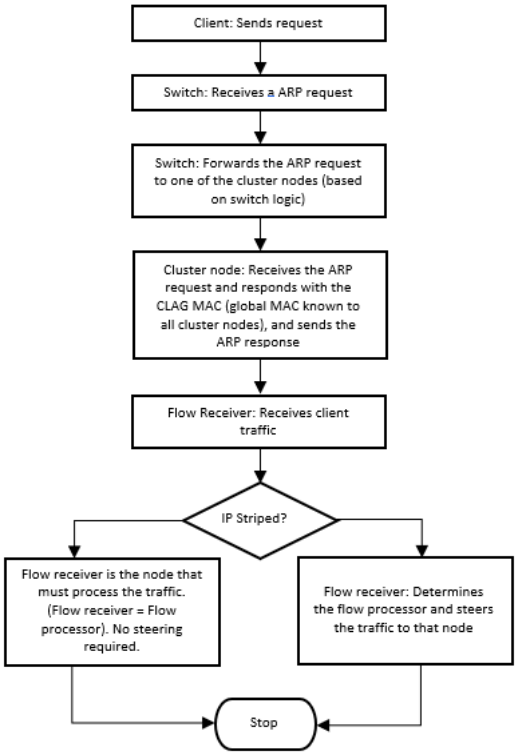
CLAG チャネルには、次の属性があります。

- 各チャネルには、クラスターノードによって合意された一意の MAC があります。
- チャネルは、ローカルノードとリモートノードの両方のインターフェイスをバインドできます。
- クラスターでは、最大 4 つの CLAG チャネルがサポートされます。
- バックプレーンインターフェイスを CLAG チャネルに含めることはできません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- インターフェイスが CLAG チャネルにバインドされている場合、チャネルパラメータはネットワークインターフェイスパラメータよりも優先されます。ネットワークインターフェイスは、1 つのチャネルにのみバインドできます。

CLAG を使用したトラフィック分散フロー



スタティッククラスタリンク集約グループ

スタティック CLAG チャネルは、クラスター IP アドレスおよび外部接続デバイスで設定する必要があります。可能であれば、MAC アドレスではなく IP アドレスまたはポートに基づいてトラフィックを分散するようにアップストリームスイッチを設定します。

静的 LA チャネルについて詳しくは、「リンク集約を手動で構成する」を参照してください。

Citrix ADC コマンドラインを使用して静的 **CLAG** チャネルを構成するには

1. クラスター IP アドレスにログオンします。

   > 注:
   >
   > 外部スイッチで CLAG を設定する前に、クラスター IP アドレスに CLAG チャネルを設定してください。そうしないと、CLAG チャネルが設定されていなくても、スイッチはトラフィックをクラスターに転送します。これにより、トラフィックが失われる可能性があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

2. CLAG チャネルを作成します。Add channel <clag channel id> -speed <speed> 。項目の意味は次のとおりです。

   - <clag channel id> は、CLAG チャネルを識別する一意の番号です。CLA/x の形式でなければなりません。x は 1 ～4 の範囲です。
   - <speed> は、CLAG のメンバーインターフェイスの速度です。

   例:

```
add channel CLA/1 -speed 1000
<!--NeedCopy-->
```

   > 注:
   >
   > 速度をAUTOとして指定しないでください。速度を 10、100、1000、または 10000 に明示的に指定する必要があります。CLAG <speed> のアトリビュートに一致する速度を持つインターフェイスだけが、アクティブな同報リストに追加されます。

3. 必要なインターフェイスを CLAG チャネルにバインドします。インターフェイスがクラスターバックプレーンに使用されていないことを確認します。Bind channel <clag channel id> <interface_name ...>。項目の意味は次のとおりです。

   - <clag channel id>は、インターフェイスをバインドする CLAG チャネルを識別します。
   - <interface_name>は、CLAG チャネルにバインドするインターフェイスを指定します。

   例:

```
bind channel CLA/1 1/1/2 2/1/2 3/1/2
<!--NeedCopy-->
```

4. CLAG チャネル設定を確認します。Show channel <clag channel id>

   例:

```
show channel CLA/1
<!--NeedCopy-->
```

   > 注:
   >
   > CLAG チャネルを VLAN にバインドするには、bind vlan コマンドを使用します。CLAG チャネルのインターフェイスは、自動的に VLAN にバインドされます。

動的クラスタリンク集約グループ

動的 CLAG は、Link Aggregation Control Protocol（LACP）を使用します。動的 LA チャネルの設定ついて詳しくは、「リンクアグリゲーション制御プロトコルを使用したリンクアグリゲーションの構成」を参照してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラスター IP アドレスと外部接続デバイスでも同様の設定を行う必要があります。可能であれば、MAC アドレスではなく IP アドレスまたはポートに基づいてトラフィックを分散するようにアップストリームスイッチを設定します。

確認事項:

- LACP を有効にします（LACP モードを ACTIVE または PASSIVE に指定します）。

  > 注:
  >
  > Citrix ADC クラスターと外部接続デバイスの両方で、LACP モードがパッシブに設定されていないことを確認します。

- チャネルの一部にする各インターフェイスで、同じ LACP キーを指定します。CLAG チャネルを作成するために、LACP キーは 5 ～8 の値を持つことができます。

  たとえば、インターフェイス 1/1/2 および 2/1/2 に LACP キーを設定すると、CLA/1 が作成されます。インターフェイス 1/1/2 および 2/1/2 は、自動的に CLA/1 にバインドされます。同様に、LACP キーを 6 に設定すると、CLA/2 チャネルが作成されます。

- LAG タイプをクラスターとして指定します。

Citrix ADC コマンドラインを使用して動的な **CLAG** チャネルを構成するには

クラスター IP アドレスで、CLAG チャネルに追加するインターフェイスごとに、次のように入力します: `set interface <interface id> -lacpMode <lacpMode> -lacpKey <lacpKey> -lagType Cluster`

3 つのインターフェイスの CLAG チャネルを設定します。

```
set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
<!--NeedCopy-->
```

リンクセットの使用

リンクセットは、一部のクラスターノードが外部ネットワークに物理的に接続されていない場合に使用する必要があります。このようなクラスタトポロジでは、接続されていないクラスターノードは、リンクセットで指定されたインターフェイスを使用して、クラスターバックプレーンを介して外部ネットワークと通信します。リンクセットは、通常、接続するデバイスにクラスターノードを接続するための十分なポートがないシナリオで使用されます。

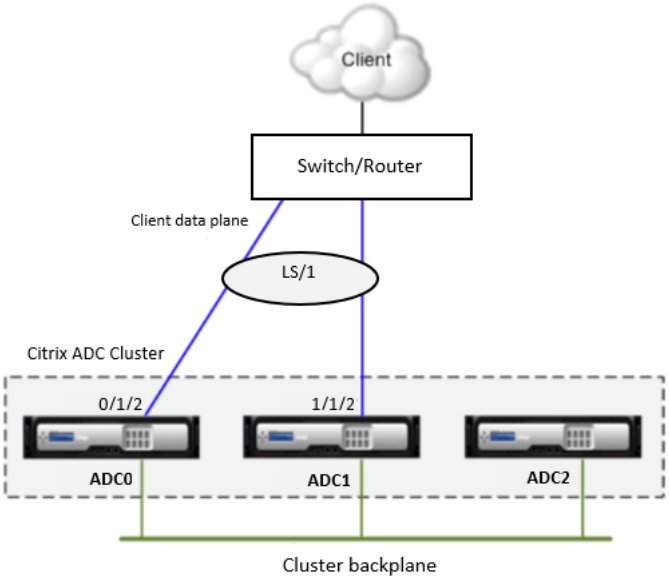
リンクセットは、クラスター IP アドレス上でのみ設定する必要があります。

たとえば、アップストリームスイッチに 2 つのポートしか使用できない 3 ノードクラスターがあるとします。リンクセットを使用すると、2 つのノードをスイッチに接続し、3 番目のノードを未接続のままにすることができます。次の図では、リンクセット（LS/1）は、インターフェイス 0/1/2 と 1/1/2 をバインドすることによって形成されています。ADC2 は、クラスターの未接続ノードです。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> MAC ベースフォワーディング（MBF）を必要とするトポロジのパフォーマンスを向上させるには、リンクセットを使用します。

リンクセットトポロジ

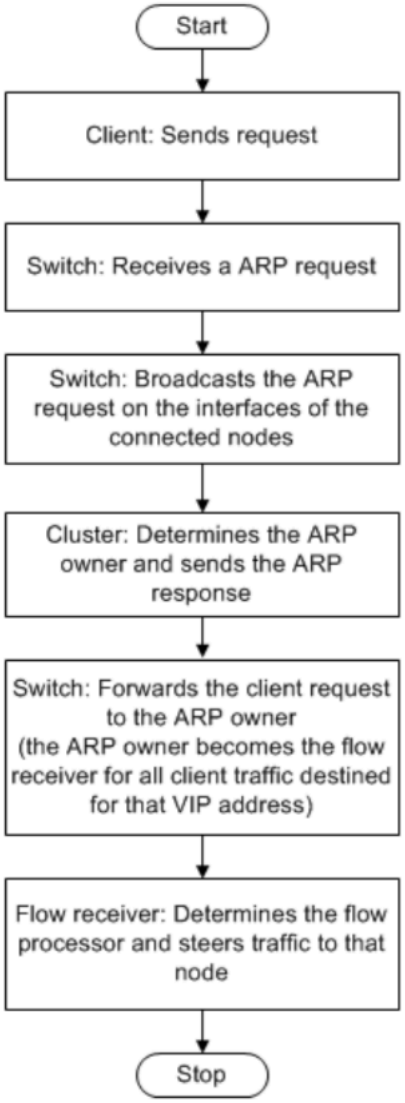


リンクセットは、ADC2 にインターフェイス 0/1/2 および 1/1/2 を使用してネットワークデバイスと通信できることを通知します。ADC2 との間で送受信されるすべてのトラフィックは、インターフェイス 0/1/2 または 1/1/2 を介してルーティングされます。

リンクセットを使用したトラフィック分散フロー

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Figure 1-10. Traffic distribution flow using linksets



Citrix ADC コマンドラインを使用してリンクセットを構成するには

1. クラスター IP アドレスにログオンします。
2. リンクセットを作成します。リンクセットを追加するには、と入力します `linkset id`。`Linkset id` はリンクセットの一意の識別子です。これは、LS/x の形式でなければなりません。例:

```
1 add linkset LS/1
2 <!--NeedCopy-->
```

3. 必要なインターフェースをリンクセットにバインドします。インターフェイスがクラスターバックプレーンに使用されていないことを確認します。リンクセットをバインドするには、と入力します <`linkset id`> –

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ifnum <interface_name...>。Interface_name は、リンクセットにバインドするインターフェイスを指定します。例:

```
bind linkset LS/1 -ifnum 0/1/2 1/1/2
<!--NeedCopy-->
```

4. リンクセットの設定を確認します。リンクセットを表示するには、と入力します linkset id。Linkset id は、検証するリンクセットの識別子です。例:

```
show linkset LS/1
<!--NeedCopy-->
```

> 注:
>
> bind vlan コマンドを使用して、リンクセットを VLAN にバインドできます。リンクセットのインターフェイスは、自動的に VLAN にバインドされます。

構成ユーティリティを使用してリンクセットを構成するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、[ネットワーク] を展開し、[リンクセット] をクリックします。
3. 詳細ウィンドウで、[追加] をクリックします。
4. [リンクセットを作成] ダイアログボックスで、次の操作を行います。
   a) Link **set** パラメータを設定して、リンクセットの名前を指定します。
   b) リンクセットに追加する インターフェイスを指定し、[**Add**] をクリックします。リンクセットに追加するインターフェイスごとに、この手順を繰り返します。
5. [作成] をクリックし、[閉じる] をクリックします。

Citrix ADC クラスターを管理する

クラスターを作成し、必要なトラフィック分散メカニズムを設定したら、クラスターはトラフィックを処理できます。クラスターの存続期間中、クラスターのノードの無効化、Citrix ADC アプライアンスの検出、統計の表示、クラスター構成、クラスタファイル、およびノード間の時間の同期、クラスターノードのソフトウェアのアップグレードまたはダウングレードなどのクラスタ管理タスクを実行できます。

クラスターノードを無効にする

そのノードのクラスターインスタンスを無効にすることで、クラスターからノードを一時的に削除できます。無効化されたノードはクラスター構成と同期されず、トラフィックを処理できません。

Citrix ADC コマンドラインを使用してクラスターノードを無効にするには

© 1999–2021 Citrix Systems, Inc. All rights reserved.

無効にするノードの Citrix ADC コマンドプロンプトで、クラスターインスタンスを無効にするには、と入力します `clId`。**ClID** は、無効にするクラスターインスタンスを識別します。

> 注:
>
> クラスターを無効にするには、クラスター IP アドレスに対して disable cluster インスタンスコマンドを実行します。

構成ユーティリティを使用してクラスターノードを無効にするには

1. 無効にするノードにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ペインの **[**はじめに**]** で、**[**クラスターの管理**]** をクリックします。
4. [クラスターインスタンスの構成] ダイアログボックスで、[クラスターインスタンスの有効化] チェックボックスをオフにします。
5. [**OK**] をクリックします。

> 注:
>
> クラスターを無効にするには、クラスター IP アドレスに対して disable cluster インスタンスコマンドを実行します。すべてのノードでクラスターインスタンスを無効にするには、クラスターにログオンし、上記の手順を実行します。

Citrix ADC アプライアンスの検出

CCO の ADCIP アドレスと同じサブネットに存在する Citrix ADC アプライアンスを検出できます。その後、検出されたアプライアンスをクラスターに追加できます。

> 注:
>
> この操作は、構成ユーティリティからのみ実行できます。

Citrix ADC 構成ユーティリティを使用してアプライアンスを検出するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックし、[ノード] をクリックします。
3. 詳細ペインで、ページの下部にある [**Citrix ADC** の検出] をクリックします。
4. [**Citrix ADC** の検出] ダイアログボックスで、次のパラメータを設定します。
   - **IP** アドレス範囲 -Citrix ADC アプライアンスを検出する IP アドレスの範囲を指定します。たとえば、10.102.29.4 ～10.102.29.15 の間のすべての ADCIP アドレスを検索するには、このオプションを 10.102.29.4 ～15 と指定します。
   - バックプレーンインターフェイス：バックプレーンインターフェイスとして使用するインターフェイスを指定します。これはオプションのパラメーターです。このパラメーターを指定しない場合は、ノードをクラスターに追加した後にパラメーターを更新する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

5. [**OK**] をクリックします。
6. クラスターに追加する Citrix ADC アプライアンスを選択します。
7. [**OK**] をクリックします。

クラスターの統計情報の表示

クラスターインスタンスとクラスターノードの統計情報を表示して、パフォーマンスを評価したり、クラスターの操作をトラブルシューティングしたりできます。

Citrix ADC コマンドラインを使用してクラスターインスタンスの統計情報を表示するには

クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します。

```
stat cluster instance <clId>
```

```
1  >stat cluster instance
2  Cluster Instance Summary
3  Cluster Size                                    3
4  Cluster Status                              ENABLED
5  Cluster Config Coordinator (CCO)        10.102.29.80
6  Current DFD Sessions                            0
7  Total Steered Packets                           0
8  Done
9  <!--NeedCopy-->
```

クラスターインスタンスの統計とエラー統計を表示するには、クラスター IP アドレスの Citrix ADC コマンドプロンプトで次のように入力します。

```
stat cluster instance -detail <clId>
```

```
1  > stat cluster instance -detail
2  Cluster Statistics
3  Summary
4  Cluster Size                                    3
5  Cluster Status                              ENABLED
6  Cluster Config Coordinator (CCO)        10.102.29.80
7  Current DFD Sessions                            0
8  Total Steered Packets                           0
9  Error Statistics
10 DFD Dropped Packets                             0
11 Propagation timeout                             0
12 Done
13 <!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC コマンドラインを使用してクラスターノードの統計情報を表示するには

クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します：`stat cluster node`。

```
> stat cluster node
Cluster Node Summary
NodeID NodeIP       State    Health  Sync State HB Tx HB Rx
0      10.102.29.70 ACTIVE   UP      ENABLED    4489  2247
1      10.102.29.80 ACTIVE   UP      ENABLED    2659  4805
2      10.102.29.60 INACTIVE UNKNOWN UNKNOWN    7145  0
Done
<!--NeedCopy-->
```

個々のクラスターノードの統計情報を表示するには、クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します。`stat cluster node <nodeid>`。

```
> stat cluster node 1
Node ID : 1
Node IP                                  10.102.29.80
Master State                                ACTIVE
Health                                          UP
Sync State                                  ENABLED
Heartbeats Sent                                3025
Heartbeats received                            5537
NNM Statistics
NNM current connections                           7
NNM total transmitted messages                   15
NNM total received messages                      18
Error Statistics
NNM Multicast/Broadcast req err                   0
Done
<!--NeedCopy-->
```

構成ユーティリティを使用してクラスターインスタンスの統計を表示するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細情報のウィンドウ領域で、ページの中央にある [統計] をクリックします。

構成ユーティリティを使用してクラスターノードの統計情報を表示するには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、**[システム]** を展開し、**[クラスター]** をクリックし、**[ノード]** をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

3. 詳細ペインでノードを選択し、[**Statistics**] をクリックしてノードの統計情報を表示します。すべてのノードの統計情報を表示するには、特定のノードを選択せずに [**Statistics**] をクリックします。

クラスター構成の同期

CCO で使用可能な Citrix ADC 構成は、次の場合にクラスターの他のノードと同期されます。

- ノードがクラスターに参加します。
- ノードがクラスターに再参加します。
- CCO で新しいコマンドが実行されます。

さらに、CCO で使用可能な構成を特定のクラスターノードに強制的に同期できます（完全同期）。一度に 1 つのクラスターノードを同期するようにしてください。同期しないと、クラスタが影響を受けます。

Citrix ADC コマンドラインを使用してクラスター構成を同期するには

CCO 構成を同期するアプライアンスの Citrix ADC コマンドプロンプトで、「強制クラスタ同期」と入力します。

構成ユーティリティを使用してクラスター構成を同期するには

1. CCO 設定を同期するアプライアンスにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ウィンドウの [ユーティリティ] で、[クラスターの同期を強制する] をクリックします。
4. [**OK**] をクリックします。

クラスタファイルの同期

CCO で使用できるファイルは、クラスタファイルと呼ばれます。これらのファイルは、ノードがクラスターに追加されると、他のクラスターノードで自動的に同期され、クラスターの存続期間中に定期的に同期されます。また、クラスタファイルを手動で同期することもできます。

同期される CCO のディレクトリとファイルは、次のとおりです。

```
- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/bookmark/
- /nsconfig/dns/
- /nsconfig/htmlinjection/
- /netscaler/htmlinjection/ens/
- /nsconfig/monitors/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
12 -  /nsconfig/inetd.conf
13 -  /nsconfig/syslog.conf
14 -  /nsconfig/snmpd.conf
15 -  /nsconfig/ntp.conf
16 -  /nsconfig/httpd.conf
17 -  /nsconfig/sshd_config
18 -  /nsconfig/hosts
19 -  /nsconfig/enckey
20 -  /var/nslw.bin/etc/krb5.conf
21 -  /var/nslw.bin/etc/krb5.keytab
22 -  /var/lib/likewise/db/
23 -  /var/download/
24 -  /var/wi/tomcat/webapps/
25 -  /var/wi/tomcat/conf/Catalina/localhost/
26 -  /var/wi/java_home/lib/security/cacerts
27 -  /var/wi/java_home/jre/lib/security/cacerts
28 -  /nsconfig/license/
29 -  /nsconfig/rc.conf-
30 <!--NeedCopy-->
```

Citrix ADC コマンドラインを使用してクラスタファイルを同期するには

クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します：`sync cluster files <mode>`。

- **mode** は、同期するディレクトリまたはファイルを指定します。可能な値は、すべて、ブックマーク、ssl、htmlinjection、インポート、その他、dns、all_plus_misc です。デフォルト値は all です。

構成ユーティリティを使用してクラスタファイルを同期するには

1. クラスターにログオンします。
2. ナビゲーションウィンドウで、[システム] を展開し、[クラスター] をクリックします。
3. 詳細ウィンドウの [ユーティリティ] で、[クラスターファイルの同期] をクリックします。
4. [クラスタファイルの同期] ダイアログボックスで、同期するファイルを [モード] ドロップダウンボックスで選択します。
5. [**OK**] をクリックします。

クラスターノードでの時刻の同期

Citrix ADC クラスターは、プレシジョンタイムプロトコル（PTP）を使用して、クラスターノード間で時刻を同期します。PTP は、マルチキャストパケットを使用して時刻を同期させます。時刻同期に問題がある場合は、PTP を無効にして、クラスターでネットワークタイムプロトコル (NTP) を構成する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC コマンドラインを使用して **PTP** を有効または無効にするには

クラスタ IP アドレスの Citrix ADC コマンドプロンプトで、次のように入力します：`set ptp -state disable`。

構成ユーティリティを使用して **PTP** を有効/無効にするには

1. クラスター IP アドレスにログオンします。
2. ナビゲーションウィンドウで、**[システム]** を展開し、**[クラスター]** をクリックします。
3. 詳細ペインの [ユーティリティ] で、[**PTP** 設定の構成] をクリックします。
4. [**PTP** の有効化/無効化] ダイアログボックスで、PTP を有効にするか無効にするかを選択します。
5. [**OK**] をクリックします。

クラスターのソフトウェアのアップグレードまたはダウングレード

すべてのクラスターノードで同じソフトウェアバージョンを実行している必要があります。クラスターのソフトウェアをアップグレードまたはダウングレードするには、各ノードのソフトウェアを一度に 1 ノードずつアップグレードまたはダウングレードする必要があります。

ノード上のソフトウェアをアップグレードまたはダウングレードしても、ノードはクラスターから削除されません。ノードは、アップグレードまたはダウングレード後にノードが再起動するときのダウンタイムを除き、クラスターの一部であり、中断なくクライアントトラフィックを処理します。ただし、クラスターノード間でソフトウェアバージョンが一致しないため、構成の伝播は無効になり、すべてのクラスターノードが同じバージョンの後にのみ有効になります。

クラスターのダウングレード時にアップグレード中に設定の伝播が無効になるため、この間はクラスター IP アドレスを通じて設定を実行できません。ただし、ノードレベルの構成は個々のノードの ADCIP アドレスを使用して実行できますが、同期を維持するには、すべてのノードで同じ構成を実行する必要があります。

> 注：
>
> クラスタソフトウェアのバージョンのアップグレードまたはダウングレード中は、クラスターノードを追加できません。

クラスターノードのソフトウェアをアップグレードまたはダウングレードするには

1. クラスターが安定しており、すべてのノードで構成が同期されていることを確認します。
2. クラスターのソフトウェアをアップグレードまたはダウングレードします。
   - クラスターノードのソフトウェアをアップグレードまたはダウングレードします。アプライアンスのソフトウェアのアップグレードおよびダウングレードについて詳しくは、「システムソフトウェアのアップグレードまたはダウングレード」を参照してください。
   - アプライアンスを再起動します。
   - 上記の 2 つの手順を他の各クラスターノードに対して繰り返します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> 前のノードがアクティブになるまで待ってから、次のノードをアップグレードすることをお勧めします。

使用例

このトピックでは、Citrix ADC クラスターを展開するためのユースケースをいくつか紹介します。

- 2 ノードクラスターの作成
- クラスターでのキャッシュリダイレクトの使用
- リンクセットでの CLAG の使用
- クライアントとサーバー用の共通インターフェイス、およびバックプレーン用の専用インターフェイス
- クライアント、サーバ、およびバックプレーン用の共通スイッチ
- クライアント/サーバー用共通スイッチ、バックプレーン用専用スイッチ
- ノードごとに複数のスイッチ
- ノードごとに異なるスイッチ
- クラスター構成の例

2 ノードクラスターの作成

2 ノードクラスターは、クラスタが最低限 (n/2 +1) のノード (**n** はクラスターノード数) がトラフィックを処理できる場合にのみ機能するという規則の例外です。この式が 2 ノードクラスターに適用された場合、1 つのノードがダウンした場合 (n/2 +1=2)、クラスターは失敗します。

2 ノードクラスターは、1 つのノードだけがトラフィックを処理できる場合でも機能します。2 ノードクラスターの作成は、他のクラスターの作成と同じです。1 つのノードを構成コーディネータとして、もう 1 つのノードを別のクラスターノードとして追加する必要があります。

> 注:
>
> 差分構成の同期は、2 ノードクラスターではサポートされません。完全同期のみがサポートされています。

HA セットアップのクラスタセットアップへの移行

既存の高可用性（HA）セットアップをクラスターセットアップに移行するには、アプライアンスを高可用性セットアップから削除し、Citrix ADC クラスターを作成します。たとえば、ADCIP アドレスが 10.102.97.131 および 10.102.97.132 である高可用性セットアップを考えてみます。

Citrix ADC コマンドラインを使用して **HA** セットアップをクラスターセットアップに変換するには

1. 各 HA ノードにログオンし、HA セットアップから削除します。`rm HA node <nodeId>`を入力します。たとえば、`rm HA node 1`のようになります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

2. HA ノードの 1 つのシェルに移動し、`ns.conf`を別の`.conf`ファイルにコピーします。たとえば、`ns_backup.conf`のようになります。
3. 新しい設定ファイルを次のように編集します。
   - クラスターでサポートされていない機能をすべて削除します。サポートされていない機能のリストについては、「クラスターでサポートされる Citrix ADC 機能」を参照してください。
   - インターフェイスを持つ設定を削除するか、c/u 規約から **n/c/u** 規約にインターフェイス名を更新します。
4. 両方のノードで、クラスターバックプレーンに使用するネットワークインターフェイスを指定します。
5. いずれかのノード（10.102.97.131 など）を CCO ノードとして設定します。詳しい手順については、「Citrix ADC クラスターをセットアップする」を参照してください。
6. クラスター IP アドレスにログオンし、バックアップ構成ファイルから構成を適用します。`batch -f <fileName>`を入力します。たとえば、`batch -f ns_backup.conf`のようになります。
7. 構成を保存します。`save ns config`を入力します。
8. もう一方のノードをクラスターに追加します。詳しい手順については、「クラスターへのノードの追加」を参照してください。

HA セットアップのアプライアンスがクラスタセットアップに移行されます。

クラスターでのキャッシュリダイレクトの使用

Citrix ADC クラスター内のキャッシュリダイレクトは、スタンドアロンの Citrix ADC アプライアンスと同じように機能します。唯一の違いは、構成がクラスター IP アドレスで実行されることです。詳しくは、「キャッシュのリダイレクト」セクションを参照してください。

トランスペアレントモードでキャッシュリダイレクトを使用する際の注意点:

- キャッシュリダイレクトを設定する前に、すべてのノードを外部スイッチに接続し、リンクセットが設定されていることを確認します。それ以外の場合、クライアント要求はドロップされます。
- ロードバランシング仮想サーバーで MAC モードが有効になっている場合は、クラスターで MBF モードが有効になっていることを確認します（`enable ns mode MBF` コマンドを使用）。それ以外の場合、要求はキャッシュサーバーに送信されるのではなく、オリジンサーバーに直接送信されます。

リンクセットでの **CLAG** の使用

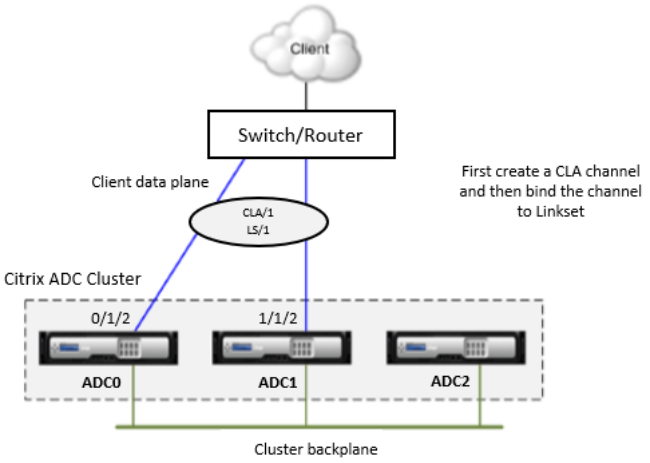
非対称クラスタートポロジでは、一部のクラスターノードがアップストリームネットワークに接続されていません。そのような場合は、リンクセットを使用する必要があります。パフォーマンスを最適化するには、スイッチに接続されているインターフェイスを CLA チャネルとしてバインドしてから、CLA チャネルをリンクセットにバインドします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

CLAG とリンクセットの組み合わせの使用方法を理解するために、アップストリームスイッチで使用できるポートが 2 つしかない 3 ノードクラスターについて考えます。2 つのクラスターノードをスイッチに接続し、もう一方のノードを接続しないままにしておくことができます。

> 注:
>
> 同様に、非対称トポロジで ECMP とリンクセットの組み合わせを使用することもできます。

リンクセットとクラスターリンク集約グループトポロジ

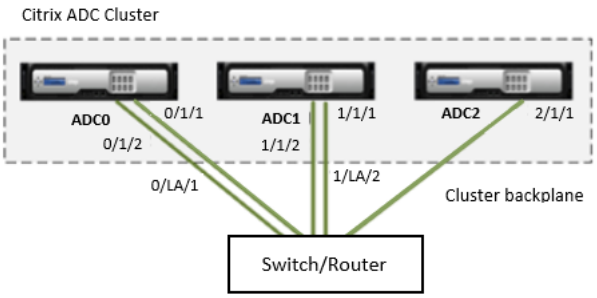


Citrix ADC コマンドラインを使用して **CLAG** とリンクセットを使用するには

1. クラスター IP アドレスにログオンします。
2. 接続されたインターフェイスを CLA チャネル`add channel CLA/1 -ifnum 0/1/2 1/1/2`にバインドする
3. CLA チャネルをリンクセット`add linkset LS/1 -ifnum CLA/1`にバインドする

LA チャネル上のバックプレーン

この配置では、LA チャネルがクラスターバックプレーンに使用されます。



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC0 - nodeId: 0, ADCIP: 10.102.29.60

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

バックプレーンインターフェイスを **LA** チャネルとしてクラスターを展開するには

1. ノード ADC0、ADC1、ADC2 のクラスターを作成します。

   - クラスターに追加する最初のノードにログオンし、次の操作を行います。

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - クラスターの IP アドレスにログオンし、次の操作を行います。

```
add cluster node 1 10.102.29.70 -state ACTIVE
add cluster node 2 10.102.29.80 -state ACTIVE
<!--NeedCopy-->
```

   - ノード 10.102.29.70 および 10.102.29.80 にログオンし、ノードをクラスターに参加させます。

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

   上記のコマンドで示されているように、インターフェイス 0/1/1、1/1/1、および 2/1/1 は、3 つのクラスターノードのバックプレーンインターフェイスとして設定されています。

2. クラスターの IP アドレスにログオンし、次の操作を行います。

   - ノード ADC0 と ADC1 の LA チャネルを作成します。

```
add channel 0/LA/1 -ifnum 0/1/1 0/1/2
add channel 1/LA/2 -ifnum 1/1/1 1/1/2
<!--NeedCopy-->
```

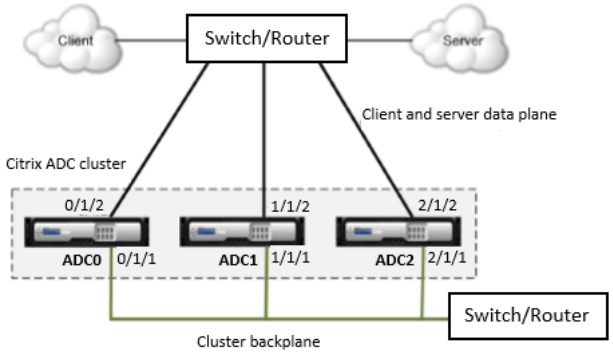
   - クラスターノードのバックプレーンを設定します。

```
set cluster node 0 -backplane 0/LA/1
set cluster node 1 -backplane 1/LA/2
set cluster node 2 -backplane 2/1/1
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クライアントとサーバ用の共通インターフェイス、およびバックプレーン用の専用インターフェイス

これは、Citrix ADC クラスターのワンアーム展開です。この展開では、クライアントネットワークとサーバーネットワークが同じインターフェイスを使用してクラスターと通信します。クラスターバックプレーンは、ノード間通信専用のインターフェイスを使用します。



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

クライアントとサーバ用の共通のインターフェイスと、クラスターバックプレーン用の異なるインターフェイスを持つクラスターを展開するには

1. ノード ADC0、ADC1、ADC2 のクラスターを作成します。

   - クラスターに追加する最初のノードにログオンし、次の操作を行います。

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - クラスターの IP アドレスにログオンし、次の操作を行います。

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```

   - ノード 10.102.29.70 および 10.102.29.80 にログオンし、ノードをクラスターに参加させます。

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
reboot -warm
<!--NeedCopy-->
```

上記のコマンドで示されているように、インターフェイス 0/1/1、1/1/1 および 2/1/1 は、3 つのクラスターノードのバックプレーンインターフェイスとして設定されています。

2. クラスター IP アドレスで、バックプレーンインターフェイスおよびクライアントインターフェイスおよびサーバインターフェイス用の VLAN を作成します。

```
//For the backplane interfaces
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
//For the interfaces that are connected to the client and server networks
add vlan 20
bind vlan 20 0/1/2 1/1/2 2/1/2
<!--NeedCopy-->
```

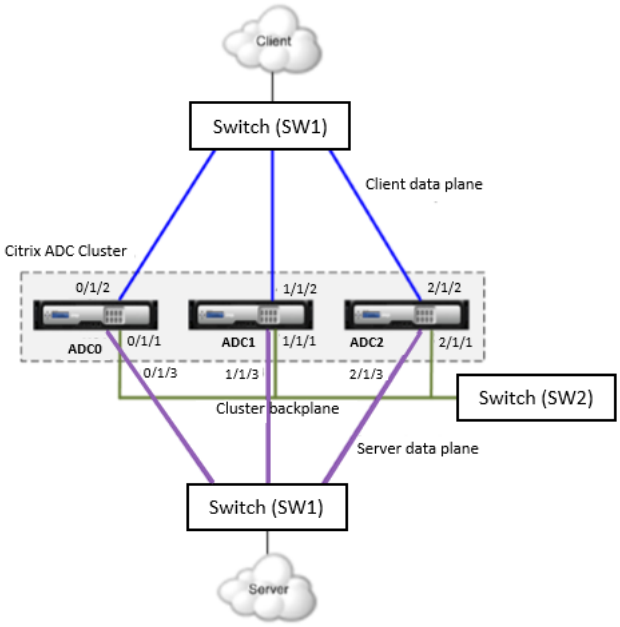
3. スイッチ上で、バックプレーンインターフェイス、およびクライアントおよびサーバインターフェイスに対応するインターフェイスの VLAN を作成します。次に、Cisco C3750 バージョン 12.2 (40) SE スイッチ用の設定例を示します。他のスイッチでも同様の設定を行う必要があります。

```
//For the backplane interfaces. Repeat for each interface...
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
end
//For the interfaces connected to the client and server networks. Repeat for each interface...
interface GigabitEthernet1/0/3
switchport access vlan 200
switchport mode access
end
<!--NeedCopy-->
```

クライアント、サーバ、バックプレーン用の共通スイッチ

この展開では、クライアント、サーバ、およびバックプレーンは同じスイッチ上の専用インターフェイスを使用して、Citrix ADC クラスターと通信します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

クライアント、サーバ、およびバックプレーン用の共通スイッチを使用してクラスターを展開するには

1. ノード ADC0、ADC1、ADC2 のクラスターを作成します。

   - クラスターに追加する最初のノードにログオンし、次の操作を行います。

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1 add ns ip 10.102.29.61 255.255.255.255 -
    type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - クラスターの IP アドレスにログオンし、次の操作を行います。

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```

   - ノード 10.102.29.70 および 10.102.29.80 にログオンし、ノードをクラスターに参加させます。

```
join cluster -clip 10.102.29.61 -password nsroot
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
save ns config
reboot -warm
<!--NeedCopy-->
```

上記のコマンドで示されているように、インターフェイス 0/1/1、1/1/1、および 2/1/1 は、3 つのクラスターノードのバックプレーンインターフェイスとして設定されています。

2. クラスター IP アドレスで、バックプレーン、クライアント、およびサーバインターフェイスの VLAN を作成します。

```
//For the backplane interfaces
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
//For the client-side interfaces
add vlan 20 bind vlan 20 0/1/2 1/1/2 2/1/2
//For the server-side interfaces
add vlan 30
bind vlan 30 0/1/3 1/1/3 2/1/3
<!--NeedCopy-->
```

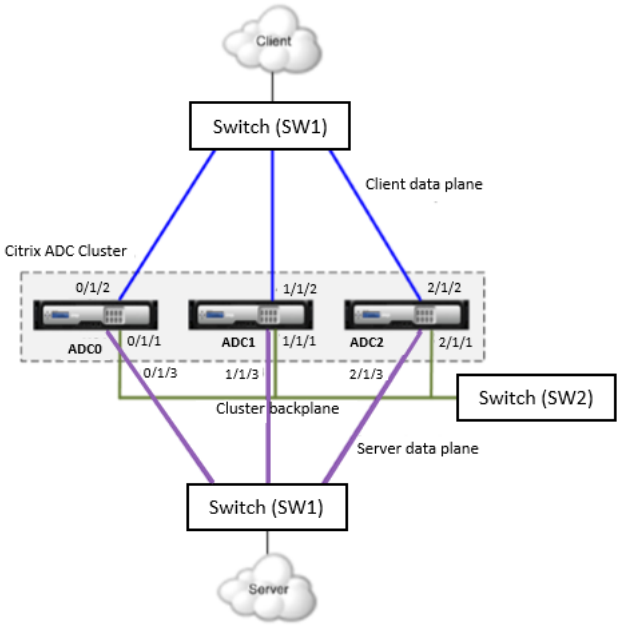
3. スイッチ上で、バックプレーンインターフェイス、およびクライアントおよびサーバインターフェイスに対応するインターフェイスの VLAN を作成します。次に、Cisco C3750 バージョン 12.2 (40) SE スイッチ用の設定例を示します。他のスイッチでも同様の設定を行う必要があります。

```
//For the backplane interfaces. Repeat for each interface...
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
end
//For the client interfaces. Repeat for each interface...

interface GigabitEthernet1/0/3
switchport access vlan 200
switchport mode access
end
//For the server interfaces. Repeat for each interface...

interface GigabitEthernet1/0/6
switchport access vlan 300
switchport mode access
end
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クライアント/サーバ用共通スイッチ、バックプレーン専用スイッチ

この展開では、クライアントとサーバーは同じスイッチ上で異なるインターフェイスを使用して Citrix ADC クラスターと通信します。クラスターバックプレーンは、ノード間通信専用のスイッチを使用します。



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

クライアントとサーバーには同じスイッチを使用し、クラスターバックプレーンには別のスイッチを使用してクラスターを展開するには

1. ノード ADC0、ADC1、ADC2 のクラスターを作成します。
   - クラスターに追加する最初のノードにログオンし、次の操作を行います。

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - クラスターの IP アドレスにログオンし、次の操作を行います。

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
<!--NeedCopy-->
```

- ノード 10.102.29.70 および 10.102.29.80 にログオンし、ノードをクラスターに参加させます。

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

上記のコマンドで示されているように、インターフェイス 0/1/1、1/1/1 および 2/1/1 は、3 つのクラスターノードのバックプレーンインターフェイスとして設定されています。

2. クラスター IP アドレスで、バックプレーン、クライアント、およびサーバインターフェイスの VLAN を作成します。

```
//For the backplane interfaces
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
//For the client-side interfaces
add vlan 20
bind vlan 20 0/1/2 1/1/2 2/1/2
//For the server-side interfaces
add vlan 30
bind vlan 30 0/1/3 1/1/3 2/1/3
<!--NeedCopy-->
```

1. スイッチ上で、バックプレーンインターフェイス、およびクライアントおよびサーバインターフェイスに対応するインターフェイスの VLAN を作成します。次に、Cisco C3750 バージョン 12.2 (40) SE スイッチ用の設定例を示します。他のスイッチでも同様の設定を行う必要があります。

```
//For the backplane interfaces. Repeat for each interface...
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
end

//For the client interfaces. Repeat for each interface...
interface GigabitEthernet1/0/3
switchport access vlan 200
switchport mode access
end

//For the server interfaces. Repeat for each interface...
interface GigabitEthernet1/0/6
switchport access vlan 300
```

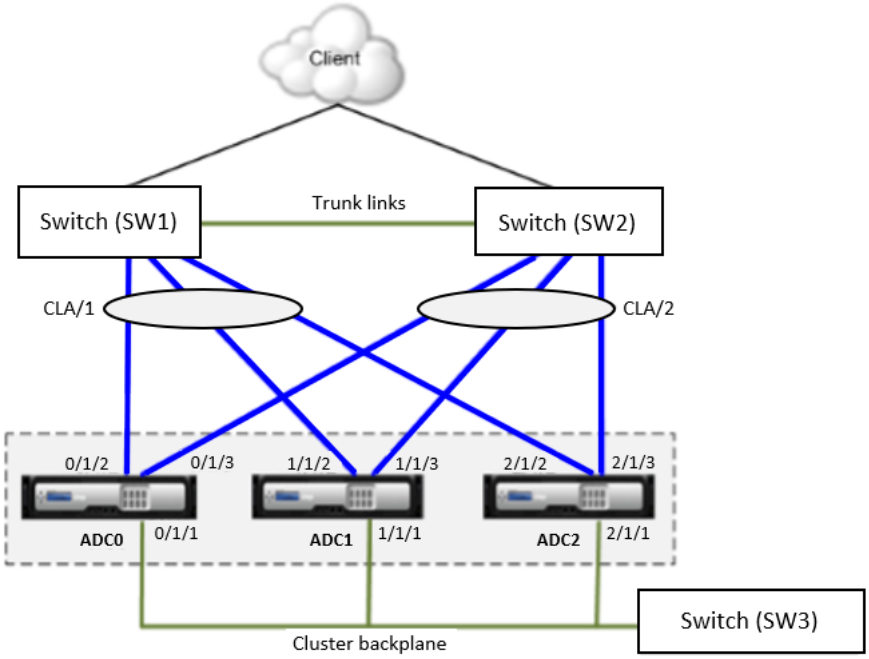
© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
16 switchport mode access
17 end
18 <!--NeedCopy-->
```

ノードごとに複数のスイッチ

この展開では、2 つのクライアント側スイッチを導入して、クライアント側のスイッチの冗長性を確保します。スイッチは、トランクリンクによって相互に接続されます。1 つのスイッチで障害が発生しても、クラスタ全体の動作には影響しません。

> 注:
>
> サーバー側の接続にも同じ展開方法を使用できます。



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

> 注:
>
> トランクリンクを使用すると、トラフィックがループで流れる可能性があります。これを回避するには、ループを回避するようにネットワークトポロジを構成する必要があります。

各ノードを **2** つのスイッチに接続し、スイッチをトランクリンクで接続したクラスターを展開するには

1. ノード ADC0、ADC1、ADC2 のクラスターを作成します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- クラスターに追加する最初のノードにログオンし、次の操作を行います。

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

- クラスターの IP アドレスにログオンし、次の操作を行います。

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```

- ノード 10.102.29.70 および 10.102.29.80 にログオンし、ノードをクラスターに参加させます。

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

上記のコマンドで示されているように、インターフェイス 0/1/1、1/1/1、および 2/1/1 は、3 つのクラスターノードのバックプレーンインターフェイスとして設定されています。

2. クラスターの IP アドレスにログオンし、次の操作を行います。

- バックプレーンインターフェイスの VLAN を作成します。

```
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
<!--NeedCopy-->
```

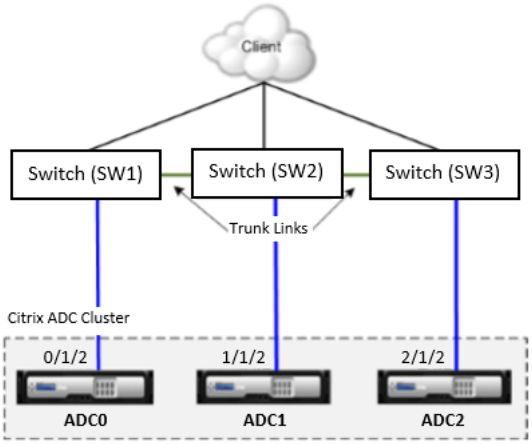
- SW1 および SW2 を使用するクライアント側インターフェイスの CLAG を作成します。

```
add channel CLA/1 -ifnum 0/1/2 1/1/2 2/1/2 -speed 1000
add channel CLA/2 -ifnum 0/1/3 1/1/3 2/1/3 -speed 1000
<!--NeedCopy-->
```

ノードごとに異なるスイッチ

この展開では、各クラスターノードは異なるスイッチに接続され、スイッチ間にトランクリンクが設定されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



クラスター構成は、他の展開シナリオと同じです。クライアント側構成のほとんどは、クライアント側スイッチで実行されます。

クラスター構成の例

次の例は、ECMP、CLAg、またはリンクセットを使用して 4 ノードクラスターを構成するために使用できます。

1. クラスターを作成します。

   - 最初のノードにログオンします。
   - クラスターインスタンスを追加します。

```
add cluster instance 1
<!--NeedCopy-->
```

   - クラスターに最初のノードを追加します。

```
add cluster node 0 10.102.33.184 -backplane 0/1/1
<!--NeedCopy-->
```

   - クラスターインスタンスを有効にします。

```
enable cluster instance 1
<!--NeedCopy-->
```

   - クラスター IP アドレスを追加します。

```
add ns ip 10.102.33.185 255.255.255.255 -type CLIP
<!--NeedCopy-->
```

   - 構成を保存します。

```
save ns config
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- アプライアンスをウォーム再起動します。

```
reboot -warm
<!--NeedCopy-->
```

2. 他の 3 つのノードをクラスターに追加します。

- クラスターにログオンします。
- 2 番目のノードをクラスターに追加します。

```
add cluster node 1 10.102.33.187 -backplane 1/1/1
<!--NeedCopy-->
```

- 3 番目のノードをクラスターに追加します。

```
add cluster node 2 10.102.33.188 -backplane 2/1/1
<!--NeedCopy-->
```

- 4 番目のノードをクラスターに追加します。

```
add cluster node 3 10.102.33.189 -backplane 3/1/1
<!--NeedCopy-->
```

3. 追加されたノードをクラスターに参加させます。この手順は、最初のノードには適用されません。

- 新しく追加された各ノードにログオンします。
- ノードをクラスターに参加させます。

```
join cluster -clip 10.102.33.185 -password nsroot
<!--NeedCopy-->
```

- 構成を保存します。

```
save ns config
<!--NeedCopy-->
```

- アプライアンスをウォーム再起動します。

```
reboot -warm
<!--NeedCopy-->
```

4. クラスター IP アドレスを使用して Citrix ADC クラスターを構成します。

```
// Enable load balancing feature enable ns feature lb
// Add a load balancing virtual server add lb vserver
    first_lbvserver http
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
....
....
<!--NeedCopy-->
```

5. クラスターの次のトラフィック分散メカニズム（ECMP、Linkset、CLAG）のいずれかを構成します。

- 欧州議会議員
  - クラスターにログオンします。
  - OSPF ルーティングプロトコルを有効にします。

```
enable ns feature ospf
<!--NeedCopy-->
```

  - VLAN を追加します。

```
add vlan 97
<!--NeedCopy-->
```

  - クラスターノードのインターフェイスを VLAN にバインドします。

```
bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
<!--NeedCopy-->
```

  - 各ノードにスポッティング SNIP を追加し、そのノードで動的ルーティングを有効にします。

```
add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 dynamicRouting
    ENABLED
add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 dynamicRouting
    ENABLED
add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 dynamicRouting
    ENABLED
add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 dynamicRouting
    ENABLED
<!--NeedCopy-->
```

  - SNIP アドレスのいずれかを VLAN にバインドします。

```
bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
<!--NeedCopy-->
```

  - vtysh シェルを使用して、ZebOS 上でルーティングプロトコルを設定します。
- リンクセット。nodeId3 のノードがスイッチに接続されていないと仮定します。接続されていないノードが他のノードインターフェイスを使用してスイッチと通信できるように、リンクセットを設定する必要があります。
  - クラスターにログオンします。
  - リンクセットを追加します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
add linkset LS/1
<!--NeedCopy-->
```

- 接続されたインターフェイスをリンクセットにバインドします。

```
bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
<!--NeedCopy-->
```

- 静的なクラグ。
  - クラスターにログオンします。
  - CLA チャネルを追加します。

```
add channel CLA/1 -speed 1000
<!--NeedCopy-->
```

  - インターフェイスを CLA チャネルにバインドします。

```
bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
<!--NeedCopy-->
```

  - スイッチ上で同等の構成を実行します。
- 動的クラグ。
  - クラスターにログオンします。
  - インターフェイスを CLA チャネルに追加します。

```
set interface 0/1/5 -lacpmode active -lacpkey 5 -lagtype
    cluster
set interface 1/1/5 -lacpmode active -lacpkey 5 -lagtype
    cluster
set interface 2/1/5 -lacpmode active -lacpkey 5 -lagtype
    cluster
set interface 3/1/5 -lacpmode active -lacpkey 5 -lagtype
    cluster
<!--NeedCopy-->
```

  - スイッチ上で同等の構成を実行します。

6. クラスターノードの状態を ACTIVE に更新します。

```
set cluster node 0 -state ACTIVE
set cluster node 1 -state ACTIVE
set cluster node 2 -state ACTIVE
set cluster node 3 -state ACTIVE
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC クラスターのトラブルシューティング

Citrix ADC クラスターで障害が発生した場合、トラブルシューティングの最初の手順は、`show cluster instance <clId>`コマンドと`show cluster node <nodeId>`コマンドをそれぞれ実行して、クラスターインスタンスとクラスターノードに関する情報を取得することです。

上記の 2 つの方法を使用して問題を見つけることができない場合は、次のいずれかを使用できます。

- 障害の原因を特定します。クラスターをバイパスしてサーバーに接続してみます。試行が成功した場合は、おそらくクラスターのセットアップに問題があります。
- 最近実行したコマンドを確認します。h **istory** コマンドを実行して、クラスターで実行した最近の設定を確認します。また、`ns.conf`ファイルを確認して、実装された構成を確認することもできます。
- **ns.log** ファイルを確認します。各ノードの`/var/log/`ディレクトリにあるログファイルを使用して、実行されたコマンド、コマンドのステータス、および状態の変化を識別します。
- **newnslog** ファイルを確認します。各ノードの`/var/nslog/`ディレクトリにある newnslog ファイルを使用して、クラスターノードで発生したイベントを識別します。複数の newnslog ファイルを 1 つのファイルとして表示するには、ファイルを 1 つのディレクトリにコピーし、次のコマンドを実行します。

```
nsconmsg -K newnslog-node<id> -K newnslog.node<id> -d current
<!--NeedCopy-->
```

それでも問題が解決しない場合は、クラスタ上のパケットをトレースするか、**show tech support scope cluster** コマンドを使用してテクニカルサポートチームにレポートを送信します。

Citrix ADC クラスターのパケットのトレース

Citrix ADC オペレーティングシステムには、アプライアンスが送受信するパケットのダンプを取得するための、nstrace というユーティリティが用意されています。このユーティリティは、パケットをトレースファイルに格納します。これらのファイルを使用して、クラスターノードへのパケットフローの問題をデバッグできます。トレースファイルは、Wireshark アプリケーションで表示する必要があります。ネイティブ（.cap）モードで収集されたトレースでは、ネイティブパケットを認識できる Wireshark の内部バージョンを使用することが重要です。

nstrace ユーティリティの重要な側面は次のとおりです。

- 従来の式とデフォルトの式を使用して、パケットを選択的にトレースするように設定できます。
- トレースを複数の形式でキャプチャできます。nstrace 形式 (.cap) と TCP ダンプ形式 (.pcap)。
- CCO 上のすべてのクラスターノードのトレースファイルを集約できます。
- 複数のトレースファイルを 1 つのトレースファイルにマージできます。

nstrace ユーティリティーは、Citrix ADC コマンドラインまたは Citrix ADC シェルから使用できます。

スタンドアロンアプライアンスのパケットをトレースするには

アプライアンスで start nstrace コマンドを実行します。このコマンドは、`/var/nstrace/<date-timestamp>`ディレクトリにトレースファイルを作成します。トレースファイル名は`nstrace<id>.cap`の形式です。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

show nstrace コマンドを実行すると、ステータスを表示できます。stop **nstrace** コマンドを実行すると、パケットのトレースを停止できます。

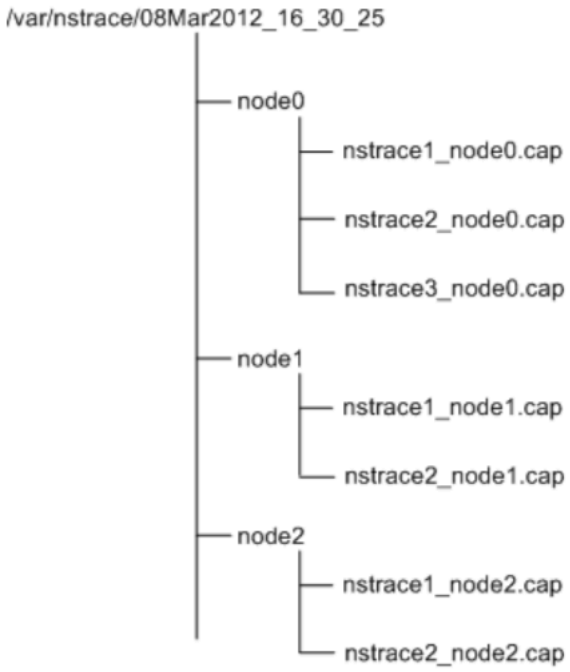
> 注:
>
> また、nstrace.sh ファイルを実行して、Citrix ADC シェルから nstrace ユーティリティを実行することもできます。Citrix ADC コマンドラインから nstrace ユーティリティを使用することをお勧めします。

クラスターのパケットをトレースするには

すべてのクラスターノード上のパケットをトレースし、CCO ノード上のすべてのトレースファイルを取得できます。

クラスター IP アドレスで **start nstrace** コマンドを実行します。コマンドが伝播され、すべてのクラスターノードで実行されます。トレースファイルは、/var/nstrace/<date-timestamp>ディレクトリ内の個々のクラスターノードに格納されます。トレースファイル名はnstrace<id>_node<id>.capの形式です。

各ノードのトレースファイルを使用して、ノードの操作をデバッグできます。ただし、すべてのクラスターノードのトレースファイルを 1 つの場所に格納する場合は、クラスター IP アドレスで **stop nstrace** コマンドを実行する必要があります。すべてのノードのトレースファイルは、次のように/var/nstrace/<date-timestamp>ディレクトリ内のクラスター構成コーディネータ (CCO) ノードにダウンロードされます。



複数のトレースファイルをマージする

クラスターノードから取得したトレースファイルから 1 つのファイルを準備できます。単一のトレースファイルは、クラスターパケットのトレースの累積的なビューを提供します。単一のトレースファイル内のトレースエントリは、クラスターでパケットが受信された時間に基づいてソートされます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

トレースファイルをマージするには、Citrix ADC シェルで、次のように入力します。nstracemerge.sh -srcdir <DIR> -dstdir <DIR> -filename <name> -filesize <num>。

- **srcdir** は、トレースファイルのマージ元のディレクトリです。このディレクトリ内のすべてのトレースファイルは、単一のファイルにマージされます。
- **dstdir** は、マージされたトレースファイルが作成されるディレクトリです。
- **filename** は、作成されるトレースファイルの名前です。
- **filesize** は、トレースファイルのサイズです。

次に、nstrace ユーティリティを使用してパケットをフィルタリングする例を示します。

- 3 つのノードのバックプレーンインターフェイス上のパケットをトレースするには、次の手順を実行します。
  - クラシックエクスプレッションの使用**:**

```
start nstrace -filter /"INTF == 0/1/1 && INTF == 1/1/1 && INTF==
    2/1/1"
<!--NeedCopy-->
```

  - 既定のエクスプレッションを使用する**:**

```
start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&CONNECTION.
    INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
<!--NeedCopy-->
```

- 送信元 IP アドレス 10.102.34.201、または送信元ポートが 80 より大きく、サービス名が”s1” でないシステムからのパケットをトレースするには、次の手順を実行します。
  - クラシックエクスプレッションの使用

```
start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
    s1 && SOURCEPORT > 80)"
<!--NeedCopy-->
```

  - 既定のエクスプレッションの使用

```
start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) ||(
    CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
<!--NeedCopy-->
```

よくある問題のトラブルシューティング

クラスターにノードを結合しているときに、次のメッセージが表示されます。「エラー**:** 無効なインターフェイス名**/**番号です。」このエラーを解決するにはどうすればいいですか**?**

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- このエラーは、**add cluster node** コマンドを使用してノードを追加するときに、無効または不正なバックプレーンインターフェイスを提供した場合に発生します。このエラーを解決するには、ノードの追加時に指定したインターフェイスを確認します。アプライアンスの管理インターフェイスをバックプレーンインターフェイスとして指定していないこと、およびインターフェイスの **nodeId** ビットがノードの Id と同じであることを確認します。たとえば、**nodeId** が **3** の場合、バックプレーンインターフェイスは3/<c>/<u>である必要があります。

ノードをクラスターに参加しているときに、次のメッセージが表示されます。「エラー**:** ローカルノードがクラスターのメンバーではないため、クラスタリングを有効にできません。」このエラーを解決するにはどうすればいいですか**?**

- このエラーは、ノードの ADCIP をクラスターに追加せずにノードに参加しようとすると発生します。このエラーを解決するには、まず add cluster node コマンドを使用して、ノードの ADCIP アドレスを クラスターに追加してから、**join cluster** コマンドを実行する必要があります。

ノードをクラスターに参加しているときに、「エラー：接続が拒否されました。」このエラーを解決するにはどうすればいいですか**?**

このエラーは、次の理由で発生する可能性があります。

- 接続の問題。ノードはクラスター IP アドレスに接続できません。参加しようとしているノードからクラスター IP アドレスに ping を実行してみます。
- クラスター **IP** アドレスが重複しています。クラスター IP アドレスが一部の非クラスターノードに存在しているかどうかを確認します。その場合は、新しいクラスター IP アドレスを作成し、クラスターに再参加してみます。

クラスターへのノードの参加中に、「エラー**:CCO** とローカルノードのライセンスが一致しません。「このエラーを解決するにはどうすればいいですか**?**

- クラスターに参加するアプライアンスには、CCO と同じライセンスが必要です。このエラーは、参加するノードのライセンスが CCO のライセンスと一致しない場合に発生します。このエラーを解決するには、両方のノードで次のコマンドを実行し、出力を比較します。

  コマンドラインから次のコマンドを実行します。

  - `show ns hardware`
  - `show ns license`

  シェルから次のコマンドを実行します。

  - `nsconmsg -g feature -d stats`
  - `ls /nsconfig/license`
  - `/var/log/license.log/var/log/license.log` ファイルの内容を表示する

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラスターノードの構成がクラスター構成と同期していない場合はどうすればよいですか**?**

- 通常、構成はすべてのクラスターノード間で自動的に同期されます。ただし、構成が特定のノードで同期されていないと思われる場合は、同期するノードから force cluster sync コマンドを実行して、同期を強制する必要があります。詳しくは、「クラスター構成の同期」を参照してください。

クラスターノード間の構成は同期されません。構成が常に同期していることを確認するにはどうすればよいですか**?**

- ノード間でクラスター構成を確実に同期させるには、各構成の後に **save ns config** コマンドを実行します。そうしないと、再起動時にクラスターノードで構成を使用できないことがあります。

クラスターノードを構成するときに、「エラー**:** セッションは読み取り専用です。クラスターの **IP** アドレスに接続して構成を変更します」

- クラスター上のすべての構成は、クラスター IP アドレスを介して実行する必要があり、構成は他のクラスターノードに伝達されます。個々のノードの Citrix ADC IP（ADCIP）アドレスを介して確立されたすべてのセッションは読み取り専用です。

ノードの健全性が「**UP**」と表示されたときに、ノードの状態が「**INACTIVE**」と表示されるのはなぜですか**?**

- 正常なノードが INACTIVE 状態になる原因はいくつかあります。`ns.log`またはエラーカウンタのスキャンは、正確な理由を特定するのに役立ちます。

ノードの健全性が「**Not UP**」と表示されている場合、ノードの健全性をどのように解決できますか**?**

- ノードの健全性が [**Not UP**] の場合は、ノードにいくつかの問題があることを示します。根本的な原因を知るには、**sh cluster node** コマンドを実行する必要があります。このコマンドは、ノードのプロパティとノード障害の理由を表示します。

set vserver コマンドを実行すると、「そのようなリソースはありません。」このエラーを解決するにはどうすればいいですか**?**

- **set vserver** コマンドは、クラスタリングではサポートされていません。vserver の設定解除、**vserver** の有効化、**vserver** の無効化、および **rm vserver** コマンドもサポートされていません。ただし、**show vserver** コマンドはサポートされています。

Telnet セッションでクラスターを構成できません。どうしたらいいですか**?**

- Telnet セッションでは、クラスター IP アドレスには読み取り専用モードでのみアクセスできます。したがって、Telnet セッションを介してクラスターを構成することはできません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラスターノード間で大きな時間差があることに気付きました。このエラーを解決するにはどうすればいいですか**?**

バックプレーンスイッチが原因で PTP パケットがドロップされた場合、または仮想環境で物理リソースが過剰にコミットされた場合、時刻は同期されません。

時刻を同期するには、クラスター IP アドレスで次の操作を行う必要があります。

1. PTP を無効にします。

```
set ptp -state disable
<!--NeedCopy-->
```

2. クラスターのネットワークタイムプロトコル (NTP) を構成します。詳しくは、「CLI または構成ユーティリティを使用したクロック同期の設定」セクションを参照してください。

よくあるご質問

クラスター内にいくつの **Citrix ADC** アプライアンスを持つことができますか**?**

- Citrix ADC クラスターには、わずか 2 台または最大 32 台の Citrix ADC nCore ハードウェアまたは仮想アプライアンスを含めることができます。

私は複数のスタンドアロンノードを持っていますが、それぞれの設定が異なります。**1** つのクラスターに追加できますか

- はい。クラスターには最大 32 個のノードを追加できます。ただし、アプライアンスの既存の構成は、ノードがクラスターに追加されるとクリアされます。個々のアプライアンスの構成を使用するには、すべての構成の 1 つの`*.conf`ファイルを手動で準備し、構成を編集してクラスタリングでサポートされていない機能を削除し、インターフェイスの命名規則を更新してから、構成を CCO に追加するには、**batch** コマンドを使用します。

スタンドアロン **Citrix ADC** アプライアンスまたは **HA** セットアップの構成をクラスター化されたセットアップに移行できますか**?**

- いいえ。ノードがクラスター化されたセットアップに追加されると、**clear ns config** コマンド（拡張オプション付き）がそのアプライアンスで実行されます。さらに、SNIP アドレスとすべての VLAN 設定（デフォルト VLAN および ADCVLAN を除く）がクリアされます。したがって、アプライアンスをクラスターに追加する前に、構成をバックアップすることをお勧めします。

Citrix ADC アプライアンスを自動的に検出してクラスターに追加することはできますか**?**

- はい。構成ユーティリティを使用すると、CCO の ADCIP アドレスと同じサブネットに存在する Citrix ADC アプライアンスを検出できます。詳しくは、「Citrix アプライアンスの検出」を参照してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラスターはライセンスされた機能ですか**?**

- はい、クラスターはライセンス機能です。クラスターに追加するすべてのアプライアンスの/nsconfig/license/ディレクトリに、クラスタライセンスファイルのコピーが必要です。さらに、クラスターに追加するすべてのアプライアンスで、同じライセンスファイルを使用できる必要があります。

Citrix ADC アプライアンスを複数のクラスターの一部にすることはできますか**?**

- いいえ。アプライアンスは 1 つのクラスターにのみ属できます。

クライアントまたはサーバネットワークに接続されていないノードは、引き続きトラフィックを処理できますか**?**

- はい。Citrix ADC クラスターは、リンクセットと呼ばれるトラフィック分散メカニズムをサポートしています。これにより、接続されていないノードは、接続されたノードのインターフェイスを使用してトラフィックを処理できます。接続されていないノードは、クラスターバックプレーンを介して接続されたノードと通信します。

ノードのクラスタライセンスの有効期限が切れた場合はどうなりますか**?**

- ノードの実行中にノードのクラスタライセンスが期限切れになった場合、クラスターは影響を受けません。ただし、そのノードを再起動すると、クラスターはこのノード上で動作上無効になるため、ノードはトラフィックを処理できません。問題を修正してノードをアクティブにするには、新しいライセンスをアップロードし、アプライアンスをウォームリブートする必要があります。

クラスターのネットワークインターフェイスは、通常の **2** タプル（**u/c**）表記ではなく **3** タプル（**n/u/c**）表記を使用して表現されるのはなぜですか**?**

- アプライアンスがクラスターの一部である場合、ネットワークインターフェイスが属するノードを特定できる必要があります。したがって、クラスターノードのネットワークインターフェース命名規則は、u/c から n/u/c に変更されます。ここで、n はノード ID を表します。

ストライピング **IP** アドレスとは何ですか**?**

- クラスターで定義されているすべての IP アドレス (VIP または SNIP) は、デフォルトではストライプ IP アドレスです。ストライピング IP アドレスは、クラスターのすべてのノードでアクティブです。

スポッティング **IP** アドレスとは何ですか**?** 実行時にスポットされた **IP** アドレスの所有権を変更できますか**?**

- スポッティング IP アドレスは、アクティブで、クラスターの 1 つのノードによって排他的に所有されている IP アドレスです。スポッティング IP アドレスは、**add ns ip** コマンドで所有者ノードを指定することによって、クラスター IP アドレスを通じて定義する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

実行時に、スポットされた IP アドレスの所有権を変更することはできません。所有権を変更するには、まず IP アドレスを削除し、新しい所有者を指定して再度追加する必要があります。

CCO とは何ですか**?**

- CCO は、構成コーディネーターの略です。このノードはクラスター IP アドレスを所有し、すべてのクラスター構成を調整します。

クラスター **IP** アドレスとは何ですか**?** サブネットマスクとは何ですか**?**

- クラスタ IP アドレスは、Citrix ADC クラスターの管理アドレスです。すべてのクラスター構成は、このアドレスを通じてクラスターにアクセスすることによって実行する必要があります。クラスター IP アドレスのサブネットマスクは、255.255.255.255 に固定されています。

クラスターに最初のノードを追加したとき、そのノードは構成コーディネータ **(CCO)** でした。これで、別のノードが **CCO** として表示されます。理由は次のとおりです**?**

- クラスタが作成されると、最初のノードが CCO になります。クラスター IP アドレスは、そのノードによって所有されています。ただし、CCO は固定ノードではありません。さまざまな理由により、時間の経過とともに変化する可能性があります。この場合、クラスターは新しい CCO を選択し、そのクラスター IP アドレスを新しい CCO に割り当てます。

クラスターノードの **ADCIP** アドレスからコマンドを実行できますか**?**

- いいえ。Citrix ADC IP（ADCIP）アドレスを通じた個々のクラスターノードへのアクセスは読み取り専用です。つまり、クラスターノードの ADCIP アドレスにログオンすると、構成と統計情報のみを表示できます。どの設定も実行できません。ただし、クラスターノードの ADCIP アドレスから実行できる操作もあります。詳しくは、「個々のノードでサポートされる操作」を参照してください。

クラスターノード間の構成の伝播を無効にできますか**?**

- いいえ。クラスターノード間のクラスター構成の伝播を明示的に無効にすることはできません。ただし、バージョンの不一致のために、ソフトウェアのアップグレードまたはダウングレード中に、設定の伝播が自動的に無効にされることがあります。

クラスターとクラスターのすべてのノードを削除するにはどうすればよいですか**?**

- クラスターおよびクラスターのすべてのノードを削除するには、クラスターノードの削除の説明に従って、各ノードを個別に削除する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC アプライアンスがクラスターの一部である場合、**ADCIP** アドレスの変更や **ADCVLAN** の変更は可能ですか**?**

- いいえ。このような変更を行うには、まずクラスターからアプライアンスを削除し、変更を実行してから、クラスターにアプライアンスを追加する必要があります。

Citrix ADC クラスターは **L2** および **L3** 仮想ローカルエリアネットワーク（**VLAN**）をサポートしていますか**?**

- はい。Citrix ADC クラスターは、クラスターノード間の VLAN をサポートします。VLAN は、クラスター IP アドレスに設定する必要があります。
  - **L2 VLAN**。クラスターの異なるノードに属するインターフェイスをバインドすることによって、レイヤ 2 VLAN を作成できます。
  - **L3 VLAN**。クラスターの異なるノードに属する IP アドレスをバインドすることによって、レイヤ 3 VLAN を作成できます。IP アドレスは同じサブネットに属している必要があります。次の基準のいずれかが満たされていることを確認してください。そうしないと、L3 VLAN バインディングが失敗する可能性があります。
    * すべてのノードは、VLAN にバインドされたサブネットと同じサブネット上に IP アドレスを持つ。
    * クラスターにはストライピングされた IP アドレスがあり、その IP アドレスのサブネットは VLAN にバインドされます。

スポットされた IP のみを持つクラスターに新しいノードを追加すると、スポットされた IP アドレスがそのノードに割り当てられる前に同期が実行されます。このような場合、L3 VLAN バインディングが失われる可能性があります。この損失を回避するには、ストライプ IP を追加するか、新しく追加されたノードの ADCIP に L3 VLAN バインディングを追加します。

Citrix ADC アプライアンスをクラスターに追加すると、**VLAN** および **VLAN** バインディングが削除されるのはなぜですか**?**

- Citrix ADC アプライアンスをクラスター化されたセットアップに追加すると、clear ns config コマンド（拡張オプション付き）がそのアプライアンスで実行されます。さらに、SNIP アドレスとすべての VLAN 設定（デフォルト VLAN および ADCVLAN を除く）がクリアされます。

Citrix ADC クラスターで **SNMP** を構成するにはどうすればよいですか**?**

- SNMP は、スタンドアロンの Citrix ADC アプライアンスを監視するのと同じ方法で、クラスターおよびクラスターのすべてのノードを監視します。唯一の違いは、クラスタ上の SNMP は、クラスター IP アドレスを使用して構成する必要があることです。ハードウェア固有のトラップを生成する場合、クラスターのノードを識別するための 2 つの追加の varbind が含まれます。ノードのノード ID と ADCIP です。

SNMP の設定について詳しくは、「SNMP」を参照してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クラスタ関連の問題についてテクニカルサポートに連絡する場合、どのような詳細情報を入手する必要がありますか**?**

- Citrix ADC には、構成データ、統計情報、およびすべての クラスターノードのログを抽出する **show techsupport-scope** cluster コマンドが用意されています。このコマンドは、クラスター IP アドレスで実行する必要があります。

このコマンドの出力は、CCO の/var/tmp/support/cluster/ディレクトリにあるcollector_cluster_<nsip_CCO>_P_<date-timestamp>.tar.gzという名前のファイルに保存されます。このアーカイブをテクニカルサポートチームに送信して、問題をデバッグします。

個々のノードでサポートされる操作

クラスター上のすべての構成は、クラスター IP アドレスを介して CCO で実行され、構成はクラスターノードに伝達されます。ただし、Citrix ADC IP（ADCIP）アドレスを通じて各クラスターノードにアクセスすることで、個々のクラスターノードで実行できる操作もあります。

```
- enable cluster instance w disable cluster instance
- set cluster instance
- rm cluster instance
- set cluster node
- rm cluster node
- force cluster sync
- sync cluster files
- send arp all
- start nstrace
- stop nstrace
- show nstrace
- set interface
- enable interface w disable interface w save ns config
- reboot
<!--NeedCopy-->
```

> 注:
>
> show コマンドと stat コマンドは構成の変更を伴わないため、すべて使用できます。

Citrix ADC プール容量検証済みリファレンス設計

May 18, 2020

Citrix ADC プール容量は、Citrix Application Delivery Management（ADM）でホストされ、提供される帯域幅プールと仮想インスタンスプールで構成されるライセンスフレームワークです。この共通プールから、データセンタ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ー内の各 Citrix ADC は、1 つの仮想インスタンスライセンスをチェックアウトし、必要な帯域幅のみをチェックアウトします。これは、プラットフォームやフォームファクタに関係なく実行されます（MPX-Z は例外で、帯域幅ライセンスのみをチェックアウトします）。ライセンスファイルと帯域幅は Citrix ADC にバインドされません。Citrix ADC がこれらのリソースを必要としなくなった場合は、それらを共通プールにチェックインし、リソースを必要とする他の ADC からリソースを利用できるようにします。

このライセンスフレームワークは、ADC が過剰な未使用の帯域幅を割り当てないようにすることで、帯域幅の使用率を最大化します。Citrix ADC では、ライセンスと帯域幅を共通プールでチェックできるため、ユーザーと管理者はインスタンスの Provisioning を自動化できます。ユーザーと管理者は、トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられた帯域幅を増減できます。さらに、プール内の Citrix ADC ライセンスは、あるインスタンスから別のインスタンスに転送できます。これらのライセンスは、すべてのフォームファクタ（MPX、SDX、VPX、CPX）で共有できます。

コンポーネント

プールされた容量は、基盤となるハードウェアからソフトウェアを切り離します。この方法では、既存のプラットフォームから新しいプラットフォームに移行可能なライセンスモデルを使用できます。プールされた容量は、次の 4 つのコンポーネントで構成されます。

1. 帯域幅なし、インスタンスなし、機能を持たないゼロキャパシティのハードウェア。
2. ソフトウェアエディション（標準、アドバンスト、プレミアム）による帯域幅のプールで、MPX、SDX、VPX、CPX を含むすべての Citrix ADC フォームファクタで共有できます。
3. インスタンスプール。SDX、スタンドアロン VPX、CPX で実行される VPX など、ソフトウェア/仮想 Citrix ADC フォームファクタ間で共有されるインスタンスのプールです。
4. Citrix ADM。帯域幅とインスタンスライセンスの管理に使用されます。Citrix ADM のこの機能は、お客様に無償で提供されます。

プールされた容量のコンポーネントについては、この記事の後半で詳しく説明します。

永久ライセンス

永久ライセンスとは、期限切れにならないライセンスです。永久ライセンスでは、ユーザーは 1 回限りの料金を支払い、ライセンスを永遠に使用する権利があります。考慮すべき事項を次に示します。

- 定期的な保守サポートコストなど、永続ライセンスには制限があることがよくあります。
- ライセンスは特定のハードウェアプラットフォームにバインドされており、通常は移動できません。
- テクノロジーが変更されると、ライセンスは時代遅れになる可能性があります。
- 特定の機能は、帯域幅などのエディション固有の永続ライセンスエンタイトルメントで有効になります。Citrix ADC の場合、これらのエディション固有のライセンスは、スタンダード、アドバンスト、プレミアムのエディションです。

これとは対照的に、プールされたキャパシティライセンスは特定のハードウェアプラットフォームにバインドされず、既存のプラットフォームから新しいプラットフォームに移行できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

容量のメリットをプールする

ユースケース **1**：クラウドへの移行

プールされた容量は、既存のインフラストラクチャへの投資保護を提供することにより、ハイブリッドクラウドの導入を促進します。お客様は、容量の一部をオンプレミス展開からクラウドに移行することを選択できるため、クラウドベースの Citrix ADC アプライアンスのコストを削減できます。

使用例 **2:** ハードウェアの更新サイクル

従来の展開で Citrix ADC を展開したことのあるお客様は、環境を更新するときにすべてを購入する必要があります。プールされた Citrix ADC ライセンスの場合、更新サイクルでは、ソフトウェアが保持されている間にハードウェアを更新するだけで済みます。ハードウェアを更新すると、ソフトウェアライセンスをレガシーアプライアンスから新しいハードウェア/ソフトウェアアプライアンスに簡単に転送できます。これにより、更新サイクルのコストが大幅に削減され、お客様は従来の 5 年間隔よりも早く更新サイクルを確認できるようになります。

ユースケース **3**：**DevOps** の展開（**VPX/CPX**）

容量ゼロのアプライアンスに投資したお客様は、CPX アプライアンスを購入し、容量の一部をマイクロサービス環境に移動できます。また、新しいアーキテクチャをサポートするための追加容量を購入することもできます。全体として、オンプレミスまたはハードウェアベースのアーキテクチャから、マイクロサービスまたはソフトウェアベースのアーキテクチャへのコスト効率に優れた移行です。

プールされた容量の仕組み

説明

プールされた容量は、基盤となるハードウェアからソフトウェアを切り離すライセンスフレームワークです。このアプローチにより、既存のプラットフォームから新しいプラットフォームに移行可能なライセンスモデルが可能になり、ADC に要件を超える帯域幅が割り当てられないようにすることで、帯域幅の使用率が最大化されます。Citrix ADC でライセンスと帯域幅を共通プールでチェックする機能により、ユーザーはインスタンスの Provisioning を自動化できます。

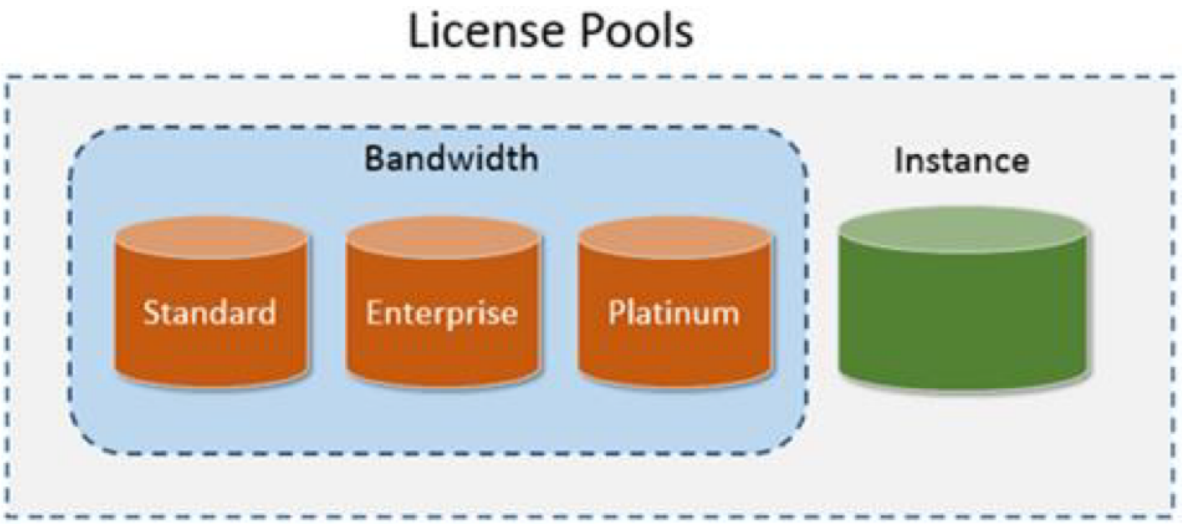
ユーザーは、トラフィックに影響を与えることなく、実行時に Citrix ADC に割り当てられた帯域幅を増減できます。また、プール内の Citrix ADC ライセンスを 1 つの Citrix ADC から別の Citrix ADC に転送することもできます。

ライセンスフロー

お客様は、Citrix ADC プール容量ライセンスを購入し、My Account ログインページからダウンロードします。

その後、これらのライセンスは Citrix ADM にインポートされます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ゼロキャパシティハードウェア

Citrix ADC プール容量を使用して管理する場合、SDX インスタンスは「ゼロキャパシティハードウェア」と呼ばれます。これらのインスタンスは、帯域幅とインスタンスプールからリソースをチェックアウトするまで機能しないためです。その結果、これらのプラットフォームは SDX-Z アプライアンスと呼ばれます。

同様に、MPX アプライアンスは、帯域幅プールからリソースをチェックアウトするまで機能しなくなるため、Citrix ADC プール容量を使用して管理する場合、「ゼロ容量ハードウェア」とも呼ばれます。その結果、これらのプラットフォームは MPX-Z アプライアンスと呼ばれます。

容量がゼロのハードウェアアプライアンスには、共通プールから帯域幅やインスタンスライセンスをチェックアウトするためのプラットフォームライセンスが必要です。まず、ハードウェアシリアル番号またはライセンスアクセスコードを使用して、プラットフォームライセンスを手動でインストールする必要があります。

現在、Citrix ADC ソフトウェアリリース 11.1 以降を実行している次のゼロキャパシティプラットフォームでは、Citrix ADC プールされたキャパシティーを新規購入およびアップグレードでサポートしています。

- MPX-14000Z
- MPX-14000Z-40G
- MPX-15000Z
- MPX-15000Z-50G
- MPX-25000Z-40G
- MPX-26000Z
- MPX-26000Z-100G
- SDX-14000Z
- SDX-14000Z-40G

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- SDX-15000Z-50G
- SDX-25000Z-40G
- SDX-26000Z-100G

現在、Citrix ADC ソフトウェアリリース 12.0 以降（MPX）および 11.1 以降（SDX）を実行する以下のゼロキャパシティプラットフォームは、新規購入およびアップグレード用に Citrix ADC プール容量をサポートします。

- MPX-14000Z-40S
- MPX-14000Z-40C
- マイルドポテト
- MPX-25000ZA
- MPX-26000Z-50S
- SDX-14000Z-40S
- SDX-14000Z-40C
- SDX
- SDX-25000ZA

現在、Citrix ADC ソフトウェアリリース 12.0 以降を実行している次のゼロキャパシティプラットフォームでは、Citrix ADC プールされたキャパシティーを新規購入およびアップグレードでサポートしています。

- MPX-8900Z
- SDX-8900Z

現在、Citrix ADC ソフトウェアリリース 12.0 以降（MPX）および 11.1 以降（SDX）を実行している次のゼロキャパシティプラットフォームでは、アップグレードのみで Citrix ADC プール容量がサポートされています。

- MPX-115xx (11515 - 11542)
- MPX-89xx/80xx
- MPX-22xxx
- MPX-24xxx
- SDX-115xx (11515 - 11542)
- SDX-89xx/80xx
- SDX-22xxx
- SDX-24xxx

現在、Citrix ADC ソフトウェアリリース 11.1 以降を実行している次のゼロキャパシティプラットフォームでは、新規購入時にのみ Citrix ADC プール容量がサポートされています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- VPX
- CPX

スタンドアロン **Citrix ADC VPX** インスタンス

以下のハイパーバイザーで Citrix ADC ソフトウェアリリース 11.1 以降を実行している Citrix ADC VPX インスタンスは、プールされた容量をサポートします。

- VMware ESX 6.0
- Citrix XenServer
- Linux KVM

以下のハイパーバイザおよびクラウドプラットフォームで Citrix ADC ソフトウェアリリース 12.0 以降を実行している Citrix ADC VPX インスタンスは、プールされた容量をサポートします。

- Microsoft Hyper-V
- Amazon AWS
- Microsoft Azure

> 注:
>
> Citrix ADM と Microsoft Azure または AWS の間の通信を有効にするには、IPSEC トンネルを構成する必要があります。詳しくは、「クラウドに展開された NetScaler VPX インスタンスの NetScaler MAS への追加」を参照してください。

スタンドアロンの **Citrix ADC CPX** インスタンス

Docker ホストに展開された Citrix ADC CPX インスタンスは、プールされた容量をサポートします。容量ゼロのハードウェアとは異なり、CPX ではプラットフォームライセンスは必要ありません。CPX では、トラフィック処理のためにプールからインスタンスライセンスをチェックアウトする必要があります。

帯域幅プール

帯域幅プールは、Citrix ADC が共有できる合計帯域幅です（物理と仮想の両方）。帯域幅プールは、ソフトウェアエディション（スタンダード、アドバンス、プレミアム）ごとに個別のプールで構成されます。特定の Citrix ADC では、異なるプールからの帯域幅を同時にチェックアウトすることはできません。Citrix ADC が帯域幅をチェックアウトできる帯域幅プールは、ライセンスされているソフトウェアのエディションによって異なります。プールからチェックアウトすると、ライセンスは CPU や PE、SSL コア、1 秒あたりのパケット数、帯域幅などのリソースのロックを解除します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

インスタンスプール

インスタンスプールは、Citrix ADC プール容量で管理できる VPX インスタンスまたは CPX インスタンスの数、または SDX-Z 内の VPX インスタンスの数を定義します。

> 注:
>
> SDX-Z の管理サービスでインスタンスが消費されることはありません。

Citrix ADM

Citrix ADC プール容量は、Citrix ADM を使用して、プール容量ライセンス（帯域幅プールライセンスおよびインスタンスプールライセンス）を管理します。ユーザーは、Citrix ADM を使用して、ADM ライセンスなしでプールされた容量ライセンスを管理できます。

帯域幅またはインスタンスプールからライセンスをチェックアウトする場合、容量がゼロのハードウェアプラットフォーム上の Citrix ADC フォームファクタとハードウェアモデル番号によって、以下が決定されます。

- Citrix ADC が機能する前にチェックアウトする必要のある最小帯域幅とインスタンス数。
- Citrix ADC がチェックアウトできる最大帯域幅とインスタンス数。
- 帯域幅チェックアウトごとの最小帯域幅単位。最小帯域幅単位は、Citrix ADC がプールからチェックアウトする必要がある帯域幅の最小単位です。チェックアウトは、最小帯域幅単位の整数倍で行う必要があります。たとえば、Citrix ADC 最小帯域幅ユニットが 1 Gbps の場合、100 Gbps はチェックアウトできますが、200 Mbps または 150.5 Gbps はチェックアウトできません。最小帯域幅単位は、最小帯域幅要件とは別のものです。Citrix ADC は、少なくとも最小帯域幅でライセンス供与された後にのみ動作します。最小帯域幅が満たされると、インスタンスは最小帯域幅ユニットで追加の帯域幅をチェックアウトできます。

次の表は、サポートされているすべての Citrix ADC プラットフォームの最大帯域幅/インスタンス、最小帯域幅/インスタンス、最小帯域幅単位をまとめたものです。

最小システム要件**:MPX** および **SDX**

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Gbps)	最小インスタンス	最大インスタンス	最小帯域幅ユニット
MPX 8005Z	30	5	-	-	1Gbps
MPX 8900Z	33	5	-	-	1Gbps
MPX 14000Z シリーズ	100	20	-	-	1Gbps
MPX 14000Z 40G シリーズ	100	20	-	-	1Gbps

© 1999–2021 Citrix Systems, Inc. All rights reserved.

製品ライン	最大帯域幅 (Gbps)	最小帯域幅 (Gbps)	最小インスタンス	最大インスタンス	最小帯域幅ユニット
MPX 14000Z FIPS シリーズ	100	20	-	-	1Gbps
MPX 14000Z 40S シリーズ	100	20	-	-	1Gbps
MPX 15000Z シリーズ	100	20	-	-	1Gbps
MPX 15000Z 50G シリーズ	100	20	-	-	1Gbps
MPX 115XX シリーズ	42	15	-	-	1Gbps
MPX 22XXX シリーズ	120	40	-	-	1Gbps
MPX 24000Z シリーズ	150	100	-	-	1Gbps
MPX 25000Z 40G	200	100	-	-	1Gbps
MPX 25000ZA	200	100	-	-	1Gbps
MPX 26000Z シリーズ	200	100	-	-	1Gbps
MPX 26000Z 100G シリーズ	200	100	-	-	1Gbps
MPX 26000Z 50S シリーズ	200	100	-	-	1Gbps
SDX 8015Z	15	2	1	2	1Gbps
SDX 89XX シリーズ	33	10	2	7	1Gbps
SDX 115XX シリーズ	42	7	2	20	1Gbps
SDX 14000Z シリーズ	100	10	2	25	1Gbps
SDX 14000Z 40G シリーズ	100	10	2	25	1Gbps

© 1999–2021 Citrix Systems, Inc. All rights reserved.

製品ライン	最大帯域幅（Gbps）	最小帯域幅（Gbps）	最小インスタンス	最大インスタンス	最小帯域幅ユニット
SDX 14000Z 40S シリーズ	100	10	2	25	1Gbps
SDX 14000Z FIPS シリーズ	100	10	2	25	1Gbps
SDX 15000Z 50G	100	10	2	55	1Gbps
SDX 15000Z	100	10	2	55	1Gbps
SDX 22XXX シリーズ	120	20	20	80	1Gbps
SDX 25000Z 40G	200	50	20	115	1Gbps
SDX 25000ZA	200	50	20	115	1Gbps
SDX 26000Z 100G	200	50	10	115	1Gbps
SDX 26000Z	200	50	10	115	1Gbps
SDX 26000Z 50S	200	50	10	115	1Gbps
SDX 24000Z シリーズ	150	50	20	80	1Gbps

Citrix ADC ADC CPX モデルの場合

帯域幅/インスタンス帯域幅ユニット	CPX
最大帯域幅（Gbps）	1
最小帯域幅（Gbps）	-
最小インスタンス数	1
最大インスタンス数	-
最小帯域幅単位	-

ハイパーバイザおよびクラウドサービスでの **Citrix ADC VPX** の場合

© 1999–2021 Citrix Systems, Inc. All rights reserved.

帯域幅/インスタンス帯域幅ユニット	Citrix XenServer	VMware ESXi	Linux KVM	Microsoft Hyper-v	AWS	AZURE
最大帯域幅（Gbps）	40 Gbps	100 Gbps	100 Gbps	3Gbps	5Gbps	3Gbps
最小帯域幅（Gbps）	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps
最小インスタンス数	1	1	1	1	1	1
最大インスタンス数	1	1	1	1	1	1
最小帯域幅単位	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps

さまざまなフォームファクタのライセンス要件

ライセンス要件	MPX	SDX	VPX	CPX
ゼロキャパシティハードウェアの購入	○	○		
帯域幅およびエディションのサブスクリプション	○	○	○	
インスタンスのサブスクリプション		○	○	○

サポートされるプラットフォーム、サポートされる最小帯域幅/インスタンス、サポートされる最大帯域幅/インスタンス、サポートされるプラットフォームの最小帯域幅単位について詳しくは、「MPX/CPX/VPX の帯域幅とインスタンス情報」を参照してください。

Citrix ADC プール容量の設定

プールされた容量により、次のことが可能になります。

- ライセンスプール内のライセンスを、必要に応じて Citrix ADC に割り当てます。
- プールされたキャパシティライセンスファイル（帯域幅プールまたはインスタンスプール）を ADM にアップロードします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- インスタンスの最小容量と最大容量に従って、Citrix ADM からライセンスを割り当てます。

Citrix Application Delivery Management（ADM）

ユーザーは、Citrix ADM を Citrix ADC プール容量のライセンスサーバーとして構成できます。Citrix ADC インスタンスで帯域幅またはインスタンスのライセンスを取得するには、2 つの方法があります。

- 最初のライセンスチェックアウト要求は、Citrix ADC（SDX/MPX/VPX）から開始して、帯域幅および/またはインスタンスライセンスを取得する必要があります。
- ユーザーは、後で Citrix ADC または Citrix ADM からライセンスのチェックアウトを開始できます。

> 注:
>
> プールされた容量は、Citrix ADM にプールされたライセンスが追加された場合にのみ Citrix ADM に表示されます。

Citrix ADM ライセンスプールのステータス

- 割り当て済み**:** ライセンスの状態は正常です。
- 猶予： Citrix ADC インスタンスのライセンス猶予期間は 30 日間です。
- 同期中： Citrix ADM は、Citrix ADC から 2 分間隔で情報を取得します。
- 同期中： Citrix ADM と Citrix ADC の間でライセンスを同期するには、15 分ほどかかる場合があります。Citrix ADM が再起動したか、ADM HAS フェイルオーバーがトリガーされた可能性があります。
- 部分的に割り当て： Citrix ADC は、最大割り当てで実行されている可能性があるため、割り当てられた容量を受け入れることができません。たとえば、Citrix ADC は 10 Gbps のライセンスプール容量で実行されています。ADC が再起動すると、10 Gbps が ADM ライセンスサーバーにチェックインされます。Citrix ADC がオンラインに戻ると、以前に割り当てられた 10 Gbps を自動的にチェックアウトしようとします。一方、他の ADC がその帯域幅をチェックアウトしている可能性があります。この ADC に完全な 10 Gbps または部分的な容量を割り当てるのに十分な容量がライセンスプールにない場合、「部分割り当て」と表示されます。
- 管理対象外： Citrix ADC は、管理しやすいように ADM に追加されません。これは Citrix ADC ライセンスには影響しませんが、ADM からのライセンス監視に影響する可能性があります。
- 接続が失われました：管理性のため、ADM から Citrix ADC にアクセスできません。たとえば、ネットワーク接続の問題、NITRO が機能しない、または Citrix ADC パスワードの不一致があります。NITRO が機能しない場合、または Citrix ADC パスワードが一致しない場合、Citrix ADC のライセンスには影響しません。ただし、ADM からのライセンス監視に影響を与える可能性があります。
- 割り当て済み：**ADC** に適用されない：ライセンスがチェックアウトされているか ADC からチェックインされているが、Citrix ADC がまだ再起動していない場合、Citrix ADC の再起動が必要になることがあります。
- 割り当てられていない：ライセンスは ADC インスタンスに割り当てられません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADM ライセンスプール：一般的な問題

- ADC は、ライセンスサーバーを「到達不能」と表示します。
  - ライセンスサーバー (ADM または ADM サービスエージェント) への接続が 15 分以上切断されました。
  - ADC は猶予モードです。
- ADC は、ライセンスサーバーのステータスを「到達可能」と表示しますが、ユーザーが割り当てを変更しようとしても効果はありません。
  - ライセンスサーバーへの接続が最近停止しましたが、ADC はまだ 2 番目のハートビートを見逃していません。したがって、それは（まだ）猶予期間ではありません。
  -「割り当ての変更」を押すと 0 0 が返されます。これにより、構成済みの容量が失われているように見える場合があります。
- ADC は容量/インスタンス数を表示しますが、ライセンスサーバーが「到達可能/到達不能」になっています。
  - ライセンスサーバーへの接続が復元されましたが、ADC が 2 番目のハートビートを逃したり、再接続プローブを送信したりします。
  - **[**割り当ての変更**]** を押すと、数値が返されますが、構成された容量は考慮されません。
- ADM サービスでプールライセンスを構成すると、ADC に「ライセンスサーバーに接続できません」というメッセージが表示されます。
  - ファイアウォールルールを確認してください：27000 と 7279。
  - エージェントが登録されていないか、ADM Service にライセンスファイルがアップロードされていない (または間違ったファイルがある)。

ユースケース：**Citrix ADM** ライセンスプールの使用状況レポート

Citrix ADM ライセンスプールの使用状況レポートでは、お客様がライセンス使用量の増加を計画し、次回のライセンスプール購入を計画するための月次ピークを特定します。

- ポーリング:
  - ライセンスデータは、15 分ごとに ADC からポーリングされます。
- 1 時間あたりのピークのみを維持する:
  - 1 時間以内の最大ライセンス使用要件は、デバイスごとに保存されます。
- レポート作成:
  - 指定された時間範囲におけるデバイスごとの使用状況を示す、生成される GUI レポート。
- エクスポート:
  - 指定した時間範囲の測光データを CSV または XLS としてエクスポートする機能。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- パージ:
  - パージジョブは、毎月 1 日の午前 12:10 に実行されます。
  - パージ期間は構成可能です（デフォルト期間は 2 か月です）。

Citrix Application Delivery Management（**ADM**）にライセンスファイルをインストールするには

1. Web ブラウザーで、Citrix ADM の IP アドレスを入力します。たとえば、`http://192.168.100.1`のようになります。
2. [ユーザー名とパスワード] フィールドに、管理者の資格情報を入力します。
3. [構成] タブで、[ネットワーク**] > [**ライセンス**] > [**設定**]** に移動し、[新しいライセンスの追加] をクリックします。
4. [ライセンスファイル] セクションで、次のいずれかのオプションを選択します。
   - ローカルコンピュータからのライセンスファイルのアップロード-ユーザーのローカルコンピュータにライセンスファイルがすでに存在する場合、ユーザーは Citrix ADM にアップロードできます。ライセンスファイルを追加するには、[参照] をクリックしてライセンスファイル (.lic) を選択します。完了したら ［完了］をクリックします。

     > 注:
     >
     > アップロードされたライセンスファイルによって Citrix ADC Pooled キャパシティにライセンスが追加されない場合は、ライセンスファイルを選択し、［**Apply Licenses** ］をクリックしてライセンスをプールに追加できます。

   - ライセンスアクセスコードの使用-お客様が購入したライセンスのライセンスアクセスコード（LAC）を Citrix からメールで送信します。ライセンスファイルを追加するには、テキストボックスに **LAC** を入力し、[**Get Licenses**] をクリックします。

     > 注:
     >
     > ユーザーは、［ライセンス設定］からいつでも Citrix ADM にライセンスを追加できます。

Citrix ADM から **Citrix ADC** プール容量ライセンスを割り当てるには

前提条件：ユーザーが Citrix ADM を使用してインスタンスプールライセンスを管理できるようにするには、Citrix ADC インスタンスを Citrix ADM に登録する必要があります。Citrix ADC GUI で、［システム］**>**［ライセンス］**>**［ライセンスの管理］の順に選択し、**Citrix ADM IP** を追加するときに［管理機能のために **Citrix ADM** に登録する］チェックボックスをオンにします。

> 注:
>
> Citrix ADM に Citrix ADC インスタンスを登録していない場合は、Citrix ADM からライセンスをチェックアウトできます。ただし、Citrix ADM から Citrix ADC プール容量が有効なインスタンスに割り当てることはで

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> きません。
>
> ［ユーザー名］フィールドと［パスワード］フィールドに、Citrix ADM の資格情報を入力します。
>
> Citrix ADC（SDX/MPX/VPX）のパスワードがデフォルトではない場合、このオプションは機能しません。

インスタンスがライセンスサーバーに登録されたら、次のようにライセンスを割り当てます

1. Web ブラウザーで、Citrix ADM の IP アドレスを入力します。たとえば、`http://192.168.100.1`のようになります。
2. [ユーザー名とパスワード] フィールドに、管理者の資格情報を入力します。
3. [構成] タブで、[ネットワーク**] > [**ライセンス**] > [**プールされた容量] に移動します。
4. 管理するライセンスプールをクリックします。
5. [**>** ］ボタンをクリックして、使用可能なインスタンスのリストから Citrix ADC インスタンスを選択します。
6. ユーザーがライセンス割り当てを変更または解放する場合は、[割り当ての変更] または [割り当てのリリース] をクリックします。
7. ユーザーが「割り当ての変更」をクリックすると、ポップアップウィンドウが開き、ライセンスサーバーで使用可能なライセンスが表示されます。
8. [**Allocate** ］ドロップダウンオプションを設定することで、Citrix ADC インスタンスの帯域幅またはインスタンスの割り当てを選択できます。必要な選択を行ったら、「割当て」をクリックします。
9. ユーザーは、[ライセンス割り当て の変更**]** ウィンドウのドロップダウンオプションから、割り当てられたライセンスエディションを変更することもできます。

ライセンスプール高可用性（**HA**）を備えた **Citrix ADM**

以前は、ライセンスプールライセンスはノードロックされ、ADM プライマリノードのホスト ID に関連付けられていました。セカンダリノードへのフェイルオーバーが発生するたびに、Citrix ADC は 30 日間の猶予期間に入り、ADM の到達不能イベントによる中断を回避します。これにより、Citrix ADM にアクセスできなくても、Citrix ADC を 30 日間実行することができました。ただし、新しい Citrix ADC インスタンスにアクセスできない場合、ADM ライセンスサーバーからライセンスをチェックアウトすることはできません。つまり、30 日間の猶予期間中に新しいライセンスチェックアウトが行われませんでした。プライマリノードが復帰せず、30 日が経過した場合、このライセンスを動作させるには、Citrix ライセンスシステムからライセンスファイルのレプリカを生成する必要がありました。つまり、新しいライセンスファイルが生成されていました。

解決策

License Pool HA ソリューションでは、プライマリノードが復帰しない場合、ADM をセカンダリノードにフェイルオーバーして新しいライセンスファイルを生成する必要はありません。新しいライセンスチェックアウトは、フェイ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ルオーバー後も引き続き機能します。ライセンスプールのライセンスと ADM ライセンスが、Citrix ADM のプライマリノードとセカンダリノード間で共有される仮想ホスト ID に関連付けられるようになりました。

仮想ホスト **ID**

Citrix ADM プライマリノードとセカンダリノードの両方が同じ仮想ホスト ID を共有します。プライマリノードまたは HA 展開の最初の Citrix ADM サーバーの実際のホスト ID が仮想ホスト ID として使用されます。仮想ホスト ID は ADM 展開で自動生成され、ADM データベースに暗号化された形式で格納され、お客様は変更できません。仮想ホスト ID は、実際のホスト ID よりも優先されます。ライセンスファイルは、ADM プライマリノードからセカンダリノードに同期されます。Citrix ADC は、ADM フローティング IP アドレスを使用してライセンスをチェックアウトします。プライマリノードからセカンダリノードへのフェイルオーバー時に、ライセンスファイルと仮想ホスト ID が、フローティング IP アドレスとともにプライマリノードからセカンダリノードに同期されます。

HA のブレーク動作

お客様が ADM の HA のブレークアクションを開始した場合、両方の ADM ノードは仮想ホスト ID を保持し、HA のブレークワークフローを開始します。ノード 1 とノード 2 はどちらもライセンスのチェックアウトを続行できます。既存の Citrix ADC は、フローティング IP アドレスが ADM から削除されるため、30 日間の猶予期間に入ります。

スプリットブレイン

Citrix ADM は、定期的にハートビートを送信することで、ADM HA ノードの可用性を監視します。ネットワークの問題によりハートビートが他のノードに到達しない場合、両方の ADM ノードは自身を ADM プライマリとしてプロモートします。このシナリオでは、ライセンスサーバーは両方のノードで実行されています。Citrix ADC は、ADM サーバーノード IP を使用して両方のノードからライセンスをチェックアウトできます。これは、両方が同じ仮想ホスト ID を共有するためです。ノード 1 とノード 2 は、ADM プライマリとしてプロモートされます。ライセンスサーバーは、同じ仮想ホスト ID を持つ両方のサーバーで実行されています。ライセンス容量は 2 倍になります。Citrix ADM スプリットブレイン関連のイベントと ADM HA 猶予期間に関連するイベントが生成されます。

スプリットブレインからの回復

Citrix ADM は、お客様の管理者がネットワークの問題を検出して修正した後、スプリットブレイン状態から回復できます。ADM スプリットブレインから回復するためのワークフローは以下の通りです。ネットワークが復元されると、Citrix ADM は ADM ノード 1 を ADM プライマリとして自動的に検出します。Citrix ADM は、ADM ノード 2 から HA への参加ワークフローを開始します。Citrix ADM ノード 1 の実ホスト ID が仮想ホスト ID として選択されます。Citrix ADM は通常の HA シナリオに復元され、ライセンスファイルと仮想ホスト ID は ADM ノード 2 に同期されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

MPX-Z でのプールされた容量の構成

MPX-Z は、Citrix ADC プール容量を有効にした Citrix ADC MPX アプライアンスです。MPX-Z は、Premium、Advanced、または Standard エディションのライセンスの帯域幅プールをサポートします。MPX-Z は、ライセンスサーバーに接続する前に、そのプラットフォームライセンスが必要です。ユーザーは、ローカルコンピューターからライセンスファイルをアップロードするか、インスタンスのハードウェアシリアル番号を使用するか、Citrix ADC インスタンスの GUI の［システム］**>**［ライセンス］セクションからライセンスアクセスコードを使用して、MPX-Z プラットフォームライセンスをインストールできます。MPX-Z プラットフォームライセンスを削除すると、プールされたキャパシティ機能が無効になり、チェックアウトされたすべてのライセンスがライセンスサーバーにチェックインされます。

ユーザーは、再起動することなく、MPX-Z ADC の帯域幅を動的に変更できます。再起動は、ユーザーがライセンスエディションを変更する場合のみ必要です。

> 注:
>
> Citrix ADC を再起動すると、構成済みの容量に必要なプールされたライセンスが自動的にチェックアウトされます。

VPX インスタンスでのプールされた容量の構成

プールされた容量が有効な Citrix ADC VPX インスタンスは、帯域幅プール（プレミアム/アドバンス/スタンダードエディション）からライセンスをチェックアウトできます。Citrix ADC GUI を使用して、ライセンスサーバーからライセンスをチェックアウトできます。

ユーザーは、再起動せずに VPX インスタンスの帯域幅を動的に変更できます。再起動は、ユーザーがライセンスエディションを変更する場合のみ必要です。

> 注:
>
> ユーザーがインスタンスを再起動すると、インスタンスは設定された容量に必要なプールされたライセンスを自動的にチェックアウトします。

MPX-Z または **VPX** インスタンスへのプールライセンスの割り当て

ライセンスを割り当てるには、次の手順に従います。

1. Web ブラウザーで、Citrix ADC インスタンスの IP アドレスを入力します。たとえば、`http://192.168.100.1`のようになります。
2. **[**ユーザー名**]** および **[**パスワード**]** のフィールドに、管理者の資格情報を入力します。
3. [構成] タブで、[システム**] > [**ライセンス**] > [**ライセンスの管理] に移動し、[新しいライセンスの追加] をクリックして、[プールライセンスの使用] を選択します。
4. **[**サーバー名**/IP** アドレス**]** フィールドにライセンスサーバーの詳細を入力します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

5. ユーザーが Citrix ADM を使用してインスタンスのプールライセンスを管理する場合は、[管理のために **Citrix ADM** に登録する] チェックボックスをオンにして、Citrix ADM の資格情報を入力します。
6. ライセンスエディションと必要な帯域幅を選択し、[**Get Licenses**] をクリックします。
7. ユーザーは、**[**割り当ての変更**]** または **[**割り当ての解放**]** を選択して、ライセンスの割り当てを変更または解放できます。
8. ユーザーが [割り当ての変更] をクリックすると、ポップアップウィンドウに、ライセンスサーバーで使用可能なライセンスが表示されます。

   > 注:
   >
   > ユーザーが帯域幅の割り当てを変更した場合は、再起動は必要ありませんが、ライセンスエディションを変更した場合は、ウォームリスタートが必要です。

9. ユーザーは、[**Allocate**] ドロップダウンリストから Citrix ADC インスタンスに帯域幅またはインスタンスを割り当てることができます。次に、[ライセンスの取得] をクリックします。
10. ユーザーは、ポップアップウィンドウのドロップダウンリストから、ライセンスエディションと必要な帯域幅を選択できます。

    > 注:
    >
    > 帯域幅の割当量は、最小帯域幅単位の倍数にする必要があります。

SDX-Z でのプール容量の設定

SDX-Z インスタンスは、Citrix ADC SDX のプールされた容量が有効なインスタンスです。SDX-Z は、Premium エディション、Advanced エディション、Standard エディションの帯域幅プーリング、およびインスタンスプーリングをサポートします。ユーザーが SDX-Z プラットフォームライセンスを適用すると、管理サービスでは、ライセンスサーバーからのライセンスのチェックアウト、および SDX-Z プラットフォーム上で実行されている Citrix ADC インスタンスに帯域幅容量を割り当てるオプションが提供されます。

> 注:
>
> SDX-Z 上で実行されている Citrix ADC VPX インスタンスは、ライセンスサーバーから直接ライセンスをチェックアウトしたり、ライセンスサーバーへチェックインしたりすることはできません。この操作は、SDX の管理サービスで行います。

ユーザーは、ローカルコンピュータからライセンスファイルをアップロードするか、インスタンスのハードウェアシリアル番号、またはライセンスアクセスコードを使用して、SDX-Z プラットフォームライセンスをインストールできます。

ユーザーが SDX-Z プラットフォームライセンスを削除すると、プールキャパシティ機能は無効化され、すべてのライセンスがライセンスサーバーにチェックインされます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> ユーザーがインスタンスを再起動すると、インスタンスは設定された容量に必要なプールされたライセンスをチェックアウトします。

SDX 上のプールされた容量

インスタンスプール

SDX アプライアンスは、SDX アプライアンスのインスタンスプールで使用可能なインスタンスと同じ数のインスタンスをプロビジョニングできます。

帯域幅プール

Citrix ADC インスタンスの Provisioning 中に、帯域幅がインスタンスに割り当てられます。ユーザーは、エディションと必要な帯域幅を選択して、仮想 Citrix ADC インスタンスをプロビジョニングできます。管理サービスでは、指定したエディションで必要な分の帯域幅がインスタンスにある場合のみプロビジョニングが許可されます。帯域幅が不十分な場合は、ユーザーに通知されます。

> 注:
>
> 帯域幅の変更では、インスタンスを再起動する必要はありません。

SDX-Z インスタンスへのプールライセンスの割り当て

ライセンスを割り当てるには、次の手順に従います。

1. Web ブラウザーで、Citrix ADC SDX-Z インスタンスの IP アドレスを入力します。たとえば、`http://192.168.100.1`のようになります。
2. **[**ユーザー名**]** および **[**パスワード**]** のフィールドに、管理者の資格情報を入力します。
3. [構成] タブで、[システム**] > [**ライセンス] に移動し、[プールされた容量] に移動します。
4. **[**サーバー名**/IP** アドレス**]** フィールドにライセンスサーバーの詳細を入力します。
5. ユーザーが Citrix ADM を使用してインスタンスのプールライセンスを管理する場合は、[管理のために **Citrix ADM** に登録する］チェックボックスをオンにして、Citrix ADM の資格情報を入力します。
6. ユーザーは、**[**割り当ての変更**]** または **[**割り当ての解放**]** を選択して、ライセンスの割り当てを変更または解放できます。

   > 注:
   >
   > チェックアウトされたライセンスは、管理サービスによって別のプールに保存されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

7. SDX-Z インスタンスの特定の VPX インスタンスのライセンス割り当てを変更するには、[インスタンス] セクションからインスタンスを選択し、[割り当ての変更] をクリックします。新しいウィンドウに、使用可能なライセンスが表示されます。
8. ユーザは、[**Feature License**] ドロップダウンリストからインスタンスの帯域幅エディションを変更し、[**Throughput (mbps)**] フィールドで必要な帯域幅を変更できます。完了したら ［**Done**］ をクリックします。

> 注:
>
> 帯域幅の割当量は、対応するフォームファクターの最小帯域幅単位の整数倍にする必要があります。

CPX インスタンスでのプールされた容量の構成

Citrix ADC CPX インスタンスの Provisioning 中に、Citrix ADC CPX インスタンスを構成して、Citrix ADC プールされたキャパシティを使用できます。ドッカーでは、ユーザーは Citrix ADC ライセンスサーバー（Citrix ADM）の詳細を提供する必要があります。Citrix ADC CPX インスタンスは、インスタンスプールからライセンスをチェックアウトします。

> 注:
>
> デフォルトでは、Citrix ADC CPX インスタンスはインスタンスプールからインスタンスライセンスをチェックアウトし、スループットは自動的に 1,000Mbps に設定されます。ユーザーは、インスタンスに割り当てられている 1,000 Mbps の帯域幅を変更できません。

ユーザーは、Docker アプリストアから Citrix ADC CPX をダウンロードできます。Docker ホストで、Citrix ADC CPX をダウンロードするには、次のコマンドを実行します。

```
docker pull store/citrix/netscalercpx:[version number]
```

Citrix ADC CPX インスタンスの Provisioning 中にプールされた容量を構成するには:

Citrix ADC CPX インスタンスの Provisioning 中に、Citrix ADC ライセンスサーバー（Citrix ADM）をドッカーホストの環境変数として定義し、次のコマンドを実行します。

```
docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name <
container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --cap-add=
NET_ADMIN >REPOSITORY<:>TAG<
```

各項目の意味は次の通りです:

- <LS_IPADDRESS>は、Citrix ADC ライセンスサーバー（Citrix ADM）の IP アドレスです。
- <LS_PORT>は、Citrix ADC ライセンスサーバーのポートです。デフォルトのポートは 27000 です。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ベストプラクティス、コーナーケース、**FAQ**

SDX ライセンスのアップグレード**-**永続的なプールへのアップグレード

SDX 上のライセンスを永久ライセンスからプールライセンスにアップグレードする場合、SDX を再起動する必要はありません。SDX と VPX のいずれも、プールされたライセンスに移行するために再起動する必要はありません。SVM は、1 つ以上の VPX をプールされたライセンスに自動的に移行します。

スムーズな移行のために、以下の点を確認する必要があります。

- SDX に適切なゼロキャパシティライセンスがあることを確認します。
- Citrix ADM サーバーに、SDX の VPX インスタンスで使用するライセンスエディションに十分な容量があることを確認します。
- すべての VPX インスタンスについて、SVM の ADM から十分な帯域幅容量がチェックアウトされていることを確認します。
  - 例：SDX に 10 個の VPX インスタンスがあり、一緒に 40 Gbps のプレミアムと 20 Gbps のアドバンストを消費する場合は、最初に SVM 経由でチェックアウトして、VPX インスタンスがこれらのライセンスを取得できるようにします。

30 日間の猶予期間中の **Citrix ADC** インスタンスの操作

プールからライセンスを受け取った後に Citrix ADC インスタンスが Citrix ADM から切断された場合、ライセンスサーバーとの接続の再確立を試行する間、30 日間の猶予期間内で動作し続けることができます。Citrix ADC が再起動しても、ライセンスは 30 日間の猶予期間内に残り、インスタンスは引き続き動作します。

クライアント側で開始されるチェックイン（ランダム化）：**Citrix ADM** が接続を開始するシナリオ

クライアント側で開始されるチェックイン（ランダム化）の場合、Citrix ADM がこの接続を開始するシナリオはありますか?

Citrix ADM（ライセンスサーバー）と Citrix ADC（ライセンスクライアント）は、ハートビートパケットを交換して、クライアントとサーバーの間で確立された接続の健全性を監視します。この期間は、すべての Citrix ADC クライアントが同時に Citrix ADM ライセンスサーバーに要求を送信しないようにするためにランダム化されます。

クライアントとサーバー間のライセンス接続に問題がある場合は、次の操作が実行されます。

- Citrix ADM が Citrix ADC クライアントからハートビートパケットを受信しない場合、Citrix ADM サーバーはその特定の Citrix ADC に割り当てられたライセンスを要求します。
- Citrix ADC がハートビートパケットを受信しない場合、Citrix ADC は 30 日間のライセンス猶予期間に移行します。
- Citrix ADC が Citrix ADM ライセンスサーバーとのライセンスサーバー接続の確立信号を受信した場合、Citrix ADC は Citrix ADM からライセンスを再度チェックアウトします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC 再起動中にプールされた帯域幅割り当て

Citrix ADC 再起動中に帯域幅が割り当てられた場合、プールされた帯域幅ライセンスは部分的に（プール内の使用可能な帯域幅まで）分散されますか? それともライセンスが配布されないのでしょうか?

Citrix ADC は、最初にユーザーが構成したプール容量をチェックアウトしようとします。この試行が失敗すると、Citrix ADC は Citrix ADM で使用可能なプールされた容量をチェックアウトしようとします。

> 注:
>
> この機能は、MPX および VPX でのみ使用できます。Citrix ADM に十分な容量がない場合、SDX はライセンスの部分的なチェックアウトを試みます。

ライセンスの不一致アラート（**Citrix ADC** がライセンスの一部または一部を受信しない）

不一致が発生した場合（たとえば、Citrix ADC がライセンスを受け取らなかったり、部分的なライセンスのみを受け取った場合）、Citrix ADM はこの状況に調整のフラグを立てることができますか?

Citrix ADC がライセンスまたは部分的なライセンスを受け取らない場合にライセンスの不一致が発生した場合、Citrix ADM はこの状況で調整のためにフラグを立てる必要があります。ライセンスの不一致は、次のシナリオで発生する可能性があります。

- Citrix ADC が再起動すると、Citrix ADC は再起動後にライセンスを再度チェックアウトします。これにより、プールされた容量の不一致イベントがクリアされます。
- Citrix ADM が再起動すると、Citrix ADC と Citrix ADM のライセンス情報がハートビート間隔内で同期され、このイベントがクリアされます。
- 再起動またはライセンスサーバーの再接続後に Citrix ADC チェックアウトが失敗した場合、自動リカバリは行われません。ユーザーは、プールからライセンスを手動でチェックアウトする必要があります。

Citrix ADM の高可用性（**HA**）フェイルオーバー

Citrix ADM の HA フェイルオーバー中に、ライセンスファイルがどのように同期され、どのような障害が発生する可能性がありますか（Citrix ADC 上の SSL 証明書がプライマリノードで更新されたときにセカンダリノードにコピーされないことがあるなど）。

Citrix ADM の高可用性（HA）によるプールライセンスサポートは、ソフトウェアリリース 12.1-50.x 以降から利用できます。Citrix ADM は、プライマリ Citrix ADM にアップロードされたファイルをセカンダリ Citrix ADM に定期的に同期します。したがって、ファイルの同期は、HA フェイルオーバーイベントが発生する前に行われます。その結果、ファイル同期の失敗は発生しにくくなります。たとえば、プライマリ Citrix ADM で更新され、セカンダリ Citrix ADM にコピーされていない Citrix ADC 上の SSL 証明書などです。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

セカンダリ **Citrix ADM** データベースの健全性チェック

セカンダリデータベースの問題について、健全性ステータスチェックは行われますか。セカンダリ Citrix ADM は、異常な情報が複製されないように、共有される情報が正常であることを検証していますか。

ライセンス情報は、ライセンスサーバーのメモリ（Citrix ADM 内）に保持されます。この情報は、Citrix ADM セカンダリと同期されません。すべてのライセンスのチェックアウト/チェックインは、ライセンスサーバーのメモリ内情報に対して実行されます。Citrix ADM データベースは、ライセンスサーバー（Citrix ADM 内）および Citrix ADC インスタンスから収集されたレポートの保存にのみ使用されます。

Citrix ADM では、Citrix ADM プライマリからセカンダリへのライセンスファイルのみが同期されます（ソフトウェアリリース 12.1-50.x 以降）。

Citrix ADM HA フェイルオーバー中、Citrix ADC はハートビート間隔の後にライセンスを ADM からチェックアウトし、ハートビート間隔の後にライセンスサーバーのメモリが更新されます。

ライセンスが使用不可になるための猶予期間を逆にする

即時にシャットダウンするのではなく、猶予期間中、インスタンスのライセンスを維持できるライセンス使用不可の逆猶予期間はありますか。たとえば、Citrix ADC はチェックインを試行し、Citrix ADM では有効なライセンスがないと表示されます。

この特定の問題の解決策が調査されています。この問題に対する解決策が提案されたら、ユーザーに通知します。

Citrix ADM でのライセンス設定可能なシステム **ID**

Citrix ADM のライセンスに使用する構成可能なシステム ID（MAC アドレスベースのシステムとは対照的に）はサポートされていますか?

ライセンス設定可能なシステム ID のサポートは現在予定されていません。

ファイルの整合性チェックまたはメカニズム

プライマリからセカンダリ Citrix ADM に複製されるライセンスを含むファイルについては、プライマリ DB の破損によって問題がセカンダリに複製されないように、整合性/破損チェックまたはメカニズムが用意されていますか。

Citrix ADM は、ライセンスファイルをファイルシステム内に保持し、RSYNC ユーティリティを使用して同期します。その結果、データベースの問題がライセンスファイルに影響を与えません。

Citrix ADM エージェントによるライセンスのチェックイン/チェックアウトの使用方法

> 注:
>
> 現在、パブリッククラウドのプールされたキャパシティでは、特定のテナントごとに 1 つのエージェントのみがサポートされています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

バーストライセンス

バーストライセンスは、消費要素を追加することで、プールされたキャパシティを拡張したものです。お客様は、帯域幅要件を正確に予測できない場合があります。これは、さまざまな理由や、合併や買収などの特別な状況、またはブラックフライデーの売り上げなどの特別な事象によって発生し、トラフィックが急増し、顧客の現在のキャパシティを上回る可能性があります。一般に、業界では、多くのクラウドサービスによって駆動される消費モデル (従量課金制) に移行しています。

プールされたキャパシティのバーストライセンスにより、お客様はプールされたキャパシティを基本サブスクリプションとして購入し、必要に応じて購入したプールされたキャパシティを上回るバーストオプションを利用できます。基本サブスクリプションプールの場合、お客様はサブスクリプション期間 (1 年、3 年、または 5 年) の間、前払いする必要があります。バーストプールの場合、顧客は前払いなしで消費することができ、消費後の年間実際の使用量に基づいて課金されます。

バーストライセンスでは、Citrix ADC は 1 つのプール、つまり、ベースプールとバーストプールを組み合わせたビューを表示します。Citrix ADC がベースプールからのチェックアウトに失敗すると、バーストプールからのチェックアウトが試行されます。

ADM でのバーストライセンスレポート

ベースおよびバーストプールのライセンス使用状況レポートが生成されます。毎月のライセンス使用状況レポートは、ライセンスプールの 1 時間あたりの最大ライセンス使用量を報告するために生成されます。これらの月次レポートのパージ間隔は、最大 3 年間です。年次ライセンス使用状況レポートは、ライセンスプールでの月あたりの最大ライセンス使用量を報告するために生成されます。これらの年次レポートのパージ間隔は、最大 6 年間です。お客様は、指定した時間範囲の計測データを CSV、XLS、PDF としてエクスポートできます。

BLX プールライセンス

BLX は、Citrix ADC VPX と同じライセンスプールを使用します。

仮想 **CPU** ライセンスの概要

データセンターは、コスト削減と拡張性の向上を実現しつつ、ネットワーク機能をシンプル化する新しいテクノロジーに移行しています。新しいデータセンターアーキテクチャには、少なくとも次の機能が含まれている必要があります。

- ソフトウェア定義ネットワーキング (SDN)。
- ネットワーク機能仮想化 (NFV)。
- ネットワーク仮想化 (NV)。
- マイクロサービス。

このような動きはまた、変化し続けるビジネスニーズを満たすために、ソフトウェア要件が動的で柔軟性が高く、俊敏であることが要求されます。ライセンスは、使用状況を完全に把握できる中央管理ツールによって管理されること

© 1999–2021 Citrix Systems, Inc. All rights reserved.

も期待されています。

以前は、Citrix SW ADC ライセンスは、インスタンスによる帯域幅消費に基づいて割り当てられていました。Citrix SW ADC は、バインドされたライセンスエディション（標準、アドバンスト、プレミアム）に基づいて、特定の帯域幅およびその他のパフォーマンスメトリックを使用するように制限されていました。使用可能な帯域幅を増やすには、より多くの帯域幅を提供するライセンスエディションにアップグレードする必要がありました。特定のシナリオでは、帯域幅要件が少なくなる可能性がありますが、SSL TPS、圧縮スループットなど、他の L7 パフォーマンスに対する要件は高くなっていました。この場合、Citrix SW ADC ライセンスのアップグレードは適切ではない場合があります。ただし、CPU を大量に消費する処理に必要なシステムリソースのロックを解除するには、帯域幅の大きいライセンスを購入する必要があります。Citrix SW ADM では、仮想 CPU（vCPU）の数に基づいたライセンスの割り当てがサポートされるようになりました。

vCPU ベースのライセンス機能では、特定の Citrix SW ADC VPX に資格が付与される vCPU の数を指定します。Citrix SW ADC VPX では、ライセンスサーバーからライセンスを動的にチェックアウトできます。ただし、ソフトウェア ADC を実行できる vCPU の数に制限はありません。vCPU ライセンスは、VPX、CPX、BLX を含むすべての SW ADC フォームファクタをサポートします。

プールされたライセンス容量および CICO（チェックイン、チェックアウト）ライセンス機能と同様に、Citrix SW ADM ライセンスサーバーは個別の vCPU ライセンスセットを管理します。また、vCPU ライセンス用に管理される 3 つのエディションは、標準、アドバンスト、プレミアムのエディションです。これらのエディションでは、バンド幅ライセンスのエディションでロック解除された機能と同じ機能のセットが解除されます。

vCPU の数が変更されたり、ライセンスエディションが変更されたりする場合があります。このような場合、ユーザーは新しいライセンスのセットのリクエストを開始する前に、常にインスタンスをシャットダウンする必要があります。ユーザーは、ライセンスをチェックアウトした後、Citrix SW ADC を再起動する必要があります。

Citrix ソフトウェア **ADC VPX** で **GUI** を使用してライセンスサーバーを構成します。

1. Citrix SW ADC VPX で、[システム] > [ライセンス] に移動し、[ライセンスの管理] をクリックします。
2. [ライセンス] ページで、[新しいライセンスの追加] をクリックします。
3. [ライセンス] ページで、[リモートライセンスを使用する] オプションを選択します。
4. [リモート ライセンスモード**]** リストから **[CPU** ライセンス] を選択します。
5. ライセンスサーバーの IP アドレスとポート番号を入力します。
6. [続行] をクリックします。

   > 注: ユーザーは、常に Citrix SW ADC VPX インスタンスを Citrix SW ADM に登録する必要があります。まだ行っていない場合は、［Citrix SW ADM で登録］を有効にして、Citrix ADM ログイン資格情報を入力します。

7. [ライセンスの割り当て] ウィンドウで、ライセンスのタイプを選択します。ウィンドウには、合計と使用可能な vCPU、および割り当て可能な CPU が表示されます。[ライセンスの取得] をクリックします。
8. 次のページで [**Reboot**] をクリックして、ライセンスを申請します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注**:** ユーザーは現在のライセンスをリリースし、別のエディションからチェックアウトすることもできます。たとえば、ユーザーはすでにインスタンスでスタンダードエディションのライセンスを実行しています。彼らはそのライセンスをリリースし、アドバンス版からチェックアウトすることができます。
> 注：ユーザーは、vCPU ごとに正しい量のメモリ（2 Gb）が割り当てられていることを確認する必要があります。vCPU あたりのメモリ割り当てを確認します。正しくない場合は、メモリを増やし、Citrix SW ADC VPX インスタンスを再起動します。

CLI を使用して、**Citrix SW ADC VPX** でライセンスサーバーを構成します。

Citrix SW ADC VPX コンソールで、以下の 2 つのタスクに対して次のコマンドを入力します。

1. ライセンスサーバーを Citrix SW ADC VPX に追加するには：
   - ライセンスサーバの IP アドレスを入力します。たとえば、http://192.168.100.1のようになります。
2. ライセンスを申請するには：
   - 容量を設定-vcpu-エディションプラチナ
   - プロンプトが表示されたら、次のコマンドを入力してインスタンスを 再起動します。**reboot-w**

Citrix ソフトウェア **ADM** での仮想 **CPU** ライセンスの管理

1. Citrix SW ADM で、[ネットワーク] > [ライセンス] > [仮想 **CPU** ライセンス] に移動します。
2. このページには、各ライセンスエディションに割り当てられたライセンスが表示されます。
3. 各ドーナツ（Standard、Advanced、Premium）内の番号をクリックして、このライセンスを使用している Citrix SW ADC インスタンスを表示します。

Citrix SW ADC CPX の仮想 **CPU** ライセンス

Citrix SW ADC CPX インスタンスの Provisioning 中に、インスタンスの CPU 使用率に応じて、ライセンスサーバーからライセンスをチェックアウトするように Citrix SW ADC CPX インスタンスを構成できます。

Citrix SW ADC CPX は、Citrix SW ADM 上で動作するライセンスサーバーに依存してライセンスを管理します。Citrix SW ADC CPX は、起動時にライセンスサーバーからライセンスをチェックアウトします。Citrix SW ADC CPX がシャットダウンすると、ライセンスはライセンスサーバーにチェックインされます。

ユーザーは、Docker アプリストアから Citrix SW ADC CPX をダウンロードすることができます. Docker ホストで、Citrix SW ADC CPX をダウンロードするには、次のコマンドを実行します。

- docker pull store/citrix/netscalercpx:[バージョン番号]

CPX ライセンスには、次の 3 つのライセンスタイプがあります。

1. CPX および VPX でサポートされる仮想 CPU サブスクリプションライセンス
2. プールされたキャパシティライセンス

© 1999–2021 Citrix Systems, Inc. All rights reserved.

3. CPX のみで単一から複数の vCPU をサポートする CP1000 ライセンス

Citrix SW ADC CPX インスタンスの **Provisioning** 中に **vCPU** サブスクリプションライセンスを構成するには:

ユーザーは、Citrix ADC CPX インスタンスが使用する vCPU ライセンスの数を指定する必要があります。

- この値は、Docker、Kubernetes、または Mesos/Marathon を通じて環境変数として入力されます。
- ターゲット変数は「**CPX_CORES**」です。CPX は 1 から 7 コアまでサポートできます。

2 つのコアを指定するには、次のように docker run コマンドを実行できます。

- docker run -dt -P –privileged=true –ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2

Citrix ADC CPX インスタンスの Provisioning 中に、以下に示すように、ドッカーの実行コマンドで Citrix SW ADC ライセンスサーバーを環境変数として定義します。

- docker run -dt -P –privileged=true –ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> cpx:11.1

各項目の意味は次のとおりです。

- <LS_IP_ADDRESS> は、Citrix ADC ライセンスサーバーの IP アドレスです。
- <LS_PORT> は、Citrix ADC ライセンスサーバーのポートです。デフォルトのポートは 27000 です。

> 注: デフォルトでは、Citrix SW ADC CPX インスタンスは vCPU サブスクリプションプールからライセンスをチェックアウトします。インスタンスが「n」の CPU で実行されている場合、CPX インスタンスは「n」個のライセンスをチェックアウトします。

Citrix SW ADC CPX インスタンスの **Provisioning** 中に、**Citrix SW ADC** プール容量または **CP1000** ライセンスを構成するには:

プールされたライセンス（帯域幅ベース）または CPX プライベートプール（CP1000 またはプライベートプールベース）を使用して CPX インスタンスのライセンスをチェックアウトする場合、ユーザーはそれに応じて環境変数を指定する必要があります。

例:

- docker run -dt -P –privileged=true –ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e PLATFORM=CP1000 cpx:11.1

CP1000. このコマンドは、CP1000 プール（CPX プライベートプール）からのチェックアウトをトリガーします。次に、Citrix SW ADC CPX インスタンスは、CPX_CORES に指定されたコア数の「n」数のインスタンスを取得します。最も一般的な使用例は、1 つのインスタンスのチェックアウトに n = 1 を指定することです。マルチコア CPX ユースケースは「n」の vCPU をチェックアウトします (「n」は 1 から 7 まで)。

- docker run -dt -P –privileged=true –ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e BANDWIDTH=2000 cpx:11.1

© 1999–2021 Citrix Systems, Inc. All rights reserved.

プールされた容量。このコマンドは、インスタンスプールから 1 つのライセンスをチェックアウトし、プラチナ帯域幅プールから 1000 Mbps の帯域幅を消費しますが、CPX は最大 2000 Mbps で実行できます。プールライセンスでは、最初の 1000 Mbps は課金されません。

> 注：次の表に示すように、帯域幅プールからチェックアウトするときに、目的のターゲット帯域幅に対応する vCPU 数を指定します。

コア数（vCPU）	最大帯域幅
1	1000Mbps
2	ビット/秒
3	3500 メガビット/秒
4	5000 メガビット/秒
5	6500 メガビット/秒
6	8000 メガビット/秒
7	9300 メガビット/秒

Citrix ADM サービスプールライセンスの概要

Citrix ADM サービスプールライセンスは、Citrix ADM サービスの機能です。Citrix ADM Service プールライセンスを使用すると、ADM Service でプールライセンスを使用できます。ADM Service プールライセンスを使用すると、ユーザーは複数のデータセンターに分散する複数の ADC にまたがるライセンス割り当てを管理できます。Citrix ADM サービスプールライセンスでは、データセンターごとに複数のエージェントがサポートされます。ライセンスは、1 つのエージェントだけでなく、ADM サービス全体によって管理されます。したがって、ユーザーはエージェントをクラウドベースのライセンスサーバーへのネットワークプロキシと考える必要があります。Citrix ADM サービスプールライセンスでは、Citrix ポータルからライセンスを取得するためのライセンスアクセスコードもサポートしています。Citrix ADM Service には、ユーザーが容量割り当てを管理し、ライセンスの使用状況を表示するためのダッシュボードが用意されています。

ADM サービスにアップロードされるライセンスは、プールされたライセンスの種類である必要があります。また、クラウド仮想ホスト ID にロックする必要があります。エージェントでは、受信ポート 27000 および 7279 が開かれている必要があります。エージェントがダウンすると、エージェントに接続されている ADC は猶予モードになります。エージェントがダウンした場合、エージェントに接続されていない ADC は、約 20 分間の構成変更を反映しません。彼らは正常に動作し続けます。ADC（またはライセンスエディション）のライセンスタイプを変更するには、ウォームリブートが必要です。ライセンスの容量を変更しても、再起動は不要です。

ADM サービスの機能を使用する前に、エージェントと ADC を登録/追加プロセスで Citrix ADM サービスに知らせる必要があります。ADM サービスの登録/追加ワークフローは次のとおりです：

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注：最初の 3 つの手順は、ADM のコンテキストを参照します。

1. エージェントを ADM サービスに登録します。
2. ADM サービスで、これらのエージェントに ADC インスタンスを追加します。
3. ADM サービスでライセンスをアップロードします。

   > 注：次の 3 つの手順は、ADC のコンテキストを参照します。

4. ADC GUI でリモートライセンスを選択します。
5. ADC が登録されているエージェントの IP アドレスを入力します。
6. 割り当て（ADC 上）

> 注**:** ADM サービスを使用して、すべての ADC のプールされたライセンスを監視したり、割り当てを変更したりできるようになりました。

Diamanti および **Nirmata** 検証済みリファレンスデザインにおける **Kubernetes** での **Citrix ADC CPX**

May 18, 2020

テストする機能と機能

テストケース: **North-South** およびヘアピン **East-West** の **Ingress Controller** およびデバイスとしての **CPX**:

North-South としての **VPX** を除くすべてのテストケースの設定:

- クラスター内の 2 つの CPX（CPX-1、CPX-2）
- ライセンスサーバーとしての ADM
- クラスター内の Prometheus エクスポーターコンテナ
- Prometheus サーバーと Grafana (Kubernetes のポッドとして、または Kubernetes サーバーの外部にあるポッドとして)
- 複数のフロントエンドアプリ
- 複数のバックエンドアプリケーション

I. North-South としての **VPX**

1. SDX フロントエンド Diamanti プラットフォーム上の VPX
   - SSL オフロードをテストし、SSL 接続ごとに X-Forward を挿入して再暗号化する
   - SSL セッションでの X フォワードの挿入

© 1999–2021 Citrix Systems, Inc. All rights reserved.

II. North-South デバイスとしての **CPX**

1. CPX-1。指定された入力クラスを持つ 2 つまたは 3 つの HTTPS アプリケーションをサポートする HTTPS 入力を設定します。
    - 複数のコンテンツスイッチポリシーの作成をデモンストレーションします（フロントエンドアプリごとに 1 つずつ）。
    - CPX ごとに複数のワイルドカード証明書をデモンストレーションします。アプリごとに 1 つのワイルドカード証明書があります。
    - フロントエンドアプリへのトラフィックオフロードと再暗号化の CPX デモを行います。
    - さまざまなロードバランシングアルゴリズムをデモンストレーションします。
    - 1 つのポッドへの永続性を示します。
2. CPX-1。指定された入力クラスで個別の TCP 入力を設定します。
    - MongoDB のような TCP アプリケーションを挿入します。
    - TCP VIP の作成を表示します。
    - MongoDB ポッドに到達する TCP クライアントトラフィックを表示します。
    - デフォルトの TCP アプリケーションの健全性チェックを表示します。
3. CPX-1。指定された入力クラスで個別の TCP-SSL 入力を設定します。
    - TCP-SSL VIP の SSL オフロードと再暗号化のデモンストレーションを行います。
    - テストケース 2 を繰り返します。
4. アプリごとの CPX です。別の入力クラスの使用：
    - 1 つのアプリのみをサポートする CPX-2 を使用して、テストケース 1～3 を繰り返します。
5. チームあたりの CPX。入力クラスの使用：
    - 2 つのチームに異なる入力クラスを割り当てます。
    - CPX が個々のチームの入力ルールを設定できるという証拠として、テストケース 1 をデモンストレーションします。
6. フロントエンドポッドを自動スケールする：
    - フロントエンドポッドへのトラフィックを増やし、ポッドが自動スケーリングされるようにします。
    - CPX-1 が新しいポッドをサービスグループに追加することを示します。
    - HTTPS 入力 VIP のデモンストレーションを行います。
7. 4 ～7 vCPU のサポート：
    - 4 個または 7 個の vCPU で CPX-1 を設定します。
    - HTTPS TPS のパフォーマンステストを表示, 全体的に暗号化された BW.

© 1999–2021 Citrix Systems, Inc. All rights reserved.

III. ヘアピン East-West デバイスとしての CPX

1. CPX-1。セクション I.1 で説明されているように、North-South トラフィック用の HTTPS 入力を作成します。
    - バックエンドアプリをフロントエンドアプリに公開します。
    - 両方のアプリ間のトラフィックを表示します。
    - バックエンドアプリを別のバックエンドアプリに公開します。
    - アプリ間のトラフィックを表示します。
2. CPX-1。手順 1 の指示に従います。また、エンドツーエンドの暗号化も示します。
    - オフロードと再暗号化を行う CPX-1 で暗号化されたバックエンドアプリからバックエンドアプリ。
3. バックエンドポッドの自動スケール:
    - CPX-1 で、バックエンドの自動スケーリングされたバックエンドポッドをサービスグループに追加することをデモンストレーションします。

IV. Prometheus と Grafana との CPX 統合

1. Prometheus コンテナを Kubernetes クラスターに挿入します。
    - 各アプリのエクスポート用に推奨されるカウンターでコンテナーを構成します。
    - Prometheus サーバーにカウンタデータを送信するエクスポーターコンテナをデモンストレーションします。
    - CPX から来る Prometheus サーバーからのデータを示す Grafana ダッシュボードを表示します.
    - 目標は、開発者が DevOps でよく使用されているクラウドネイティブツールを使用できることを示すことです。
2. 統合の Kubernetes ローリング展開をデモンストレーションします。
    - Nirmata に新しいバージョンのアプリを挿入します。
    - クラスターに新しいアプリケーションバージョンを展開する Kubernetes を表示します。
    - Kubernetes からのローリング展開コマンドに応答する CPX をデモンストレーションして、古いバージョンのアプリから新しいバージョンのアプリへのトラフィックの 100% を奪います。

Citrix ADC CPX 展開のための Citrix ADC ソリューション

1. カスタムプロトコル：デフォルトでは、CITRIX INGRESS CONTROLLER はデフォルトのプロトコル（HTTP/SSL）を使用して設定を自動化します。CITRIX INGRESS CONTROLLER は、注釈を使用してカスタムプロトコル（TCP/SSL-TCP/UDP）を設定することをサポートしています。

   注釈:

© 1999–2021 Citrix Systems, Inc. All rights reserved.

`ingress.citrix.com/insecure-service-type: "tcp"` [選択 LB プロトコルへの注釈]

`ingress.citrix.com/insecure-port: "53"` [カスタムポートをサポートする注釈]

2. **CS/LB/**サービスグループパラメータの微調整：デフォルトでは、CITRIX INGRESS CONTROLLER は ADC をデフォルトパラメータで設定します。これらのパラメータは、NetScaler ADC エンティティパラメータ（**lb/**サービスグループ）アノテーションを使用して微調整できます。

   注釈：

   LB-方 法:`ingress.citrix.com/lbvserver: '{ "app-1":{ "lbmethod":"ROUNDROBIN" } } '`

   持　続　性:`ingress.citrix.com/lbvserver: '{ "app-1":{ "persistencetype":"sourceip" } } '`

   NITRO API

3. アプリごとの **SSL** 暗号化：CITRIX INGRESS CONTROLLER は、スマートな注釈を使用して、アプリの SSL 暗号化を選択的に有効にすることができます。

   注釈：

   `ingress.citrix.com/secure_backend: '{ "web-backend": "True" }` [アプリケーションごとに暗号化を選択的に有効にする注釈]

4. 入力のデフォルト証明書： CITRIX INGRESS CONTROLLER はデフォルトの証明書を引数として使用することができます。入力定義にシークレットがない場合は、デフォルトの証明書が使用されます。シークレットは名前空間に一度作成する必要があり、名前空間にあるすべての入力がそれを使用できます。

5. **Citrix** の複数入力クラスのサポート：デフォルトでは、CITRIX INGRESS CONTROLLER は k8s クラスター内のすべての入力オブジェクトをリッスンします。入力クラス注釈の助けを借りて、ADC（Tier-1 MPX/VPX & Tier-2 CPX）の構成を制御することができます。これにより、各チームが ADC の構成を個別に管理できるようになります。Ingress クラスは、特定の名前空間と名前空間グループの ADC を構成するためのソリューションの展開に役立ちます。サポートは、他のベンダーが提供するよりも一般的です。

   注釈：

   `kubernetes.io/ingress.class: "citrix"` [特定のクラスに属する入力のみを設定するように CITRIX INGRESS CONTROLLER に通知する]

6. 可視性：Citrix `k8s`ソリューションは、Prometheous/Grafana などの`cncf`可視性ツールと統合され、測定基準収集が向上し、デバッグや分析機能が向上します。Citrix の Prometheus エクスポーターは、Grafana で時系列チャートとして可視化するために利用可能なメトリックを Prometheus に提供します.

マイクロサービスアーキテクチャの使用について詳しくは、GitHub のREADME.mdファイルを参照してください。構成フォルダ内の`.yaml`ファイルを見つけることができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

POC ストーリー

kubernetes クラスターでアプリを実行するチームが 3 つあります。各チームの設定は、Citrix の入力クラスの助けを借りて、異なる CPX 上で独立して管理されています。

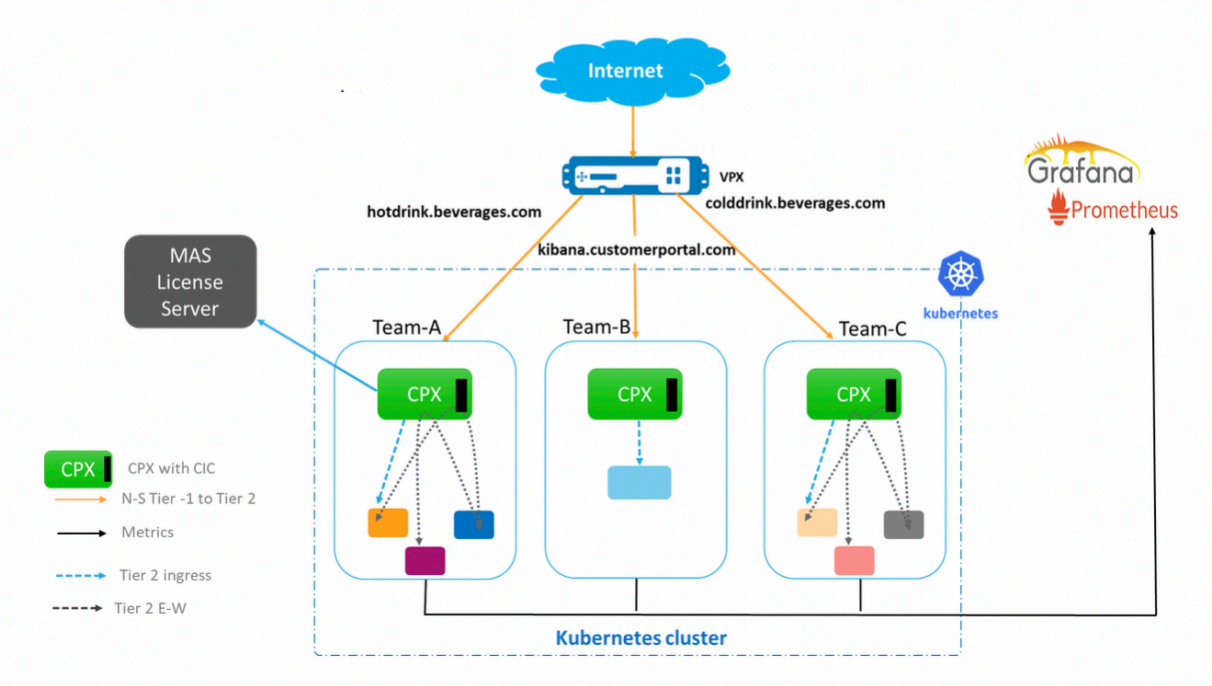
各チームのアプリは別々の名前空間（team-hotdrink, team-colddrink, and team-redi）で実行されており、すべての CPX は CPX 名前空間で実行されています。

team-hotdrink:SSL/HTTP 入力、永続性、lbmethod、アプリケーションごとの暗号化/説明、デフォルト証明書。

team-colddrink:SSL TCP 入力

team-redis: TCP 入力

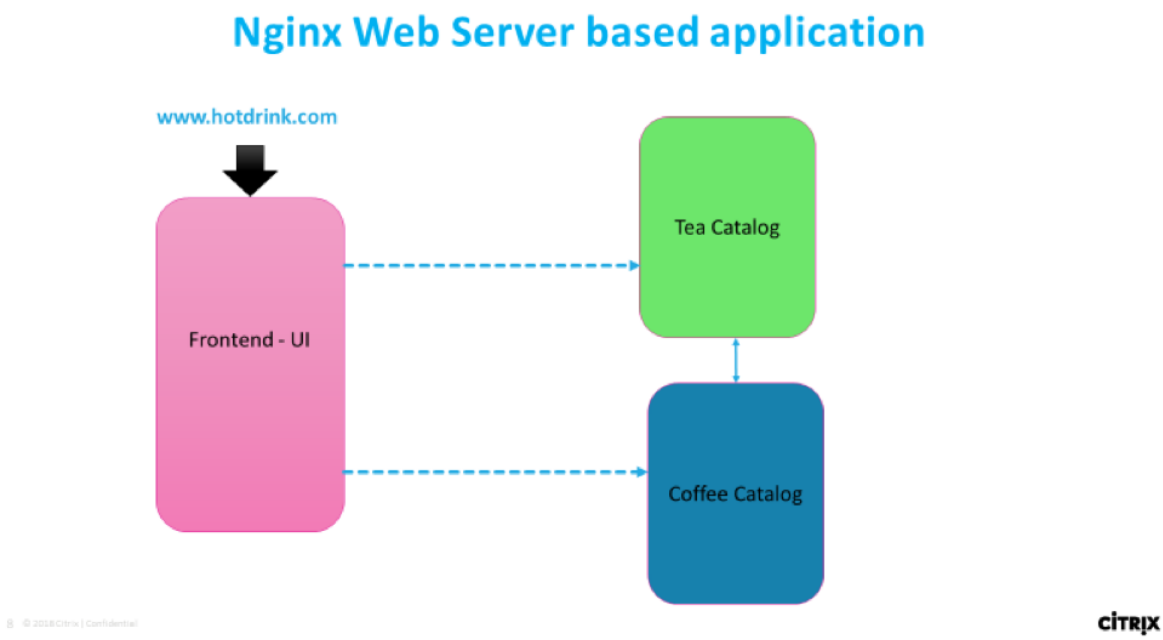
POC の設定



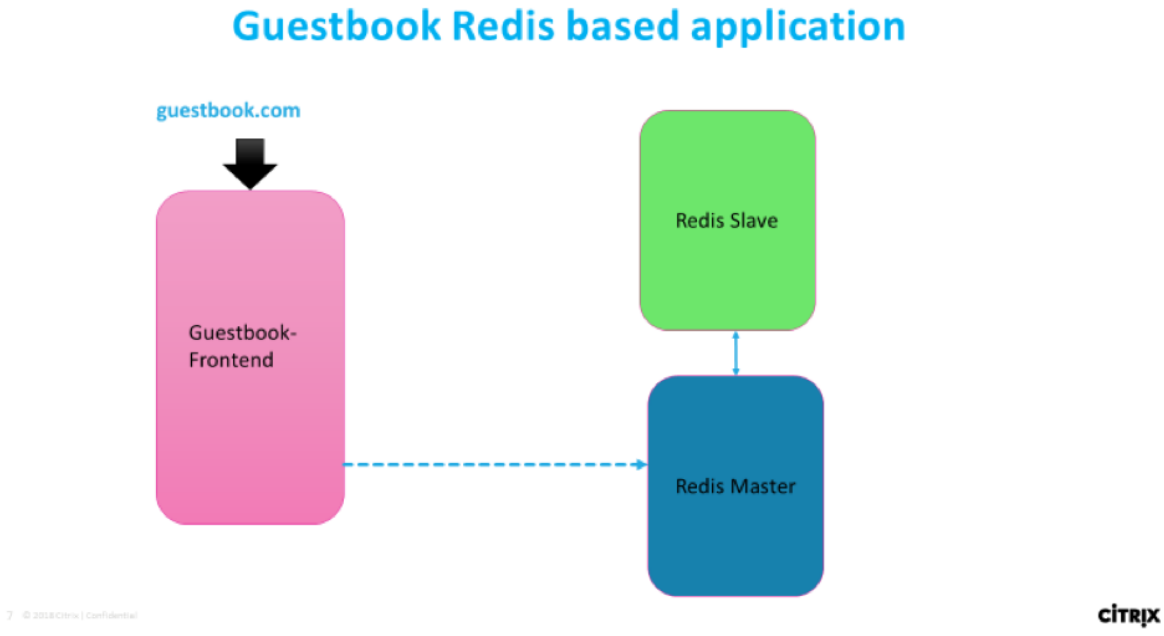
アプリケーションの流れ

HTTP/SSL/SSL/SSLTCP のユースケース:

© 1999–2021 Citrix Systems, Inc. All rights reserved.



TCP ユースケース:



ドッカーのイメージを取得する

提供された YAML コマンドは、キーリポジトリから画像を取得しています。

イメージをプルしてローカルリポジトリに保存することもできます。YAML で **Image** パラメータを編集することで利用できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Nirmata を使用したステップバイステップのアプリケーションおよび **CPX** の展開

1. クラスタロールとクラスタロールバインディングを YAML にアップロードし、Nirmata (rbac.yaml) を使用してクラスターに適用します。

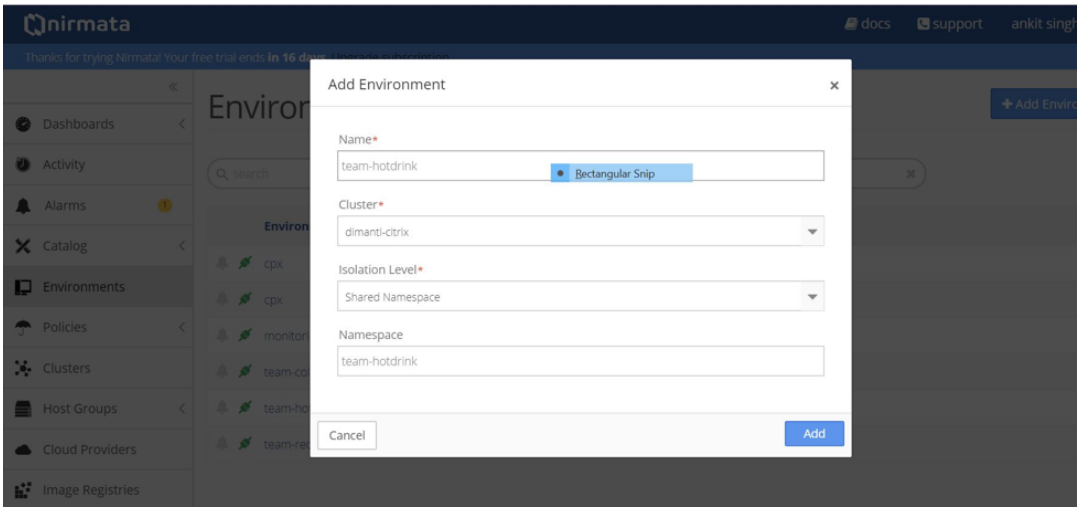
   a) [クラスタ] タブに移動します。
   b) クラスターを選択します。
   c) 設定では、[YAML を 適用] オプションから **YAML** を適用します。

2. CPX とアプリを実行するための環境を作成します。

   a) **[**環境**]** タブに移動します。

   b) [環境を追加] タブをクリックします。

      - クラスターを選択し、共有名前空間に環境を作成します。



   c) Prometheus、CPX、および異なるチーム用のアプリを実行するために、以下の環境を作成します。

      - 環境の作成：cpx
      - 環境の作成：team-hotdrink
      - 環境の作成：team-colddrink
      - 環境の作成：team-redis

3. Nirmata を使用して `.yaml` アプリケーションをアップロードします。

   a) **[**カタログ**]** タブに移動します。

   b) **[**アプリケーションの追加**]** をクリックします。

   c) [追加] をクリックして、アプリケーションを追加します。

      アプリケーションを追加 team-hotdrink (team_hotdrink.yaml)。アプリケーション名：`team-hotdrink`。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

アプリケーションを追加：team-colddrink (team_coldrink.yaml)。アプリケーション名：`team-colddrink`。

アプリケーションを追加：team-redis (team_redis.yaml)。アプリケーション名：`team-redis`。

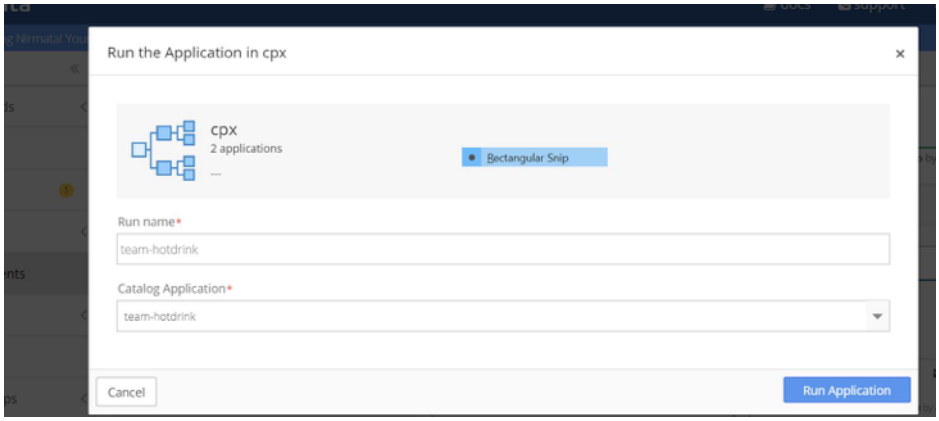
アプリケーションを追加：cpx-svcacct (cpx_svcacct.yaml)。アプリケーション名：cpx-svcacct。

> 注：
>
> CITRIX INGRESS CONTROLLER を内蔵した CPX では、実行中の名前空間にサービスアカウントが必要です。Nirmata の現在のバージョンでは、cpx 環境で`cpx_svcacct.yaml`を使用してこれを作成します。

アプリケーションを追加：cpx (cpx_wo_sa.yaml)。アプリケーション名：cpx。

4. Nirmata を使用して CPX を実行します。

   a) [環境] タブに移動し、正しい環境を選択します。
   b) [アプリケーションの実行] をクリックして、アプリケーションを実行します。
   c) cpx 環境で、`cpx-svcacct`アプリケーションを実行します。カタログアプリケーションから実行名`cpx-svcacct`の`cpx-svcacct`を選択します。
   d) cpx 環境で、cpx アプリケーションを実行します。カタログアプリケーションから「cpx」を選択します。



> 注：
>
> CPX の展開には、セットアップで以前のバージョンの Nirmata を使用しているため、いくつかの小さな回避策が必要です。
>
> a) CPX 配置を作成するときは、`serviceAccountName`を設定しないでください。`serviceAccountName`は後で追加できます。回避策として、ポッドを自動的に再展開します。
> b) 入力の TLS シークレットを環境に直接インポートします。これにより、タイプフィールドが保持されます。

   a) アプリケーションを実行した後、**CPX** アプリケーションに移動します。
   b) [展開] **> [StatefulSets & DaemonSets]** タブで、`cpx-ingress-colddrinks`展開をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

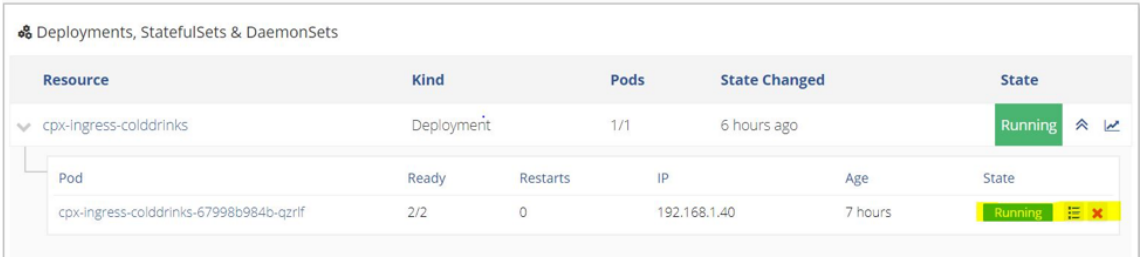
c) 次のページで、**Pod** テンプレートを編集します。サービスアカウントに **CPX** と入力します。
d) **CPX** アプリケーションに戻ります。
e) cpx-ingress-hotdrinksおよびcpx-ingress-redis展開でも同じ手順を繰り返します。

サービスアカウントを適用すると、ポッドが再展開されます。ポッドが起動するのを待ち、サービスアカウントが適用されているかどうかを確認します。

同じことは、**Diamanti** クラスターで次のコマンドを使用して確認できます。

```
[diamanti@diamanti-250 ~]$ kubectl get deployment -n cpx -o yaml |
    grep -i account
        serviceAccount: cpx
        serviceAccountName: cpx
        serviceAccount: cpx
<!--NeedCopy-->
```

> 注: serviceAccountが適用されていない場合は、CPX ポッドをキャンセルします。それを再作成する展開は、serviceAccountを使用します。

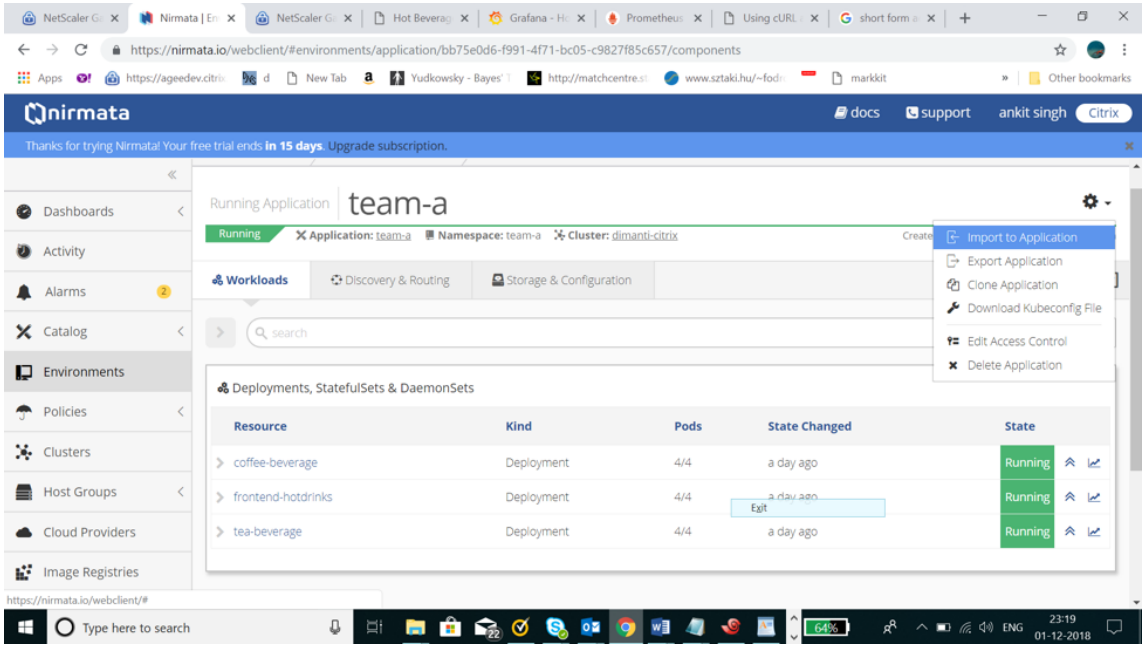


5. Nirmata を使用してアプリケーションを実行します。

チームホットドリンクアプリケーション:

a) [環境] タブに移動し、正しい環境を選択します。team-hotdrink
b) team-hotdrink 環境で、実行名でteam-hotddrink アプリケーションteam-hotdrink を実行します。カタログアプリケーションからteam-hotdrinkを選択します。
c) team-hotdrinkアプリケーションに移動します。画面の右上隅にある [設定] をクリックし、[アプリケーションにインポート] を選択します。hotdrink-secret.yamlをアップロードします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



チームコールドドリンクのアプリケーション:

a) [環境] タブに移動し、正しい環境を選択します。`team-colddrink`
b) `team-colddrink`環境で、実行名で`team-coldddrink`アプリケーション`team-colddrink`を実行します。カタログアプリケーションから`team-hotdrink`を選択します。
c) `team-colddrink`アプリケーションに移動します。画面の右上隅にある [設定] をクリックし、[アプリケーションにインポート] を選択します。`colddrink-secret.yaml`をアップロードします。

チーム**-Redis** アプリケーション:

a) [環境] タブに移動し、正しい環境を選択します。`team-redis`
b) `team-colddrink`環境で、実行名`team-redis`でアプリケーションを実行します。カタログアプリケーションから`team-redis`を選択します。
   - `team-redis`環境で、実行名`team-redis`でアプリケーションを実行します。

VPX 上の **Tier-2** の **CPX** を公開するコマンド

Tier-1 VPX は、SSL 暗号化/解読を行い、Tier-2 CPX に送信中に X-forward ヘッダーを挿入する必要があります。Tier-1 構成は手動で実行する必要があります。X-Forward ヘッダーは、サービスグループで-cip ENABLED を使用して挿入することができます。`config.txt`を開きます。

csverver を作成します。

`certkey`を Citrix ADC にアップロードします。`wild.com-key.pem`, `wild.com-cert.pem`

```
1 add cs vserver frontent_grafana HTTP <CS_VSERVER_IP> 80 -cltTimeout 180
2 <!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Tier-1 VPX で **www.hotdrinks.com**、**www.colddrinks.com**、**www.guestbook.com** で公開:

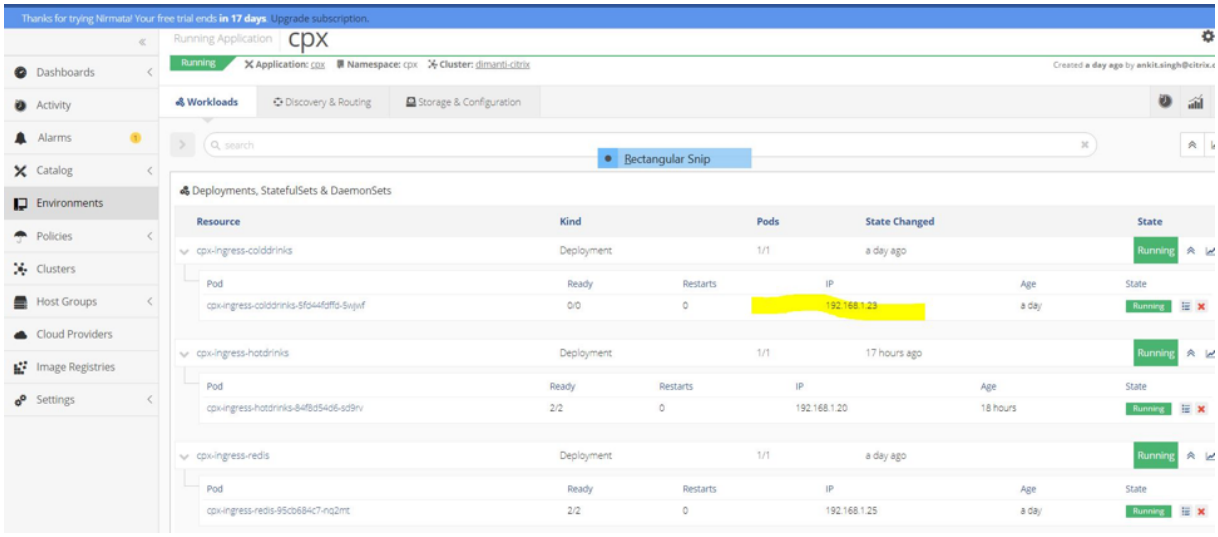
```
add serviceGroup team_hotdrink_cpx SSL -cip ENABLED
add serviceGroup team_colddrink_cpx SSL -cip ENABLED
add serviceGroup team_redis_cpx HTTP
add ssl certKey cert -cert "wild-hotdrink.com-cert.pem" -key "wild-
    hotdrink.com-key.pem"
add lb vserver team_hotdrink_cpx HTTP 0.0.0.0 0
add lb vserver team_colddrink_cpx HTTP 0.0.0.0 0
add lb vserver team_redis_cpx HTTP 0.0.0.0 0
add cs vserver frontent SSL 10.106.73.218 443
add cs action team_hotdrink_cpx -targetLBVserver team_hotdrink_cpx
add cs action team_colddrink_cpx -targetLBVserver team_colddrink_cpx
add cs action team_redis_cpx -targetLBVserver team_redis_cpx
add cs policy team_hotdrink_cpx -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www
    .hotdrinks.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    team_hotdrink_cpx
add cs policy team_colddrink_cpx -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("
    www.colddrinks.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    team_colddrink_cpx
add cs policy team_redis_cpx -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www.
    guestbook.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    team_redis_cpx
bind lb vserver team_hotdrink_cpx team_hotdrink_cpx
bind lb vserver team_colddrink_cpx team_colddrink_cpx
bind lb vserver team_redis_cpx team_redis_cpx
bind cs vserver frontent -policyName team_hotdrink_cpx -priority 10
bind cs vserver frontent -policyName team_colddrink_cpx -priority 20
bind cs vserver frontent -policyName team_redis_cpx -priority 30
bind serviceGroup team_hotdrink_cpx 10.1.3.8 443
bind serviceGroup team_colddrink_cpx 10.1.2.52 443
bind serviceGroup team_redis_cpx 10.1.2.53 80
bind ssl vserver frontent -certkeyName cert
<!--NeedCopy-->
```

サービスグループの **CPX** ポッド **IP** アドレスに **IP** アドレスを更新します。

```
root@ubuntu-211:~/demo-nimata/final/final-v1# kubectl get pods -n cpx -
    o wide
NAME                                      READY     STATUS    RESTARTS
     AGE       IP              NODE
cpx-ingress-colddrinks-5bd94bff8b-7prdl   1/1       Running   0
             2h        10.1.3.8   ubuntu-221
cpx-ingress-hotdrinks-7c99b59f88-5kclv    1/1       Running   0
             2h        10.1.2.52  ubuntu-213
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
5  cpx-ingress-redis-7bd6789d7f-szbv7         1/1       Running   0
               2h         10.1.2.53   ubuntu-213
6  <!--NeedCopy-->
```



- **www.hotdrinks.com**、**www.colddrinks.com**、**www.guestbook.com** にアクセスするには、（ページにアクセスするマシンの）ホストファイルに、次の値を追加する必要があります。

  <CS_VSERVER_IP> www.hotdrinks.com

  <CS_VSERVER_IP> www.colddrinks.com

  <CS_VSERVER_IP> www.guestbook.com

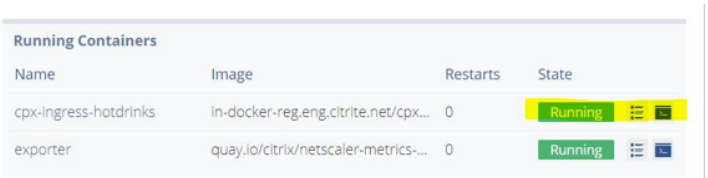
  これが完了したら、アプリにアクセスすることができます：**www.hotdrinks.com**、**www.colddrinks.com**、**www.guestbook.com**

Tier-2 CPX 構成の検証

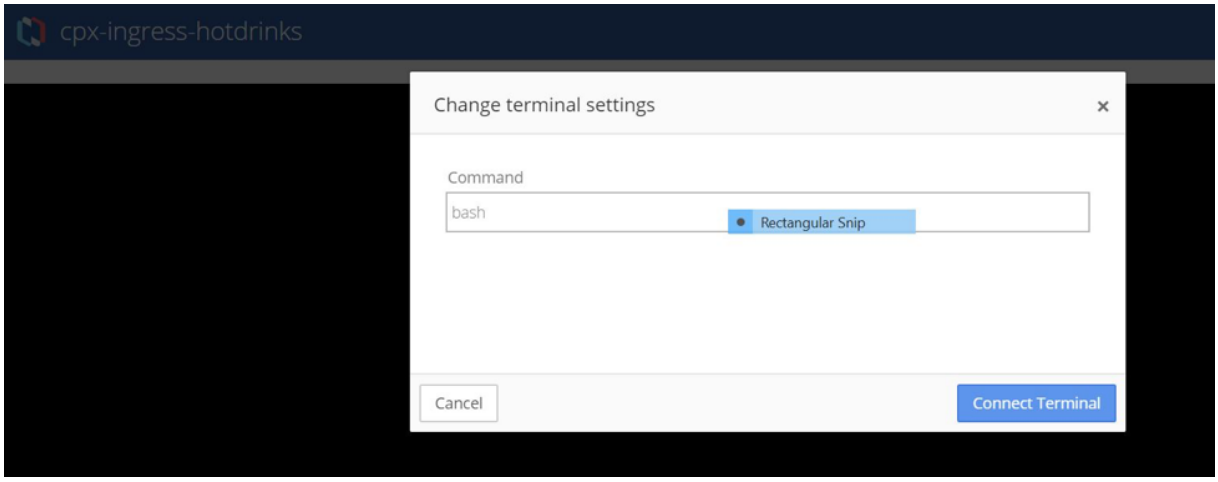
CPX 構成を検証するには、CPX 環境に移動します。CPX 実行中のアプリケーションを選択します。

cpx-ingress-hotdrinks展開を選択し、cpx-ingress-hotdrinks-xxxx-xxxxポッドをクリックします。

次のページで、実行中のコンテナに移動し、「bash” コマンド cpx-ingress-hotdrinks を入力しての端末を起動します。



© 1999–2021 Citrix Systems, Inc. All rights reserved.



ターミナルが接続されると、`cli_script.sh`で通常の NetScaler コマンドを使用して構成を検証します。

- `cli_script.sh "sh cs vs"`
- `cli_script.sh "sh lb vs"`
- `cli_script.sh "sh servicegroup"`

検証は、`team-colddrink`および`team-mongodb`の他の CPX 展開についても同じ方法で実行できます。

スケールアップ/スケールダウンの実行

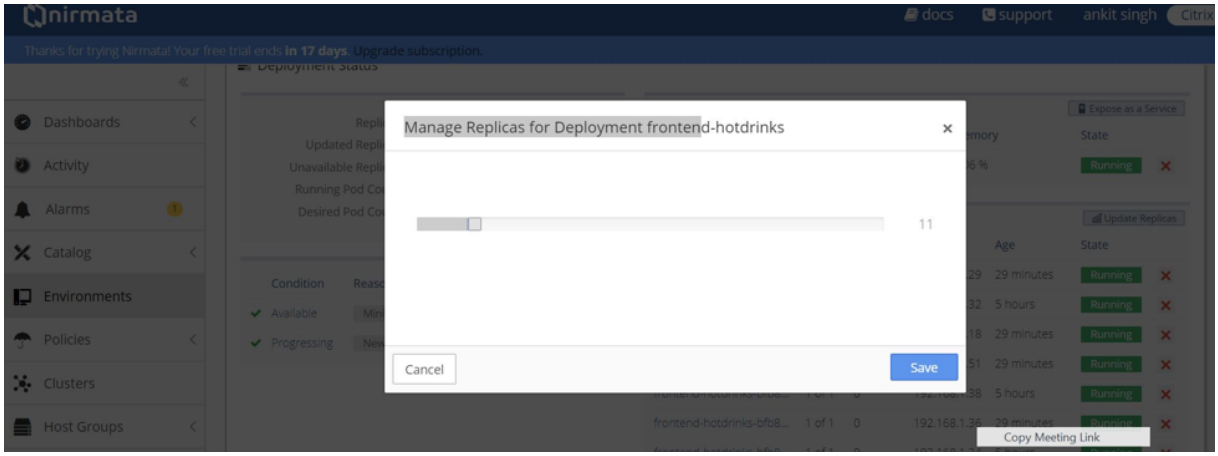
スケールアップ/スケールダウンを実行するには、次の手順に従います。

1. `team-hotdrink`環境に移動します。`team-hotdrink`実行中のアプリケーションを選択します。
2. `frontend-hotdrinks`展開をクリックします。
3. 次のページで、[レプリカの更新] をクリックします。この値を 10 に増やします。

参照：**Tier-2 CPX** 構成を検証して **CPX** の構成を確認 **(**展開**: cpx-ingress-hotdrinks)**。

1. CPX 環境に移動します。実行中の CPX アプリケーションを選択します。
2. `cpx-ingress-hotdrinks`展開をクリックします。
3. `cpx-ingress-hotdrinks-xxxx-xxxx`ポッドをクリックします。
4. 次のページで、実行中のコンテナに移動し、「bash” コマンド `cpx-ingress-hotdrinks` を入力しての端末を起動します。
5. 「`cli_script.sh "sh servicegroup < servicegroup name >"`」を参照してください。

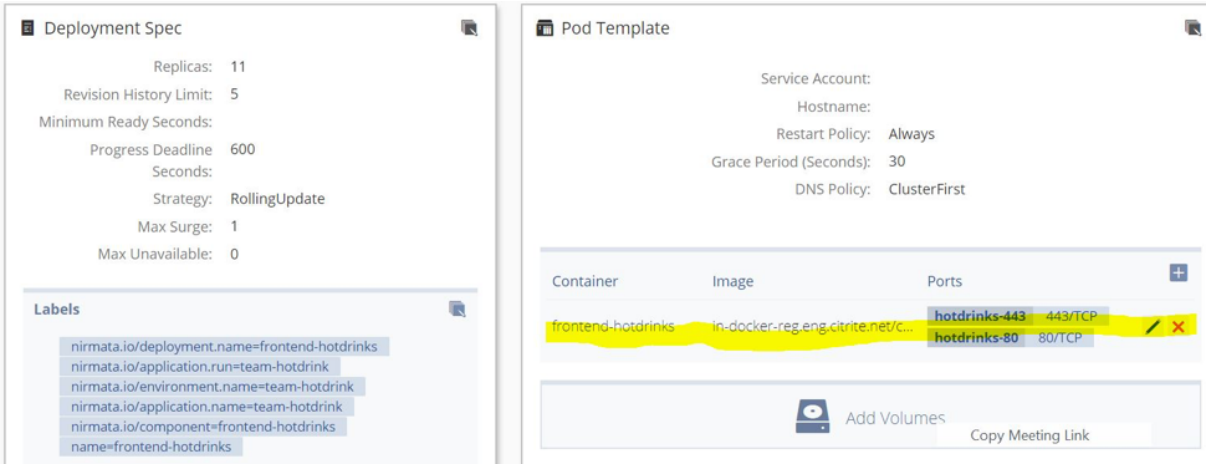
© 1999–2021 Citrix Systems, Inc. All rights reserved.



ローリング更新の実行

ローリング更新を実行するには、次の手順に従います。

1. `team-hotdrink`環境に移動します。`team-hotdrink`実行中のアプリケーションを選択します。
2. フロントエンドのホットドリンクを展開します。
3. 次のページで、ポッドテンプレートに移動します。
4. イメージの更新先：*quay.io/citrix/hotdrinks-v2: latest*。
5. 更新を完了させます。
6. アプリケーションにもう一度アクセスします。新しいページには、更新をローリングした後、更新されたイメージが付属しています。



Prometheus の展開

NetScaler メトリックスエクスポーター、Prometheus、および Grafana を使用して、入力 CPX からメトリックを自動的に検出して収集します。

Prometheus の展開手順**:**

© 1999–2021 Citrix Systems, Inc. All rights reserved.

CPX とアプリを実行する環境を作成します。

1. **[**環境**]** タブに移動します。
2. [環境を追加**]** をクリックします。
3. エクスポーター、Prometheus、Grafana. を実行するための環境を作成します。
    - 環境を作成します。監視。

Nirmata を使用して `.yaml` ファイルをアップロードします。

1. **[**カタログ**]** タブに移動します。
2. **[**アプリケーションの追加**]** をクリックします。
3. [追加] をクリックして、アプリケーションを追加します。
    - アプリケーションの追加：監視（.yaml の監視）。

Prometheus アプリケーションを実行しています：

1. [環境] タブに移動し、適切な環境（監視）を選択します。
2. 名前の 監視を使用して [アプリケーションの実行] をクリックします。
3. これにより、Exporter、Prometheus、および Grafana ポッドが展開され、メトリックスの収集が開始されます。
4. Prometheus と Grafana は VPX を通して公開する必要があります。

Prometheus と **Grafana** を公開する **VPX** 上のコマンド：

csvserver を作成します。

```
add cs vserver frontent_grafana HTTP <CS_VSERVER_IP> 80 -cltTimeout 180
<!--NeedCopy-->
```

Prometheus を公開する：

```
add serviceGroup prometheus HTTP
add lb vserver prometheus HTTP 0.0.0.0 0
add cs action prometheus -targetLBVserver prometheus
add cs policy prometheus -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www.
    prometheus.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    prometheus
bind lb vserver prometheus prometheus
bind cs vserver frontent_grafana -policyName prometheus -priority 20
bind serviceGroup prometheus <PROMETHEUS_POD_IP> 9090
<!--NeedCopy-->
```

> 注：
>
> “kubectl get pods -n monitoring -o wide” を使用して prometheus-k8s-0 pod IP を取得します

グラファナを公開:

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
add serviceGroup grafana HTTP
add lb vserver grafana HTTP 0.0.0.0 0
add cs action grafana -targetLBVserver grafana
add cs policy grafana -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www.grafana.
    com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action grafana
bind lb vserver grafana grafana
bind cs vserver frontent_grafana -policyName grafana -priority 10
bind serviceGroup grafana <GRAFANA_POD_IP>  3000
<!--NeedCopy-->
```

> 注:
>
> `kubectl get pods -n monitoring -o wide`を使用して grafana-xxxx-xxx pod IP を取得します

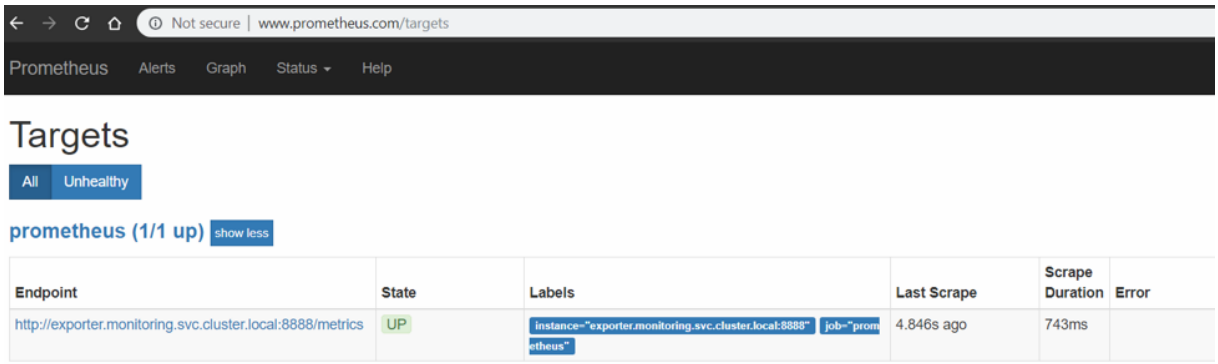
- これで、Prometheus と Grafana のページが VPX の csvserver 経由でアクセスできるように公開されました。
- Prometheus と Grafana にアクセスするには、（ページにアクセスするマシンの）hosts ファイルに以下の値を付加する必要があります。

  ```
  <CS_VSERVER_IP> www.grafana.com
  <CS_VSERVER_IP> www.prometheus.com
  ```

- これが完了したら、**www.prometheus.com** にアクセスして Prometheus に移動します。Grafana にアクセスするには、**www.grafana.com** に移動します。

指標を視覚化する**:**

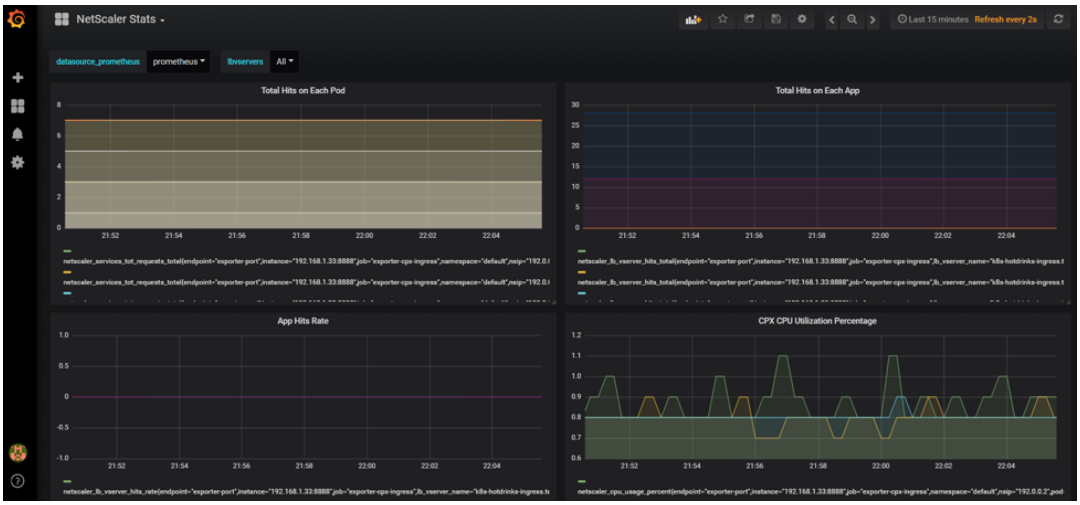
- Prometheus がエクスポーターを検出したことを確認するには、**www.prometheus.com/targets** にアクセスしてください。CPX および VPX デバイスを監視しているすべてのエクスポーターのリストが含まれている必要があります。すべてのエクスポータが **UP** 状態であることを確認します。以下の例を参照してください:



- 収集中の値をプロットするために Grafana を使用することができます。これを行うには、次の操作を行います。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

1. **www.grafana.com** に移動します。ホストファイルに適切なエントリが追加されていることを確認します。
2. デフォルトのユーザ名 **admin** とパスワード **admin** を使用してログインします。
3. ログイン後、ホームダッシュボードで **[**データソースの追加**]** をクリックします。
4. **[Prometheus]** オプションを選択します。
5. 次の詳細情報を入力/変更します。
   - 名前：prometheus (すべて小文字)。
   - URL:`http://prometheus:9090`。
   - 残りのエントリはデフォルト値のままにします。
6. [保存してテスト] をクリックします。画面の下部に **[**データソースが動作しています] というメッセージが表示されるまで、数秒間待ちます。
7. 左パネルの+アイコンをクリックして、あらかじめデザインされた Grafana テンプレートを読み込みます。「インポート」を選択します。
8. 「**json** をアップロード」ボタンをクリックし、**sample_grafana_dashboard.json** ファイルを選択します（名前、フォルダ、一意の識別子は変更しません）。
9. 「**Prometheus**」ドロップダウンメニューから「Prometheus」を選択し、「インポート」をクリックします。
10. これにより、次の画像のようなダッシュボードがアップロードされます。



ライセンスおよびパフォーマンステスト

PERF およびライセンス用の **CPX** の実行。

CPX コアの数とライセンスサーバーの詳細は、以下の環境変数に記載されています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

コア数を選択する環境変数

- 名前**:**「**CPX** コア」
- 値**: 3**

ライセンスサーバーを選択する環境変数

- 名前**:**「**LS_IP**」
- 値**:**「**X.X.X.X**」

  ダイアマンティ注釈**:**
  `diamanti.com/endpoint0: '{ "network":"lab-network","perfTier":"high" }`

  上記の正しい **IP** を設定して、ライセンスサーバーを修正します。

  1. 上記の環境変数と Diamanti 固有の注釈を`cpx-perf.yaml`ファイルに追加します。
  2. [環境] タブに移動し、`cpx-perf`環境を作成します。

  Nirmata を使用して **YAML** アプリケーションをアップロードします。

  1. **[**カタログ**]** タブに移動します。
  2. **[**アプリケーションの追加**]** をクリックします。
  3. 追加をクリックしてアプリケーションを追加します: `cpx-perf.yaml`。アプリケーション名: `cpx-perf`。

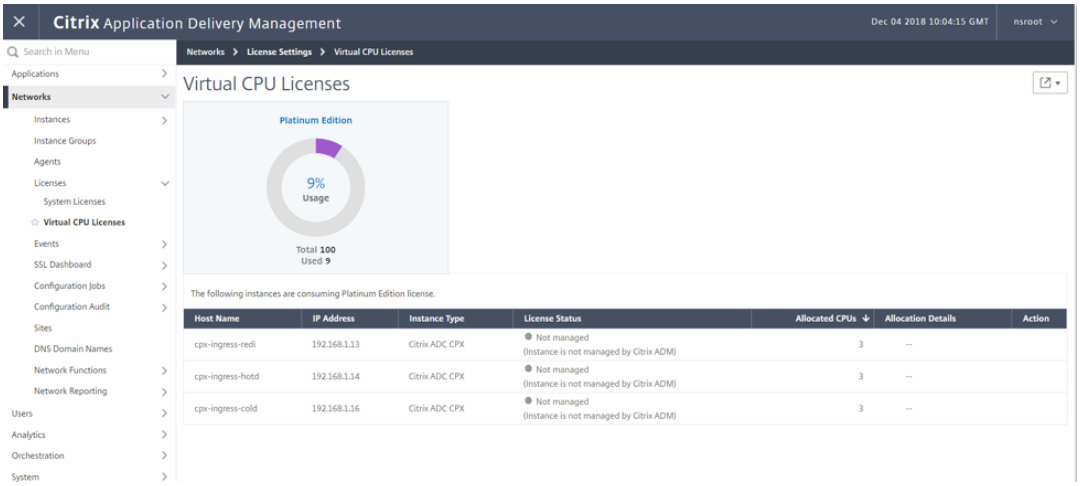
  CPX を実行中:

  1. [環境] タブに移動し、`cpx-perf`環境を選択します。
  2. `cpx-perf`環境で、`cpx-svcacct`アプリケーションを実行します。
  3. `cpx-perf`環境で、`cpx-perf`アプリケーションを実行します。
  4. アプリケーションを実行した後、`cpx-perf`アプリケーションに移動します。
  5. [展開**] > [StatefulSets & DaemonSets**] タブで、`cpx-ingress-perf`展開をクリックします。次のページで、ポッドテンプレートを編集します。サービスアカウントに **CPX** と入力します。
  6. ライセンスが動作していること、および Citrix ADM でライセンスのチェックアウトが行われていることを確認します。
     - CPX で検証するには、次の手順に従います。
       * kubectl get pods -n cpx
       * kubectl exec -it <CPX_POD_NAME> -n cpx bash
       * cli_script.sh 'sh licenseserver'
       * sh 'sh キャパシティ'
     - 同様の出力を表示します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
root@cpx-ingress-colddrinks-66f4d75f76-kzf8w:/# cli_script.sh
    'sh licenseserver'
exec: sh licenseserver
1)  ServerName:  10.217.212.228Port:  27000           Status:
     1              Grace:  0              Gptimeleft:  0
Done
root@cpx-ingress-colddrinks-66f4d75f76-kzf8w:/# cli_script.sh
    'sh capacity'
exec: sh capacity
    Actualbandwidth:  10000 VcpuCount:  3           Edition:
        Platinum      Unit:  Mbps             Maxbandwidth:
        10000    Minbandwidth:  20       Instancecount:  0
Done
<!--NeedCopy-->
```

- ADM で検証するには、ライセンスサーバーに移動し、**[ネットワーク] > [ライセンス] > [仮想 CPU ライセンス]** に移動します。
- ここでは、ライセンスされた CPX とコア数が表示されます。



「アノテーション」テーブル

© 1999–2021 Citrix Systems, Inc. All rights reserved.

注釈	指定可能な値	説明	デフォルト（存在する場合）
kubernetes.io/ingress.c	入力クラス名	これは、特定の入力リソースと Ingress Controller を関連付ける方法です。たとえば、`kubernetes.io/ingress.class:"Citrix"`	すべての入力を設定します。
ingress.citrix.com/secure_backend	json 形式を使用して、安全なバックエンドのためのサービスを一覧表示します	Citrix ADC でセキュアな HTTPS 接続を使用してアプリケーションを接続する場合は、**True** を使用します。Citrix ADC で安全でない HTTP 接続を使用してアプリケーションを接続する場合は、**False** を使用します。たとえば、`ingress.citrix.com/secure_backend: { 'app1':"True", 'app2':"False", 'app3':"True"}`	「偽」

© 1999–2021 Citrix Systems, Inc. All rights reserved.

注釈	指定可能な値	説明	デフォルト（存在する場合）
ingress.citrix.com/lbvse	JSON 形式で、lbvserver 用の設定	スマートな注釈機能を提供します。これを使用すると、上級ユーザー（NetScaler LB Vserver とサービスグループオプションに関する知識を持つユーザー）が直接適用できます。値は、.json 形式である必要があります。入力のバックエンドアプリケーションごとに、キー値のペアを指定します。キー名は、対応する CLI 名と一致する必要があります。たとえば、`ingress.citrix.com/lbvserver: '{ "app-1":{ "lbmethod":"ROUNDROBIN" } }'`	デフォルト値

Citrix ADC SSL プロファイル検証済みリファレンスデザイン

May 18, 2020

概要

Citrix ADC のサマリー

Citrix ADC はオールインワンのアプリケーション配信 Controller で、アプリケーションを最大 5 倍に実行し、アプリケーションの所有コストを削減し、ユーザーエクスペリエンスを最適化し、アプリケーションを常に使用できるようにします。

- 高度な L4-7 ロードバランシングとトラフィック管理
- 実証済みのアプリケーションアクセラレーション（HTTP 圧縮やキャッシュなど）
- アプリケーションセキュリティのための統合されたアプリケーションファイアウォール

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- サーバのオフロードにより、コストを大幅に削減し、サーバーを統合

サービスとアプリケーションデリバリのリーダーとして、Citrix ADC は世界中の何千ものネットワークに展開され、エンタープライズおよびクラウドサービスの提供を最適化し、セキュリティで保護し、制御しています。Citrix ADC は、Web サーバーとデータベースサーバーの前に直接配置され、高速負荷分散とコンテンツスイッチ、http 圧縮、コンテンツキャッシュ、SSL アクセラレーション、アプリケーションフローの可視性、強力なアプリケーションファイアウォールを統合し、使いやすい統合プラットフォームに統合します。ネットワークデータを実用的なビジネスインテリジェンスに変換するエンドツーエンドの監視により、SLA への対応が大幅に簡素化されます。Citrix ADC では、プログラミングの専門知識を必要とせずに、シンプルな宣言型ポリシーエンジンを使用してポリシーを定義および管理できます。

Citrix ADC SSL プロファイルの概要

SSL プロファイルを使用して、Citrix ADC が SSL トラフィックを処理する方法を指定できます。このプロファイルは、仮想サーバ、サービス、サービスグループなどの SSL エンティティの SSL パラメータ設定の集まりであり、設定の容易さと柔軟性を提供します。グローバルパラメータのセットを 1 つだけ設定することに限定されません。グローバルパラメータの複数のセット（プロファイル）を作成し、異なる SSL エンティティに異なるセットを割り当てることができます。SSL プロファイルは、次の 2 つのカテゴリに分類されます。

- フロントエンドプロファイル。フロントエンドエンティティに適用可能なパラメーターを含みます。つまり、クライアントからの要求を受信するエンティティに適用されます。
- バックエンドプロファイル。バックエンドエンティティに適用可能なパラメータを含みます。つまり、クライアント要求をサーバーに送信するエンティティに適用されます。

TCP または HTTP プロファイルとは異なり、SSL プロファイルはオプションです。SSL プロファイル（グローバルパラメータ）が有効になると、すべての SSL エンドポイントはデフォルトプロファイルを継承します。複数のエンティティ間で同じプロファイルを再利用できます。図形に縦断がアタッチされていない場合は、グローバルレベルで設定された値が適用されます。動的に学習されたサービスには、現在のグローバル値が適用されます。

個々の SSL エンドポイントで SSL パラメータ、暗号化、ECC 曲線の構成を必要とする代替方法と比較して、Citrix ADC SSL プロファイルはすべての関連エンドポイントに対して SSL 構成の単一ポイントとして機能し、構成管理を簡素化します。さらに、暗号の順序変更や暗号の順序変更時のダウンタイムなどの設定の問題は、SSL プロファイルを使用して解決されます。

SSL プロファイルは、従来はこれらのパラメータとバインディングを設定できなかった SSL エンドポイントに必須の SSL パラメータと暗号バインディングを設定するのに役立ちます。SSL プロファイルは、セキュリティで保護されたモニターでも設定できます。

次の表に、各プロファイルの一部であるパラメータを示します。

フロントエンドプロファイル	バックエンドプロファイル
cipherRedirect, cipherURL	denySSLReneg
clearTextPort*	encryptTriggerPktCount

© 1999–2021 Citrix Systems, Inc. All rights reserved.

フロントエンドプロファイル	バックエンドプロファイル
clientAuth, clientCert	nonFipsCiphers
denySSLReneg	pushEncTrigger
dh, dhFile, dhCount	pushEncTriggerTimeout
dropReqWithNoHostHeader	pushFlag
encryptTriggerPktCount	quantumSize
eRSA, eRSACount	serverAuth
insertionEncoding	commonName
nonFipsCiphers	sessReuse, sessTimeout
pushEncTrigger	SNIEnable
pushEncTriggerTimeout	ssl3
pushFlag	sslTriggerTimeout
quantumSize	strictCAChecks
redirectPortRewrite	トールズ 1.0, トールズ 1.1, トールズ 1.2
sendCloseNotify	
sessReuse, sessTimeout	
SNIEnable	
ssl3	
sslRedirect	
sslTriggerTimeout	
strictCAChecks	
tls1, tls11, tls12	

*clearTextPort パラメーターは、SSL 仮想サーバーにのみ適用されます。

プロファイルに含まれないパラメータを設定しようとすると（たとえば、バックエンドプロファイルで clientAuth パラメータを設定しようとした場合）、エラーメッセージが表示されます。

CRL メモリサイズ、OCSP キャッシュサイズ、UndefAction コントロール、UndefAction データなど、一部の SSL パラメータは、これらのパラメータはエンティティから独立しているため、上記のプロファイルには含まれません。これらのパラメータは、[トラフィック管理] **> [SSL] > [**高度な **SSL** 設定**]** にあります。

SSL プロファイルでは、次の操作がサポートされます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- 追加：Citrix ADC 上に SSL プロファイルを作成します。プロファイルがフロントエンドかバックエンドかを指定します。フロントエンドがデフォルトです。
- 設定-既存のプロファイルの設定を変更します。
- 設定解除-指定したパラメータをデフォルト値に設定します。パラメータを指定しない場合は、エラーメッセージが表示されます。エンティティのプロファイルを設定解除すると、そのプロファイルはエンティティからバインド解除されます。
- 除去-プロファイルを削除します。どのエンティティでも使用されているプロファイルも削除できません。設定をクリアすると、すべてのエンティティが削除されます。その結果、プロファイルも削除されます。
- 「バインド」(Bind)-プロファイルを仮想サーバーにバインドします。
- バインド解除-仮想サーバーからプロファイルをバインド解除します。
- [表示]：Citrix ADC で使用可能なすべてのプロファイルを表示します。プロファイル名を指定すると、そのプロファイルの詳細が表示されます。図形を指定すると、その図形に関連付けられた縦断が表示されます。

SSL プロファイルの使用例

SSL デフォルトプロファイル

Citrix ADC アプライアンスには、2 つのデフォルトプロファイル（

1. ns_default_ssl_profile_frontend — すべての SSL タイプの仮想サーバーおよび内部サービスのデフォルトのフロントエンドプロファイル。
2. ns_default_ssl_profile_backend — SSL タイプのサービス、サービスグループ、セキュアなモニター用のデフォルトのバックエンドプロファイル。

新しいエンドポイントが作成されると、対応するデフォルトの SSL プロファイルがバインドされます。

デフォルトの SSL プロファイルの SSL パラメータと暗号を変更できます。これにより、顧客は、対応するエンドポイントによって参照される一点で設定とバインディングを変更できるようになります。

> 重要：
>
> ソフトウェアをアップグレードしてデフォルトのプロファイルを有効にする前に、設定を保存してください。
>
> 拡張プロファイルインフラストラクチャをサポートするビルドにソフトウェアをアップグレードし、既定のプロファイルを有効にします。特定の展開に応じて、2 つのアプローチのいずれかを使用できます。展開にエンドポイント間で共通の SSL 設定がある場合は、「ユースケース 1」を参照してください。展開に大きな SSL 設定があり、SSL パラメータと暗号がエンドポイント間で共通でない場合は、「ユースケース 2」を参照してください。
>
> ソフトウェアをアップグレードした後で、プロファイルを有効にすると、変更を元に戻すことはできません。つまり、プロファイルを無効にすることはできません。したがって、変更を元に戻す唯一の方法は、古い構成を使用して再起動することです。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注：単一の操作（デフォルトプロファイルの有効化または ssl パラメーターの設定-defaultProfile ENABLED）により、デフォルトのフロントエンドプロファイルとデフォルトのバックエンドプロファイルの両方が有効になります（バインド）。
>
> 注意**:** v11.1 以降のクラスタリングでデフォルトの SSL プロファイルを使用できるようになりました。

Citrix ADC コマンドラインを使用して構成を保存するには、コマンドプロンプトで次のように入力します。

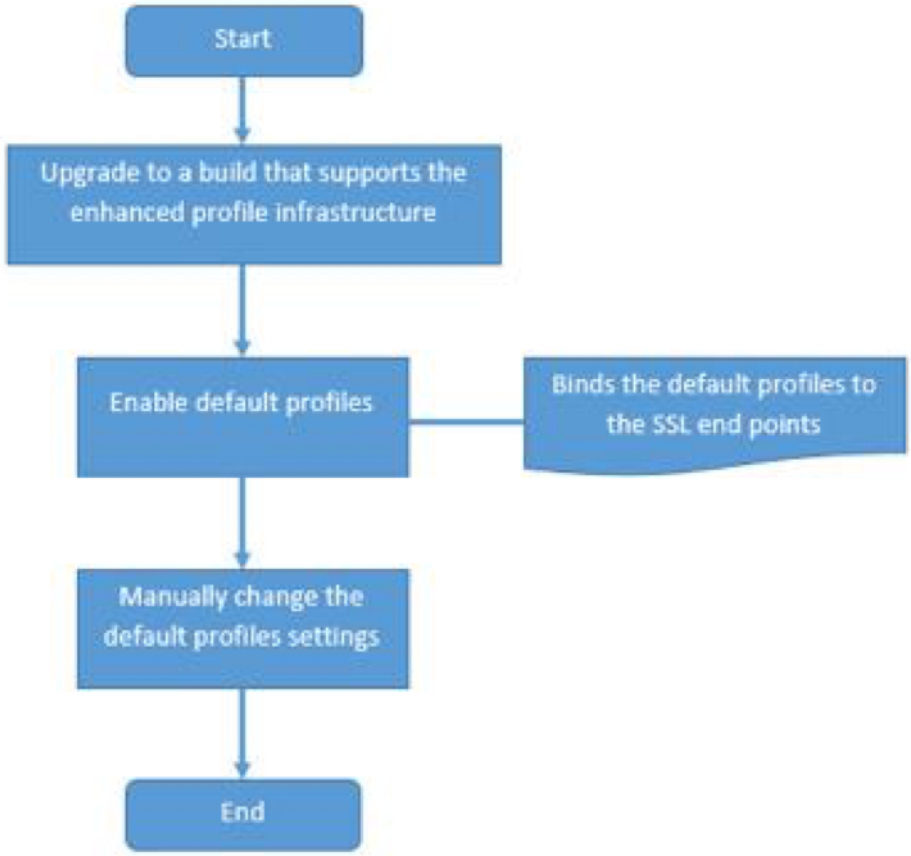
```
1 >save config
2
3 >shell
4
5 root@ns# cd /nsconfig
6
7 root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
     >
8 <!--NeedCopy-->
```

使用例 **1**

デフォルトプロファイルを有効にすると、すべての SSL エンドポイントにバインドされます。既定のプロファイルは編集可能です。展開でほとんどのデフォルト設定が使用され、少数のパラメータしか変更されない場合は、デフォルトのプロファイルを編集できます。変更内容は、すべてのエンドポイントに即座に反映されます。

次のフローチャートでは、実行する必要がある手順について説明します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



1. ソフトウェアのアップグレードについては、「システムソフトウェアのアップグレード」を参照してください。
2. Citrix ADC コマンドラインまたは GUI を使用して、デフォルトのプロファイルを有効にします。
   - コマンドラインで、次のように入力します: set ssl parameter -defaultProfile ENABLED
   - GUI を使用する場合は、**[**トラフィック管理**] > [SSL] > [**高度な **SSL** 設定の変更**]** に移動し、下にスクロールして **[**デフォルトプロファイルの有効化**]** を選択します。
3. （オプション）デフォルトプロファイルの設定を手動で変更します。
   - コマンドラインで、変更するパラメータに続けて`set ssl profile <name>`を入力します。
   - GUI を使用する場合は、**[**システム**] > [**プロファイル**]** に移動します。「SSL プロファイル」でプロファイルを選択し、「編集」をクリックします。

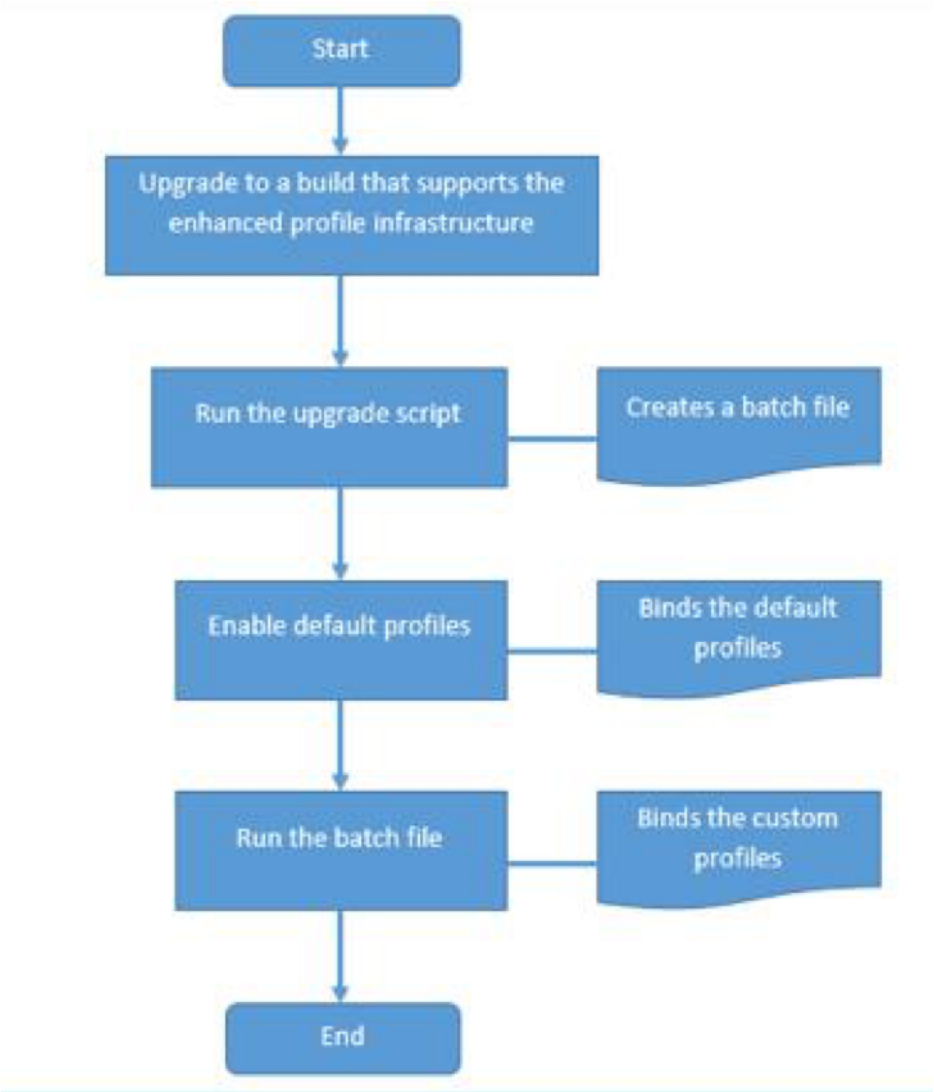
使用例 **2**

展開でほとんどの SSL エンティティに特定の設定を使用している場合は、各エンドポイントのカスタムプロファイルを自動的に作成し、エンドポイントにバインドするスクリプトを実行できます。このセクションで説明する手順を使用して、展開内のすべての SSL エンドポイントの SSL 設定を保持します。ソフトウェアのアップグレード後、移行スクリプトをダウンロードして実行し、SSL 固有の変更をキャプチャします。このスクリプトを実行した場合の出力

© 1999–2021 Citrix Systems, Inc. All rights reserved.

はバッチファイルです。既定のプロファイルを有効にして、バッチファイル内のコマンドを適用します。アップグレード後の SSL 設定の移行例については、付録を参照してください。

次のフローチャートでは、実行する必要がある手順について説明します。



1. ソフトウェアのアップグレードについては、「システムソフトウェアのアップグレード」を参照してください。
2. SSL 固有の変更をキャプチャするスクリプトをダウンロードして実行します。他の移行アクティビティに加えて、スクリプトは古い ns.conf ファイルを分析し、特別な設定（デフォルト以外）を SSL エンドポイント設定からカスタムプロファイルに移動します。設定の変更を適用するには、アップグレード後にデフォルトプロファイルを有効にする必要があります。

   スクリプトをダウンロードするには、https://www.citrix.com/にログインします。[ダウンロード] タブで [Citrix ADC] を選択し、リリース（[リリース 12.0] など）を選択します。リリースの「ファームウェア」で、ビルドを選択します。SSL デフォルトプロファイルスクリプトは、[追加コンポーネント] で使用できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注**:** 移行スクリプトの実行時に、プロファイル名を自動的に生成するか、対話的にユーザーにプロファイル名の入力を求めるように選択することができます。移行スクリプトは、以下をチェックし、それに応じてプロファイルを作成します。
>
> - デフォルト設定と類似した暗号と暗号グループ設定を持つエンドポイント: スクリプトによって 1 つのプロファイルが作成されます。
> - デフォルト設定で、異なる暗号グループまたは異なる優先順位を持つエンドポイント: いずれの場合も、スクリプトはユーザ定義の暗号グループを作成し、プロファイルにバインドし、各プロファイルを適切なエンドポイントにバインドします。
> - デフォルト設定とデフォルト暗号を使用するエンドポイント: デフォルトのプロファイルがエンドポイントにバインドされます。

```
1 スクリプトを実行するには、コマンドプロンプトで次のように入力します。
```

```
1 ./default_profile_script /nsconfig/ns.conf -b > <output file name
    >`
2 <!--NeedCopy-->
```

```
1 このコマンドは、スクリプトを格納するフォルダーから実行する必要があります。
```

3. Citrix ADC コマンドラインまたは GUI を使用して、デフォルトのプロファイルを有効にします。
   - コマンドラインで、次を入力します: `set ssl parameter -defaultProfile ENABLED`。
   - GUI を使用する場合は、**[**トラフィック管理**] > [SSL] > [**高度な **SSL** 設定の変更**]** に移動し、下にスクロールして **[**デフォルトプロファイルの有効化**]** を選択します。

カスタム **SSL** プロファイル

デフォルトの SSL プロファイルのほかに、お客様は特定のユースケース用にカスタムのフロントエンドおよびバックエンド SSL プロファイルを作成できます。異なるアプリケーションが異なる暗号と SSL パラメータを必要とするシナリオが存在する可能性があります。このような場合、お客様は新しいプロファイルを作成し、エンドポイントにバインドできます。

システムに作成できるカスタムプロファイルの数には上限はありません。

SSL プロファイルなどを有効にする方法については、SSL プロファイルドキュメントを参照してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

SSL フロントエンドプロファイル

フロントエンド SSL プロファイルは、SSL タイプの仮想サーバーおよび内部サービスに関連しています。フロントエンドプロファイルは、負荷分散仮想サーバー、コンテンツスイッチ仮想サーバー、AAA-TM 仮想サーバー、Gateway VPN 仮想サーバーカテゴリのすべての SSL タイプの仮想サーバーに適用されます。

SSL、SSL_TCP、SIP_SSL、SSL_FIX、SSL_DIAMETER-仮想サーバーの次のタイプは、フロントエンドプロファイルをサポートしています。

すべての内部サービスは、フロントエンドプロファイルをサポートしています。

SSL バックエンドプロファイル

バックエンドプロファイルは、SSL タイプサービス、サービスグループ、およびセキュアモニタに関連しています。次のタイプのサービスおよびサービスグループは、SSL、SSL_TCP、SIP_SSL、SSL_FIX、SSL_DIAMETER のバックエンドプロファイルをサポートします。

一部のモニタは、セキュアな接続を介してバックエンドサーバの健全性をチェックするように設定できます。SSL プロファイルをこのようなモニタにバインドして、SSL パラメータと暗号を設定できます。このようなモニターは、HTTP、HTTP-ECV、HTTP-インライン、TCP、および TCP-ECV です。

Citrix ADC と **Amazon Web Services** 検証済みのリファレンスデザイン

March 2, 2021

概要 **Citrix Networking VPX**

Citrix ADC はオールインワンのアプリケーション配信 Controller で、アプリケーションを最大 5 倍に実行し、アプリケーションの所有コストを削減し、ユーザーエクスペリエンスを最適化し、アプリケーションを常に使用できるようにします。

- 高度な Layer4-7 ロードバランシングとトラフィック管理
- 実証済みのアプリケーションアクセラレーション（HTTP 圧縮やキャッシュなど）
- アプリケーションセキュリティのための統合されたアプリケーションファイアウォール
- サーバのオフロードにより、コストを大幅に削減し、サーバーを統合

サービスとアプリケーションデリバリのリーダーとして、Citrix ADC は世界中の何千ものネットワークに展開され、エンタープライズおよびクラウドサービスの提供を最適化し、セキュリティで保護し、制御しています。Citrix ADC は、Web サーバーとデータベースサーバーの前に直接配置され、高速負荷分散とコンテンツスイッチ、HTTP 圧縮、コンテンツキャッシュ、SSL アクセラレーション、アプリケーションフローの可視性、強力なアプリケーションファイアウォールを統合し、使いやすい統合プラットフォームに統合します。ネットワークデータを実用的なビジネスイ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ンテリジェンスに変換するエンドツーエンドの監視により、SLA への対応が大幅に簡素化されます。Citrix ADC では、プログラミングの専門知識を必要とせずに、シンプルな宣言型ポリシーエンジンを使用してポリシーを定義および管理できます。

概要 **Amazon Web Services** での **Citrix ADC**

Amazon Web Services（AWS）内の Citrix Networking VPX のサポートは、バージョン 10.5～61.11 以降で利用可能です。Citrix Networking VPX は、AWS Marketplace に Amazon マシンイメージ（AMI）として表示されます。Citrix Networking VPX on AWS では、AWS クラウドコンピューティング機能を活用し、Citrix ADC の負荷分散機能とトラフィック管理機能をビジネスニーズに合わせて利用できます。Citrix ADC on AWS は、物理 Citrix ADC アプライアンスのすべてのトラフィック管理機能をサポートします。AWS で実行されている Citrix ADC インスタンスは、スタンドアロンインスタンスとして、または HA ペアで展開できます。

Citrix Networking VPX AMI は、AWS VPC 内で起動される EC2 インスタンスとしてパッケージ化されています。この VPX AMI インスタンスには 2 つ以上の仮想 CPU と 2GB 以上のメモリが必要です。また、AWS VPC 内で起動される EC2 インスタンスは、複数のインターフェイス、インターフェイスごとに複数の IP アドレス、VPX 構成に必要なパブリックおよびプライベート IP アドレスも提供できます。現在、AWS では、各 VPX インスタンスには少なくとも 3 つの IP アドレスが必要であるため、VPX は VPC 内でのみ起動できます。（AWS の VPX は 1 つまたは 2 つのエラスティックなネットワークインターフェイスを使用して実装することもできますが、標準的な AWS の VPX では 3 つのネットワークインターフェイスを使用することをお勧めします）。AWS では現在、AWS VPC 内で実行しているインスタンスについてのみ複数の IP を使用する機能をサポートしています。VPC 内の VPX インスタンスを使用して、EC2 インスタンスで実行しているサーバーの負荷を分散できます。

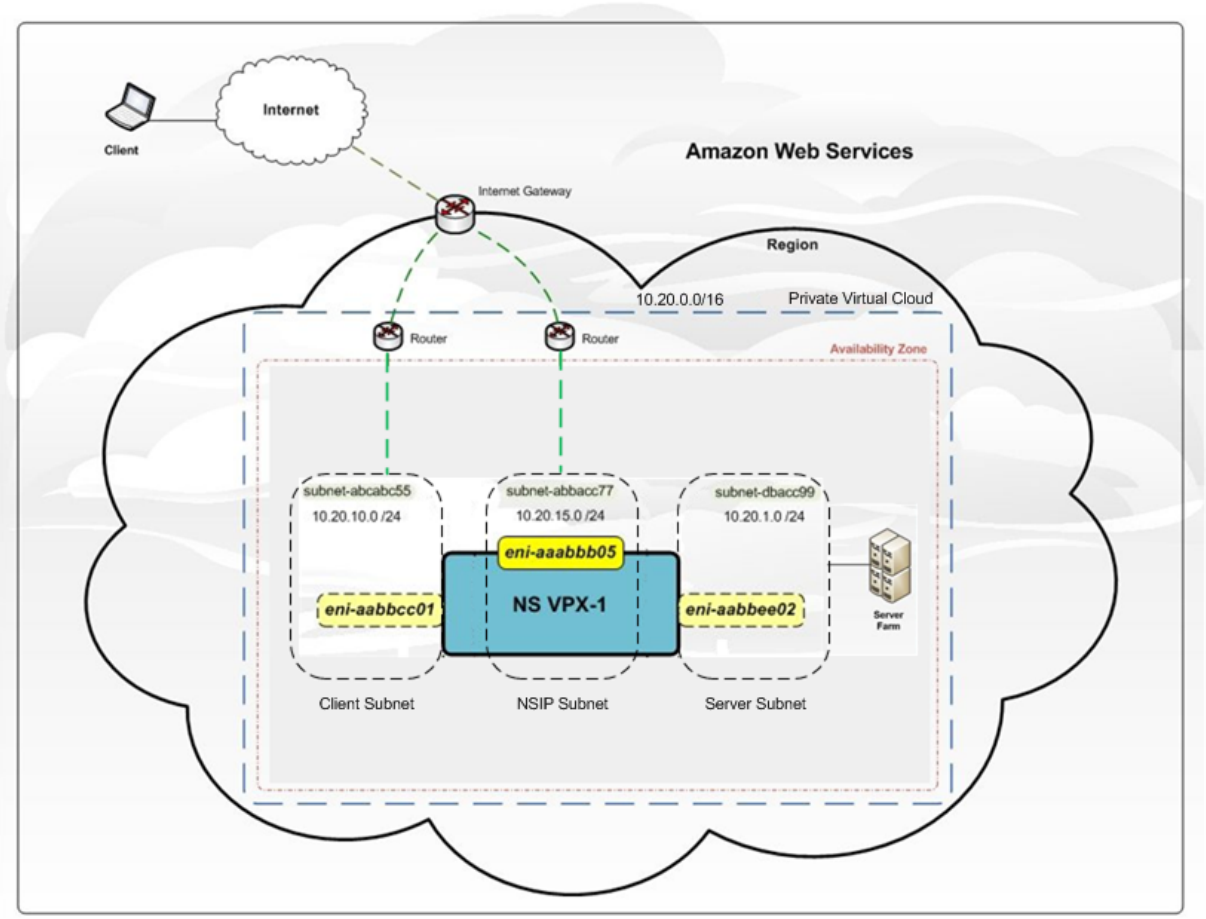
Amazon VPC を使用すれば、独自の IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどを含めて、仮想ネットワーク環境を作成および管理できます。

> 注:
>
> デフォルトでは、各 AWS アカウントの AWS リージョンごとに最大 5 つの VPC インスタンスを作成できます。Amazon のリクエストフォームを送信することで、より高い VPC 制限をリクエストできます。

Citrix Networking VPX（AMI イメージ）の EC2 インスタンスは、AWS VPC 内で起動されます。

次の図は、AWS での一般的な VPX の展開を示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



この図は、Citrix Networking VPX 展開を使用した AWS VPC のシンプルなトポロジを示しています。AWS VPC は、以下の要素で構成されています。

1. VPC からの送受信トラフィックをルーティングするための単一のインターネットゲートウェイ。
2. インターネットゲートウェイとインターネット間のネットワーク接続。
3. 3 つのサブネット（管理、クライアント、サーバー用に 1 つずつ）。
4. インターネットゲートウェイと 2 つのサブネット（管理用とクライアント用）間のネットワーク接続。
5. VPC 内に展開された単一の Citrix Networking VPX。VPX インスタンスには、各サブネットに 1 つずつ接続された ENI（Elastic Network Interface：エラスティックネットワークインターフェイス）が 3 つあります。

制限事項と使用上のガイドライン

- クラスタリング機能は、VPX ではサポートされていません。
- 高可用性機能を正しく使用するには、管理インターフェイスに専用の NAT デバイスを関連付けるか、EIP を NSIP に関連付けてください。NAT について詳しくは、「NAT インスタンス AWS ドキュメント」を参照してください。
- 異なるサブネットに属する ENI を使用して、データトラフィックと管理トラフィックを分離する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- 管理 ENI には、NSIP アドレスだけを設定する必要があります。
- セキュリティ上の理由により、EIP を NSIP に関連付ける代わりに NAT インスタンスを使用する場合は、VPC レベルでルーティングを適切に変更する必要があります。VPC レベルのルーティングの変更手順については、AWS ドキュメントの「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC」を参照してください。
- VPX インスタンスは、ある EC2 インスタンスタイプから別のインスタンスタイプへ（たとえば、m3.large から m3.xlarge へ）移動できます。
- AWS での VPX のストレージには、永続的でインスタンスから切断した後もデータにアクセス可能な EBS をお勧めします。
- VPX への ENI の動的追加はサポートされていません。更新を適用するには、VPX インスタンスを再起動する必要があります。スタンドアロンインスタンスまたは HA インスタンスを停止し、新しい ENI を接続してからインスタンスを再起動することをお勧めします。
- 1 つの ENI に複数の IP アドレスを割り当てることができます。ENI ごとの IP アドレスの最大数は、EC2 インスタンスの種類によって異なります。「EC2 でサポートされる ENI 数と IP アドレス数」を参照してください。
- Citrix Networking VPX インターフェイスでは、インターフェイスの有効化および無効化コマンドは使用しないことをお勧めします。

AWS の制限により、次の機能はサポートされていません。

レイヤ 3 の制限事項:

- 動的ルーティング
- IPV6

レイヤ 2 の制限事項:

- GARP（Gratuitous ARP）
- L2 モード
- タグ付き VLAN
- 仮想 MAC（VMAC）

サポートされる **EC2** インスタンス

Citrix ADC AMI は、次のいずれかの EC2 インスタンスタイプで起動できます。

- m4.large
- m4.xlarge
- m4.2xlarge
- m4.4xlarge
- m4.10xlarge
- m3.large
- m3.xlarge
- m3.2xlarge

© 1999–2021 Citrix Systems, Inc. All rights reserved.

詳しくは、「Amazon EC2 EC2 インスタンス」を参照してください。

ENI サポート

次の表は、EC2 インスタンスのタイプとサポートされる ENI 数、および ENI ごとのプライベート IP アドレス数の一覧です。

Instance Name - インスタンス名	ENI 数	ENI ごとのプライベート IP アドレス数
m4.large	2	10
m4.xlarge	4	15
m4.2xlarge	4	15
m4.4xlarge	8	30
m4.10xlarge	8	30
m3.large	3	10
m3.xlarge	4	15
m3.2xlarge	4	30

使用例

各サービスを個別の仮想アプライアンスとして展開する必要がある代替ソリューションと比較して、Citrix ADC on AWS は、L4 負荷分散、L7 トラフィック管理、サーバーオフロード、アプリケーションアクセラレーション、アプリケーションセキュリティ、およびその他の重要なアプリケーション配信機能を単一の VPX に統合します。インスタンスを作成し、AWS Marketplace から便利に利用できます。さらに、すべてが単一のポリシーフレームワークによって管理され、オンプレミスの Citrix ADC 展開を管理するのと同じ強力なツールセットで管理されます。その結果、AWS の Citrix ADC では、今日の企業の即時のニーズだけでなく、レガシーコンピューティングインフラストラクチャからエンタープライズクラウドデータセンターへの継続的な進化をサポートする魅力的なユースケースがいくつか可能になります。

Web アプリケーションおよび Virtual Apps およびデスクトップアプリケーション向けの本番配信

AWS をサービスとしてのインフラストラクチャ（IaaS）サービスとして積極的に採用している企業は、世界最大のウェブサイトやクラウドサービスプロバイダーが使用しているのと同じクラウドネットワーキングプラットフォームで、これらのアプリケーションをフロントエンドできるようになりました。広範なオフロード、アクセラレーション、セキュリティ機能を活用して、パフォーマンスを向上させ、コストを削減できます。

XenDesktop 7.5 および XenApp 7.5 は、あらゆる Windows アプリケーションまたはデスクトップを、あらゆるネットワークを経由してあらゆるデバイスに配信するクラウドサービスとして再設計されました。この拡張されたア

© 1999–2021 Citrix Systems, Inc. All rights reserved.

プリおよびデスクトップ配信プラットフォームを今すぐ展開することで、仮想インフラストラクチャまたはクラウド管理プラットフォームを活用できます。これにより、クラウドコンピューティングの自動化機能とオーケストレーション機能を活用できます。

ハイブリッドクラウド設計

ハイブリッドクラウド戦略に従っているエンタープライズ IT 組織は、プライベートクラウドに最も適したアプリケーションと使用シナリオを選択し、パブリッククラウドに最も適したアプリケーション、および最新のワークプレイスの要求を満たすために柔軟性、成長、および変革を実現することで、両方の世界を最大限に活用できます。

Citrix ADC on AWS を使用すると、エンタープライズデータセンターにまたがり、AWS に拡張されるハイブリッドクラウドは、同じクラウドネットワーキングプラットフォームの恩恵を受けることができます。Citrix ADC は、プライベートデータセンターと AWS 間のアプリケーションとワークロードの移行を大幅に容易にします。DataStream によるインテリジェントなデータベース負荷分散から、AppFlow® による前例のないアプリケーションの可視化、Action Analytics によるリアルタイムの監視と応答に至るまで、すべての機能を、Citrix ADC on AWS で活用できます。

ビジネス継続性

災害復旧およびビジネス継続性計画の一環として AWS を使用することを検討している企業は、オンプレミスと AWS の両方で実行されている Citrix ADC グローバルサーバー負荷分散を利用して、エンタープライズデータセンターと AWS 環境の両方の可用性とパフォーマンスを継続的に監視し、ユーザーを保証できます。は常に最適な場所に送信されます。

Citrix ADC アプライアンスで GSLB を構成し、メトリック交換プロトコル（MEP）を有効にすると、アプライアンスは DNS インフラストラクチャを使用して、設定した基準に最適なデータセンターにクライアントを接続します。この基準では、負荷が最も低いデータセンター、最も近いデータセンター、クライアントのロケーションからの要求に最も迅速に応答するデータセンター、それらのメトリックの組み合わせ、および SNMP メトリックを指定できます。アプライアンスは、各データセンターの場所、パフォーマンス、負荷、可用性を追跡し、これらの要因を使用して、クライアント要求の送信先となるデータセンターを選択します。GSLB 構成は、構成内の各アプライアンス上の GSLB エンティティのグループで構成されます。これらのエンティティには、GSLB サイト、GSLB サービス、GSLB 仮想サーバー、ロードバランシングおよび/またはコンテンツスイッチングサーバー、および ADNS サービスが含まれます。

開発とテスト

企業はオンプレミスで本番配信を実行しますが、AWS を開発およびテストに使用することで、AWS テスト環境に Citrix ADC を含めることができるようになりました。これにより、テスト環境内での本番実装の模倣が改善されるため、本番稼働までの時間が短縮されます。

各ユースケースにおいて、ネットワークアーキテクトは、スタンドアロンインスタンスとして、または Citrix ADC プラチナエディションインスタンスの機能として構成された Citrix CloudBridge を活用して、1 つ以上のエンタープ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ライズデータセンターと AWS クラウド間の接続を安全かつ最適化し、データ転送速度を向上させます/同期とネットワークコストの最小化。

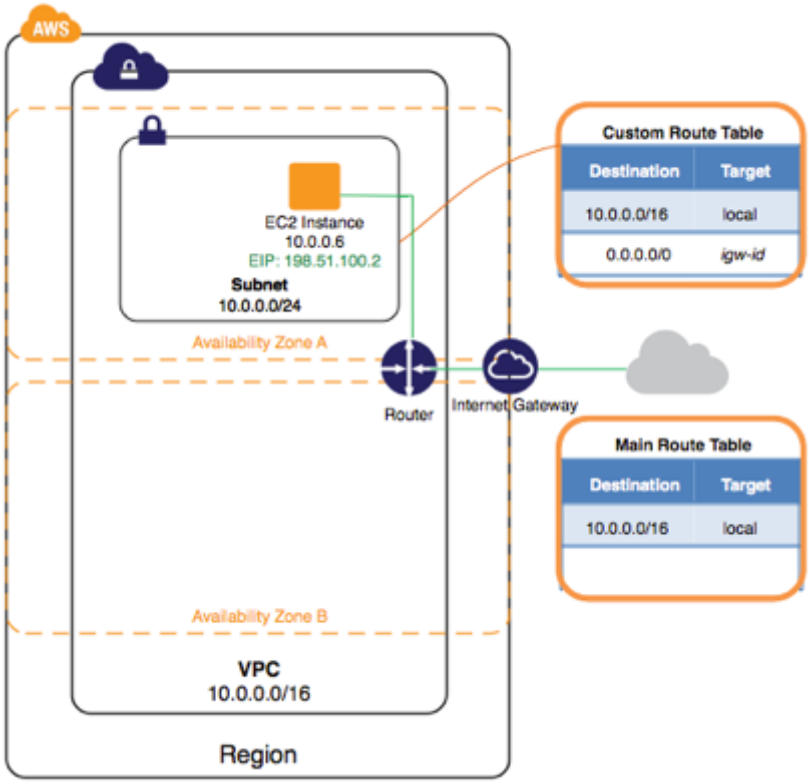
AWS ネットワークアーキテクチャ — ENI および EIP

VPC 内に起動された Citrix ADC インスタンスは、最大 8 つの伸縮自在なネットワークインターフェイス（ENI）を持つことができます。次に、各 ENI に 1 つ以上のプライベート IP アドレスを割り当てることができます。これらの各プライベート IP アドレスは、オプションでパブリックにルーティング可能な Elastic IP アドレスにマッピングされます。

この場合、ネットワークインターフェイスと IP アドレスが「弾力的」になるのは、プログラムによって他のインスタンスに再マッピングできることです。これは、ハードウェアの交換を待たずに、インスタンスまたはアベイラビリティーゾーンの障害から復旧できる機能です。また、DNS の変更があなたの顧客。

その他の詳細は以下のとおりです。

- インスタンスは、異なるサブネットで異なる ENI を持つことができます（ただし、異なるアベイラビリティーゾーンにはありません）。
- 各 ENI には少なくとも 1 つの IP アドレスが割り当てられており、セキュリティグループに割り当てる必要があります（下記参照）。
- 各サブネットのアドレス 1 ～4 (10.x.x.1-4) は、Amazon で使用するために予約されています。
- Citrix ADC は、プライベート IP アドレスしか認識しません。割り当てられた EIP は、Citrix ADC CLI または関連する管理ツールには表示されません。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

EC2 と **VPC** の比較

AWS には、Amazon Simple Storage Services（S3）、Amazon Elastic Compute Cloud（EC2）、Amazon Virtual Private Cloud（VPC）など、複数の異なるサービスが含まれています。この場合、後者の 2 つの区別が重要です。特に EC2 では、仮想マシンインスタンスは 1 つのネットワーキングインターフェイスと 1 つの IP アドレスに制限されます。さらに、最小限のネットワーク機能とコントロールがあります。これにより、Citrix ADC に EC2 を使用することができず、少なくとも 3 つの IP アドレスを必要とします。そのため、Citrix ADC インスタンスは AWS VPC 内でのみ起動できます。

VPC は、複数のインターフェイスと複数のプライベート IP アドレスとパブリック IP アドレスを持つ仮想マシンをサポートするだけでなく、独自の IP アドレス範囲、サブネット、ルーティングテーブル、およびネットワークゲートウェイを使用して、分離された仮想ネットワーク環境を作成および制御することもできます。

リージョンとアベイラビリティーゾーン

AWS クラウド内では、リージョンは米国東部などの特定の地理的な場所を参照します。各リージョンには少なくとも 2 つのアベイラビリティーゾーンがあります。それぞれのアベイラビリティーゾーンは、他のアベイラビリティーゾーンでの障害から隔離され、同じリージョンの他のアベイラビリティーゾーンに低コストで低遅延のネットワーク接続を提供するように設計された独立したクラウドデータセンターと考えることができます。

インスタンスを別々のアベイラビリティーゾーンに実装することで、1 つの場所に影響する障害からアプリケーションを保護できます。

ネットワークアーキテクトがこのレベルで認識すべき制限と依存関係には、次のものがあります。

- 仮想プライベートクラウドは複数のアベイラビリティーゾーンにまたがることができますが、複数のリージョンにまたがることはできません。
- VPC 内の個々のサブネットは、複数のアベイラビリティーゾーンにまたがることはできません。
- VPC に出入りするすべてのトラフィックは、対応するデフォルトのインターネット Gateway を介してルーティングされる必要があります。

AWS での **VPX** の設定

この演習では、VPC とサブネットを作成し、パブリック側のインスタンスをサブネットで起動します。インスタンスはインターネットと通信でき、SSH（Linux インスタンスの場合）またはリモートデスクトップ（Windows インスタンスの場合）を使用してローカルコンピュータからインスタンスにアクセスできます。実際の環境では、このシナリオを使用して、ブログをホストするなど、一般向け Web サーバーを作成できます。

> 注:
>
> この演習は、デフォルト以外の VPC をすばやくセットアップできるようにすることを目的としています。すでにデフォルト VPC があり、その中にインスタンスの起動を開始する場合（新しい VPC を作成または設定しな

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> い場合）は、「デフォルト VPC への EC2 インスタンスの起動」を参照してください。

この演習を完了するには、次の操作を行います。

- 単一のパブリックサブネットを持つデフォルト以外の VPC を作成します。サブネットを使用すると、セキュリティと運用上のニーズに基づいてインスタンスをグループ化できます。パブリックサブネットは、インターネット Gateway を介してインターネットにアクセスできるサブネットです。
- 特定のポートのみを通過するトラフィックを許可するインスタンスのセキュリティグループを作成します。
- サブネット内で Amazon EC2 インスタンスを起動します。
- Elastic IP アドレスをインスタンスに関連付けます。これにより、インスタンスはインターネットにアクセスできるようになります。

初めて Amazon VPC を使用する前に、AWS にサインアップする必要があります。サインアップすると、AWS アカウントは、Amazon VPC を含む AWS のすべてのサービスに自動的にサインアップされます。AWS アカウントをまだ作成していない場合は、http://aws.amazon.comに進み、[無料アカウントを作成] を選択します。

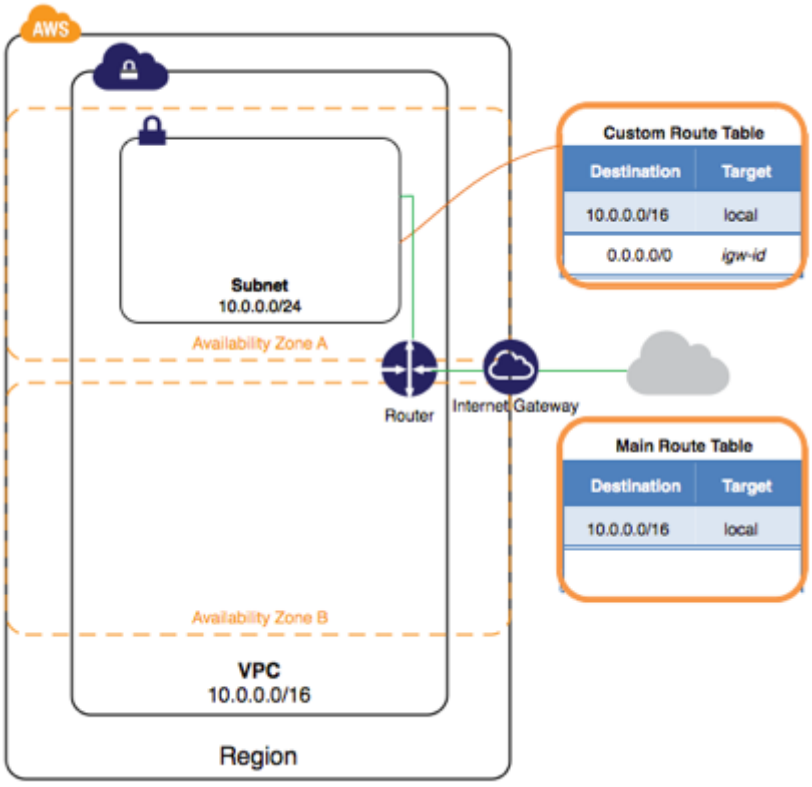
手順 **1: VPC** を作成する

このステップでは、Amazon VPC コンソールで Amazon VPC ウィザードを使用して VPC を作成します。ウィザードでは、次の手順が実行されます。

- /16 CIDR ブロック（65,536 個のプライベート IP アドレスを持つネットワーク）を持つ VPC を作成します。CIDR 表記と VPC のサイズ設定について詳しくは、「VPC」を参照してください。
- インターネット Gateway を VPC にアタッチします。インターネットゲートウェイについて詳しくは、「インターネットゲートウェイ」を参照してください。
- VPC 内にサイズ /24 のサブネット（256 のプライベート IP アドレスの範囲）を作成します。
- カスタムルートテーブルを作成し、サブネットに関連付けて、サブネットとインターネット Gateway の間でトラフィックが流れるようにします。ルートテーブルについて詳しくは、「ルートテーブル」を参照してください。

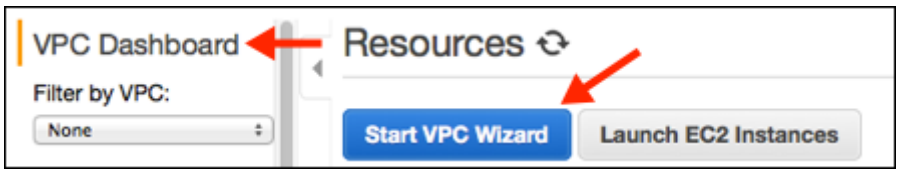
次の図は、この手順を完了した後の VPC のアーキテクチャを示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



Amazon VPC ウィザードを使用して **VPC** を作成する

1. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。
2. 右上のナビゲーションバーで、VPC を作成するリージョンをメモします。別のリージョンから VPC にインスタンスを起動することはできないため、この演習の残りの部分でも同じリージョンで作業を継続してください。リージョンについて詳しくは、「リージョンとアベイラビリティーゾーン」を参照してください。
3. ナビゲーションペインで、[**VPC Dashboard**] を選択し、**[VPC** ウィザードの開始**]** を選択します。



> 注:
>
> ナビゲーションペインで [Your VPC] を選択しないでください。このページから VPC ウィザードにアクセスすることはできません。

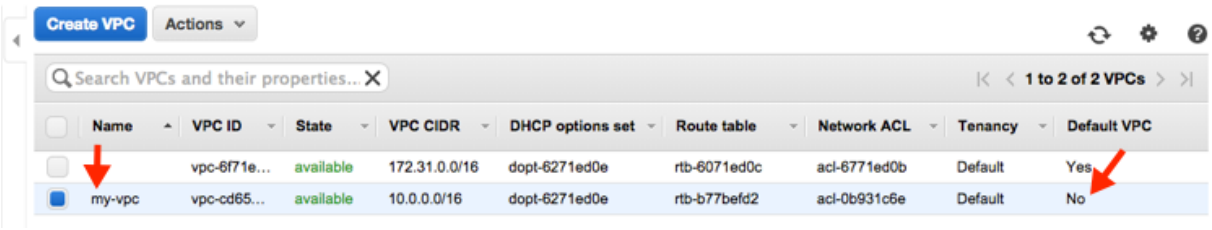
4. 最初のオプション、[単一のパブリックサブネットを持つ **VPC**] を選択し、**[Select]** を選択します。
5. 設定ページで、[VPC name] フィールドに VPC の名前（my-vpc など）を入力し、[**Subnet** name] フィールドにサブネットの名前を入力します。これにより、作成後に Amazon VPC コンソールで VPC とサブネットを識別できます。この演習では、ページの残りの設定はそのままにして、**[Create VPC]** を選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

（オプション）必要に応じて、次のように設定を変更し、**[Create VPC]** を選択します。

- IP CIDR ブロックには、VPC に使用する IP アドレス範囲（10.0.0.0/16）が表示され、[Public subnet] フィールドにはサブネットに使用する IP アドレス範囲（10.0.0.0/24）が表示されます。デフォルトの CIDR 範囲を使用しない場合は、独自の CIDR 範囲を指定できます。詳しくは、「VPC とサブネットのサイズ設定」を参照してください。
- [Availability Zone] リストでは、サブネットを作成するアベイラビリティーゾーンを選択できます。[No Preference] のままにしておくと、アベイラビリティーゾーンが AWS によって選択されます。詳しくは、「リージョンとアベイラビリティーゾーン」を参照してください。
- [S3 のエンドポイントをサブネットに追加する] セクションで、同じリージョンの Amazon S3 に VPC エンドポイントを作成するサブネットを選択できます。詳しくは、「VPC エンドポイント」を参照してください。
- `Enable DNS hostnames`オプションを [Yes] に設定すると、VPC 内で起動されるインスタンスが DNS ホスト名を受け取ります。詳しくは、「VPC での DNS の使用」を参照してください。
- [Hardware tenancy] オプションでは、VPC 内で起動されるインスタンスを共有ハードウェアで実行するか、専用ハードウェアで実行するかを選択できます。専用テナンシーを選択すると、追加コストが発生します。ハードウェアテナンシーについて詳しくは、「ハードウェア専有インスタンス」を参照してください。

6. ステータスウィンドウには、進行中の作業が表示されます。作業が完了したら、「**OK**」を選択してステータスウィンドウを閉じます。
7. `Your VPCs page`に、デフォルトの VPC と先ほど作成した VPC が表示されます。作成した VPC はデフォルト以外の VPC であるため、**[Default VPC]** 列には [No] と表示されます。



VPC に関する情報を表示する

VPC を作成したら、サブネット、インターネット Gateway、ルートテーブルに関する情報を表示できます。作成した VPC には 2 つのルートテーブルがあります。1 つはすべての VPC がデフォルトで持つメインルートテーブルと、ウィザードによって作成されたカスタムルートテーブルです。カスタムルートテーブルはサブネットに関連付けられています。つまり、そのテーブルのルートによって、サブネットのトラフィックがどのように流れるかが決まります。VPC に新しいサブネットを追加すると、デフォルトでメインルートテーブルが使用されます。

VPC に関する情報を表示するには

1. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

2. ナビゲーションペインで、[**Your VPC**] を選択します。作成した VPC の名前と ID を書き留めます（[Name] 列と [VPC ID] 列を確認します）。この情報を使用して、VPC に関連付けられているコンポーネントを特定します。
3. ナビゲーションペインで、[**Subnets**] を選択します。コンソールには、VPC の作成時に作成されたサブネットが表示されます。[**Name]** 列でサブネットの名前で識別することも、前の手順で取得した VPC 情報を使用して [VPC] 列を調べることもできます。
4. ナビゲーションペインで、[インターネットゲートウェイ] を選択します。VPC にアタッチされているインターネット Gateway を確認するには、VPC 列を確認します。この列には、VPC の ID と名前（該当する場合）が表示されます。
5. ナビゲーションペインで、[**Route Tables**] を選択します。VPC には 2 つのルートテーブルが関連付けられています。カスタムルートテーブルを選択し ([Main] 列に [No] と表示される)、[Routes] タブを選択して、詳細ペインにルート情報を表示します。
    - テーブルの最初の行はローカルルートで、VPC 内のインスタンスが通信できるようにします。このルートはデフォルトですべてのルートテーブルに存在し、削除することはできません。
    - 2 行目は、VPC 外の IP アドレス（0.0.0.0/0）宛てのトラフィックがサブネットからインターネット Gateway に流れるように、Amazon VPC ウィザードが追加したルートを示しています。
6. メインルートテーブルを選択します。メインルートテーブルにはローカルルートがありますが、他のルートはありません。

手順 **2:** セキュリティグループ **12** を作成する

セキュリティグループは、関連付けられたインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。セキュリティグループを使用するには、インスタンスへの着信トラフィックを制御するインバウンドルールを追加し、インスタンスからの送信トラフィックを制御するアウトバウンドルールを追加します。セキュリティグループをインスタンスに関連付けるには、インスタンスの起動時にセキュリティグループを指定します。セキュリティグループに対してルールを追加または削除すると、セキュリティグループに関連付けられたインスタンスにそれらの変更が自動的に適用されます。

VPC にはデフォルトのセキュリティグループが付属しています。起動時に別のセキュリティグループに関連付けられていないインスタンスは、デフォルトのセキュリティグループに関連付けられます。この演習では、新しいセキュリティグループ WebServerSG を作成し、VPC でインスタンスを起動するときにこのセキュリティグループを指定します。

トピック

- WebServerSG セキュリティグループの作成
- WebServerSG セキュリティグループのルール

WebServerSG セキュリティグループの作成

Amazon VPC コンソールを使用してセキュリティグループを作成できます。

WebServerSG セキュリティグループのルール

© 1999–2021 Citrix Systems, Inc. All rights reserved.

次の表では、WebServerSG セキュリティグループのインバウンドルールとアウトバウンドルールについて説明します。インバウンドルールは自分で追加します。アウトバウンドルールは、すべてのアウトバウンド通信を許可するデフォルトのルールです。このルールを自分で追加する必要はありません。

受信			
接続元 IP	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	どこからでもインバウンド HTTP アクセスを許可します。
0.0.0.0/0	TCP	443	どこからでもインバウンド HTTPS アクセスを許可します。
ホームネットワークのパブリック IP アドレス範囲	TCP	22	ホームネットワークから Linux/UNIX インスタンスへのインバウンド SSH アクセスを許可します。
ホームネットワークのパブリック IP アドレス範囲	TCP	3389	ホームネットワークから Windows インスタンスへのインバウンド RDP アクセスを許可します。

送信			
接続先 IP	プロトコル	ポート範囲	コメント
0.0.0.0/0	すべて	すべて	すべてのアウトバウンド通信を許可するデフォルトのアウトバウンドルール。

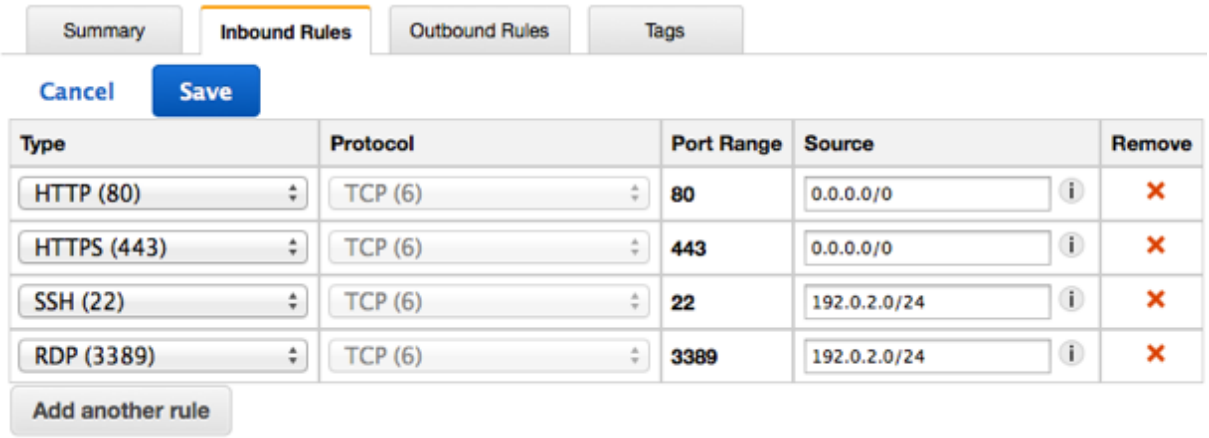
WebServerSG セキュリティグループを作成してルールを追加するには

1. https://aws.amazon.com/console/で Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[**Security Groups**] を選択します。
3. [セキュリティグループの作成] を選択します。
4. [グループ名] フィールドに、セキュリティグループの名前として WebServerSG と入力し、説明を入力します。オプションで [Name tag] フィールドを使用して、Name のキーと指定した値を持つセキュリティグループのタグを作成できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

5. [VPC] メニューから **VPC** の **ID** を選択し、[**Yes, Create**] を選択します。
6. 先ほど作成した **WebServerSG** セキュリティグループを選択します（「グループ名」列でその名前を表示できます）。
7. [**Inbound Rules**] タブで、[**Edit**] を選択し、次のようにインバウンドトラフィックのルールを追加し、完了したら **[Save]** を選択します。
   - [タイプ] リストから [**HTTP**] を選択し、[ソース] フィールドに **0.0.0.0/0** と入力します。
   - [別のルールを追加] を選択し、[タイプ] リストから [**HTTPS**] を選択し、[ソース] フィールドに **0.0.0.0/0** と入力します。
   - [別のルールを追加**]** を選択します。Linux インスタンスを起動する場合は、[Type] リストから [**SSH**] を選択します。Windows インスタンスを起動する場合は、[Type] リストから [**RDP**] を選択します。[**Source**] フィールドに、ネットワークのパブリック IP アドレスの範囲を入力します。このアドレス範囲がわからない場合は、この演習で 0.0.0.0/0 を使用できます。

> 注意：
>
> 0.0.0.0/0 を使用する場合は、すべての IP アドレスが SSH または RDP を使用してインスタンスにアクセスできるようにします。これは短い演習では許容されますが、実稼働環境では安全ではありません。本稼働環境では、特定の IP アドレスまたはアドレス範囲のみにインスタンスへのアクセスを許可します。

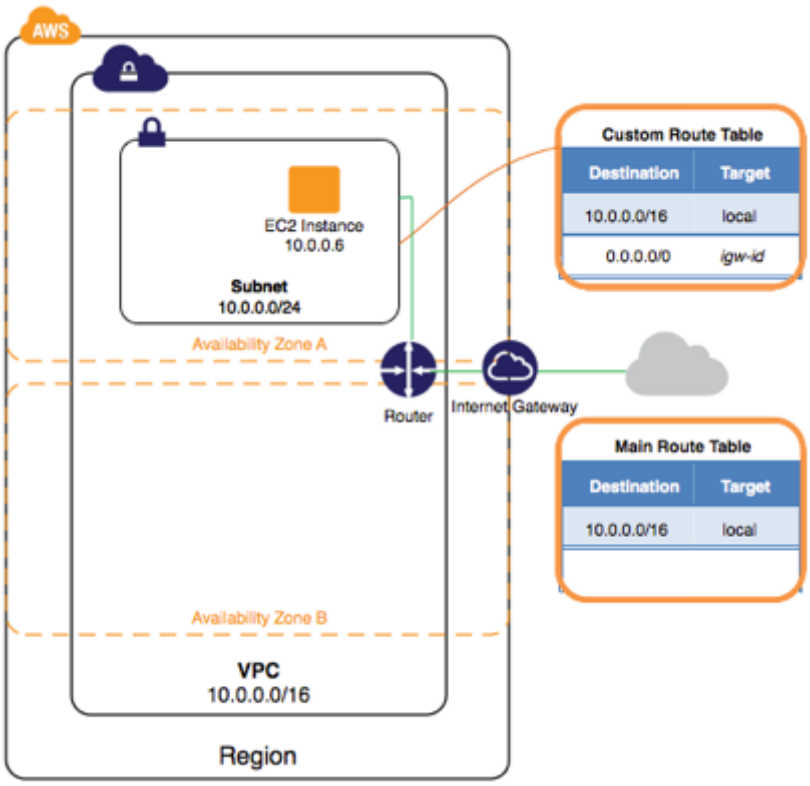


手順 **3: VPC 14** でインスタンスを起動する

VPC で EC2 インスタンスを起動するときは、インスタンスを起動するサブネットを指定する必要があります。この場合、作成した VPC のパブリックサブネットにインスタンスを起動します。Amazon EC2 コンソールの Amazon EC2 起動ウィザードを使用して、インスタンスを起動します。

次の図は、この手順を完了した後の VPC のアーキテクチャを示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



EC2 インスタンスを VPC 内に起動するには

1. Amazon EC2 EC2 コンソールを開きます。
2. 右上のナビゲーションバーで、VPC とセキュリティグループを作成したリージョンと同じリージョンが選択されていることを確認します。
3. ダッシュボードから、[**Launch Instance**] を選択します。
4. ウィザードの最初のページで、使用する AMI を選択します。この演習では、**Amazon Linux AMI** または **Windows AMI** を選択することをお勧めします。
5. [**Choose an Instance Type**] ページで、起動するインスタンスのハードウェア設定とサイズを選択できます。デフォルトでは、選択した AMI に基づいて、使用可能な最初のインスタンスタイプが選択されます。デフォルトの選択のままにして、[次へ**:** インスタンスの詳細を設定**]** を選択します。
6. [**Configure Instance Details**] ページで、[Network] リストから作成した **VPC** を選択し、[**Subnet**] リストからサブネットを選択します。残りのデフォルト設定のままにして、[Tag Instance] ページが表示されるまで、ウィザードの次のページに進みます。
7. [タグインスタンス] ページでは、インスタンスに Name タグをタグ付けできます。たとえば、Name=MyWebServer などです。これは、起動後に Amazon EC2 コンソールでインスタンスを識別するのに役立ちます。完了したら、[次へ**:** セキュリティグループの設定**]** を選択します。
8. [**Configure Security Group**] ページで、ウィザードによって launch-wizard-x セキュリティグループが自動的に定義され、インスタンスに接続できるようになります。代わりに、[既存のセキュリティグループの選択] オプションを選択し、以前に作成した WebServerSG グループを選択して、[確認と起動] を選択します。
9. [インスタンスの起動の確認] ページで、インスタンスの詳細を確認し、[**Launch**] を選択します。

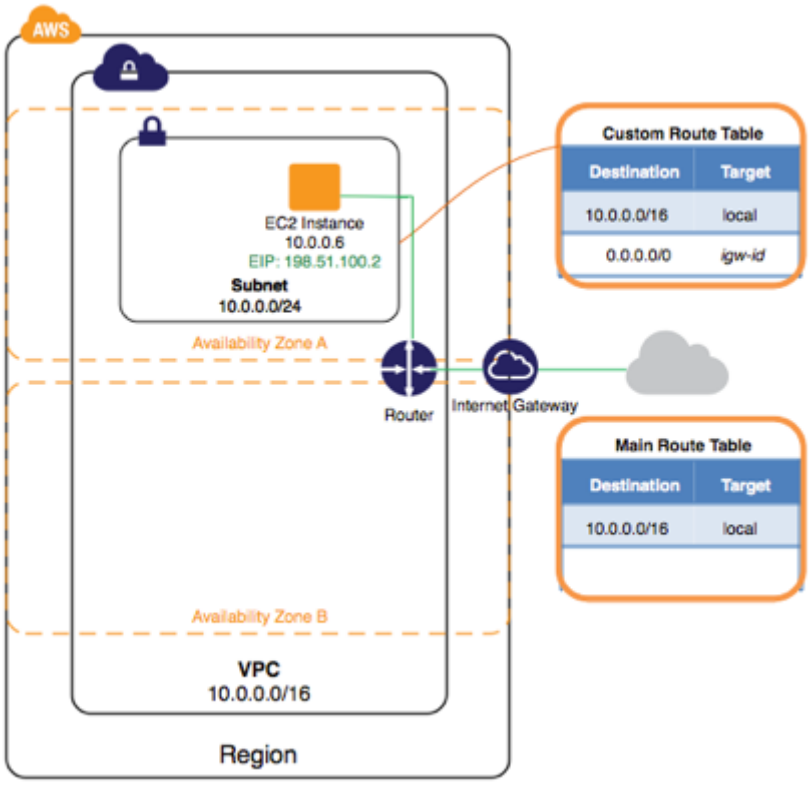
© 1999–2021 Citrix Systems, Inc. All rights reserved.

10. [**Select a existing key pair** または **create a new key pair**] ダイアログボックスで、既存のキーペアを選択するか、新しいキーペアを作成できます。新しいキーペアを作成する場合は、必ずファイルをダウンロードし、安全な場所に保存してください。プライベートキーの内容は、起動後にインスタンスに接続するために必要です。インスタンスを起動するには、確認のチェックボックスをオンにして、[**Launch Instances**] を選択します。
11. 確認ページで、**[View Instances]** を選択し、**[Instances]** ページでインスタンスを表示します。インスタンスを選択し、[**Description**] タブで詳細を表示します。[Private IP] フィールドには、サブネット内の IP アドレスの範囲からインスタンスに割り当てられたプライベート IP アドレスが表示されます。

手順 **4: Elastic IP** アドレスをインスタンスに割り当てる

前のステップでは、パブリックサブネット（インターネット Gateway へのルートを持つサブネット）にインスタンスを起動しました。ただし、サブネット内のインスタンスは、インターネットと通信できるようにパブリック IP アドレスも必要です。デフォルトでは、デフォルト以外の VPC のインスタンスにはパブリック IP アドレスが割り当てられません。このステップでは、Elastic IP アドレスをアカウントに割り当てて、それをインスタンスに関連付けます。Elastic IP アドレスについて詳しくは、「エラスティック IP アドレス」を参照してください。

次の図は、この手順を完了した後の VPC のアーキテクチャを示しています。



Elastic IP アドレスを割り当てて割り当てるには

1. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[**Elastic IP**] を選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

3. [新しいアドレスの割り当て]、[はい、割り当て] の順に選択します。

   > 注:
   >
   > アカウントが EC2-Classic をサポートしている場合は、まず [ネットワークプラットフォーム] リストから [**EC2-VPC**] を選択します。

4. リストから **Elastic IP** アドレスを選択し、**[**アクション**]**、**[**アドレスの関連付け**]** の順に選択します。
5. ダイアログボックスで、**[**関連付け**]** リストから **[**インスタンス**]** を選択し、**[**インスタンス**]** リストからインスタンスを選択します。完了したら、**[**はい、関連付け**]** を選択します。

これで、インスタンスはインターネットからアクセスできるようになります。SSH またはリモートデスクトップを使用して、Elastic IP アドレスを使用してインスタンスに接続できます。Linux インスタンスへの接続方法について詳しくは、Linux インスタンス用 Amazon EC2 ユーザーガイドの「Linux インスタンスへの接続」を参照してください。Windows インスタンスへの接続方法について詳しくは、Windows インスタンス用 Amazon EC2 ユーザーガイドの「RDP を使用して Windows インスタンスに接続する」を参照してください。

これで実習は完了です。VPC でインスタンスを引き続き使用するか、インスタンスが必要ない場合は、インスタンスを終了し、Elastic IP アドレスを解放して、料金が発生しないようにすることができます。VPC を削除することもできます。この演習で作成された VPC および VPC コンポーネント（サブネットやルートテーブルなど）に対しては課金されないことに注意してください。

Citrix Virtual Apps and Desktops の **Unified Gateway** を構成する

Citrix ADC の管理コンソールに移動します。

nsroot と AWS がビルドプロセス中に割り当てたインスタンス ID を使用して、Citrix ADC にログインします。

SSL 証明書のインストール:

1.「トラフィック管理**-SSL**」に移動します。右クリックして、この機能を有効にします。
2. SSL 証明書にキーペアをインポートします。

SSL 証明書のインストール:

1. Citrix Gateway を展開し、［仮想サーバー］を選択します。
2. ［追加］をクリックします。

   Citrix ADC ビルドプロセス中に割り当てたパブリックサブネットにある Gateway の名前と IP アドレスを入力します。

   > 注:
   >
   > 後で Elastic IP アドレスを割り当てるときに、この IP アドレスを必要に応じて書き留めます。

3. [**OK**] をクリックし、[サーバー証明書なし] をクリックして、先にインポートした証明書を選択します。［バインド］をクリックします。

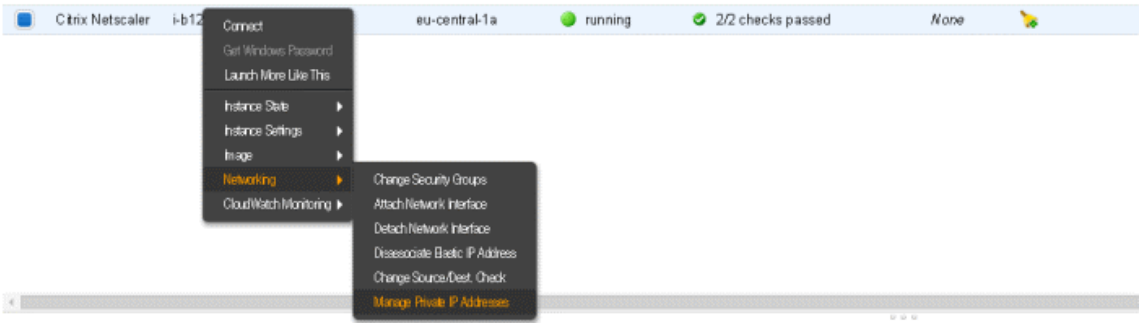
© 1999–2021 Citrix Systems, Inc. All rights reserved.

4. [**OK**] と [完了] をクリックすると、この段階で、Citrix Gateway が [Up] 状態になっているはずです。

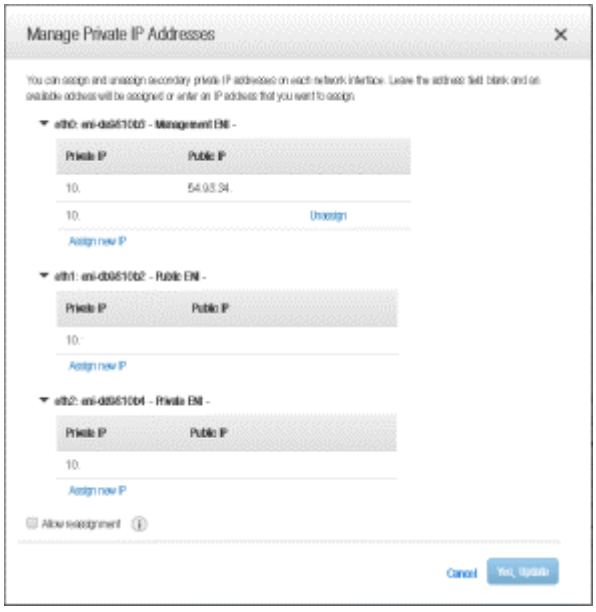
Unified Gateway を設定するには、https://support.citrix.com/article/CTX205485を参照してください。

Unified Gateway インスタンスへの外部アクセスを提供します。

1. aws.amazon.com の AWS ポータルにログインし、インスタンスに移動します。
2. Citrix ADC を右クリックし、[ネットワーク]、[プライベート **IP** アドレスの管理**]** の順に選択します。

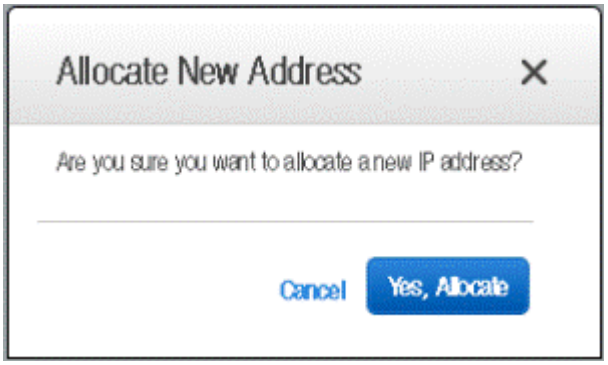


3. Citrix ADC Gateway を実行するインターフェイスで、［新しい **IP** の割り当て］をクリックします。
4. IP アドレスを割り当てます。必ず Citrix ADC Gateway に割り当てたアドレスと同じアドレスを使用してください。

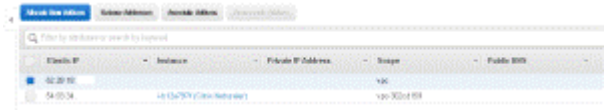


5. [はい**] [**更新**]** をクリックします。これにより、AWS レベルで新しい IP アドレスがインスタンスに割り当てられます。これで、このプライベート IP に新しい Elastic IP を割り当てることができます。
6. [ネットワークとセキュリティ] と [Elastic IP] に移動します。
7. プロンプトが表示されたら、[新しいアドレスの割り当て] をクリックします。新しい IP アドレスを取得するには [はい] を選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



8. リストからアドレスを選択し、[アドレスの関連付け] を選択します。



9.「インスタンスリスト」から、以前に構築した **Citrix ADC** インスタンスを選択します。これを選択すると、インスタンスに静的に割り当てた IP アドレス（Citrix Gateway と同じアドレス）を選択し、[**Associate**] を選択できるようになります。

10. DNS 名レコードに Amazon が割り当てた Elastic IP アドレスを指定します。
11. Citrix Gateway にログインします。

StoreFront 用の高可用性負荷分散

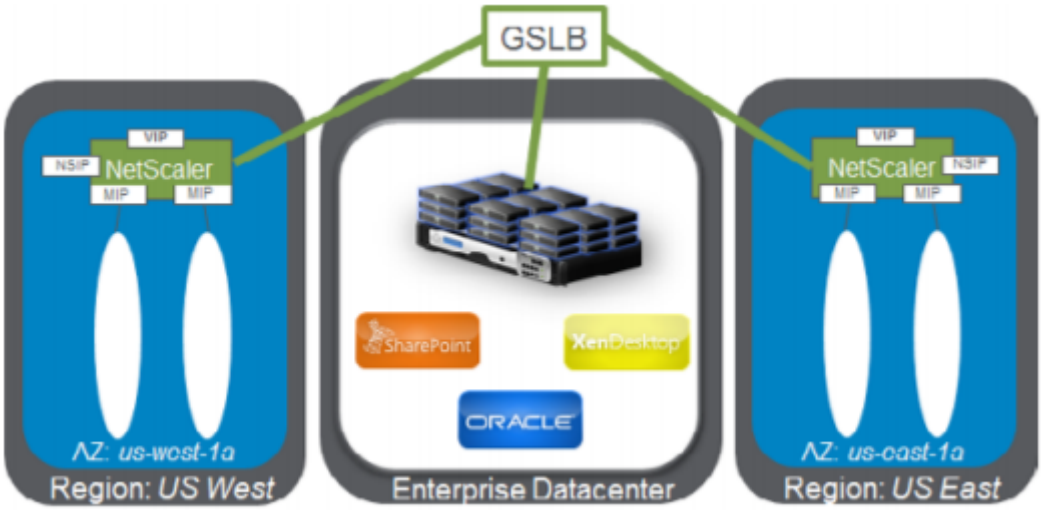
「Citrix 構成手順」を参照してください。

---

2 つの **AWS** ロケーションで **GSLB** を設定する

AWS 上の Citrix ADC 用 GSLB をセットアップするには、主に、Citrix ADC が属する VPC の外部にあるサーバー (たとえば、別のアベイラビリティーリージョンやオンプレミスのデータセンターなど) へのトラフィックを負荷分散するように Citrix ADC を設定します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



クラウドロードバランサーを使用したドメイン名ベースのサービス（**GSLB DBS**）

GSLB および **DBS** の概要

クラウドロードバランサー用の DBS（ドメインベースサービス）を使用した Citrix ADC GSLB のサポートにより、クラウドロードバランサーソリューションを使用した動的クラウドサービスの自動検出が可能になります。この構成により、Citrix ADC はアクティブ/アクティブ環境でグローバルサーバー負荷分散ドメイン名ベースのサービス（GSLB DBS）を実装できます。DBS を使用すると、AWS および Microsoft Azure 環境のバックエンドリソースを DNS 検出から拡張できます。

このセクションでは、AWS 環境と Azure Auto Scaling 環境における Citrix ADC 間の統合について説明します。ドキュメントの最後のセクションでは、AWS リージョンに固有の 2 つの異なるアベイラビリティーゾーン（AZ）にまたがる Citrix ADC の HA ペアをセットアップする機能について詳しく説明します。

前提条件

Citrix ADC GSLB サービスグループの前提条件には、セキュリティグループ、Linux ウェブサーバー、AWS 内の Citrix ADC、Elastic IP、およびエラスティックロードバランサーを設定するための知識と能力を備えた、機能する AWS/Microsoft Azure 環境が含まれます。

GSLB DBS サービスの統合には、AWS ELB および Microsoft Azure ALB ロードバランサーインスタンス用に、Citrix ADC バージョン 12.0.57 が必要です。

Citrix ADC GSLB サービスグループ機能の拡張

GSLB サービスグループエンティティ:Citrix ADC バージョン 12.0.57

© 1999–2021 Citrix Systems, Inc. All rights reserved.

BDS 動的検出を使用した自動スケーリングをサポートする GSLB サービスグループが導入されました。

DBS 機能コンポーネント（ドメインベースのサービス）は、GSLB サービスグループにバインドする必要があります

例:

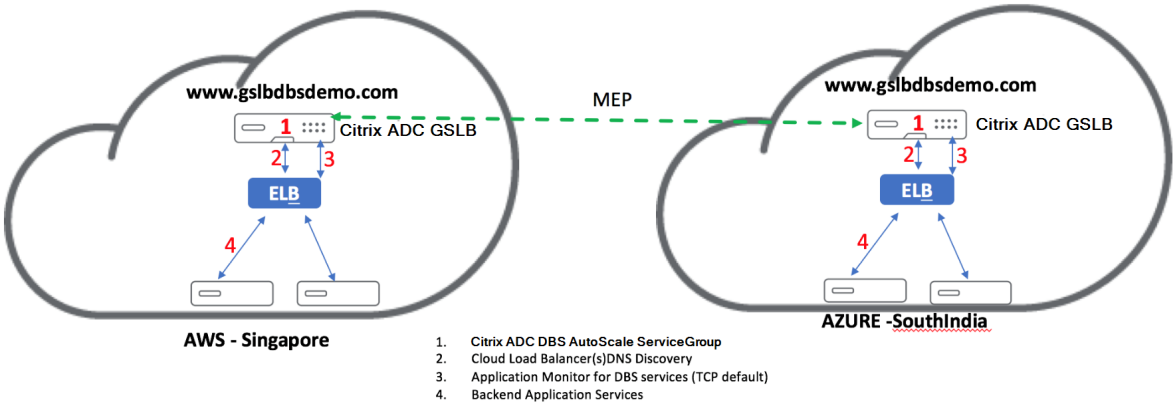
```
1 > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
    amazonaws.com
2 > add gslb serviceGroup sydney_sg HTTP -autoScale DNS -siteName sydney
3 > bind gslb serviceGroup sydney_sg sydney_server 80
4 <!--NeedCopy-->
```

ドメイン名ベースのサービス **— AWS ELB**

GLSB DBS は、Elastic Load Balancer の FQDN を使用して、AWS 内で作成および削除されるバックエンドサーバーを含めるように GSLB サービスグループを動的に更新します。AWS のバックエンドサーバーまたはインスタンスは、ネットワーク需要または CPU 使用率に基づいてスケーリングするように設定できます。この機能を設定するには、Citrix ADC を Elastic Load Balancer に指し、AWS 内でインスタンスが作成および削除されるたびに Citrix ADC を手動で更新することなく、AWS 内の異なるサーバーに動的にルーティングします。GSLB サービスグループ用の Citrix ADC DBS 機能は、DNS 認識サービス検出を使用して、AutoScaler グループで識別される DBS 名前空間のメンバーサービスリソースを決定します。

図:

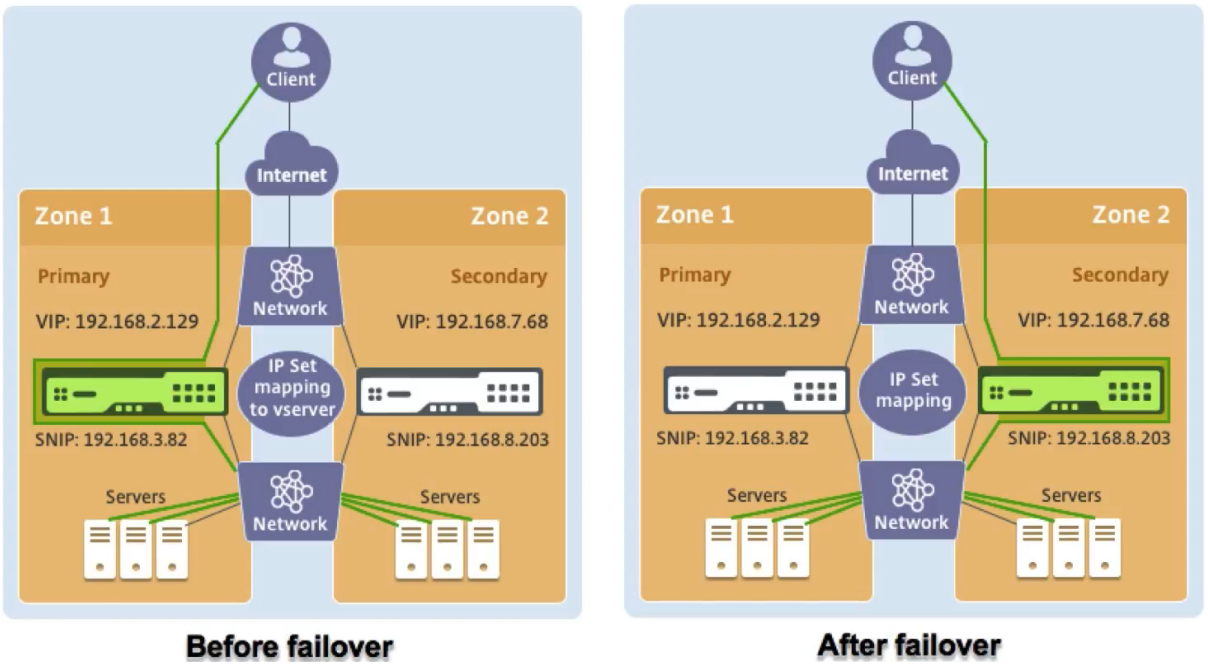
クラウドロードバランサーを使用した Citrix ADC GSLB DBA AutoScale コンポーネント



複数のアベイラビリティーゾーンで **AWS** で **Citrix ADC HA** を使用する

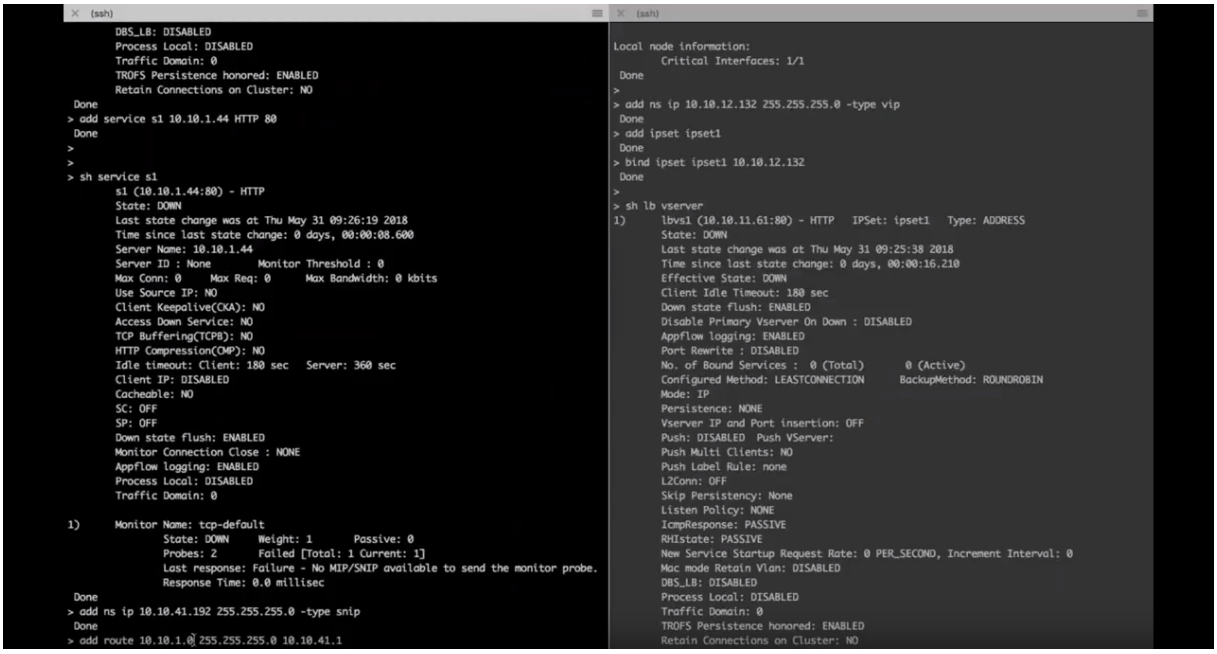
AWS で Citrix ADC をさまざまなアベイラビリティーゾーンに展開することは、Citrix ADC 12.1 用にリリースされた新機能です。これは、Citrix ADC をエラスティックネットワーク IP アドレス（ENI）に接続することによって行われます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



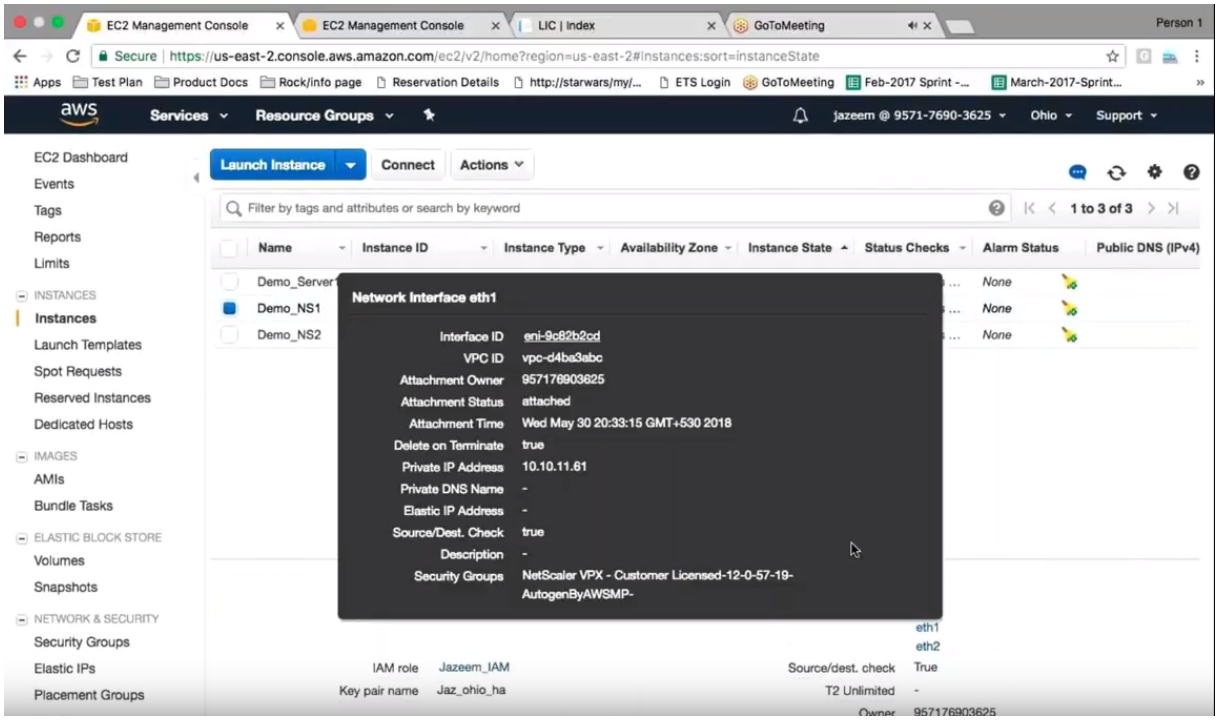
ソリューションの動作方法は、VPX 上の HA と独立したネットワーク構成を設定する必要があるため、他のソリューションとは若干異なります。このソリューションでは、仮想サーバの IP セット機能の新機能を使用して、フェイルオーバーを維持します。

まず、Citrix ADC にログインし、サーバー側のネットワークアドレス、クライアント側のアドレス、および両方へのルーティングを定義または立ち上げる必要があります。

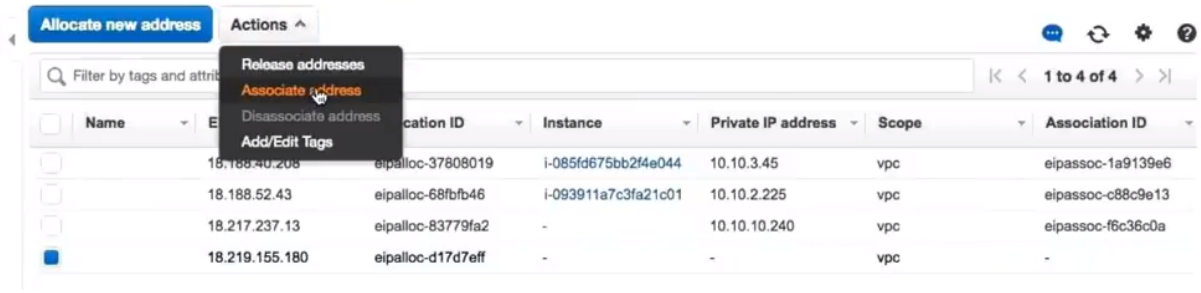


AWS コンソールでは、最初の VPX は伸縮自在な IP で設定されています。

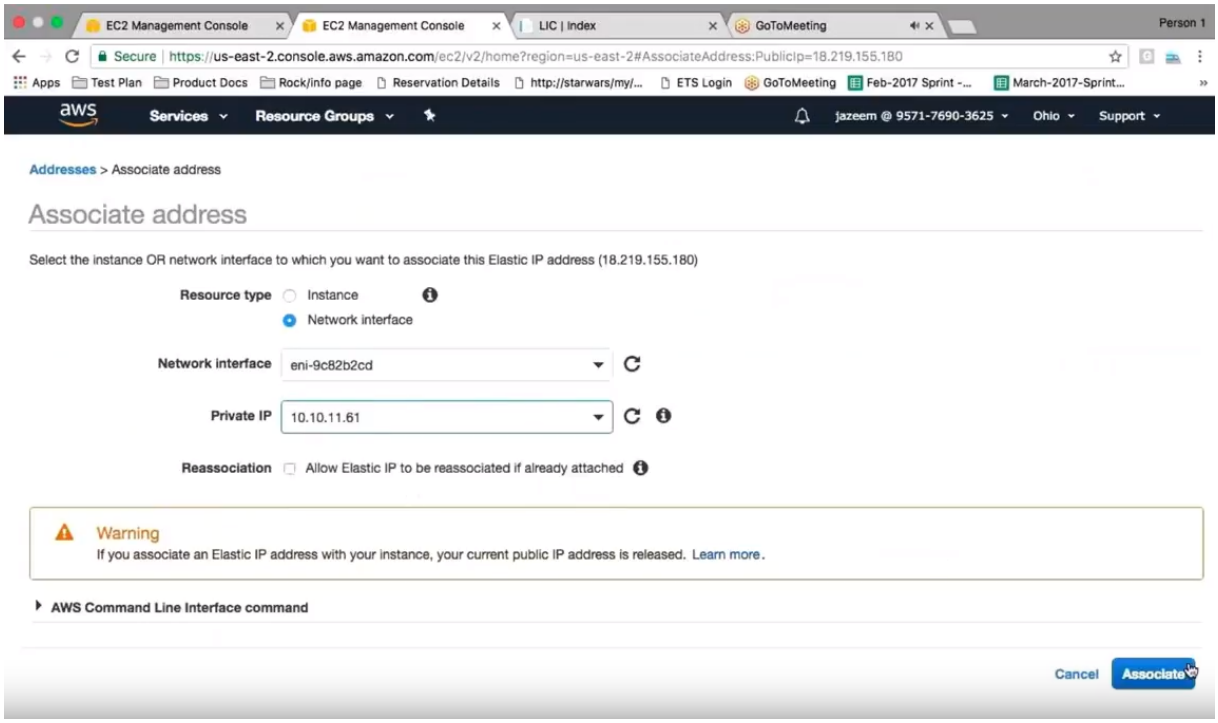
© 1999–2021 Citrix Systems, Inc. All rights reserved.



Elastic インターフェイスに入ると、ソリューションが機能する最初のことは、その Elastic IP をそのインターフェイス上の既存のプライベートアドレスに関連付けることです。



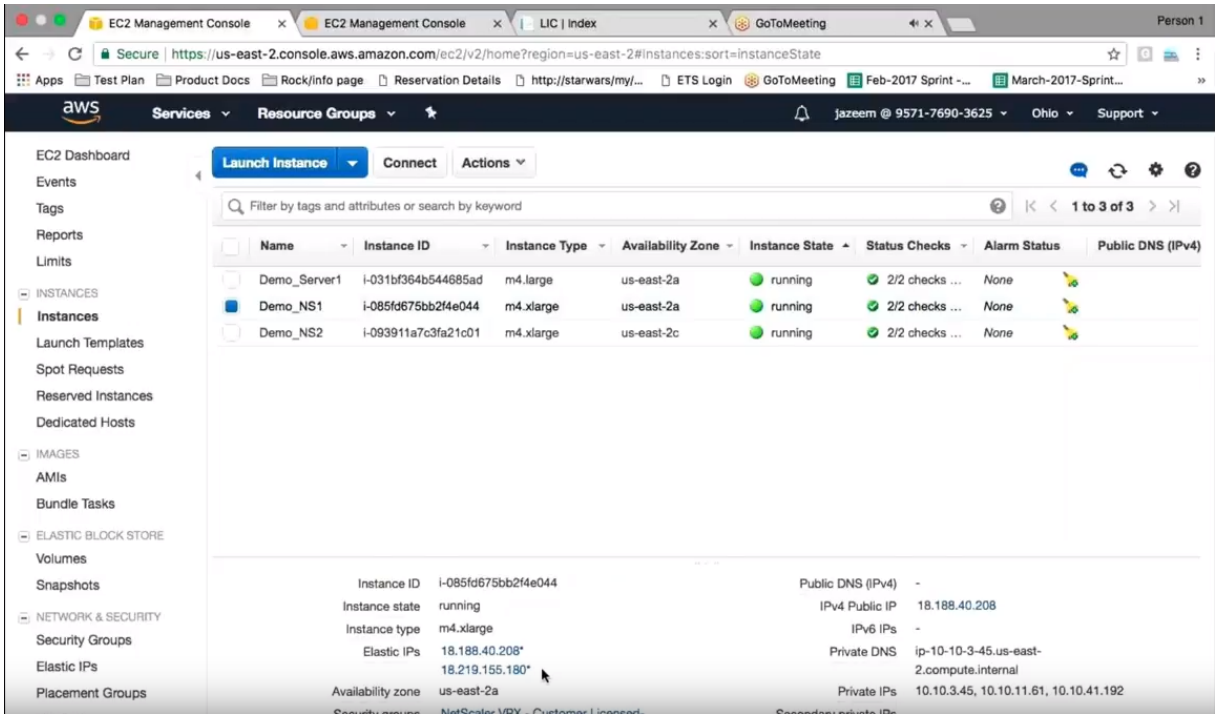
© 1999–2021 Citrix Systems, Inc. All rights reserved.



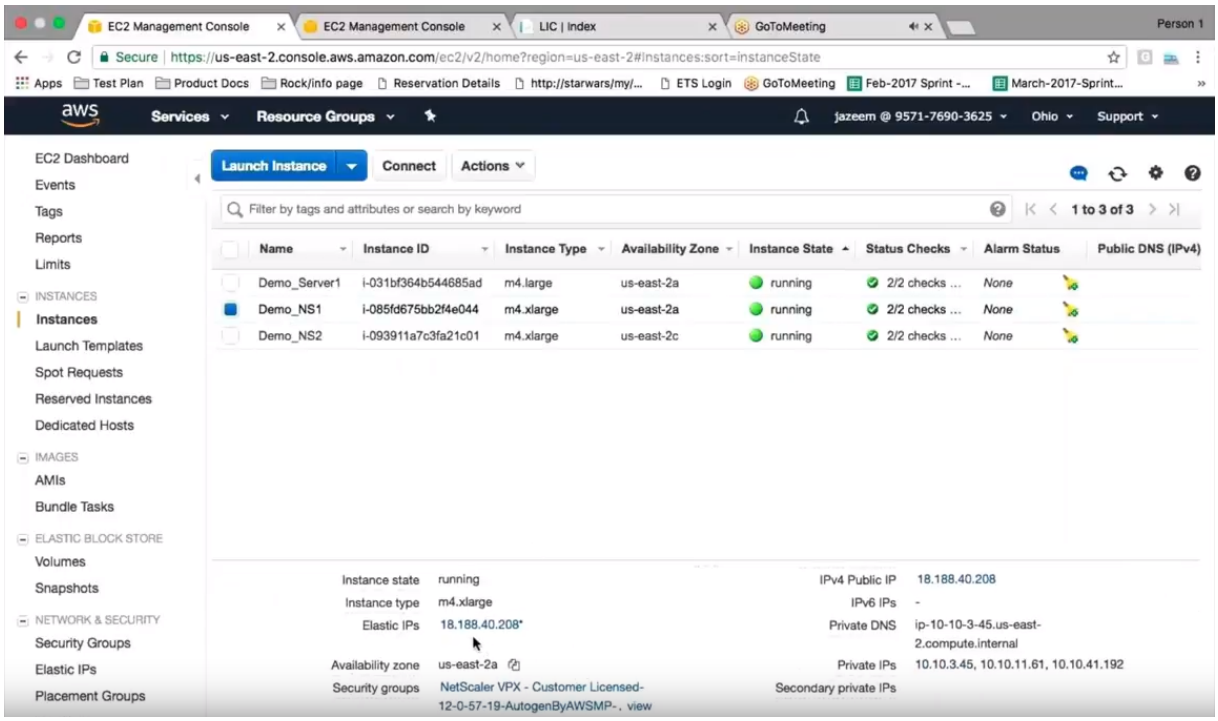
アソシエーションが作成されたら、フェイルオーバーを実行する準備が整いました。

下部には、VPX 上に 2 番目の弾性 IP があるはずです。

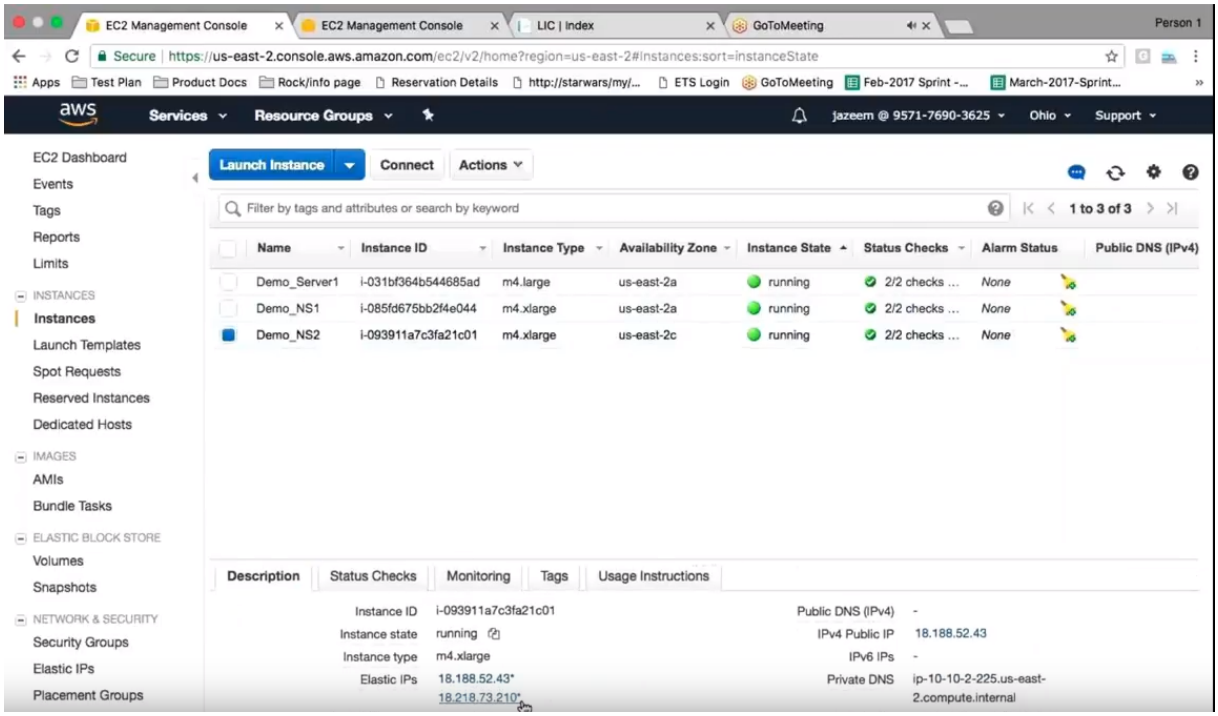
© 1999–2021 Citrix Systems, Inc. All rights reserved.



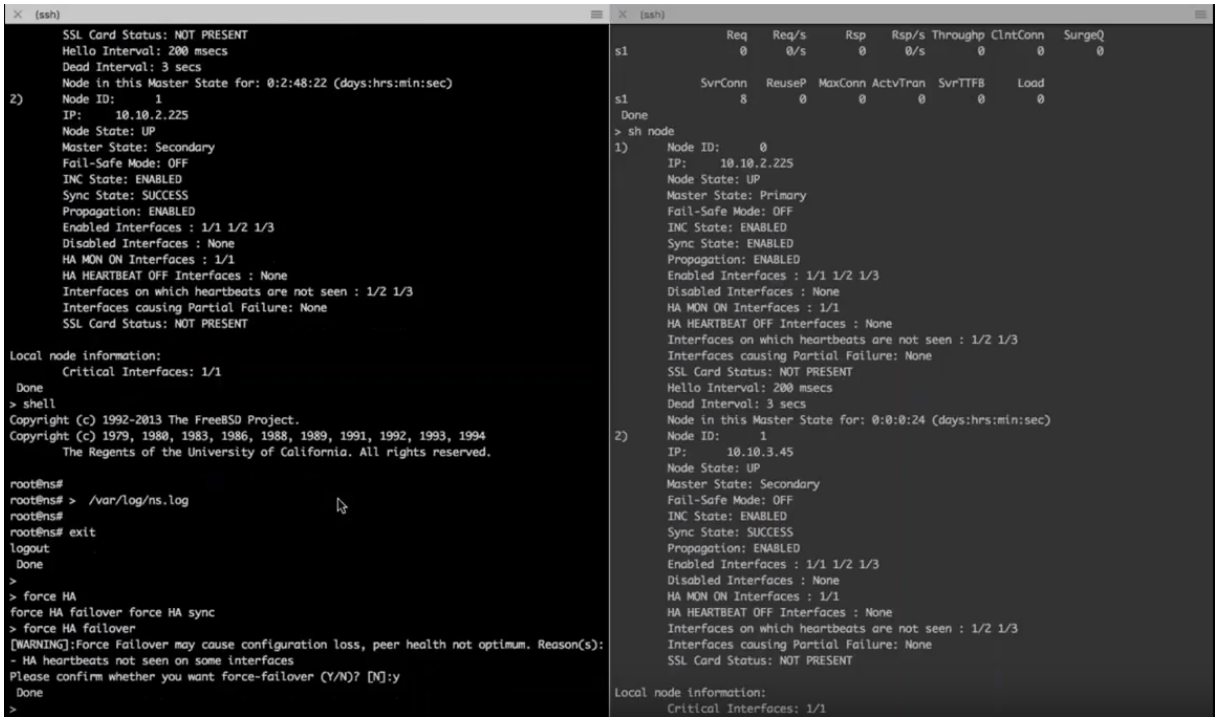
そのため、VPX にアクセスしてフェイルオーバーを開始し、AWS コンソールに戻ります。今回は、最初の Citrix ADC に属する弾性 IP を見て, 新しい EIP が存在しないことに注意してください, それは今、2 番目の Citrix ADC に移動されているように.



© 1999–2021 Citrix Systems, Inc. All rights reserved.

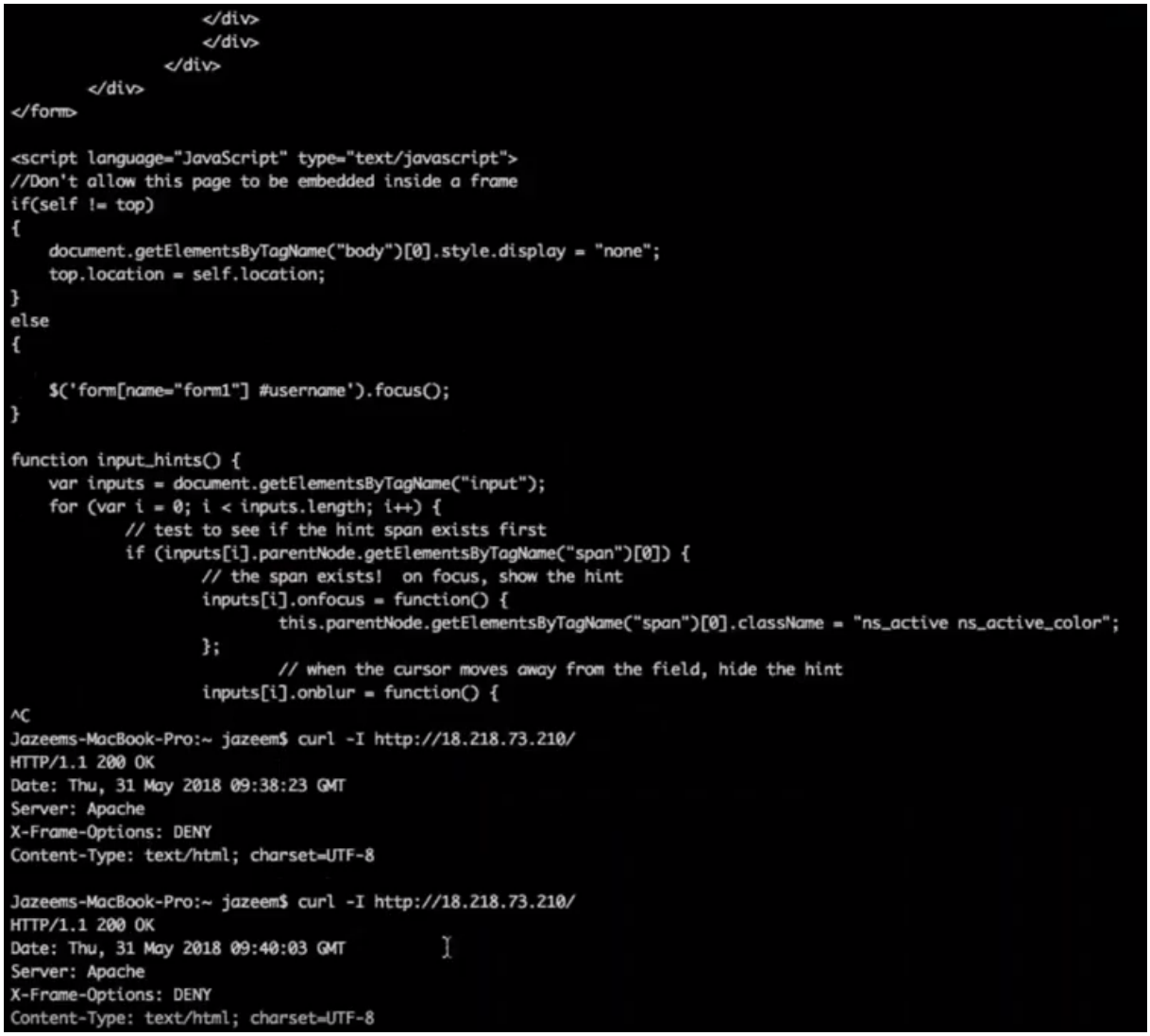


これを確認するには、1 番目と 2 番目の Citrix ADC で **show node** コマンドを入力し、2 番目の Citrix ADC が **standby** 状態になる前と同じように **Primary** 状態に設定されていることを確認します。



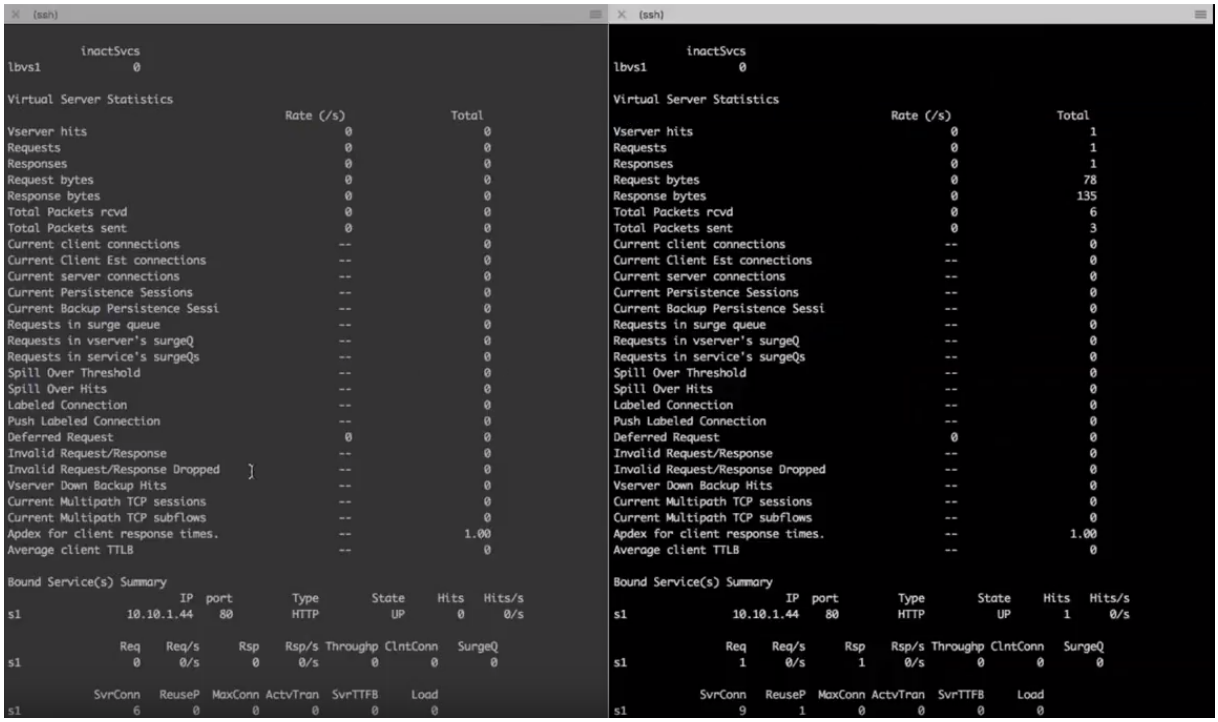
これで、リアルタイムのトラフィックフローを見ることができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

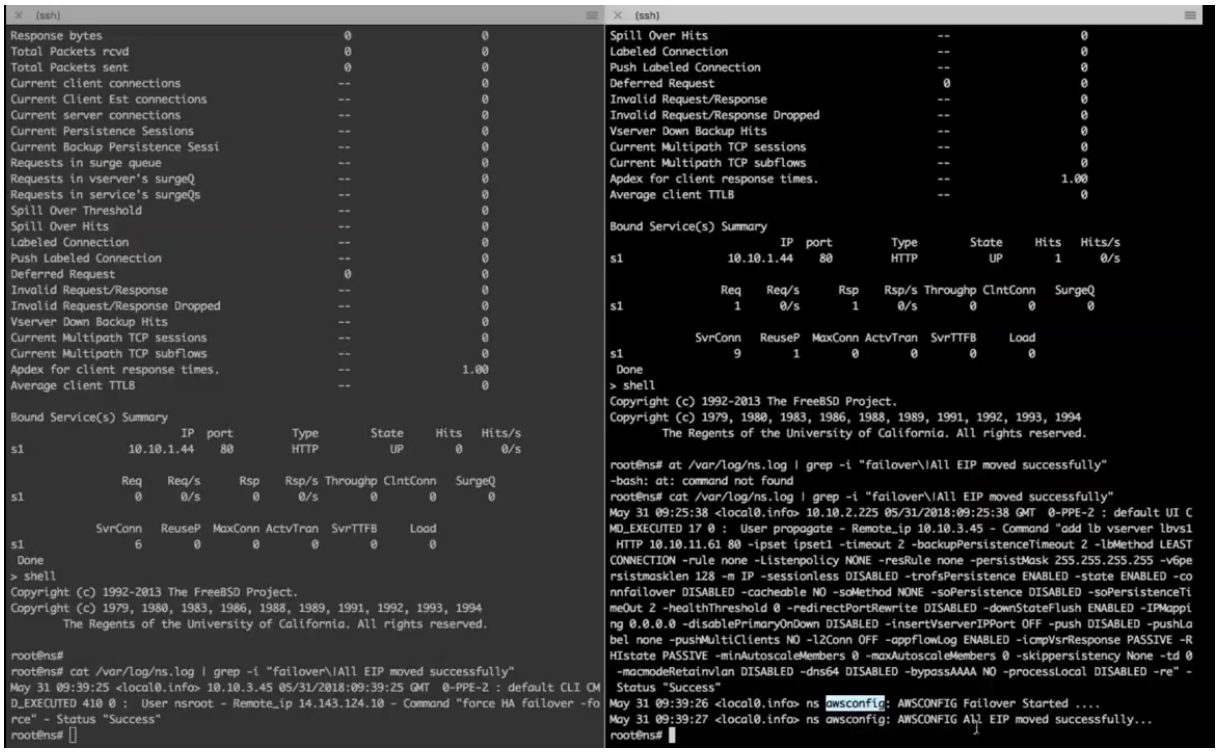


フェイルオーバー後に VIP に要求を送信できます。最初にアクティブだった Citrix ADC 上の LB 仮想サーバーで stat を実行した場合、そこには要求がないことに注意してください。以前のスタンバイ、現在アクティブな Citrix ADC で同じコマンドを実行すると、仮想サーバーが表示されます。高可用性の移行後、トラフィックは新しい Citrix ADC に送信されたことを示す。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ここで、デバッグを行ったり、現在のステータスを確認したりする場合は、シェルにドロップして、HA フェイルオーバーが発生したときや、AWS 設定または API コールアウトによってすべての EIP がプライマリ Citrix ADC からセカンダリにスイングされたときを示すレコードを探すことができます。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

AWS コンポーネントを設定する

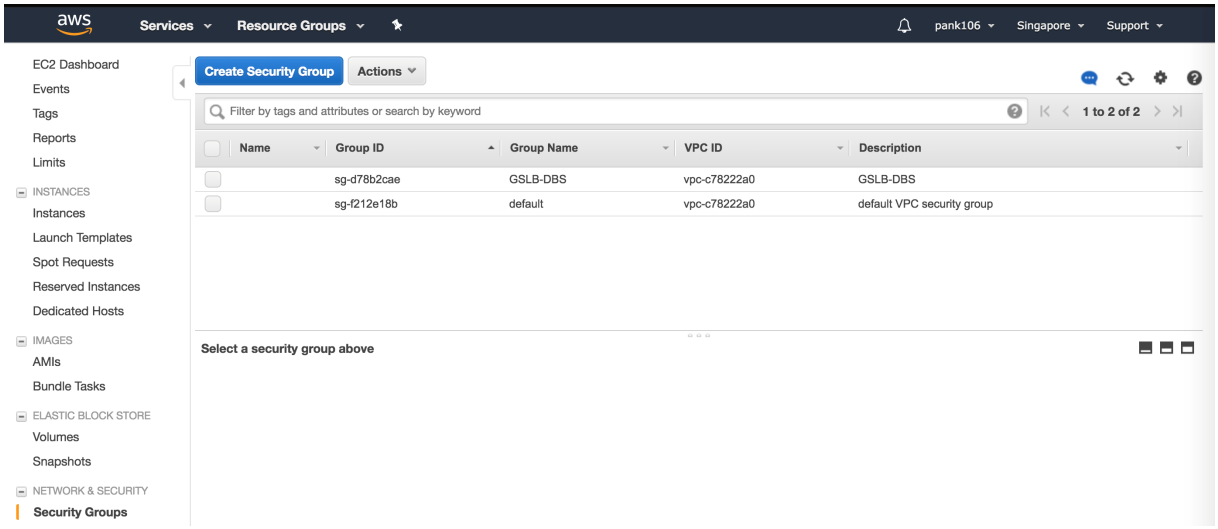
セキュリティグループ

> 注:
>
> ELB、Citrix ADC GSLB インスタンス、および Linux インスタンスに対して異なるセキュリティグループを作成することをお勧めします。これらのエンティティごとに必要なルールセットが異なるためです。この例では、簡潔にするために、統合セキュリティグループ設定があります。

仮想ファイアウォールの適切な設定については、VPC のセキュリティグループを参照してください。

手順 1:

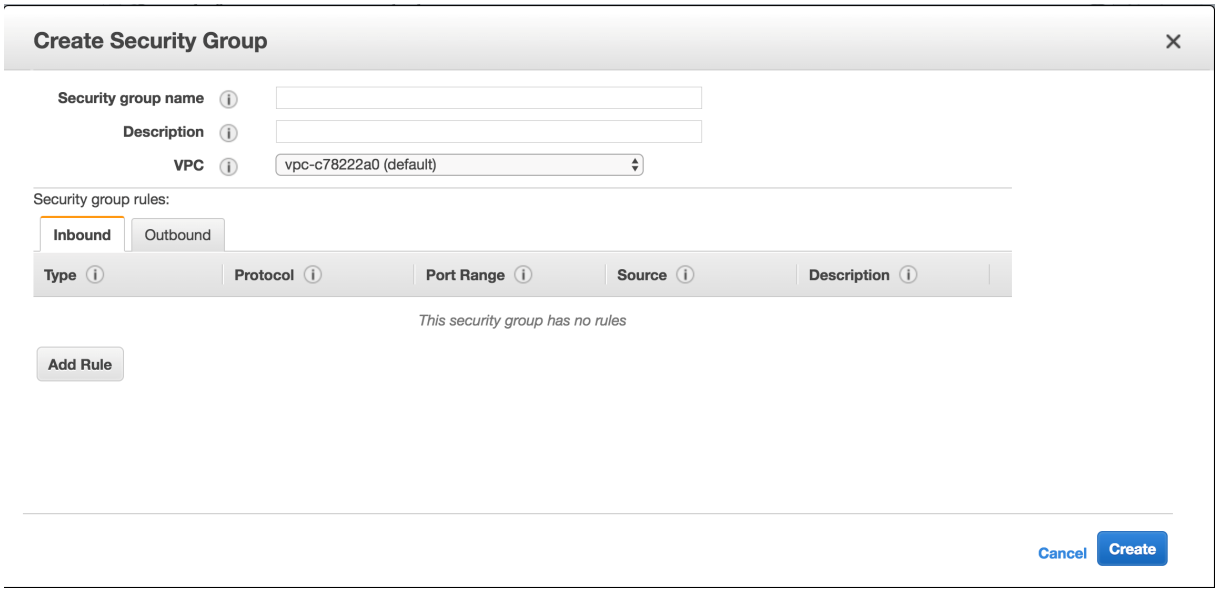
AWS リソースグループにログインし、**EC2** に移動します。EC2 内で、[ネットワークとセキュリティ] **>** [セキュリティグループ] に移動します。



手順 2:

[セキュリティグループの作成] をクリックし、名前と説明を入力します。このセキュリティグループには、Citrix ADC および Linux バックエンド Web サーバーが含まれます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 3:

次のスクリーンショットのインバウンドポートルールを追加します。

> 注:
>
> 詳細なセキュリティ強化には、送信元 IP アクセスを制限することをお勧めします。

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-web-server

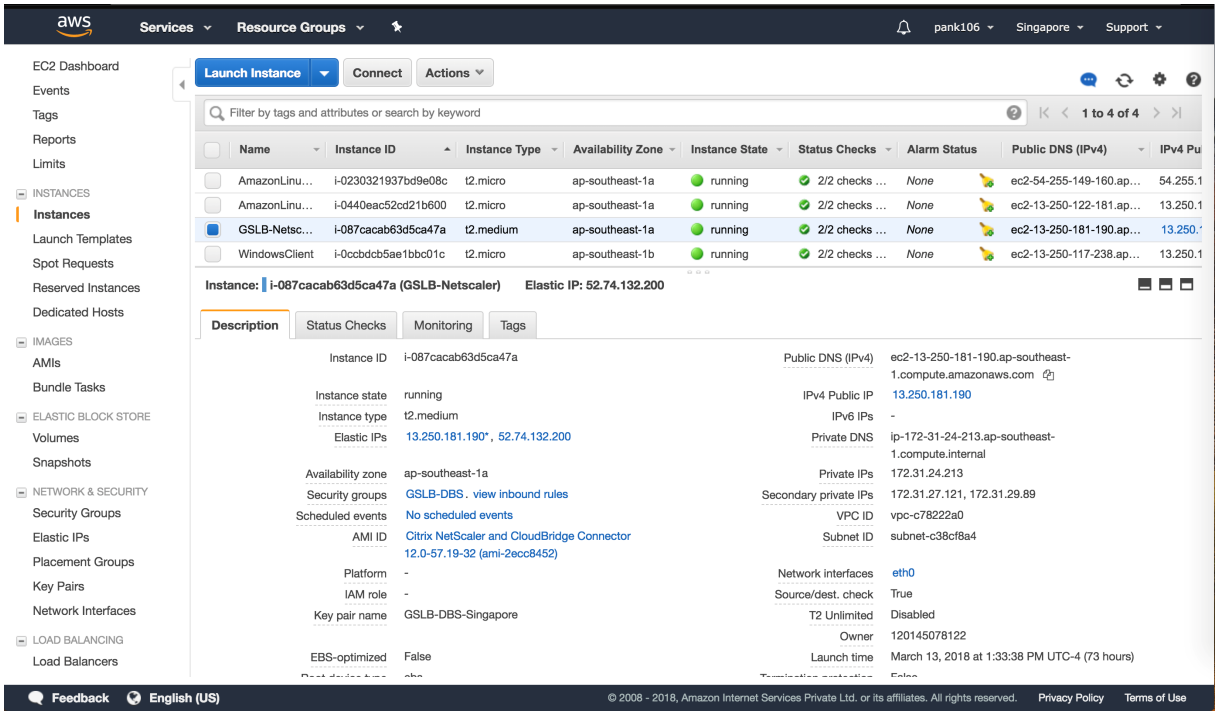
Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
SSH	TCP	22	0.0.0.0/0	
DNS (UDP)	UDP	53	0.0.0.0/0	
DNS (UDP)	UDP	53	::/0	
Custom TCP Rule	TCP	3389	0.0.0.0/0	
Custom TCP Rule	TCP	3389	::/0	
All ICMP - IPv4	All	N/A	0.0.0.0/0	
All ICMP - IPv4	All	N/A	::/0	
Custom TCP Rule	TCP	5985	0.0.0.0/0	
Custom TCP Rule	TCP	5985	::/0	
Custom TCP Rule	TCP	3008 - 3011	0.0.0.0/0	
Custom TCP Rule	TCP	3008 - 3011	::/0	

Amazon Linux バックエンドウェブサービス

手順 4:

AWS リソースグループにログインし、**EC2** に移動します。EC2 内で **[**インスタンス**]** に移動します。

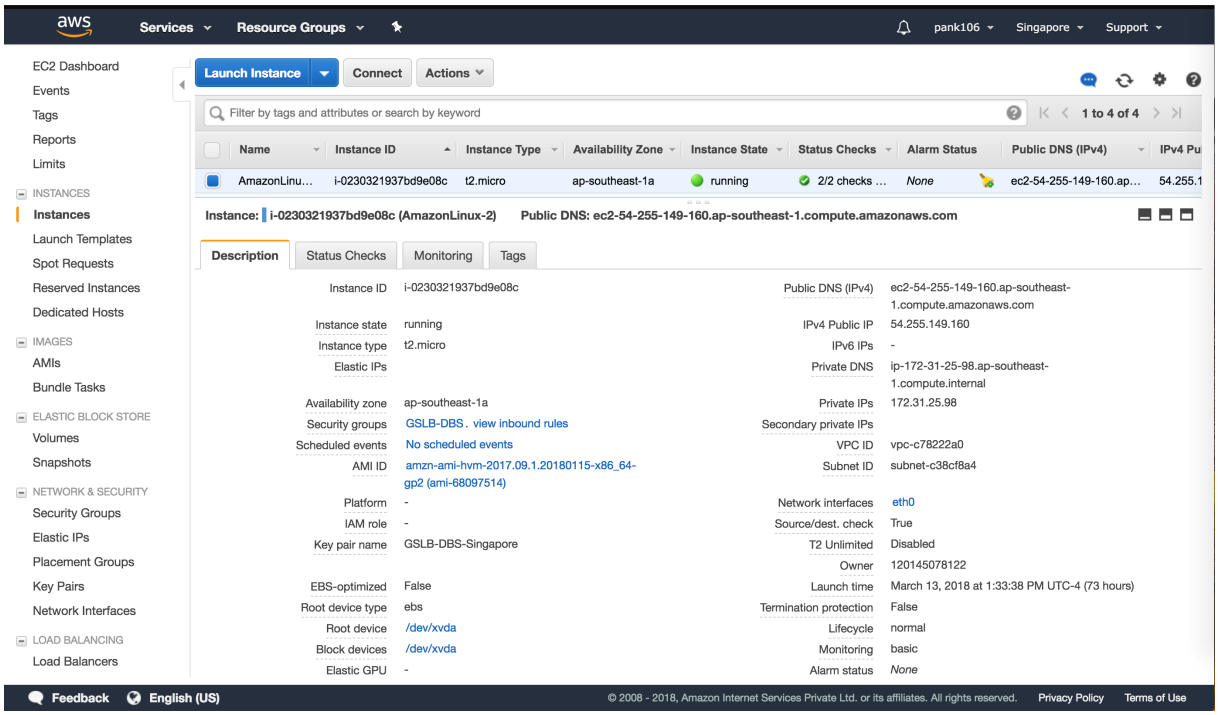
© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 5:

Amazon Linux インスタンスを設定するには、以下の詳細を使用して **[**インスタンスを起動**]** をクリックします。

このインスタンスでの Web サーバーまたはバックエンドサービスの設定に関する詳細を入力します。

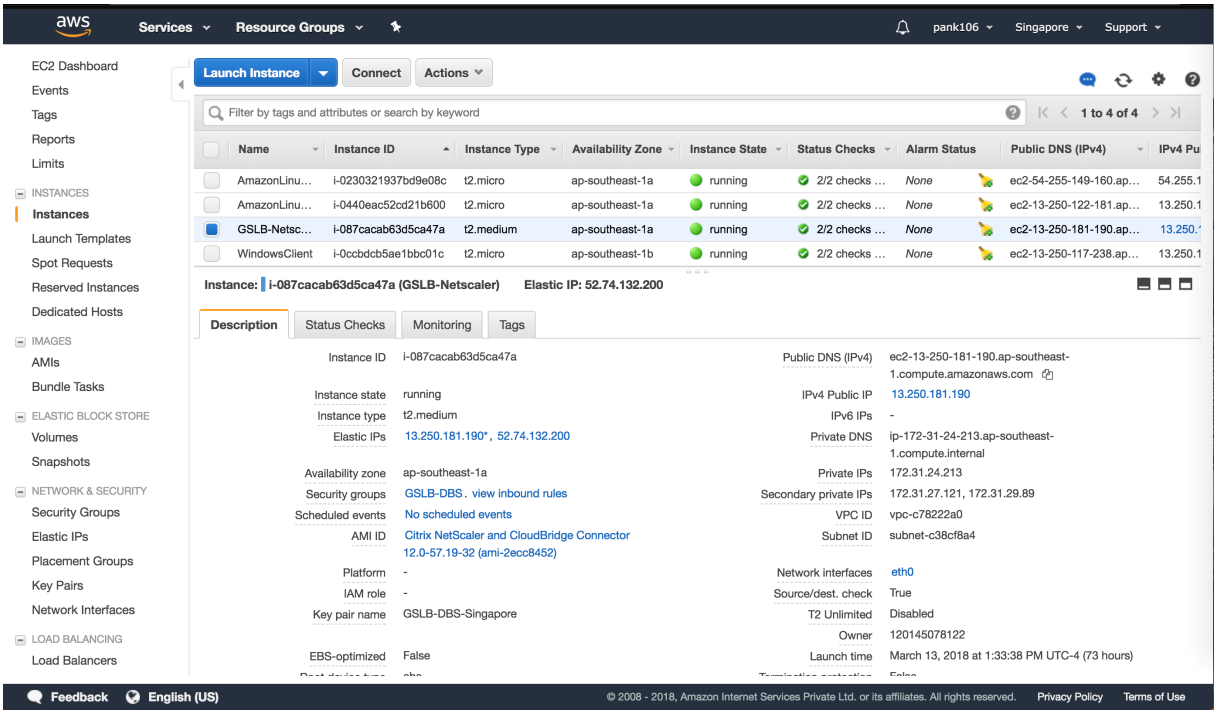


© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix ADC ADC の構成

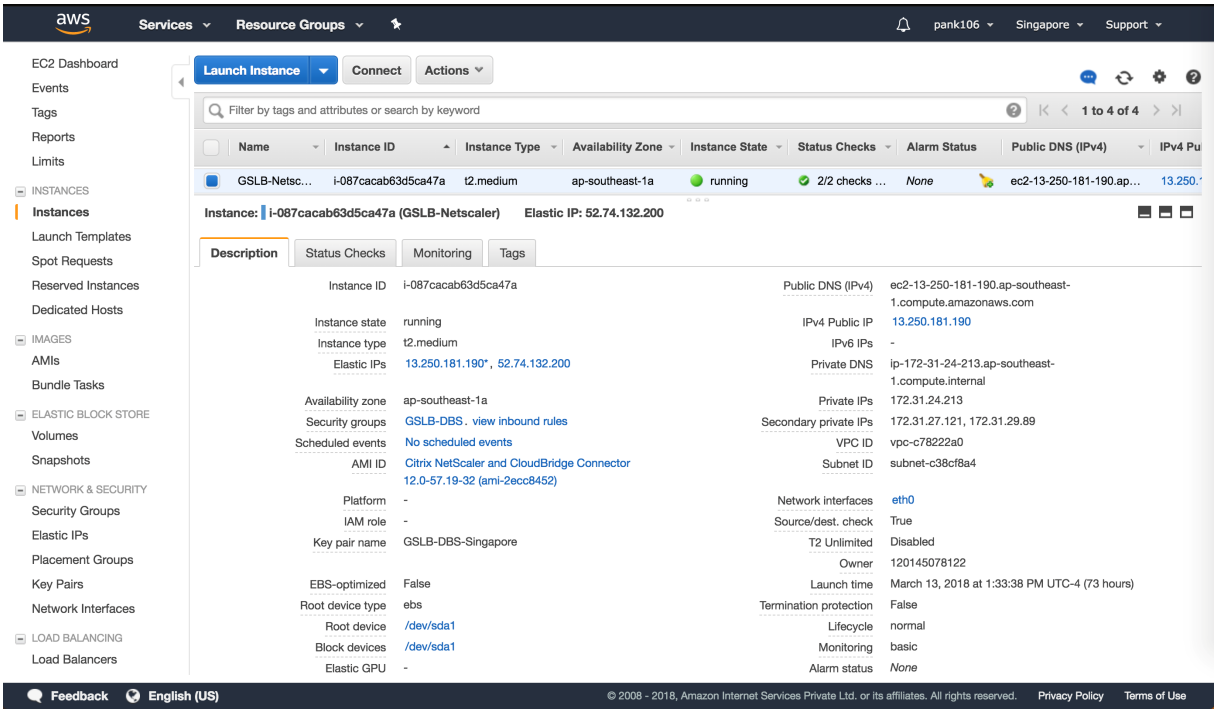
手順 6:

AWS リソースグループにログインし、**EC2** に移動します。EC2 内で **[**インスタンス**]** に移動します。



手順 7:

Amazon AMI インスタンスを設定するには、以下の詳細を使用して **[**インスタンスを起動**]** をクリックします。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

エラスティック **IP** 設定

> 注:
>
> Citrix ADC は、NSIP のパブリック IP を持たないため、必要に応じて単一の Elastic IP で実行することもできます。代わりに、ボックスへの管理アクセスのためにカバーすることができます SNIP に弾性 IP を添付します, だけでなく、GSLB サイト IP と ADNS IP.

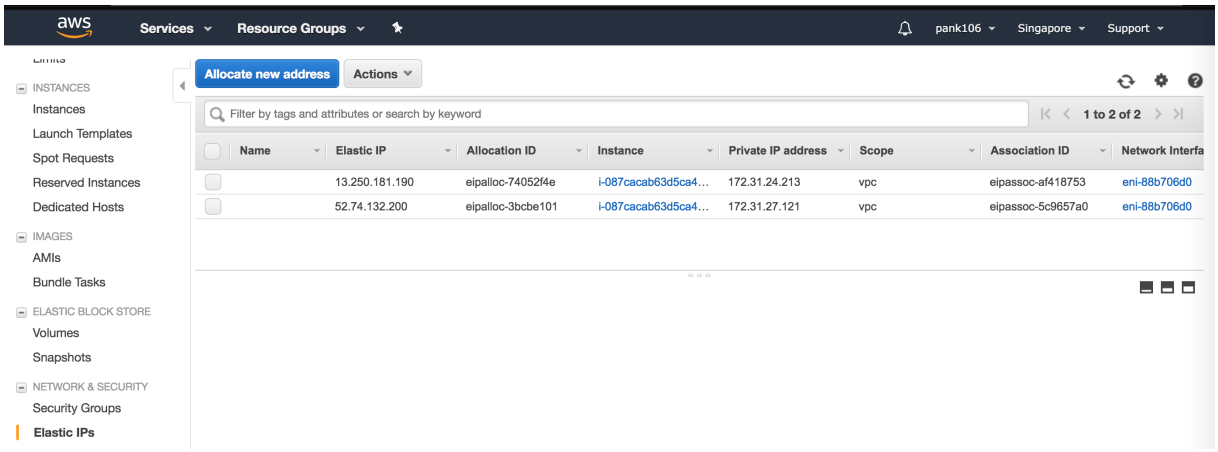
手順 8:

AWS リソースグループにログインし、**EC2** に移動します。EC2 内で [ネットワークとセキュリティ] に移動し、**Elastic IP** を設定します。

[新しいアドレスを割り当て] をクリックして、新しい Elastic IP アドレスを作成します。

AWS 内で実行中の Citrix ADC インスタンスを指すように Elastic IP を設定します。

2 つ目の Elastic IP を設定し、実行中の Citrix ADC インスタンスを再度指定します。

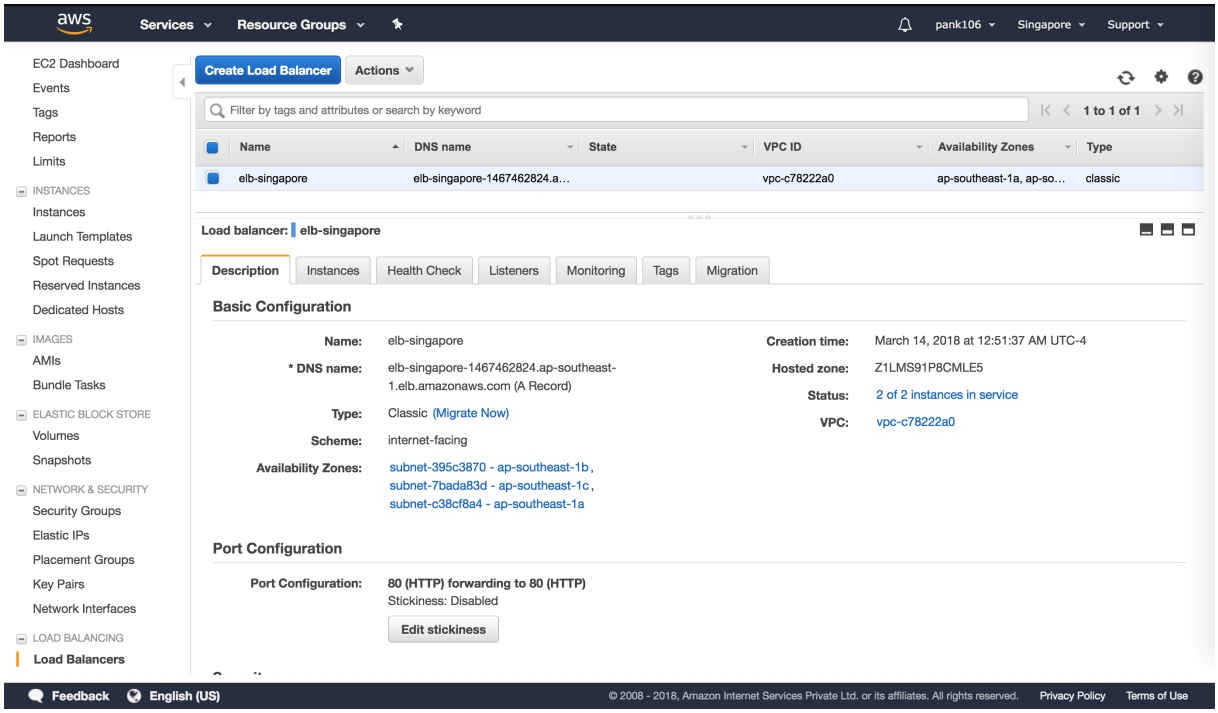


伸縮自在なロードバランサー

手順 9:

AWS リソースグループにログインし、**EC2** に移動します。EC2 内で、[ロードバランシング]、[ロードバランサー] の順に選択します。

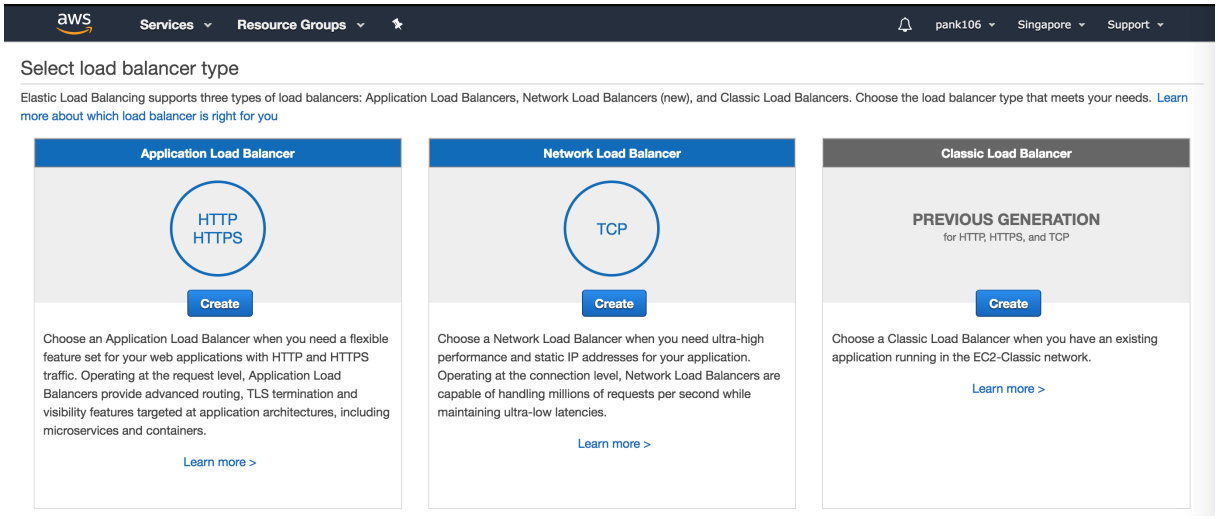
© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 10:

[**Load Balancer** の作成] をクリックして、クラシックロードバランサーを設定します。

Elastic Load Balancers を使用すると、バックエンドの Amazon Linux インスタンスの負荷分散が可能になると同時に、需要に基づいてスピンアップされる追加のインスタンスをロードバランシングできます。



グローバルサーバロードバランシングドメイン名ベースのサービスの設定

トラフィック管理の設定

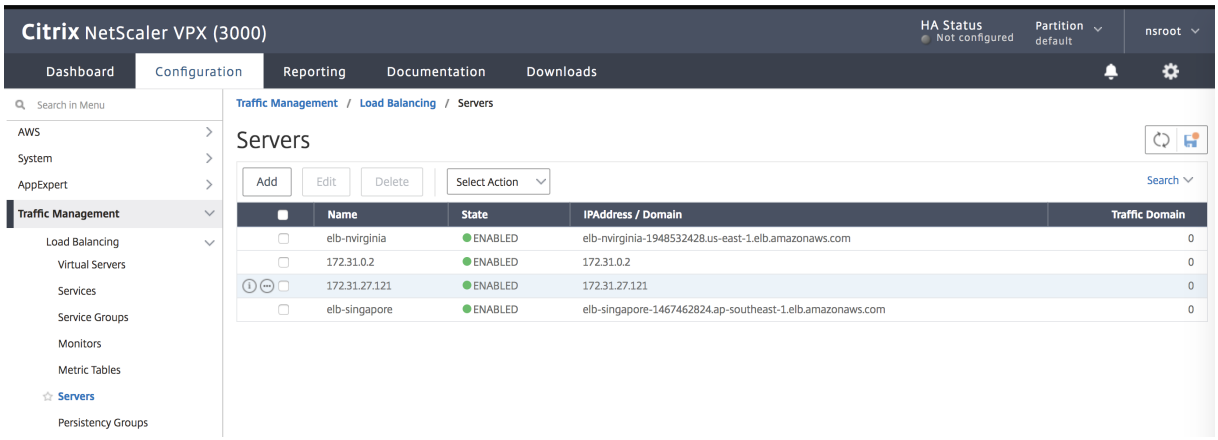
© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> DBS サービスグループに対して ELB/ALB ドメインを解決するネームサーバーまたは DNS 仮想サーバーのいずれかを使用して Citrix ADC を構成する必要があります。

https://developer-docs.citrix.com/projects/netscaler-command-reference/en/12.0/dns/dns-nameserver/dns-nameserver/

手順 1:

[** トラフィック管理] > [負荷分散] > [サーバー]** に移動します。

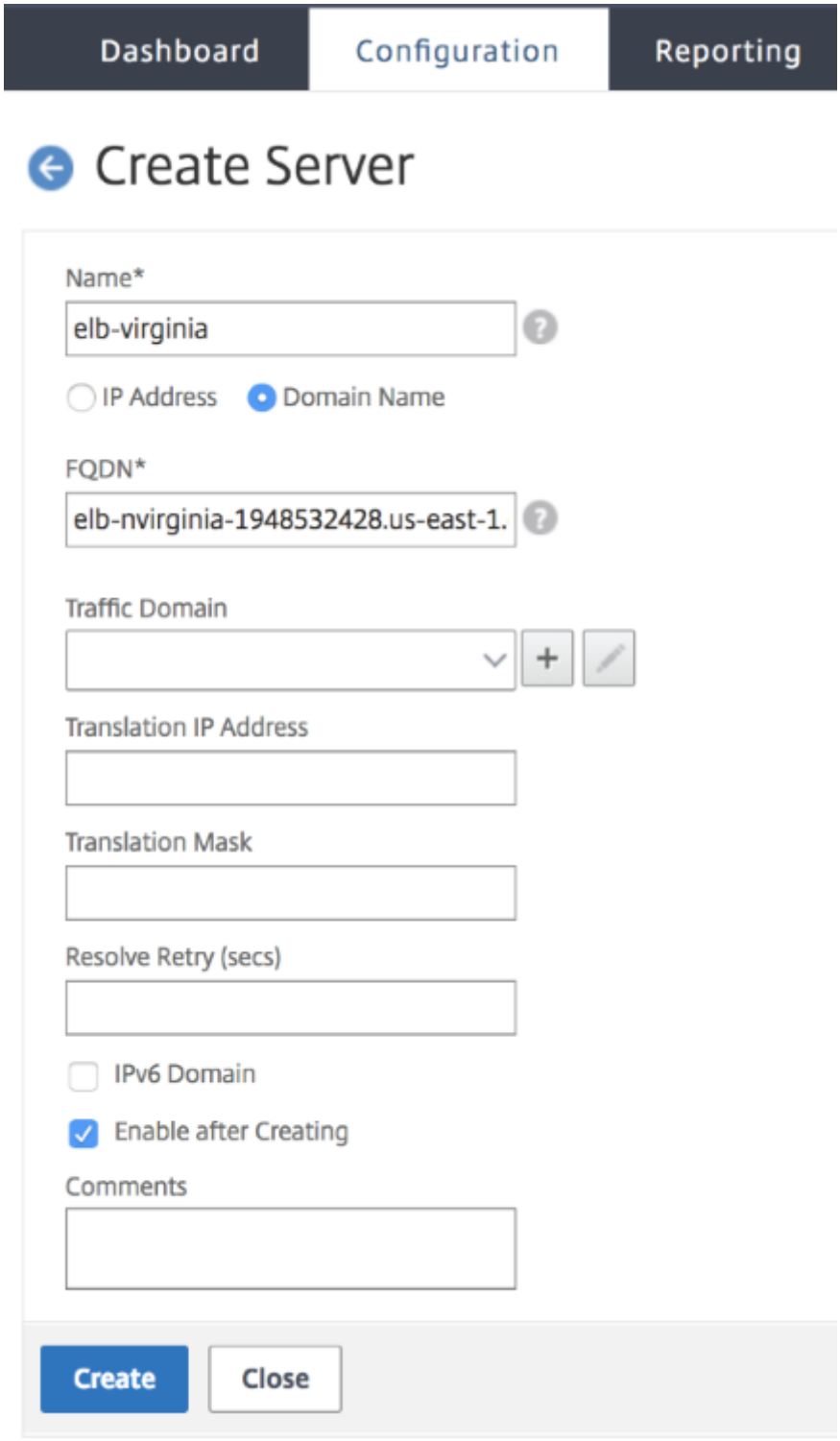


手順 2:

[**Add**] をクリックしてサーバーを作成し、Elastic Load Balancer（ELB）用の AWS の A レコード（ドメイン名）に対応する名前と FQDN を指定します。

手順 2 を繰り返して、AWS の 2 番目のリソースの場所から 2 番目の ELB を追加します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

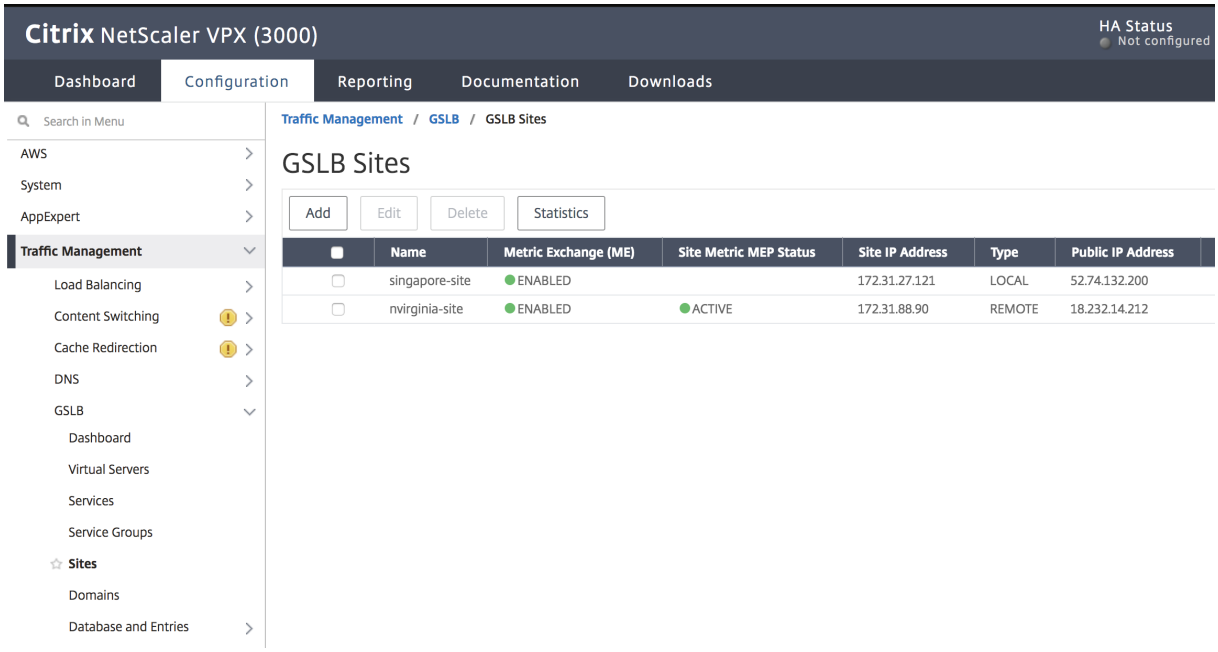


GSLB 構成

手順 1:

© 1999–2021 Citrix Systems, Inc. All rights reserved.

[** トラフィック管理] > [GSLB] > [サイト]** に移動します。

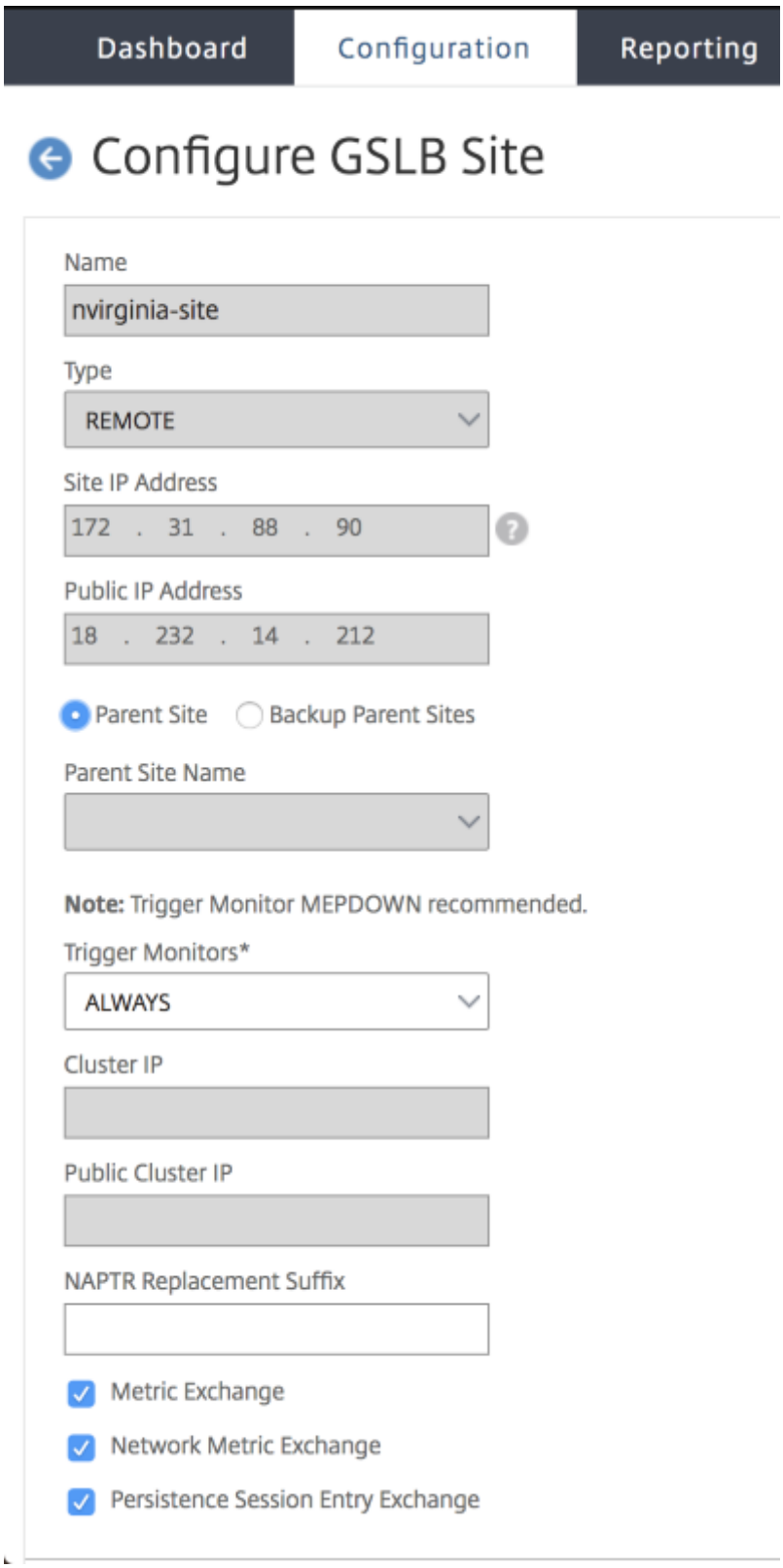


手順 3:

「追加」ボタンをクリックして、GSLB サイトを設定します。

「サイト」に名前を付けます。[種類] は、サイトを構成している Citrix ADC に基づいて、[リモート] または [ローカル] として構成されます。サイトの IP アドレスは、GSLB サイトの IP アドレスです。GSLB サイトは、この IP アドレスを使用して、他の GSLB サイトと通信します。パブリック IP アドレスは、特定の IP が外部のファイアウォールまたは NAT デバイスでホストされているクラウドサービスを使用する場合に必要です。サイトは親サイトとして構成する必要があります。[トリガーモニター] が [常に] に設定されていることを確認し、[メトリック交換]、[ネットワークメトリック交換]、および [持続性セッションエントリ交換] の下部にある 3 つのチェックボックスをオフにします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



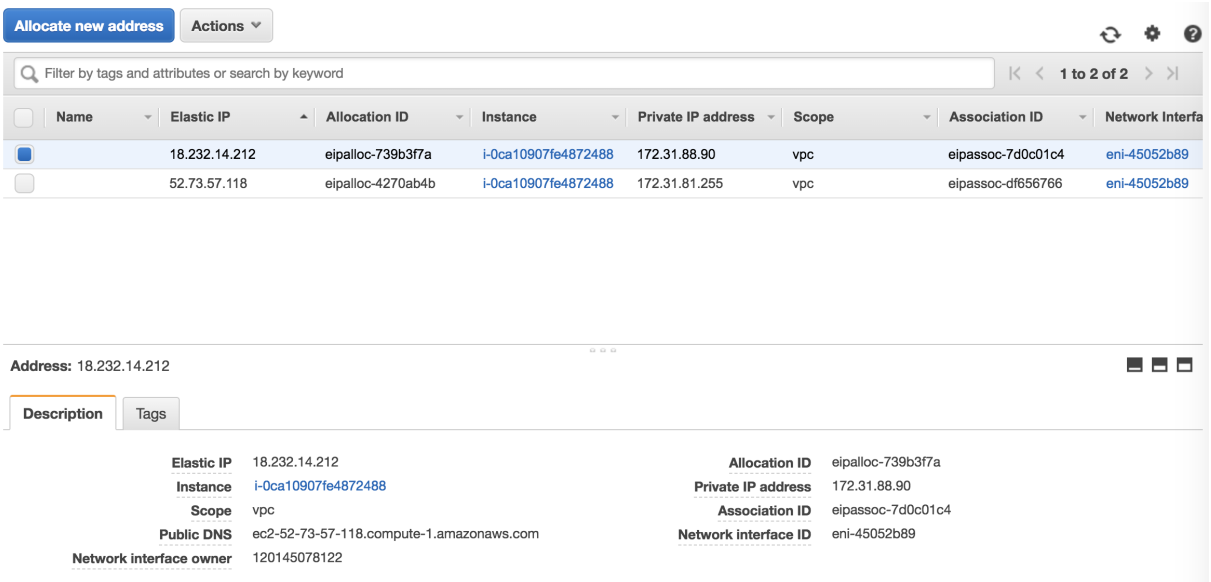
トリガモニタの設定を MEPDOWN に設定することが推奨されます。詳しくは、「GSLB サービスグループの構成」を参照してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

手順 4:

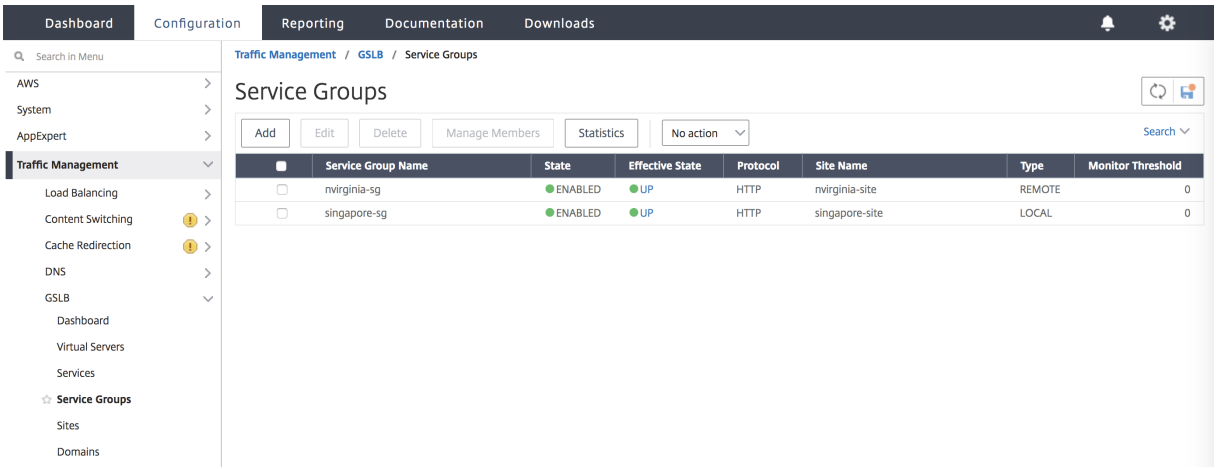
以下は、AWS 設定のスクリーンショットです。サイトの IP アドレスとパブリック IP アドレスがどこにあるかを示しています。これらは、[ネットワークとセキュリティ] **> [Elastic IP**] にあります。

[作成] をクリックし、手順 3 と 4 を繰り返して、Azure 内の他のリソースの場所に GSLB サイトを構成します (これは、同じ Citrix ADC 上で構成できます)。



手順 5:

「トラフィック管理」**>**「**GSLB**」**>**「サービスグループ」に移動します。

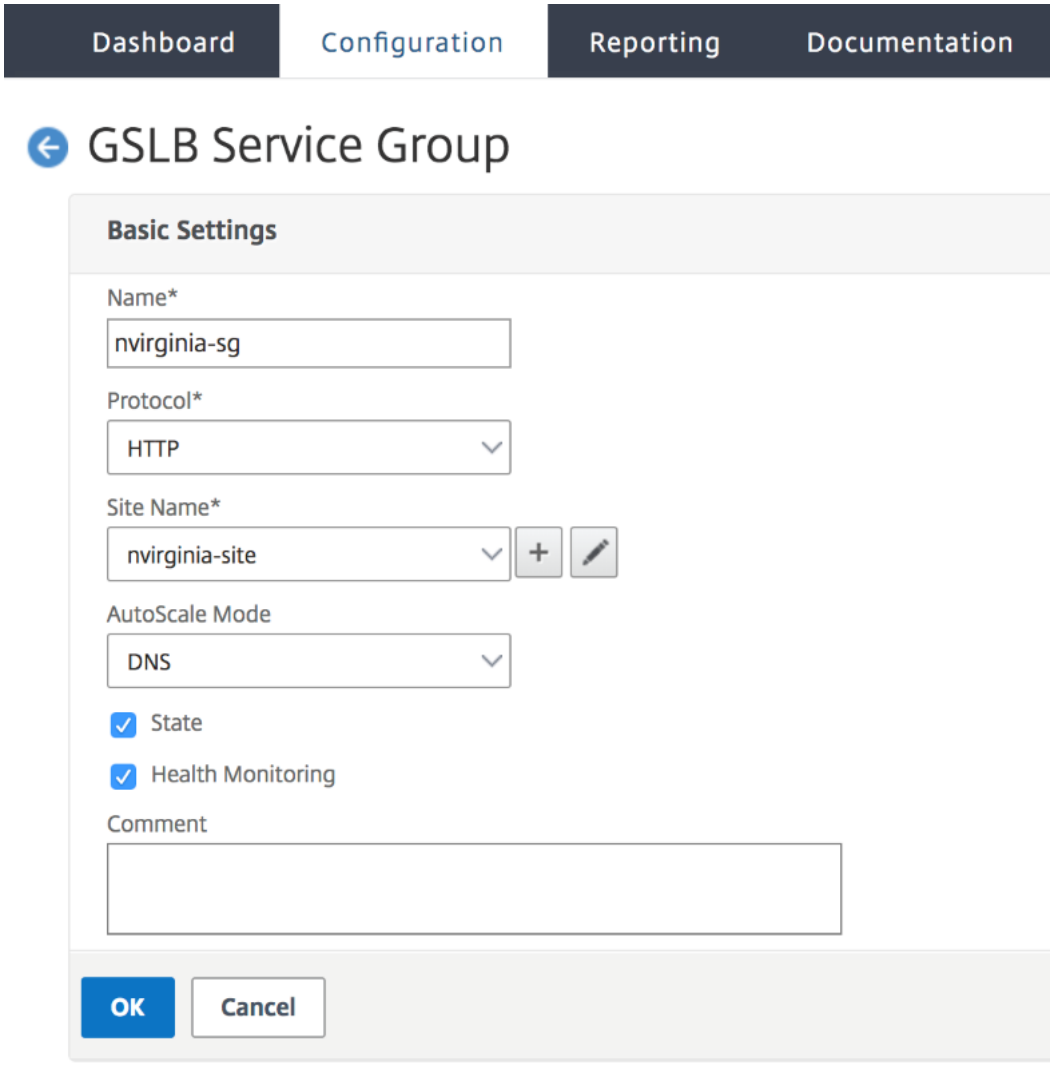


手順 6:

[追加] をクリックして、新しいサービスグループを追加します。サービスグループに名前を付け、HTTP プロトコルを使用し、[サイト名] で、前の手順で作成した各サイトを選択します。[AutoScale モード] を DNS として設定し、[状態] および [ヘルスモニタ] のチェックボックスをオフにします。

[OK] をクリックして、サービスグループを作成します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

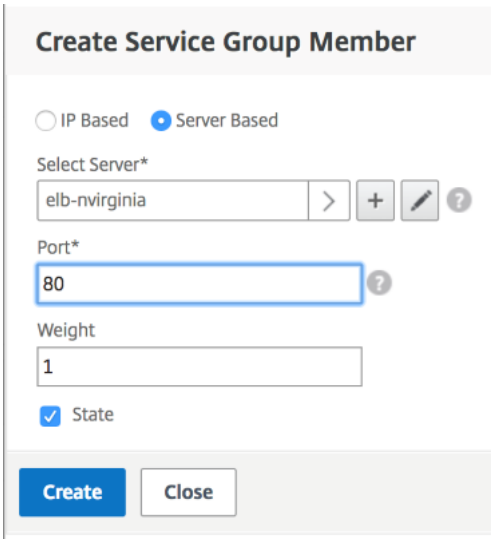


手順 7:

[サービスグループメンバー] をクリックし、**[サーバーベース]** を選択します。実行ガイドの開始時に設定された、それぞれの Elastic Load Balancing Serve を選択します。トラフィックがポート 80 を通過するように設定します。

［作成］をクリックします。

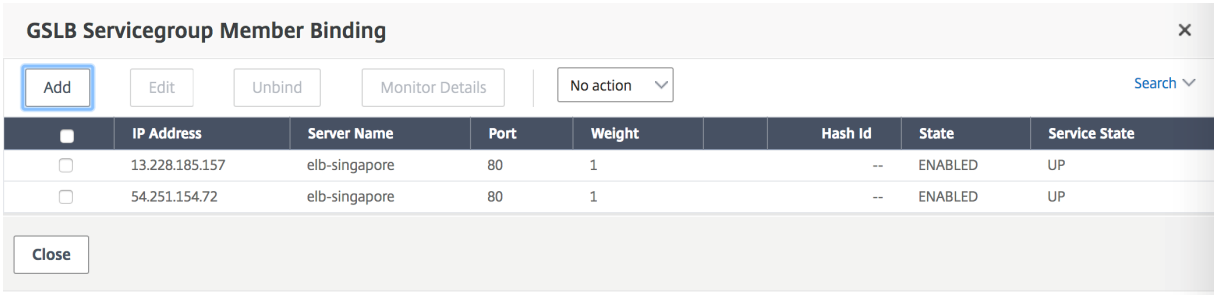
© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 8:

サービスグループのメンバーバインディングには、Elastic Load Balancer から受信する 2 つのインスタンスが設定されます。

ステップを繰り返して、AWS の 2 番目のリソースロケーションにサービスグループを設定します。（これは同じ場所から行うことができます）。

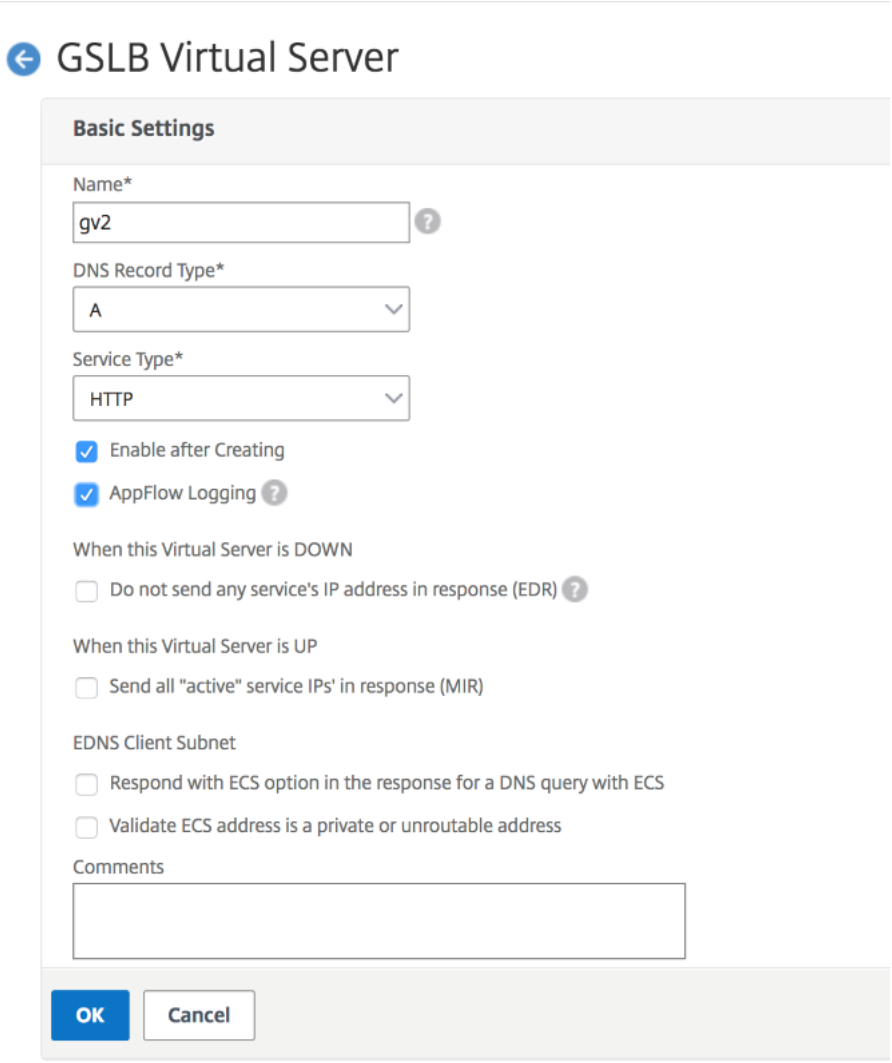


手順 9:

[トラフィック管理**] > [GSLB] > [**仮想サーバー**]** に移動します。

[追加] をクリックして、仮想サーバーを作成します。サーバーの名前を指定し、DNS レコードタイプが A に設定され、サービスタイプが HTTP に設定され、AppFlow ロギングの作成後に有効にするチェックボックスをオンにします。[**OK**] をクリックして、GSLB 仮想サーバーを作成します。（Citrix ADC ADC GUI）

© 1999–2021 Citrix Systems, Inc. All rights reserved.

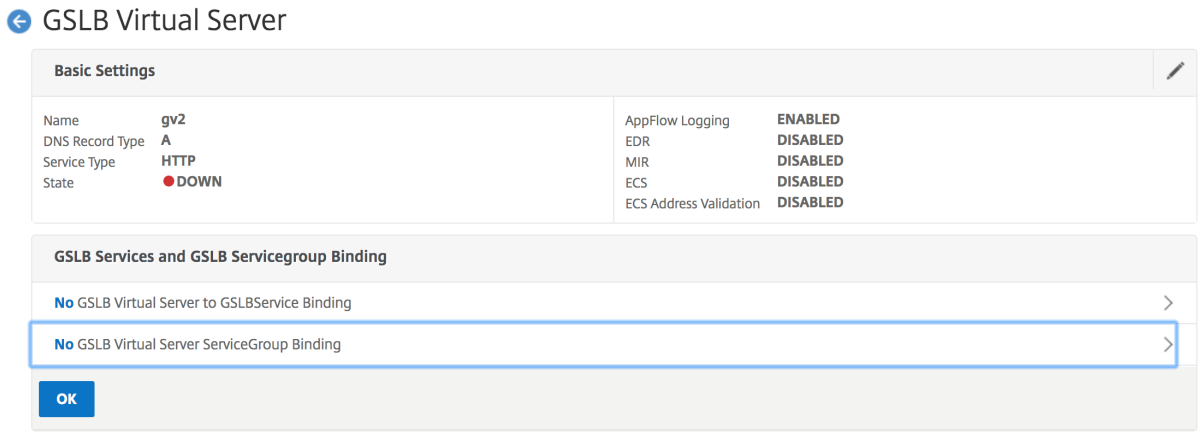


手順 10:

GSLB 仮想サーバーが作成されたら、[**GSLB** 仮想サーバーサービスグループバインドなし] をクリックします。

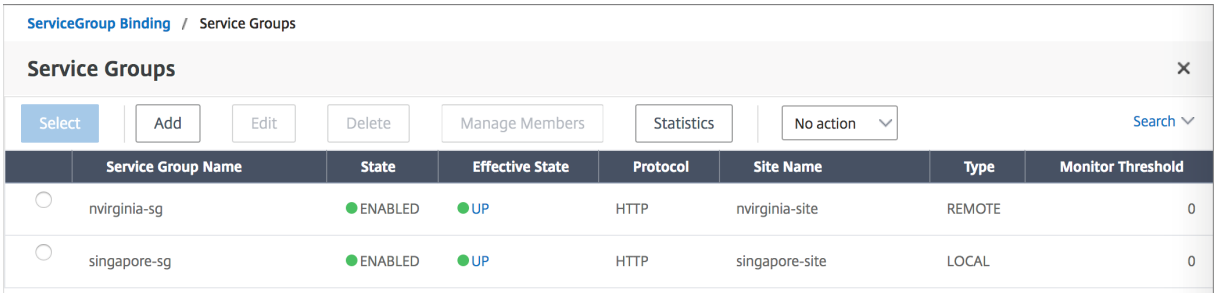
[追加] をクリックして、仮想サーバーを作成します。サーバーの名前を指定し、DNS レコードタイプが A に設定され、サービスタイプが HTTP に設定され、AppFlow ロギングの作成後に有効にするチェックボックスをオンにします。[**OK**] をクリックして、GSLB 仮想サーバーを作成します。(Citrix ADC ADC GUI)

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 11:

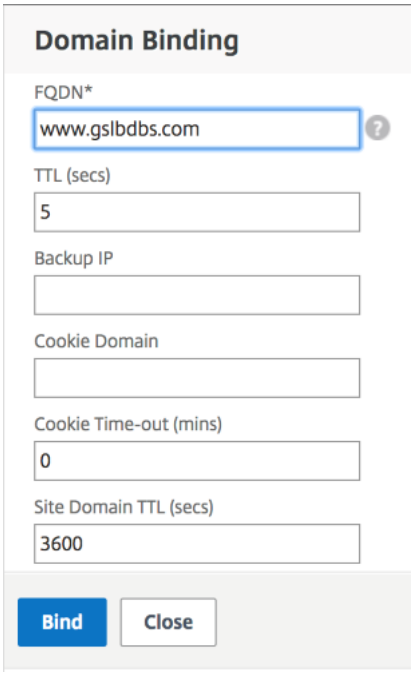
[ServiceGroup Binding] で、**[**サービスグループ名の選択**]** を使用して、前の手順で作成したサービスグループを選択して追加します。



手順 12:

次に、**[GSLB** 仮想サーバードメインバインディングなし**]** をクリックして、GSLB 仮想サーバードメインバインディングを設定します。FQDN とバインドを構成し、残りの設定をデフォルトのままにしておくことができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



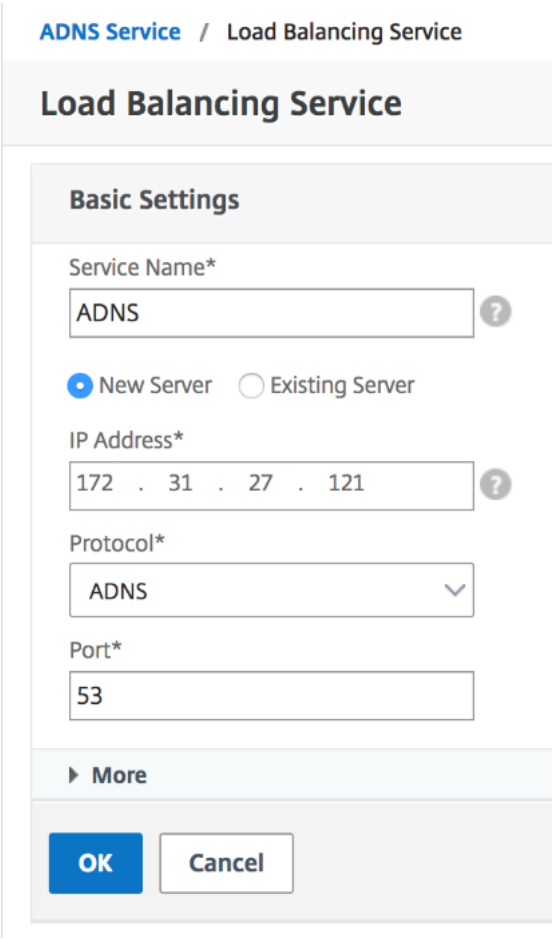
手順 13:

[サービスなし] をクリックして、ADNS サービスを構成します。サービス名を追加し、[新しいサーバー] をクリックして、ADNS サーバーの IP アドレスを入力します。

また、ADNS がすでに構成されている場合は、[既存のサーバー] を選択し、メニューから ADNS を選択できます。プロトコルが ADNS で、トラフィックがポート 53 経由であることを確認します。

メソッドを LEASTCONNECTION、バックアップメソッドを ROUNDROBIN として構成する

© 1999–2021 Citrix Systems, Inc. All rights reserved.



AWS による Citrix ADC バックエンド自動スケーリング

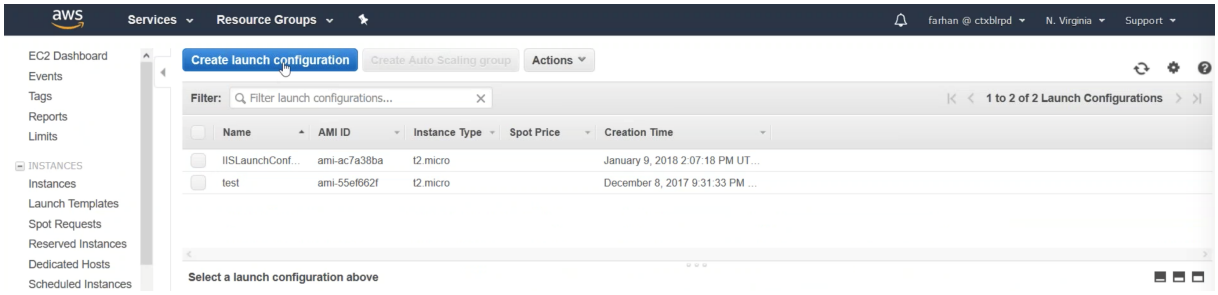
AWS には、管理者が設定したルールに基づいて、AWS で実行されている追加のインスタンスをスピンアップする Auto Scaling という機能が含まれています。これらのルールは CPU 使用率によって定義され、オンデマンドでインスタンスを作成および削除することを中心に行われます。Citrix ADC は AWS Auto Scaling ソリューションと直接統合し、Citrix ADC は負荷分散が可能なすべての利用可能なバックエンドサーバーを認識します。この機能の制限は、現在 AWS の 1 つの AZ 内でのみ機能することです。

AWS コンポーネントを設定する

手順 1:

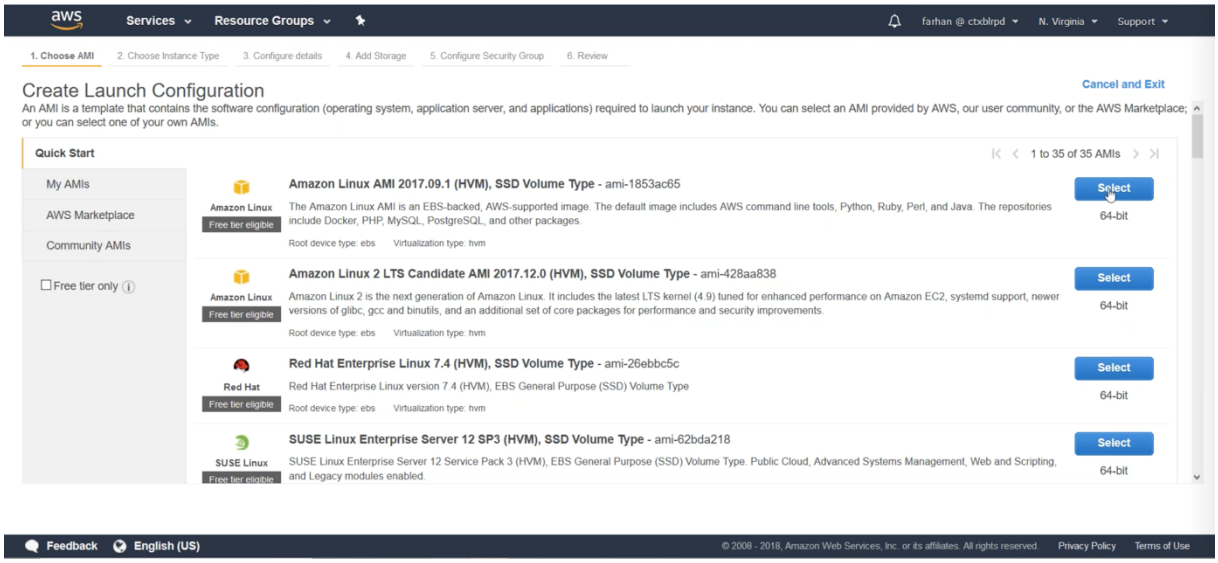
AWS リソースグループにサインインし、**EC2** に移動します。EC2 で [自動スケーリング] **>** [起動設定] に移動します。[起動設定の作成] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 2:

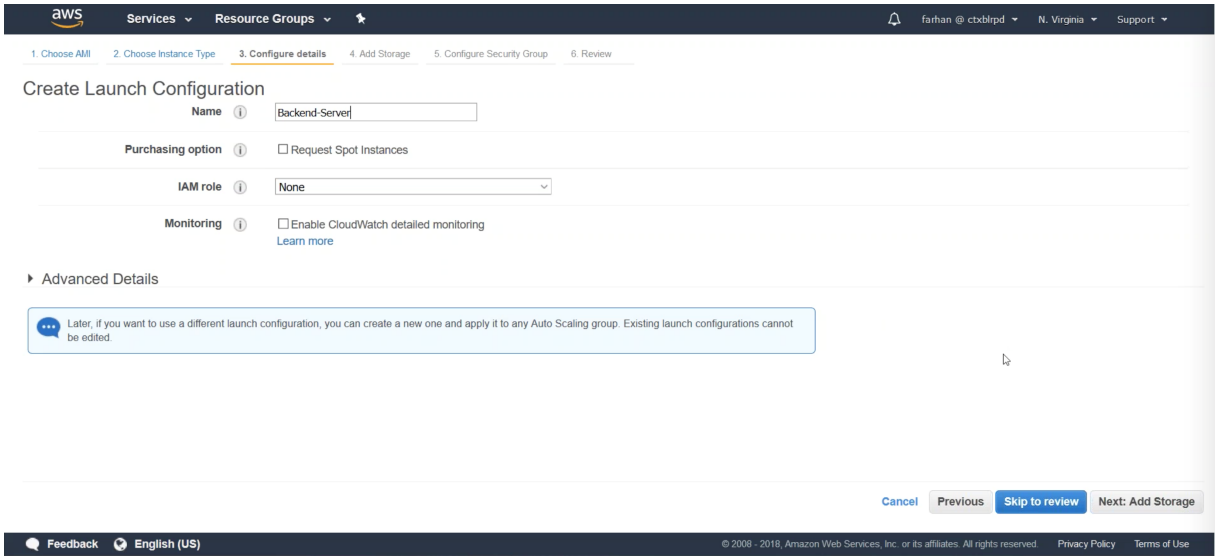
この手順から、選択したサーバーの種類を選択できます。ここで、自動スケーリングする VM を設定します。この例では、**Amazon Linux AMI** を選択する必要があります。



手順 3:

バックエンドリソースの潜在的な差異から選択して、必要なインスタンスのタイプを選択します。実行ガイドの残りの部分として、インスタンスに名前を付けます。インスタンスの名前は、バックエンドサーバーと呼ばれます。インスタンスのストレージを設定してセキュリティグループに追加するか、この実行ガイドで作成したすべての AWS コンポーネントを含む新しいセキュリティグループを作成します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 4:

セキュリティグループに関する追加の注意事項。この実行ガイドでは、以下のポートが開いています。

Type	Protocol	Port Range	Source
All traffic	All	All	0.0.0.0/0
SSH	TCP	22	185.25.64.249/32
SSH	TCP	22	125.16.224.135/32

Citrix ADC バックエンド自動スケーリンググループとポリシー

AWS で Citrix ADC フロントエンド Auto Scaling を構成します:

手順 1:

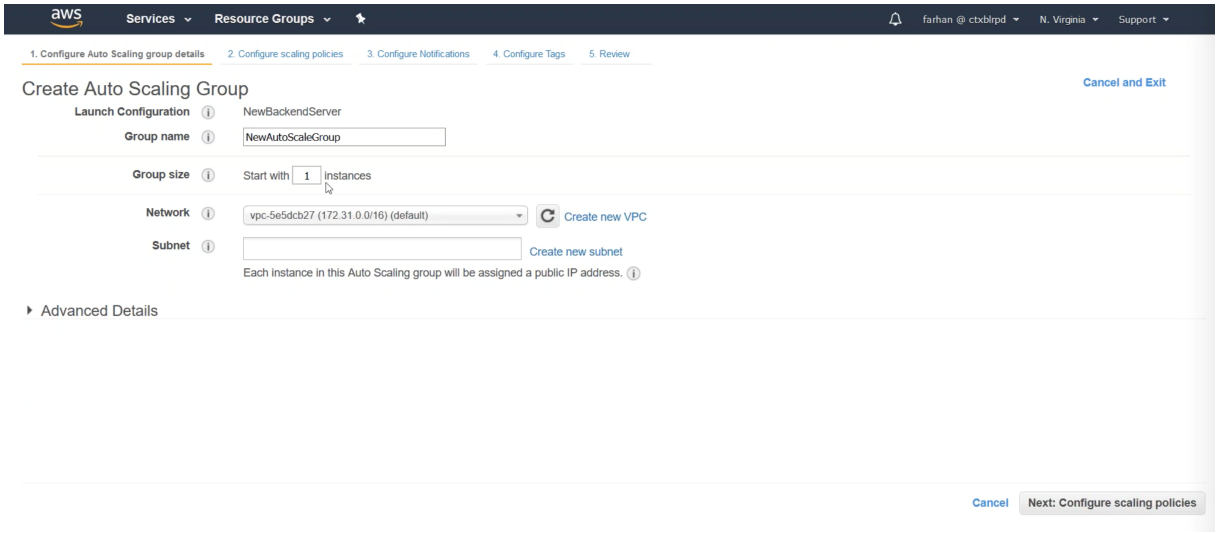
AWS リソースグループにサインインし、**EC2** に移動します。EC2 内で [**AUTO SCALING**] **> [Auto Scaling** グループ] に移動します。

[**Radio**] ボタンをクリックして、既存の起動設定から Auto Scaling グループを作成します。ラボガイドの前のステップで作成した BackendServer を必ず選択してください。

[**Create Auto Scaling Group**] でグループ名を追加し、初期グループサイズを選択し、[**Network**] と [**Subnet**] を選択して、[**Next**]
をクリックします。

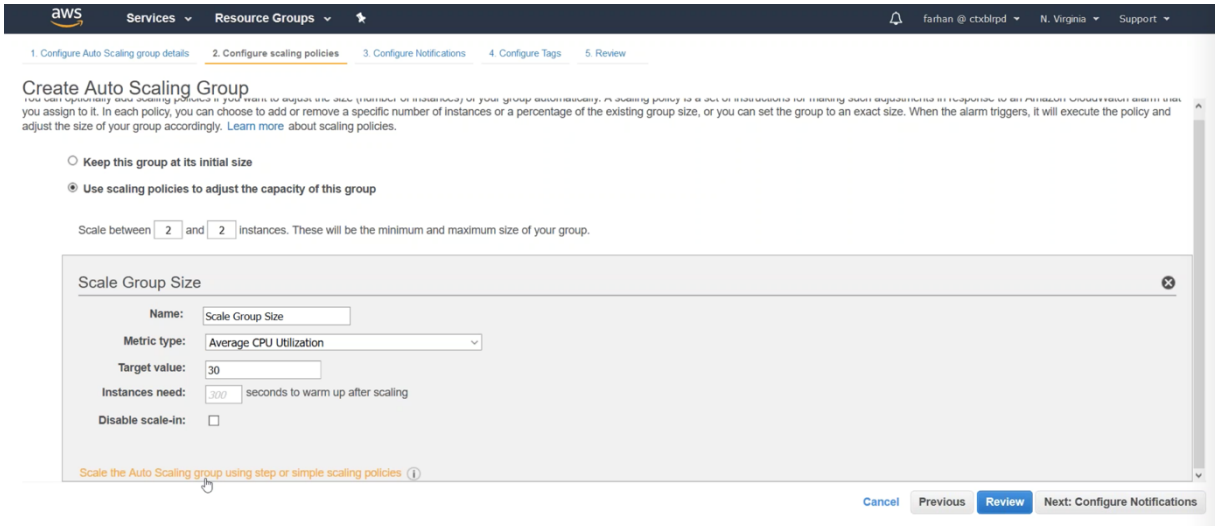
> 注:
>
> サブネットは、Citrix ADC サブネット IP（SNIP）から到達可能である必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 2:

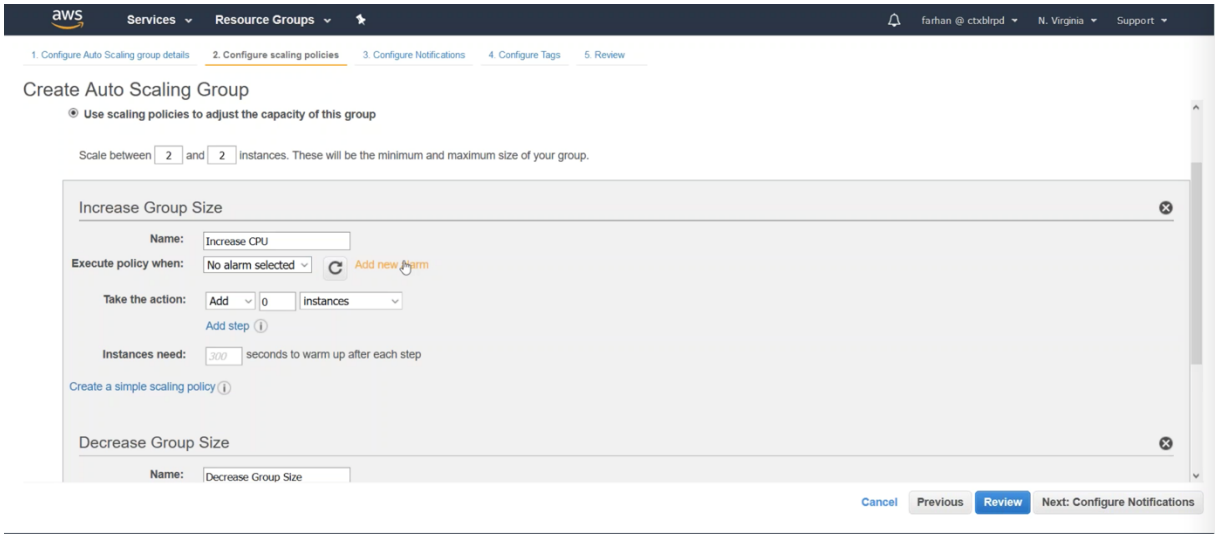
Auto Scaling グループの作成設定ページで、スケーリングポリシーを設定します。このためには、スケーリングポリシーを使用してこのグループの容量を調整するためのラジオボタンをクリックします。次に、ステップまたは単純な スケーリングポリシーを使用して **Auto Scaling** グループをスケーリングします。



手順 3:

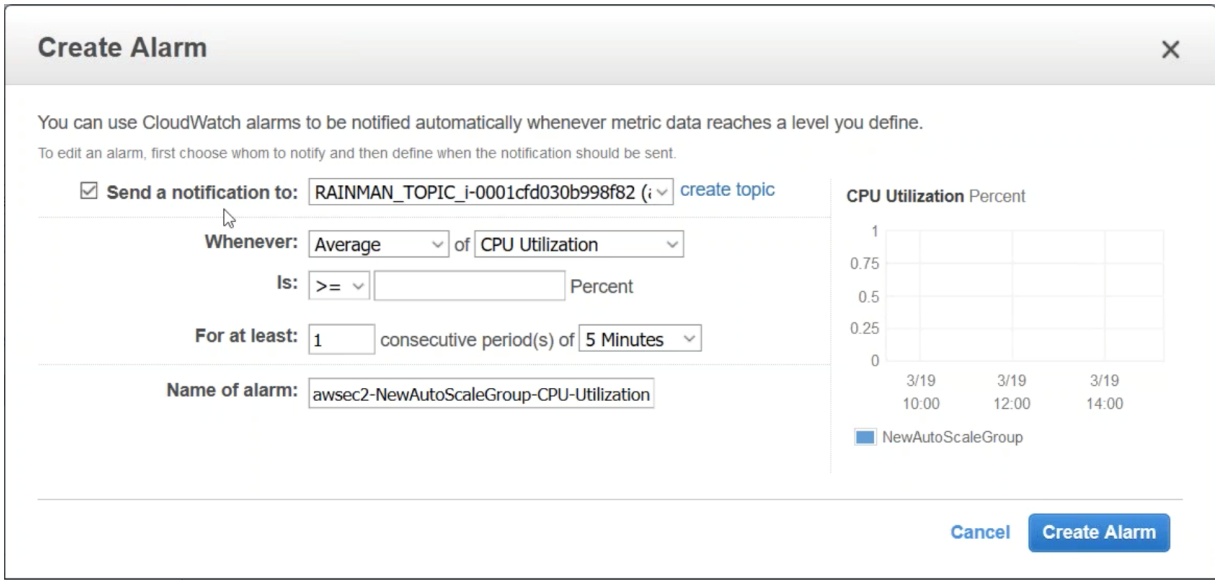
[新しいアラームの追加] を選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 4:

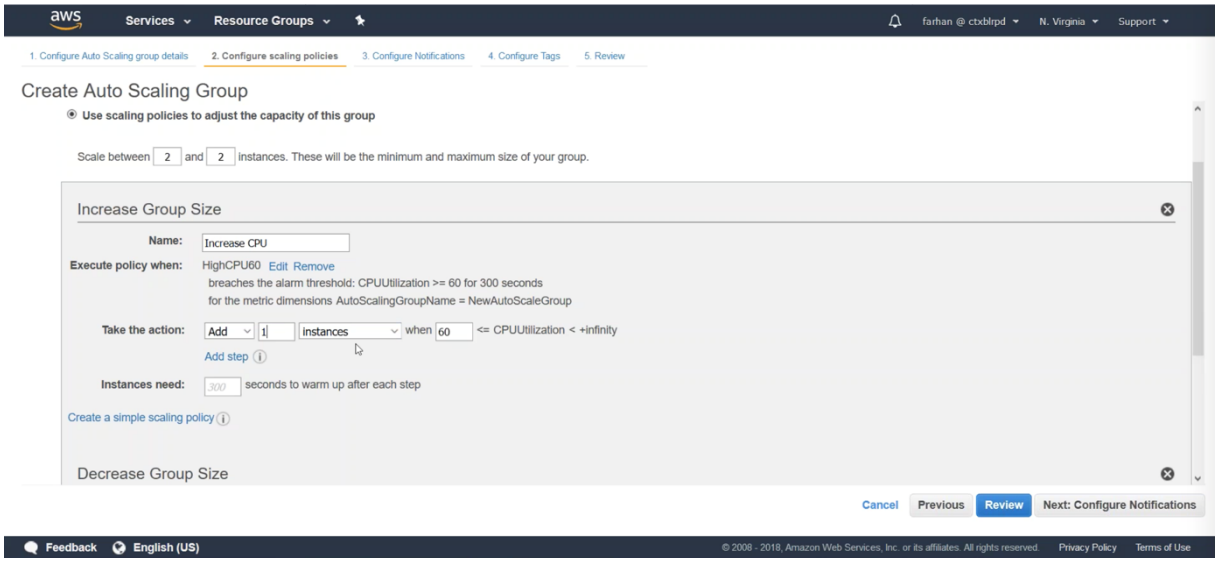
アラームの作成中に、Citrix ADC に通知を送信するように設定します。5 分間連続して 1 回以上の CPU 使用率の平均が 70 以上になるようにアラームを設定します。ポリシーを適用します。



手順 5:

ポリシーがトリガーされたときに 1 つのインスタンスを追加するように Auto Scaling グループを設定します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



手順 6:

同じアラームとポリシーを設定しますが、今回は、CPU の平均が 5 分間 30 未満のときにバックエンドサーバーを削除します。減少ポリシーがトリガーされたときに、減少グループサイズを [削除 1 インスタンス] に設定します。

> 注:
>
> サーバーの削除については、Citrix ADC に、削除対象としてマークされたバックエンドサーバーにトラフィックを送信しないように通知しています。

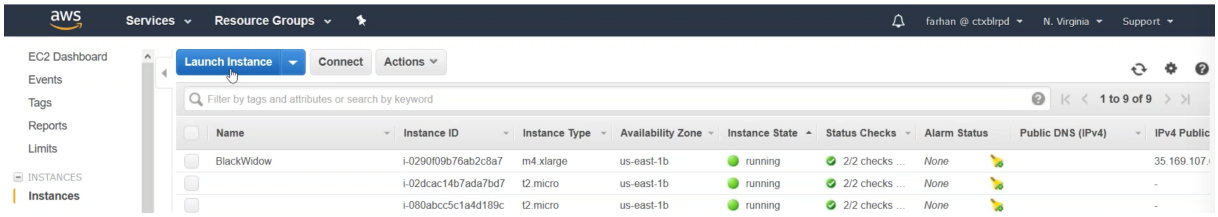
Auto Scaling グループを確認および作成するには、[通知の設定] および [タグの設定] をクリックします。

> 注:
>
> Min 変数と Max 変数は、Auto Scaling グループ内で作成および実行されるインスタンスの最小数と最大数を設定するように設定できます。現在、AWS では、1 つのネットワークインターフェイスだけで追加のインスタンスをスピンアップできます。

AWS で **Citrix ADC** を作成する

手順 1:

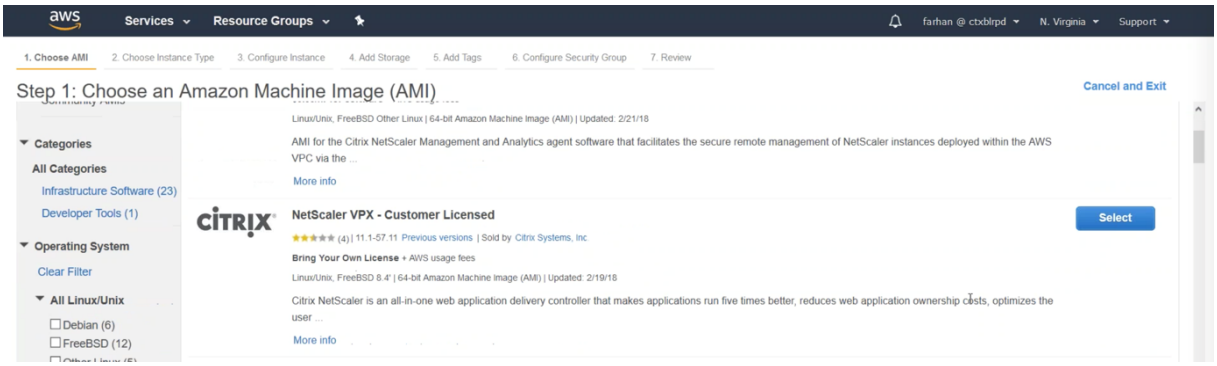
AWS リソースグループにサインインし、**EC2** に移動します。EC2 で **[**インスタンス**] > [**インスタンス**]** に移動します。



手順 2:

© 1999–2021 Citrix Systems, Inc. All rights reserved.

左側の AWS Marketplace に移動し、「Citrix ADC」を検索します。「**Citrix Networking VPX-**カスタマーライセンス」を選択します。Auto Scaling を使用するには、バージョン番号が 12.0.51.x であることを確認してください。以前のバージョンを選択して、Auto Scaling をサポートする Citrix ADC のバージョンを選択できます。



手順 3:

左側の AWS Marketplace に移動し、「Citrix ADC」を検索します。「**Citrix Networking VPX-**カスタマーライセンス」を選択します。Auto Scaling を使用するには、バージョン番号が 12.0.51.x であることを確認してください。以前のバージョンを選択して、Auto Scaling をサポートする Citrix ADC のバージョンを選択できます。

インスタンスタイプを選択します。たとえば、汎用 m4.xlarge の 4vCPU や 16gb RAM などです。[次へ] をクリックします。

手順 4:

[インスタンスの詳細の構成] タブで、[サブネット] を選択します（3 つのサブネットは、最終的に NSIP、SNIP、VIP/ゲートウェイ用に構成する必要があります）。また、IAM ロールを追加する必要があります。新しい IAM ロールを作成するときにクリックします。次のステップで見つかった IAM ロールを追加します。この役割を作成したら、Citrix ADC クラウドプロファイルに追加する必要があります。

手順 5:

クラウドプロファイルの設定は次のとおりです。

CloudFormation テンプレートは、デフォルトでは以下の IAM ロールを作成し、割り当てます

```
"Version": "2012-10-17",
"Statement": [
   {

       "Action": [
       "ec2:DescribeInstances",
       "ec2:DescribeNetworkInterfaces",
       "ec2:DetachNetworkInterface",
       "ec2:AttachNetworkInterface",
       "ec2:StartInstances",
       "ec2:StopInstances",
       "ec2:RebootInstances",
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
13          "autoscaling:\*",
14          "sns:\*",
15          "sqs:\*"
16           “iam: SimulatePrincipalPolicy”
17           “iam: GetRole”
18          ],
19          "Resource": "\*",
20          "Effect": "Allow"
21       }
22
23   ]
24   }
25
26  <!--NeedCopy-->
```

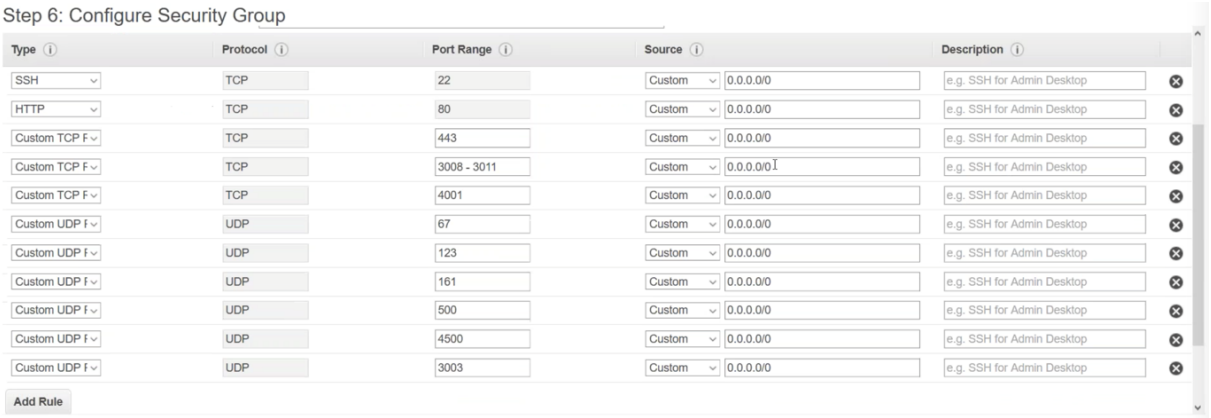
手順 6:

[ストレージの追加] オプションをクリックします。[タグの追加] タブで、[キー] 値を [名前] に設定し、[値] を [Citrix ADC-Autoscale] に設定して、これらの EC2 リソースにタグを付けます。

手順 7:

[**Configure Security Group**] タブで、次のポート要件で新しいセキュリティグループを作成します。

インスタンスを確認して起動します。

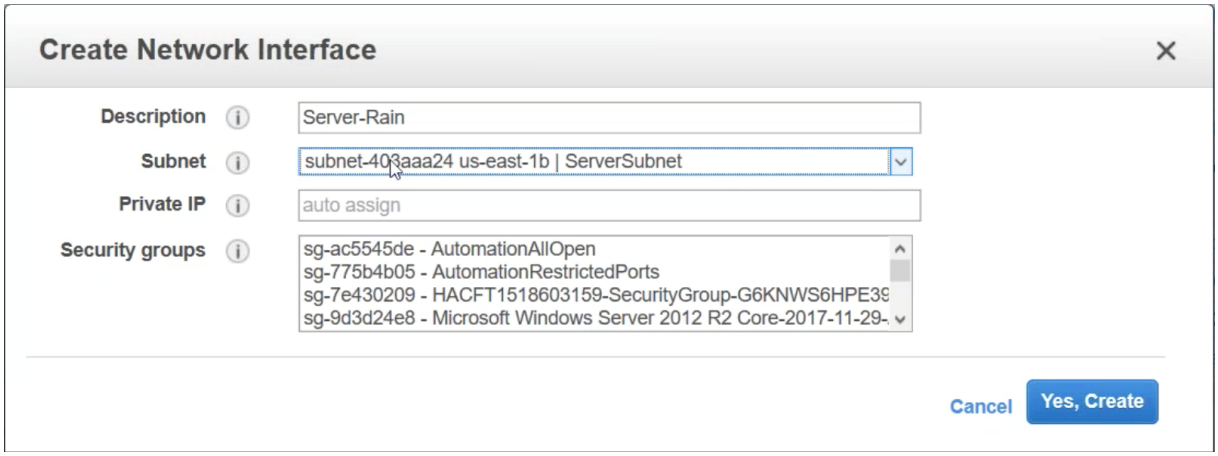


手順 8:

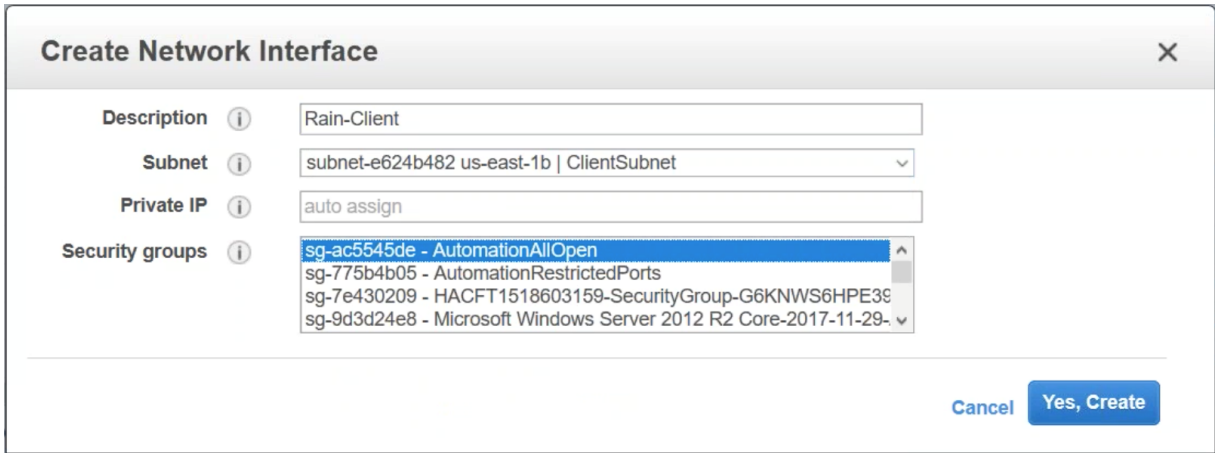
[ネットワークとセキュリティ] **>** [ネットワークインターフェイス] に移動し、[ネットワークインターフェイスの作成] をクリックします。

説明を追加し、サブネットを選択します。このサブネットは SNIP に使用されるため、内部ネットワークのサブネットに配置する必要があります。また、前の手順でクレートされたセキュリティグループを選択します。[**Yes, Create**] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



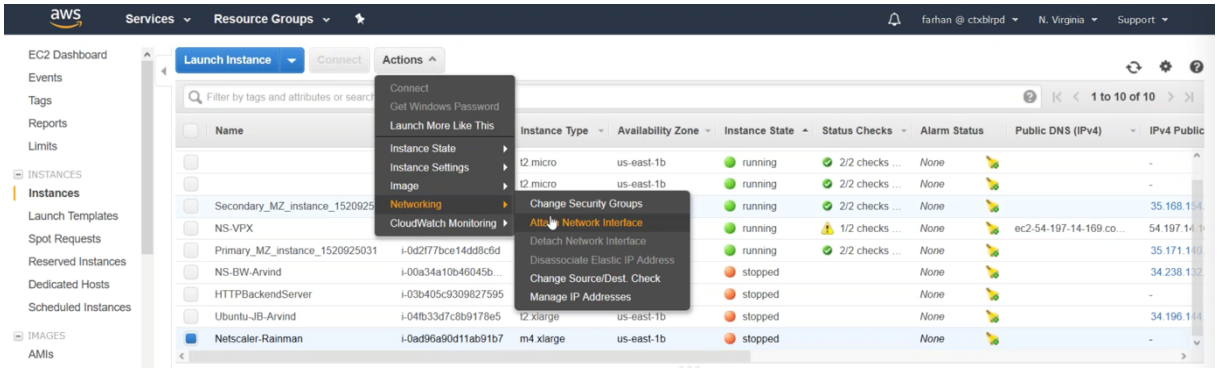
追加のネットワークインターフェイスを追加します。これは、ゲートウェイ/LB VIP 用のパブリック向けサブネットです。説明を作成し、上記で設定したセキュリティグループを選択します。



手順 9:

インスタンスに戻り、Citrix ADC を選択します。ネットワークインターフェイスを Citrix ADC に追加するには、インスタンスを停止する必要があります。「アクション」リストで「インスタンスの状態」を選択し、「停止」をクリックします。

もう一度 [アクション] ボタンをクリックし、[ネットワークとネットワークインターフェイスの接続] に移動します。



NSIP インターフェイスはすでに VM に接続されており、次に追加するインターフェイスは LB-VIP であり、続いて

© 1999–2021 Citrix Systems, Inc. All rights reserved.

SNIP 用のサーバ/内部インターフェイスを追加する必要があります。ネットワークインターフェイスがアタッチされると、インスタンスを起動できます。

新しい Elastic IP を設定し、NSIP インターフェイスに関連付けます。

AWS Auto Scaling と統合するように **Citrix ADC** を設定する

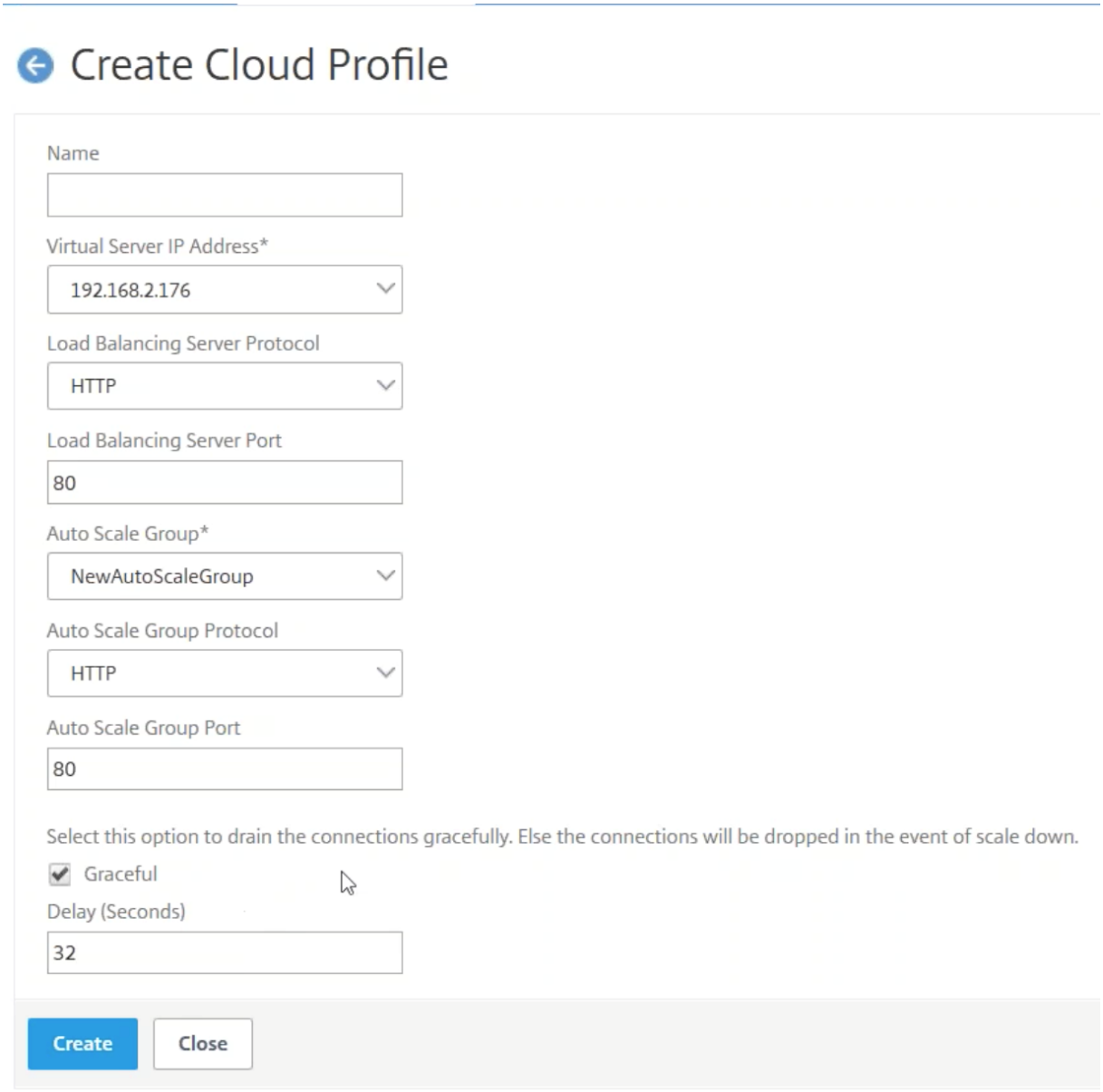
手順 1:

この実習ガイドの前のステップで NSIP に関連付けた Elastic IP に移動して、Citrix ADC 管理コンソールにアクセスします。

Citrix ADC を構成する最初のステップは、クラウドプロファイルをアタッチすることです。[**AWS**]、[クラウドプロファイル**]** の順にクリックします。次に、[追加] をクリックして、クラウドプロファイルを作成します。

クラウドプロファイルの名前を指定します。仮想サーバーの IP アドレスが入力され、Citrix ADC 上の内部 IP と相関関係があるはずです。Auto Scale Group は、このラボガイドの前のステップで作成したものです。[**Graceful**] を選択すると、バックエンドインスタンスのタイムアウトが削除され、すべてのパケット転送が完了し、猶予期間内にセッションが終了しないようにできます。猶予期間の遅延は調整できます。

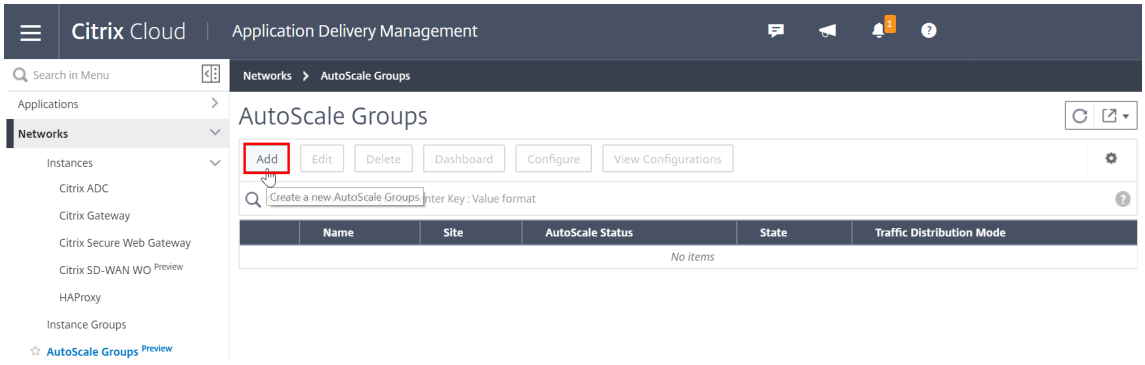
© 1999–2021 Citrix Systems, Inc. All rights reserved.



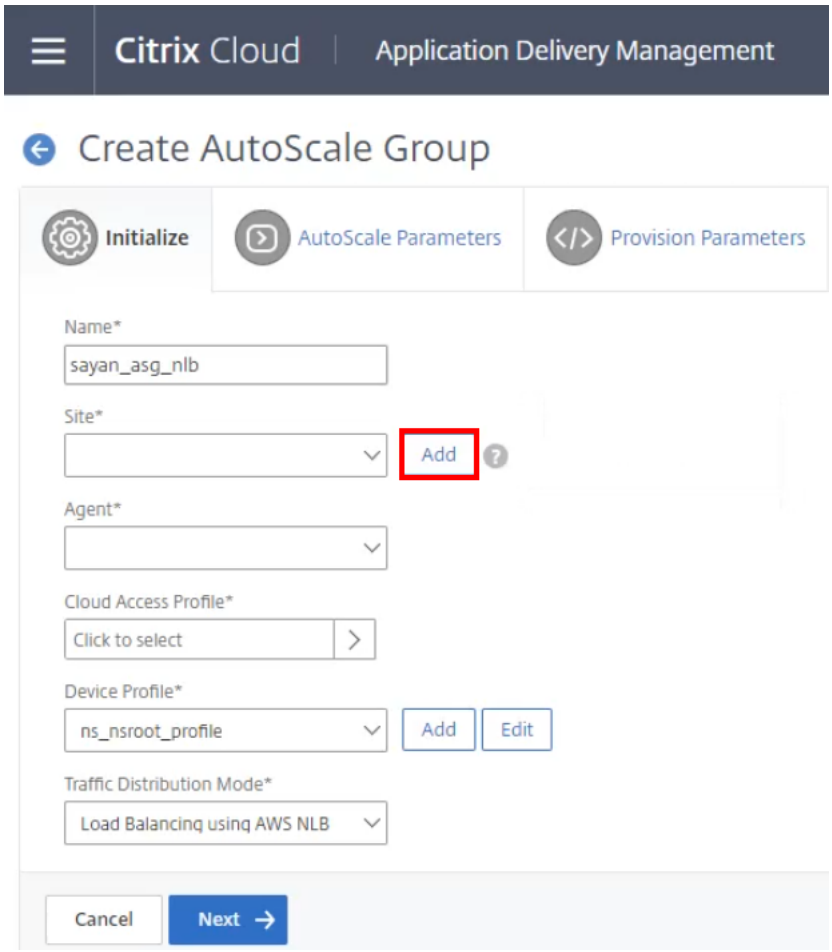
AWS で **Citrix ADC** フロントエンド **Auto Scaling** を構成します

1. Auto Scaling グループを作成するには、Citrix ADM にサインインします。
2. **[**ネットワーク**] > [AutoScale** グループ] に移動し、[追加] をクリックしてグループ名を作成します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



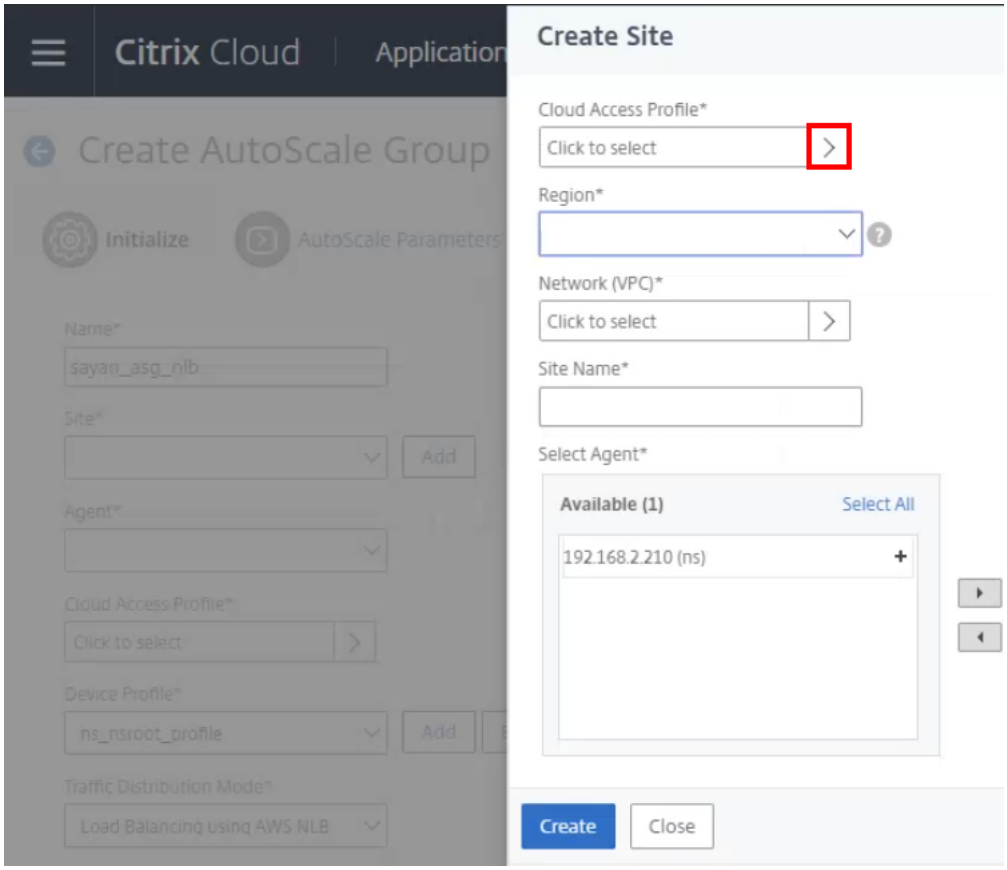
3. [サイト] 設定で、[追加] をクリックします。



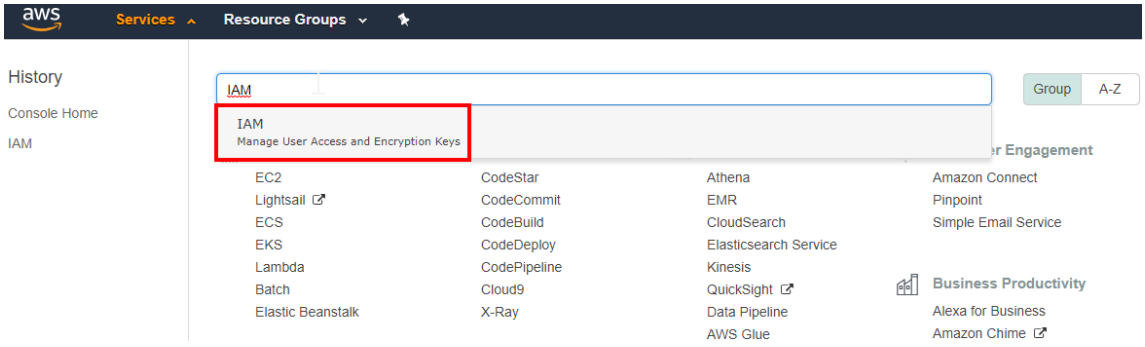
クラウドアクセスプロファイルの作成

1. サイトを作成するときに、クラウドアクセスプロファイルで **AWS** を追加します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

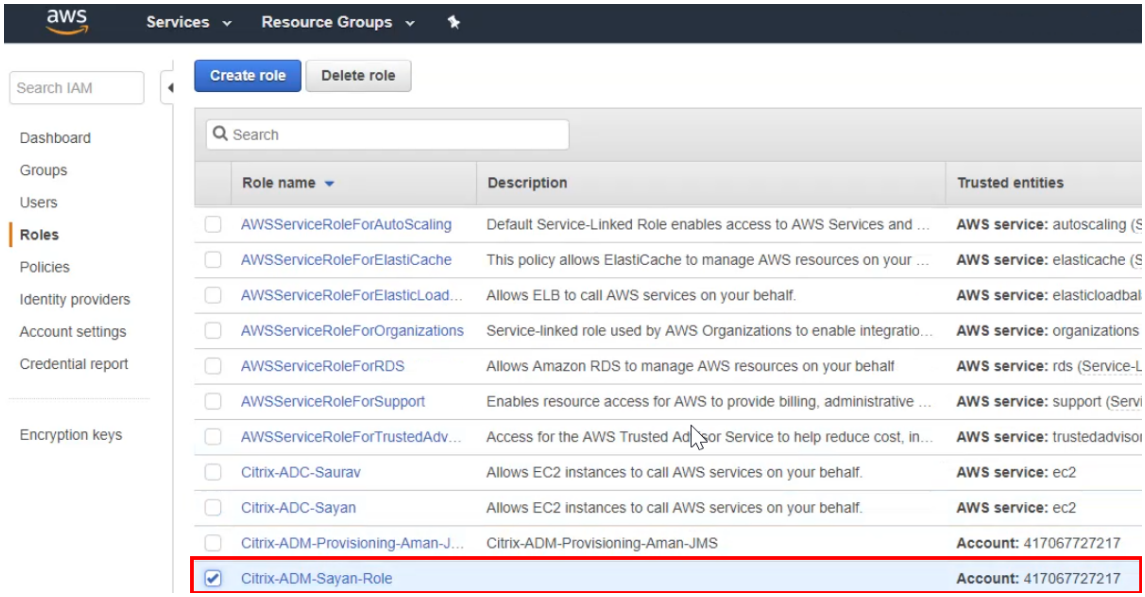


2. プロフィールに名前を付け、AWS ポータルにサインインします。**ID** とアクセス管理 **(IAM)** サービスを検索して、ユーザーアクセスと暗号化キーを管理します。

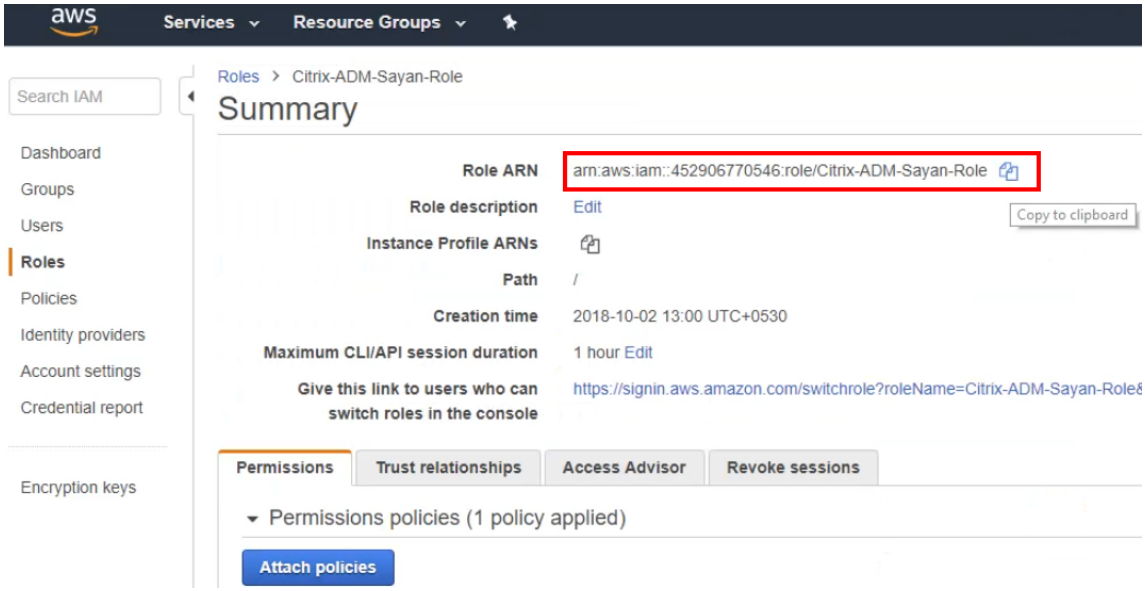


3. **IAM** ダッシュボードで、左側のパネルで [**Roles**] を選択し、対応する Citrix ADM ロールを検索します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



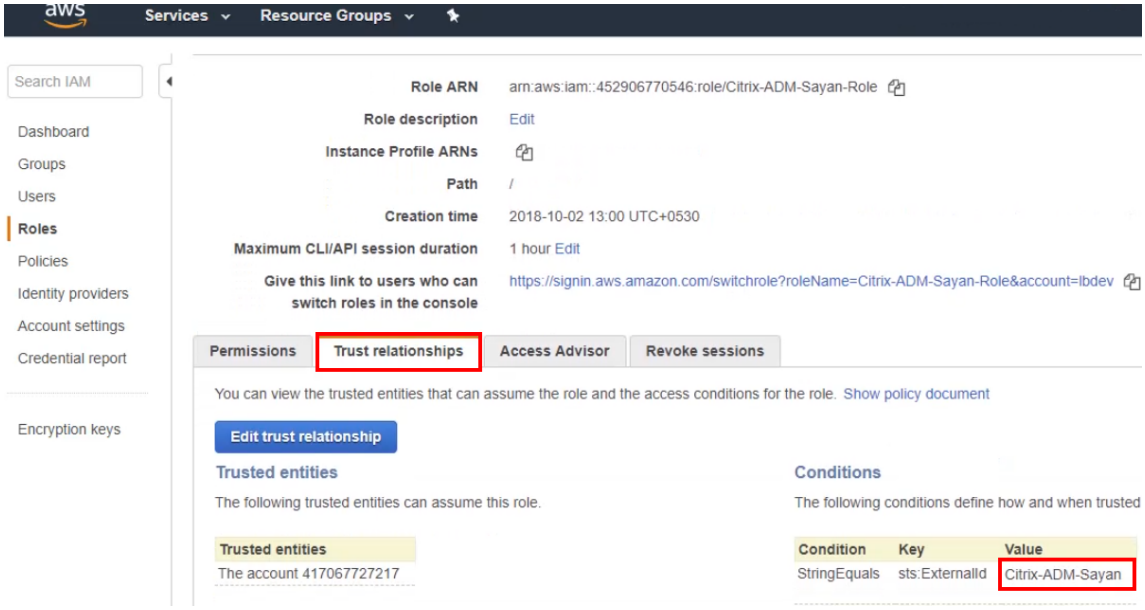
4. ロール **ARN** をクリップボードにコピーします。



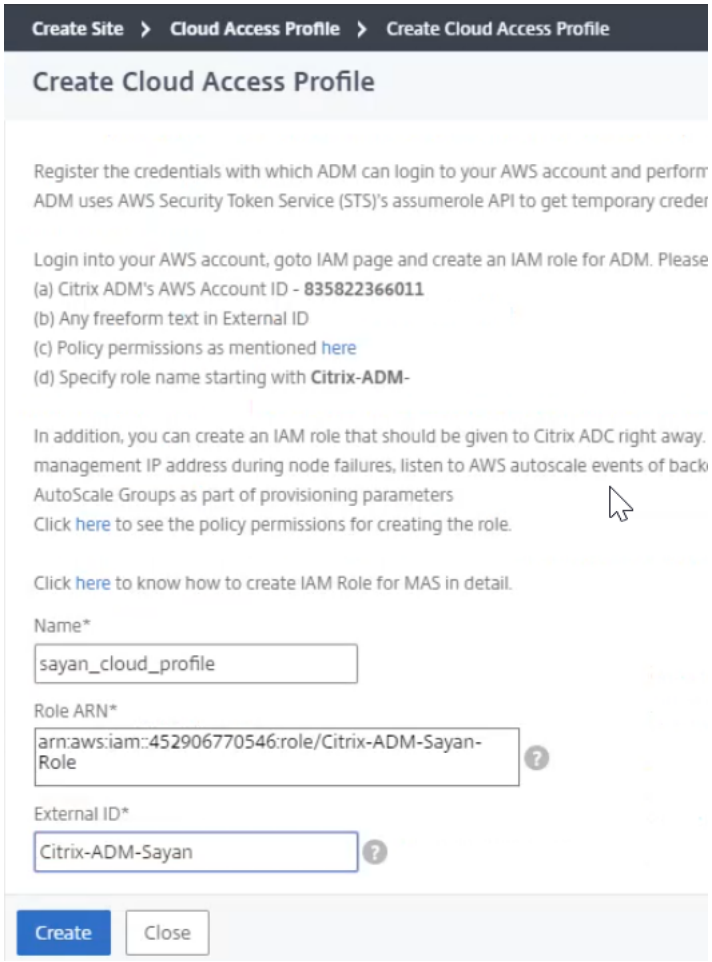
5. 名前をコピーしたら、Citrix ADM コンソールに戻り、ロール **ARN** テキストフィールドに名前を貼り付けます。

6. 外部 ID を取得するには、AWS ロールダッシュボードに戻り、[信頼関係] タブに移動し、[条件] から値をコピーします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

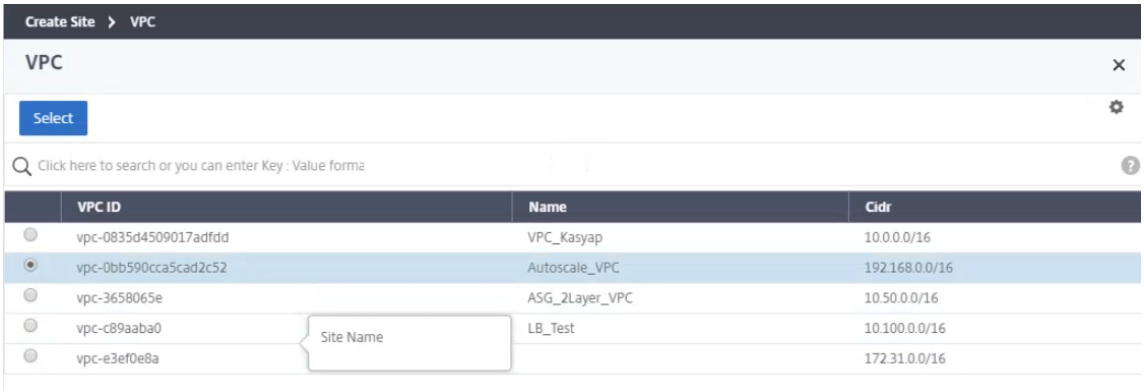


7. Citrix ADM コンソールで、値を 外部 **ID** フィールドに貼り付け、「作成」をクリックします。

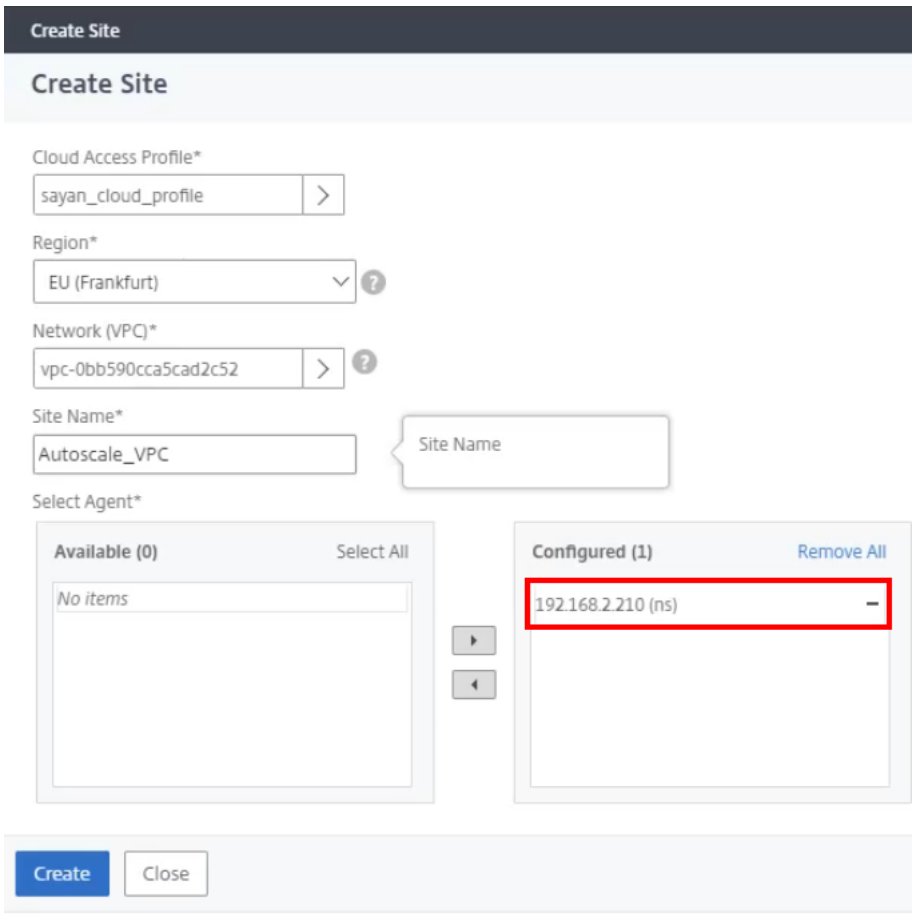


8. リージョンを選択し、適切な VPC ネットワークを選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

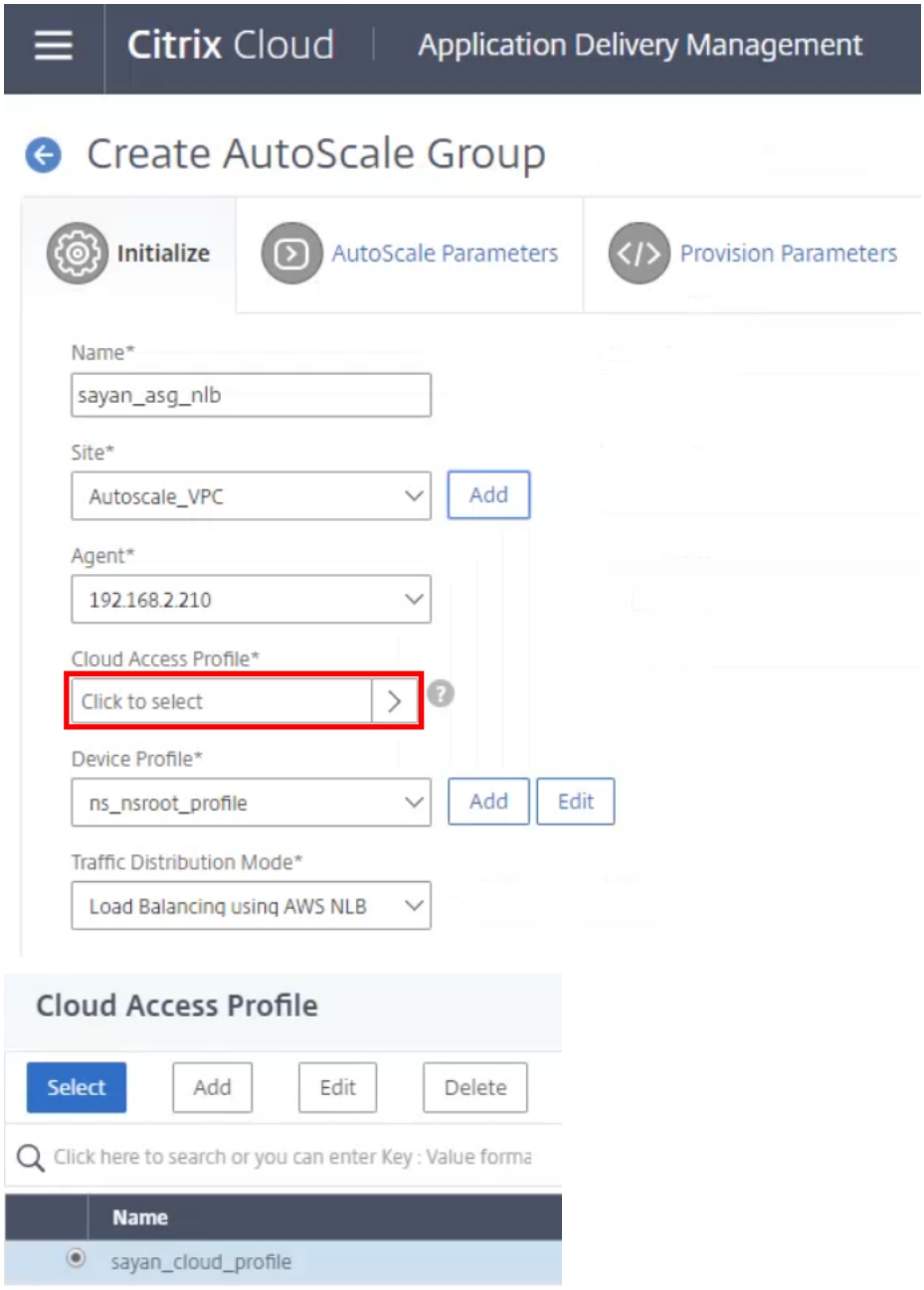


9. エージェントを [使用可能] から [構成済み] に移動します。



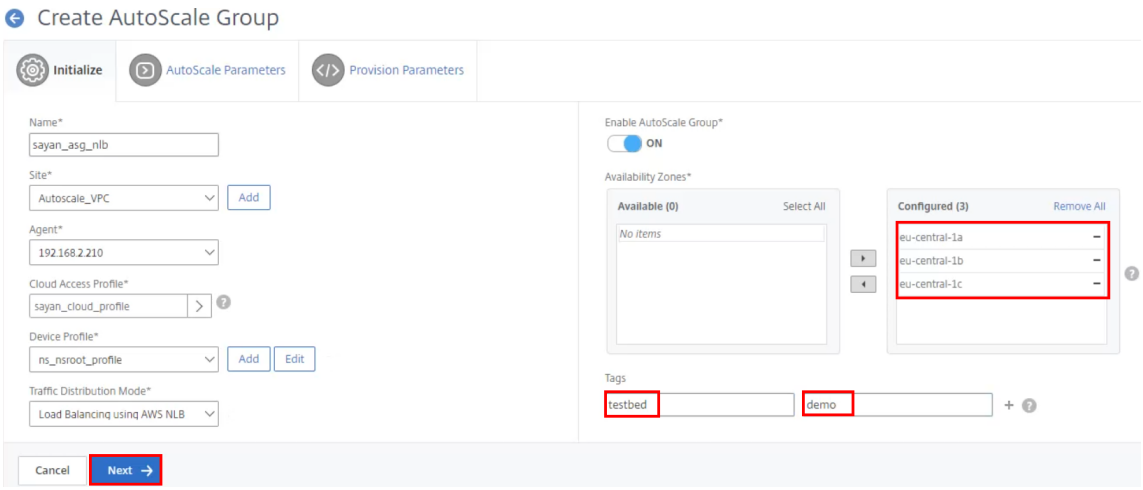
10. 対応する クラウドアクセスプロファイルを選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



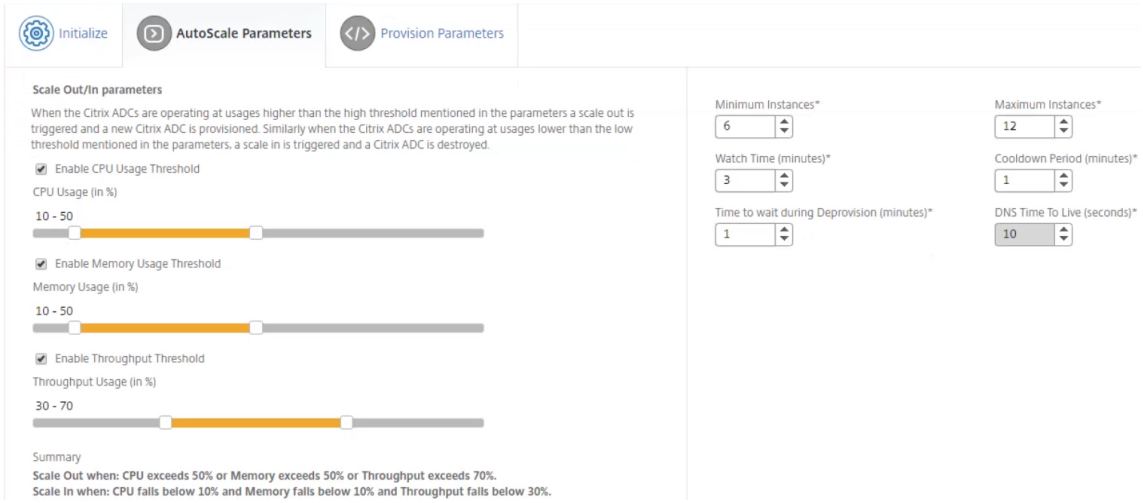
11. ロードされたら、アベイラビリティーゾーンを **[使用可能]** から **[構成済み]** に移動し、対応するタグを **AutoScale** グループに追加します。**[次へ]** を選択して、**AutoScale** パラメーターの設定を開始します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



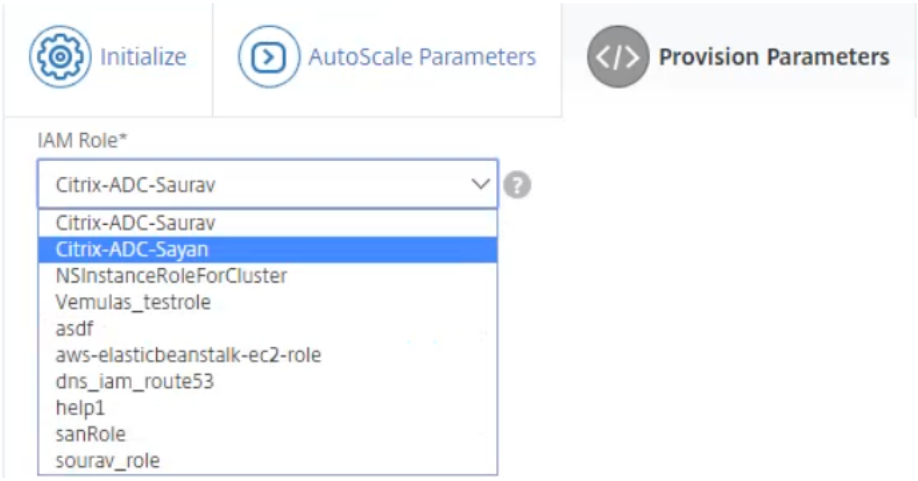
AutoScale パラメーターを設定する

1. AutoScale パラメーターを設定するときは、**[**しきい値**]** と **[**パラメーター**]** を希望の設定に調整します。次に、[次へ] をクリックして、プロビジョニングパラメーターの設定を開始します。

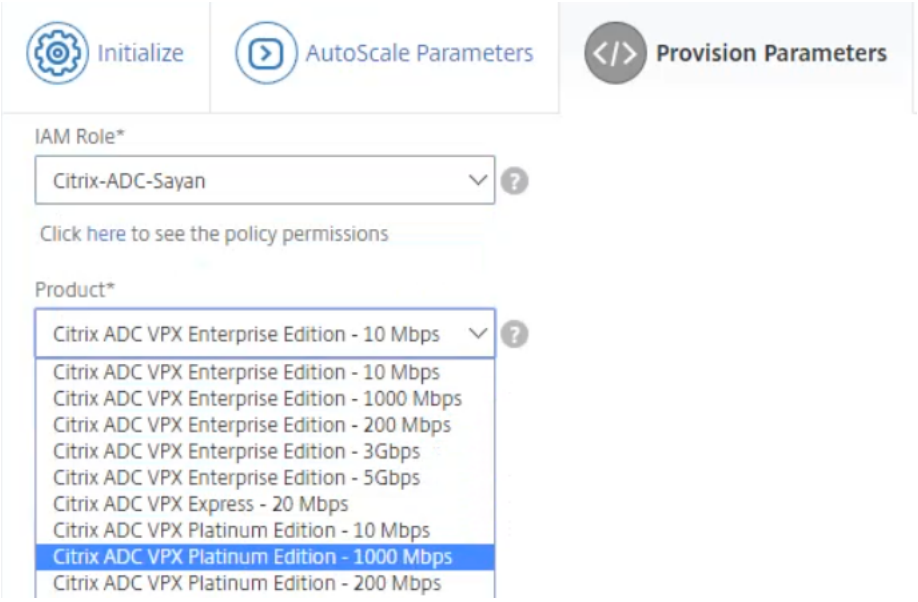


2. **[**プロビジョニングパラメーター**]** セクションで、**[IAM** ロール**]** フィールドからロールを選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



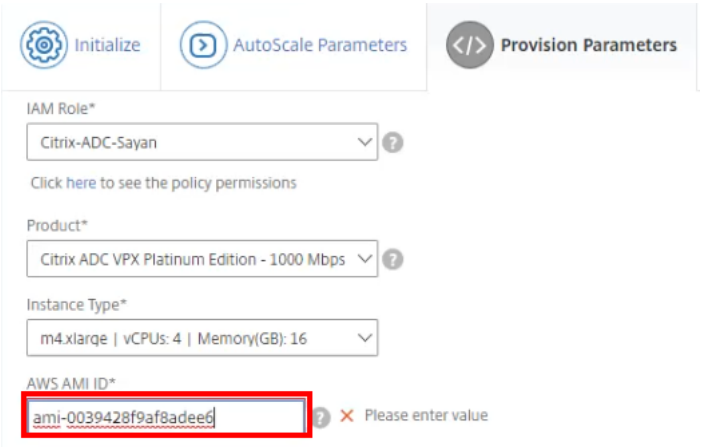
3. 適切な Citrix ADC 製品とエディションを選択します。



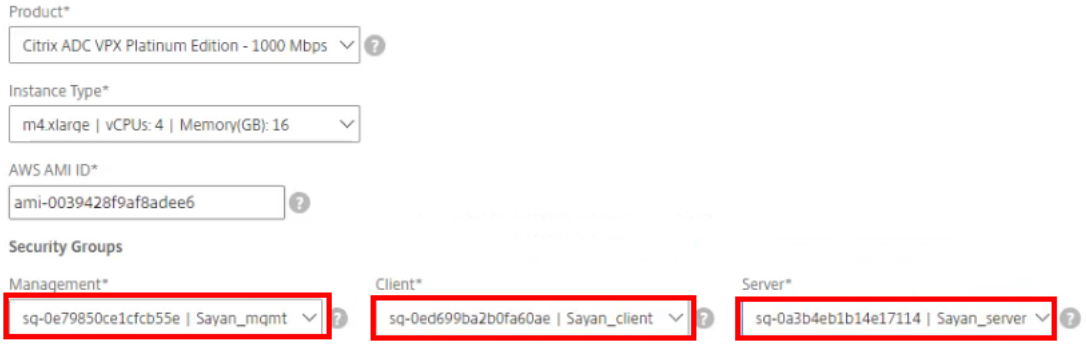
4. AWS の特定のインスタンスから Amazon マシンイメージ（AMI）ID を収集します。**AWS AMI ID** フィールドにその **ID** を入力します。

```
AMI ID:
--------------
ami-0039428f9af8adee6
```

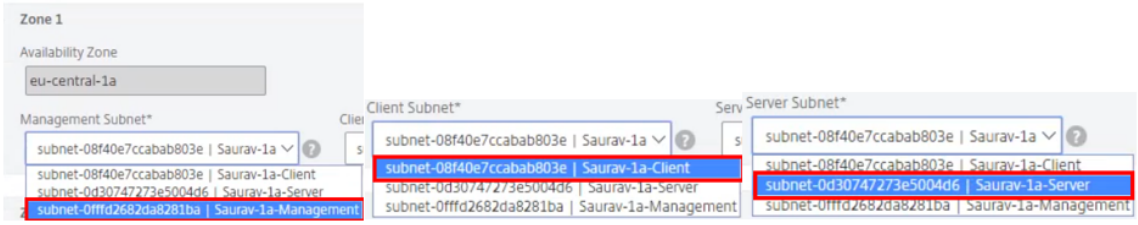
© 1999–2021 Citrix Systems, Inc. All rights reserved.



5. **AMI ID** を追加したら、セキュリティグループを適切なグループで更新します。

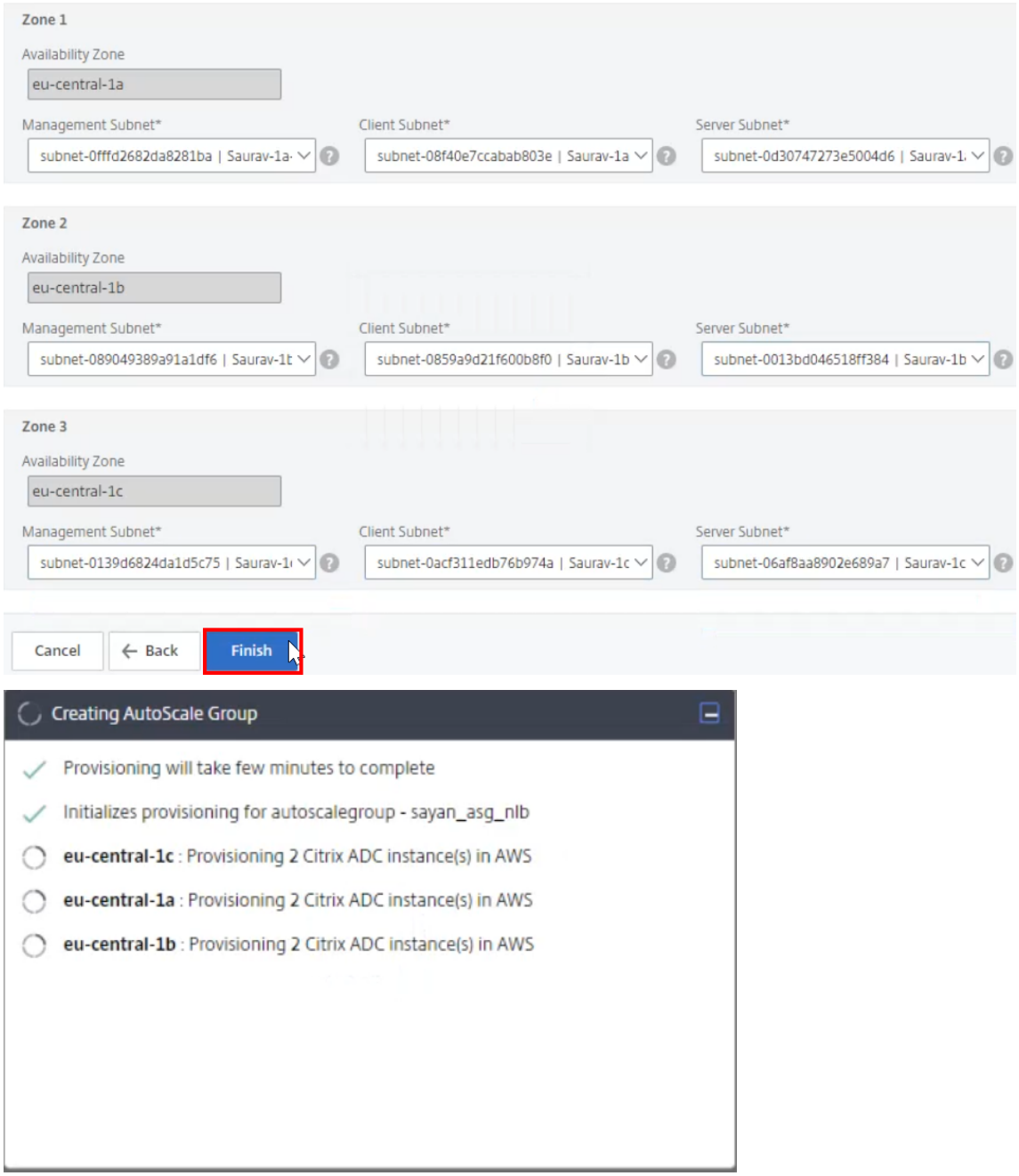


6. ゾーン 1、2、3 の構成を開始するには、対応する管理サブネット、クライアントサブネット、およびサーバーサブネットを割り当てます。



7. ［完了］をクリックして、この Auto Scaling グループの設定を作成します。作成プロセスには最大で 10 ～20 分かかります。

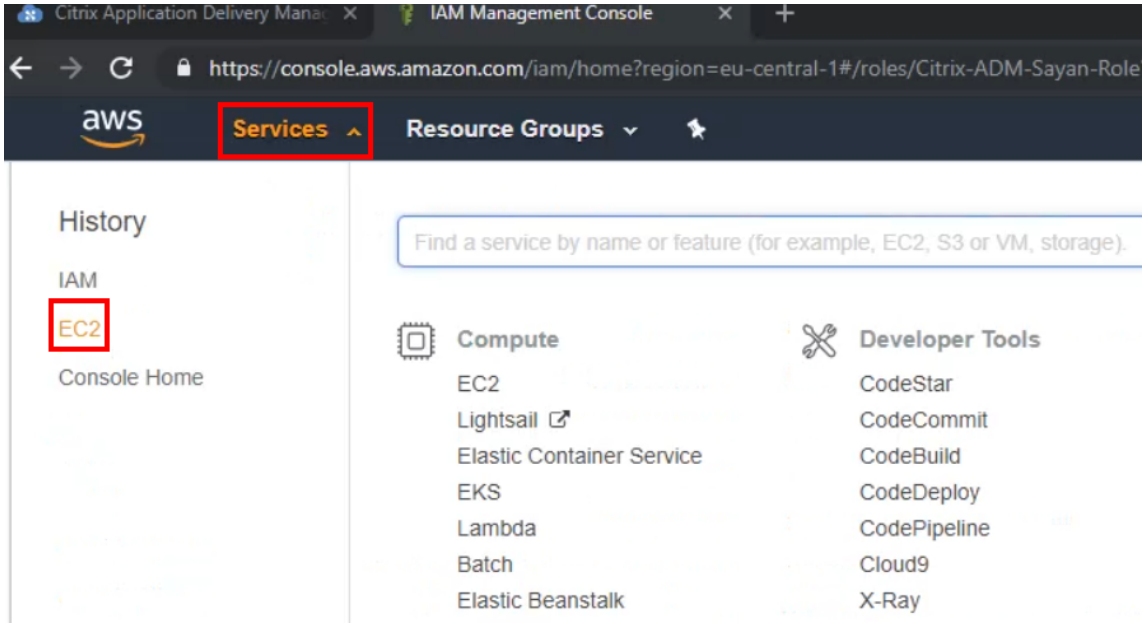
© 1999–2021 Citrix Systems, Inc. All rights reserved.



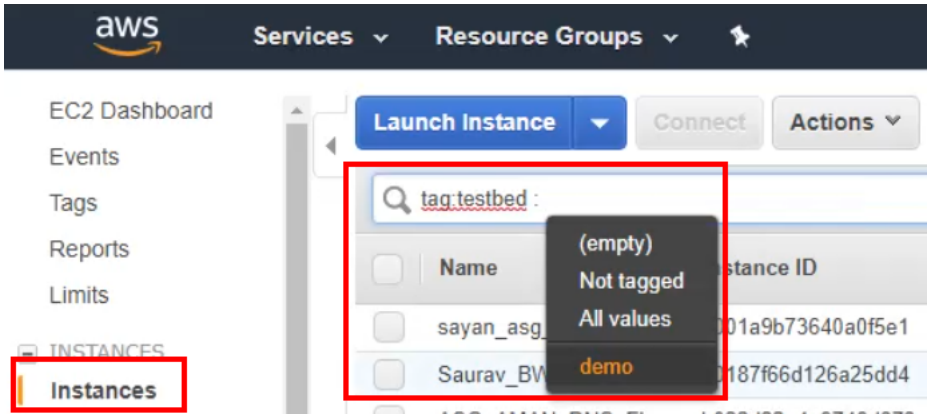
AWS でのインスタンスの初期化

1. Auto Scaling グループの作成中に、AWS コンソールを開き、[サービス] タブに移動します。**Amazon Elastic Compute Cloud**（**EC2**）サービスを選択します。

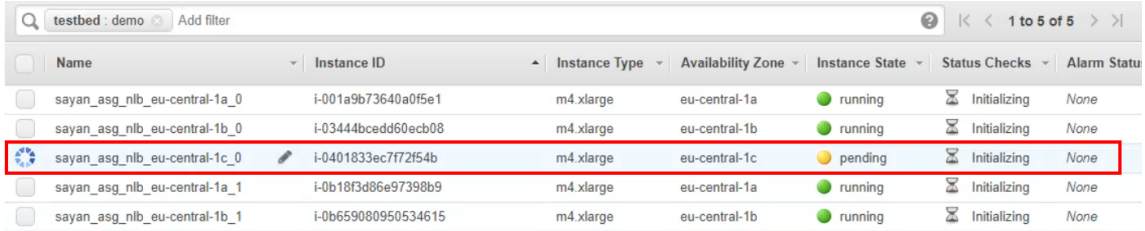
© 1999–2021 Citrix Systems, Inc. All rights reserved.



2. EC2 ダッシュボードで、[インスタンス] タブを選択し、[**AutoScale** グループ] セクションで設定されたタグを使用してフィルタリングします。

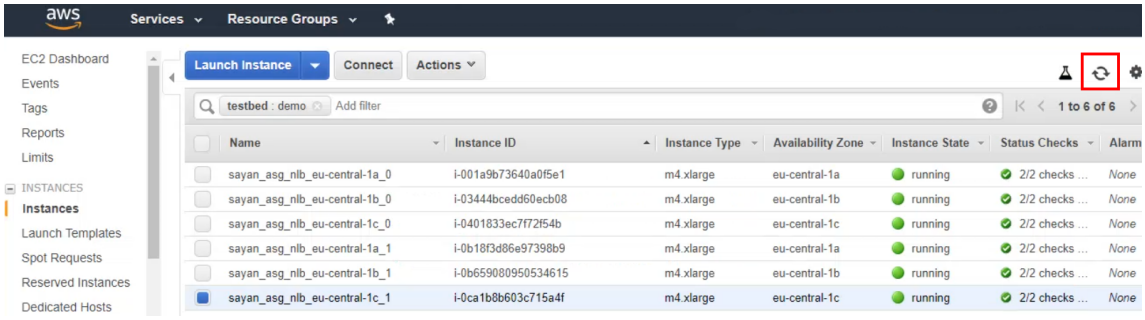


3. フィルタリングすると、まだ初期化されている保留中のインスタンスが表示されます。



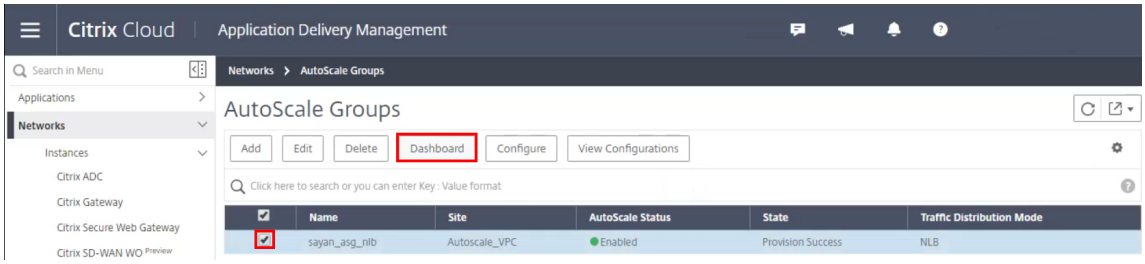
4. インスタンスは、作成後に初期化を完了する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

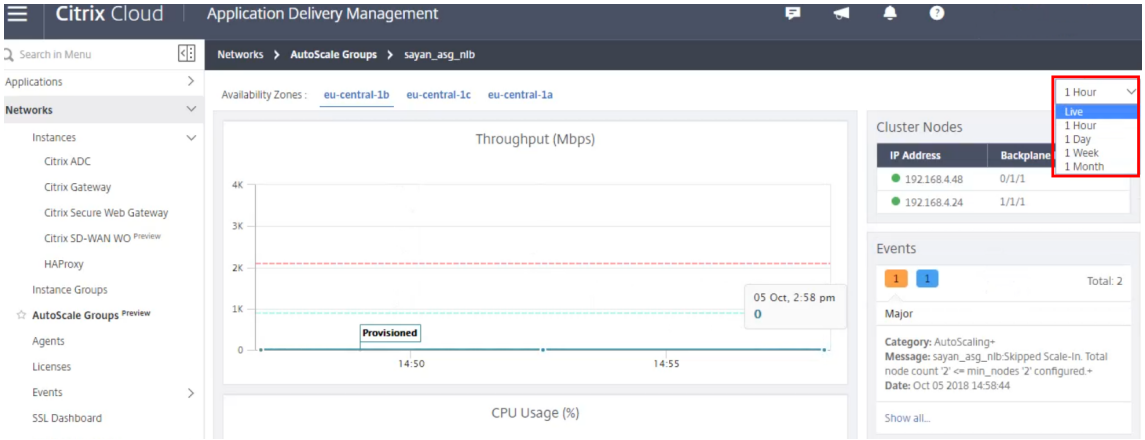


Auto Scaling グループイベントをモニタリングする

1. Auto Scaling グループを作成したら、グループを選択し、[**AutoScale** グループ] ダッシュボードに進みます。



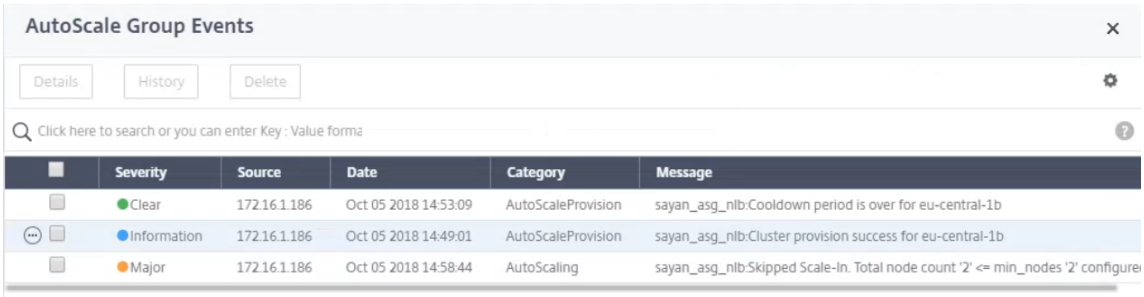
2. 特定の期間を除外して、Auto Scaling グループをモニタリングします。リアルタイムの洞察を得るには、モニタリング期間を [**Live**] に変更します。



3. グラフに表示されている次のデータポイントをクリックすると、グループイベントが表示されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

4. 特定のライブイベントを表示するときに、対応する Auto Scaling グループの特定のイベントをモニタリングできます。



Citrix ADM サービスを使用して **Citrix ADC VPX** インスタンスをプロビジョニングする

Citrix ADM Service は、Citrix ADC インスタンスを監視し、アプリケーションの正常性、パフォーマンス、セキュリティを可視化できるクラウドベースのソリューションです。さらに、Provisioning ツールを利用して AWS などのパブリッククラウドでインスタンスを自動作成することで、オンプレミスかクラウドかにかかわらず、複数の場所にある ADC インスタンスの管理も簡素化されます。

前提条件

Citrix ADM サービスを使用して AWS で Citrix ADC インスタンスをプロビジョニングするには、前提条件のドキュメントにまとめられているいくつかの手順を実行する必要があります。詳しくは、「AWS での Citrix ADC VPX インスタンスのプロビジョニング」を参照してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

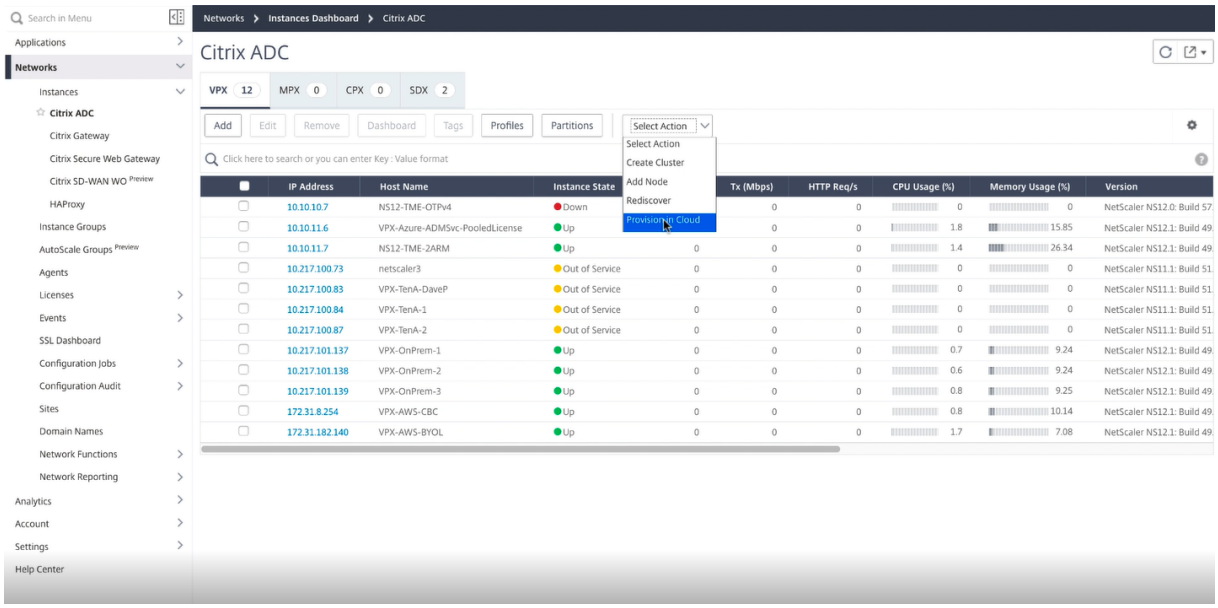
これらの手順には、Citrix ADM で Citrix ADC VPX インスタンスをプロビジョニングする前に、AWS で以下のタスクを実行することが含まれます。

- サブネットの作成
- セキュリティグループの作成
- IAM ロールを作成してポリシーを定義する

IAM ロールは、Citrix ADM サービスが AWS アカウントにアクセスできるようにするアクセス許可で設定する必要があります。すべての設定が完了したら、Citrix ADM サービスを活用して、AWS で VPX インスタンスをプロビジョニングできます。

Citrix ADM サービスを使用して **Citrix ADC VPX** インスタンスをプロビジョニングする

Citrix Cloud ADM サービスにサインインし、「ネットワーク」**>**「インスタンス」**>**「**Citrix ADC**」の順に選択します。次に、**[**アクションの選択] タブで、[クラウドでプロビジョニング] をクリックします。



これにより、プロビジョニングするインスタンスに関する情報を定義するよう求められます。

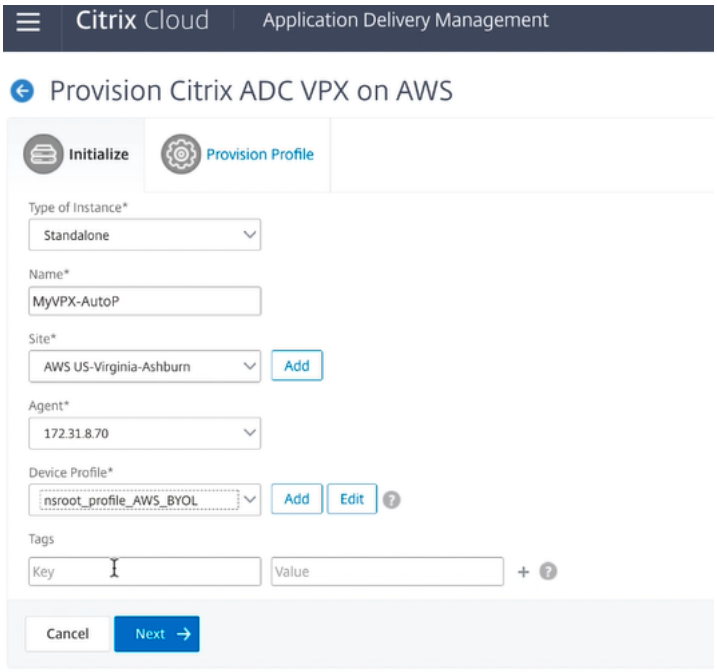
具体的には、以下を定義する必要があります。

- **[**インスタンスのタイプ**]:** [スタンドアロンインスタンス] が選択されています。
- **Name:** プロビジョニング時にインスタンスで採用する名前。
- サイト**:** サイトは、配置を行うエリアまたはリージョンを定義します。
- エージェント**:** エージェントは、サイト内で利用可能な ADM エージェントを指定します。これは、自動プロビジョニングを実行する前に設定する必要があります。この実習を開始する前に、サイトとそのサイトに属するエージェントの両方を作成する必要があります。
- デバイスプロファイル: ユーザー名として「nsroot」と必要なパスワードを持つデバイスプロファイル。Citrix ADC が Citrix ADM によってプロビジョニングされると、ADC の nsroot ユーザーのパスワードは、プロフ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ファイルに記載されているパスワードに設定されます。さらに、このプロファイルは、インスタンスにログインする必要があるときはいつでも、Citrix ADM によって使用されます。

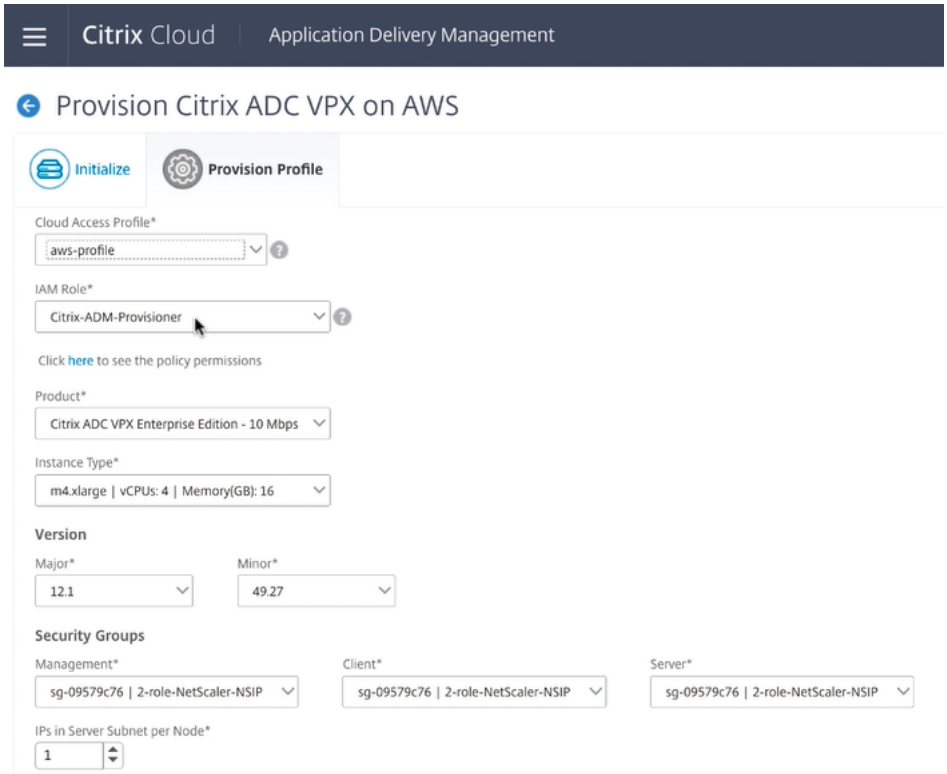
- タグ**:** インスタンスまたはインスタンスのグループのオプションのタグ。



次に、AWS アカウントの クラウドアクセスプロファイルを選択します。これは、Citrix ADM が AWS アカウントにサインインしてエンティティを取得し、プロビジョニングやプロビジョニング解除などの操作を実行するために使用するプロファイルです。Citrix ADM Service は、そのプロファイルを使用して、残りのフィールドにアカウントに関連するオブジェクトを入力します。

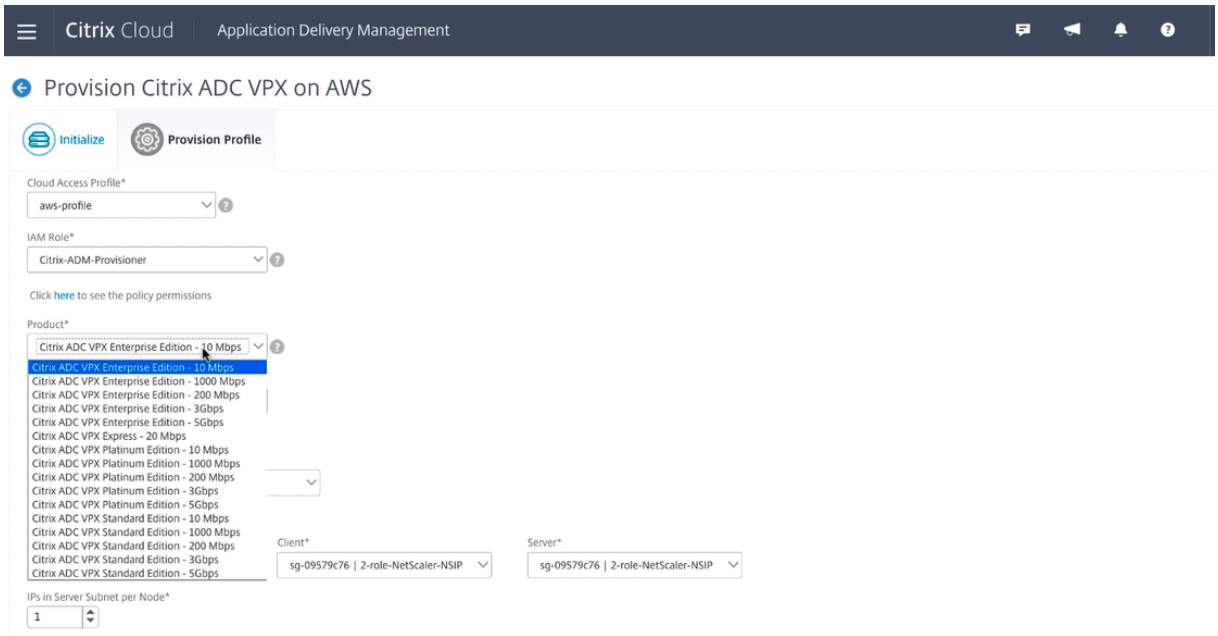
このシナリオでは、Citrix ADM サービスによって VPX インスタンスのプロビジョニングに使用される IAM ロールが事前定義されていますが、他のロールを作成することもできます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



次に、目的のスループットに基づいて、展開する VPX インスタンスの製品エディションを選択する必要があります。

> 注:
>
> VPX Express は、ライセンスなしで VPX インスタンスを展開するために含まれています。



バージョン

© 1999–2021 Citrix Systems, Inc. All rights reserved.

メジャーリリースとマイナーリリースを選択して、実行するソフトウェアのリリースを決定します。

セキュリティグループ

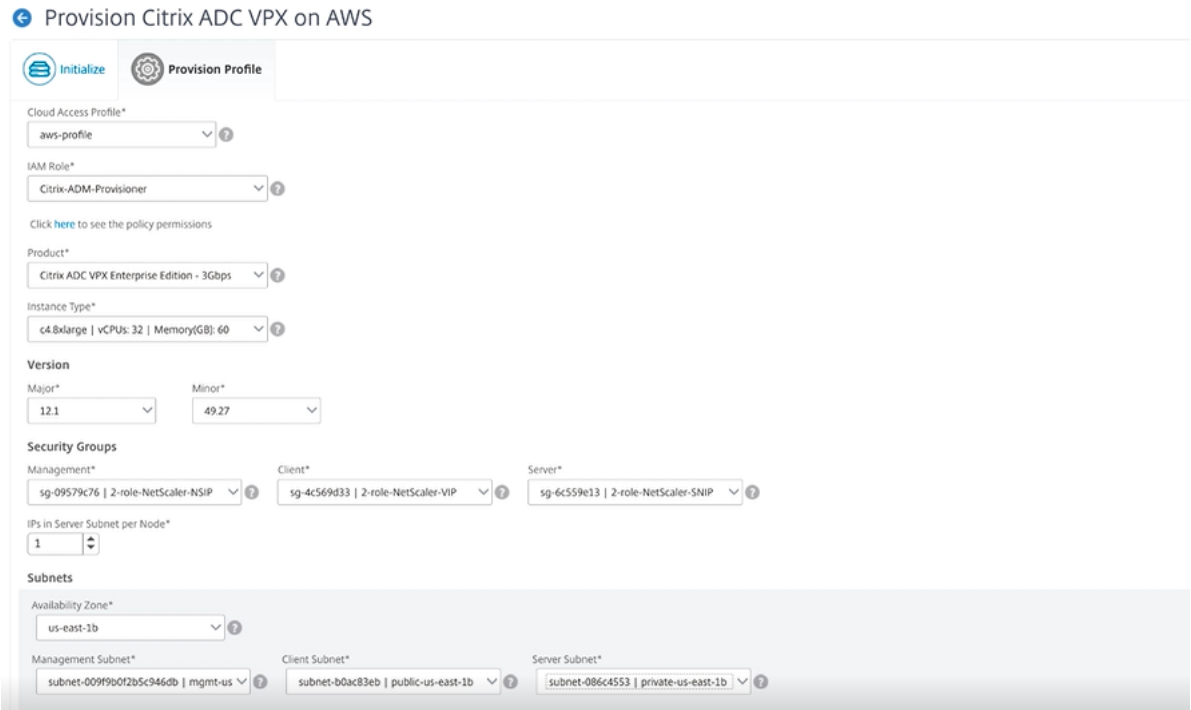
セキュリティグループには、異なる仮想プライベートクラウド（VPC）にアクセスするための事前定義されたアクセス権限が必要です。各インスタンスには 3 つのネットワークインターフェイスまたは vNIC が必要であるため、展開するサービスに 3 つの異なるセキュリティグループを適用する必要があります。

- 1 つはリモート管理用（役割 NSIP）
- 1 つはクライアント側アクセス（ロール VIP）
- サーバ側の通信用（SNIP の役割）

また、このソリューションのスケーラビリティに必要な IP の数を選択する必要があります。

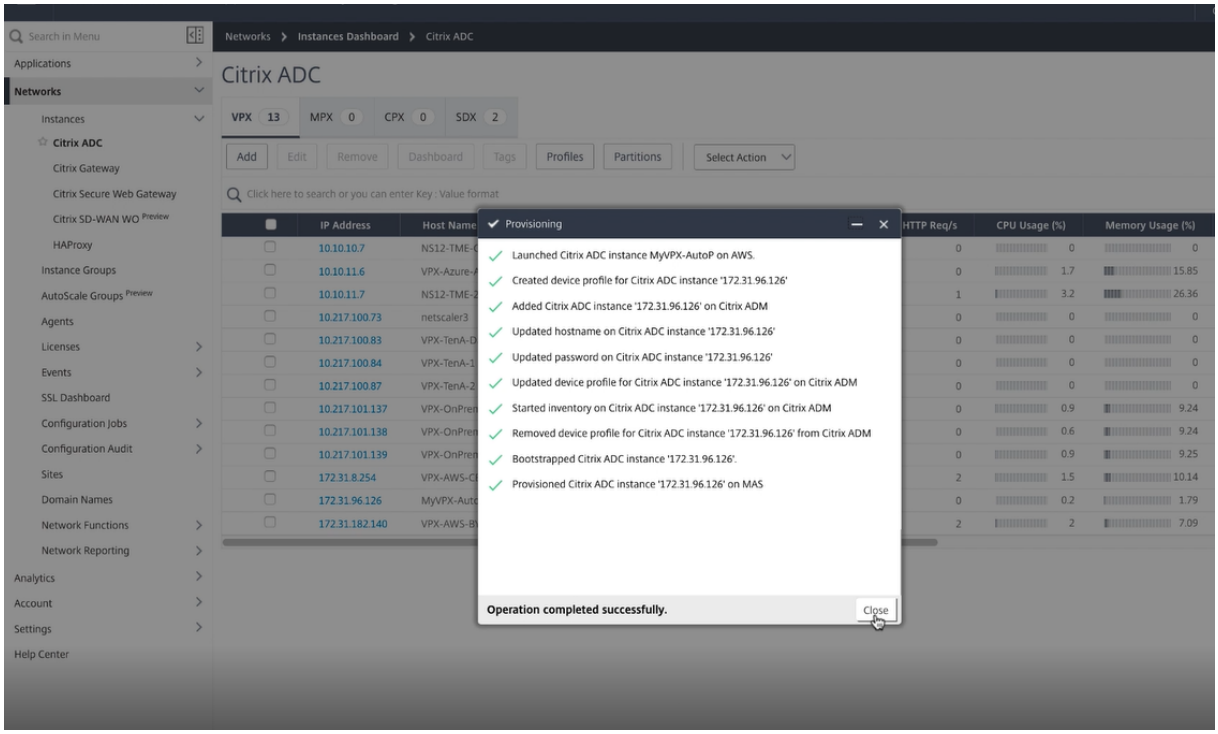
最後に、展開するアベイラビリティーゾーンを選択し、サブネットごとに一致する VPC サブネット情報を定義する必要があります。

- 1 つは管理インターフェイス（NSIP）用
- 1 つはクライアントがアクセスする (VIP)
- SNIP がバックエンドサーバー（SNIP）にアクセスするために 1 つ

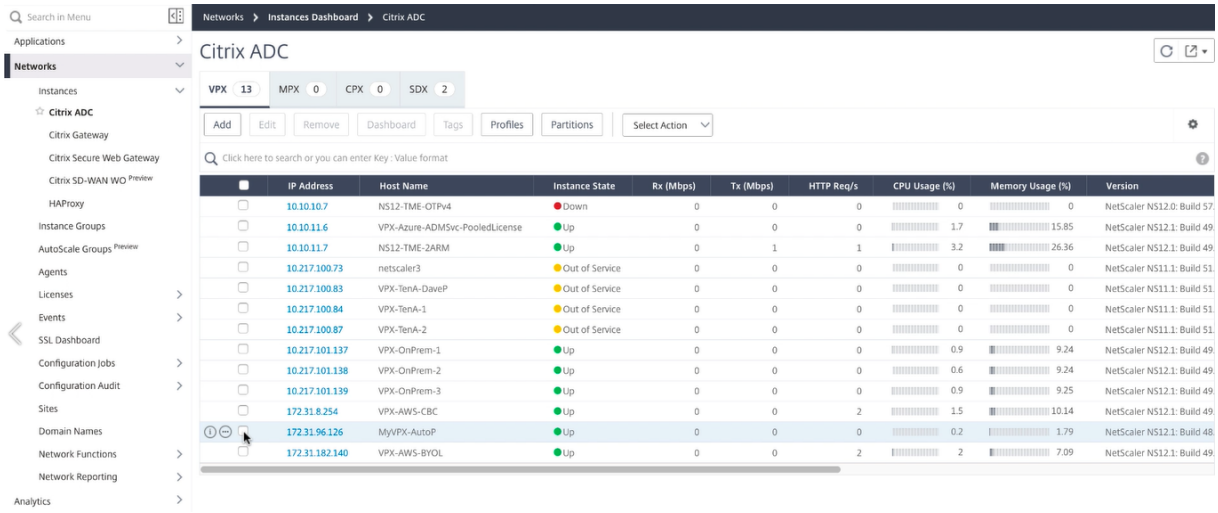


[完了] をクリックすると、展開が開始されます。展開が正常に完了すると、VPX が展開されたという通知を受け取ります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



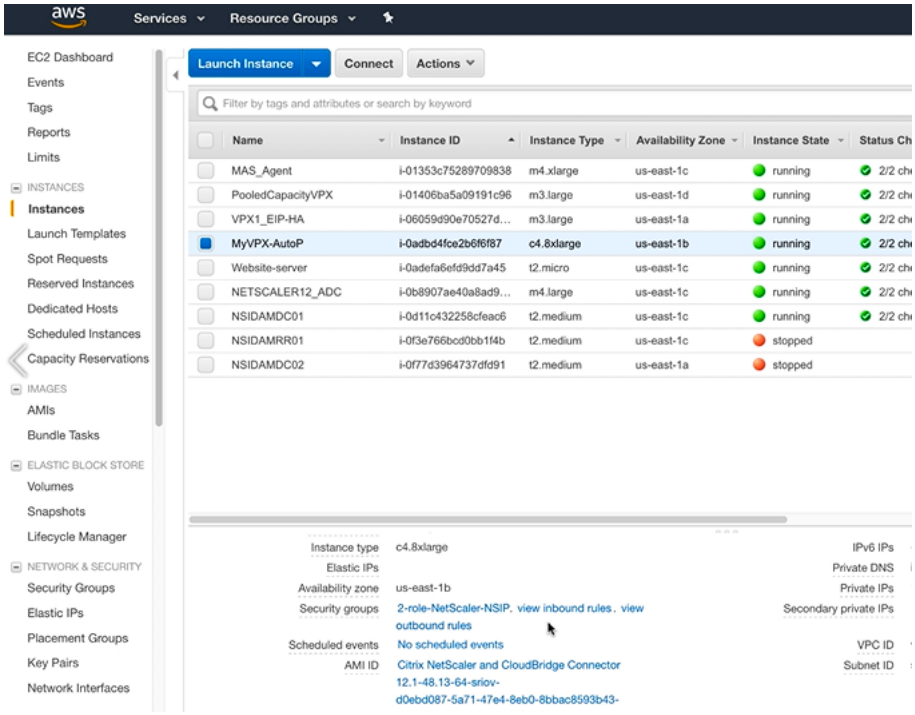
展開が完了すると、すべての管理と展開の目的で、Citrix ADM で Citrix ADC VPX インスタンスを確認できます。



その後、EC2 コンソールに移動して、Citrix ADM 設定で設定した名前で作成された新しいインスタンスを確認できます。これは、すべて Citrix ADM の管理のために同期され、Citrix ADC へのアプリケーションの展開のための準備ができています。

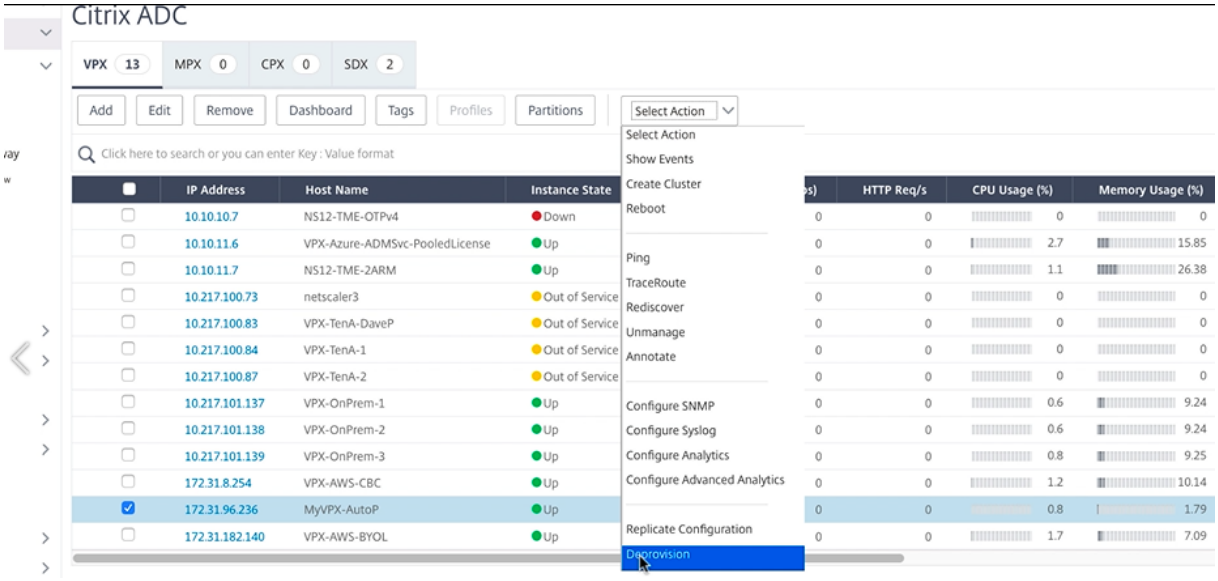
AWS 展開

© 1999–2021 Citrix Systems, Inc. All rights reserved.



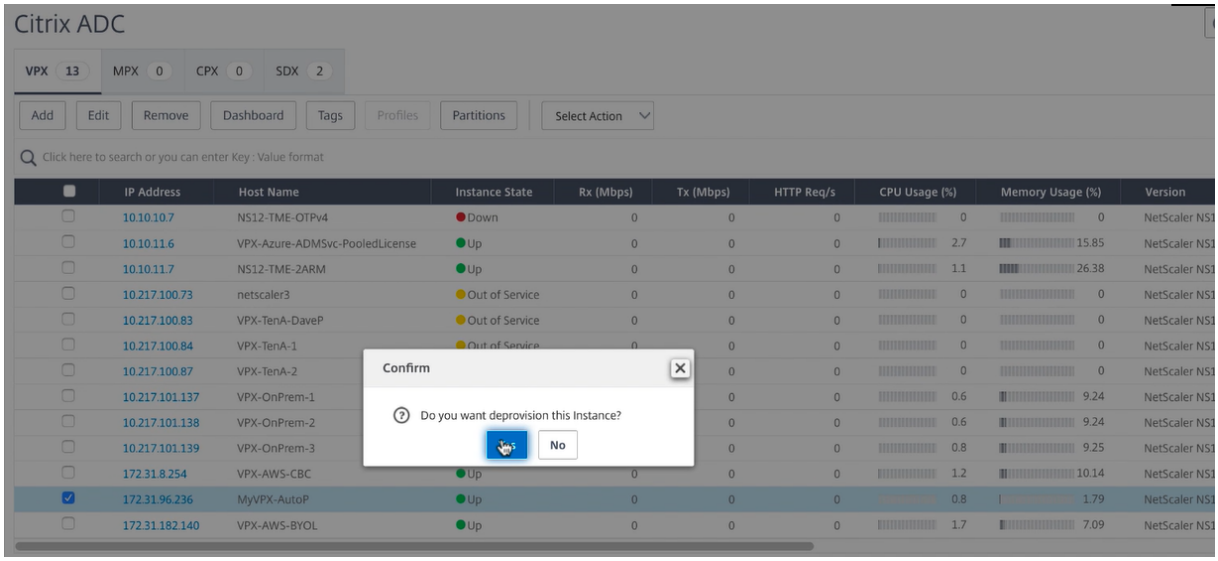
これらのインスタンスのプロビジョニングを解除するには、Citrix Cloud ADM サービスに戻り、「ネットワーク」**>**「インスタンス」**>**「**Citrix ADC**」の順に選択します。[アクションの選択] タブで、[プロビジョニング解除] をクリックします。

AWS のプロビジョニング解除

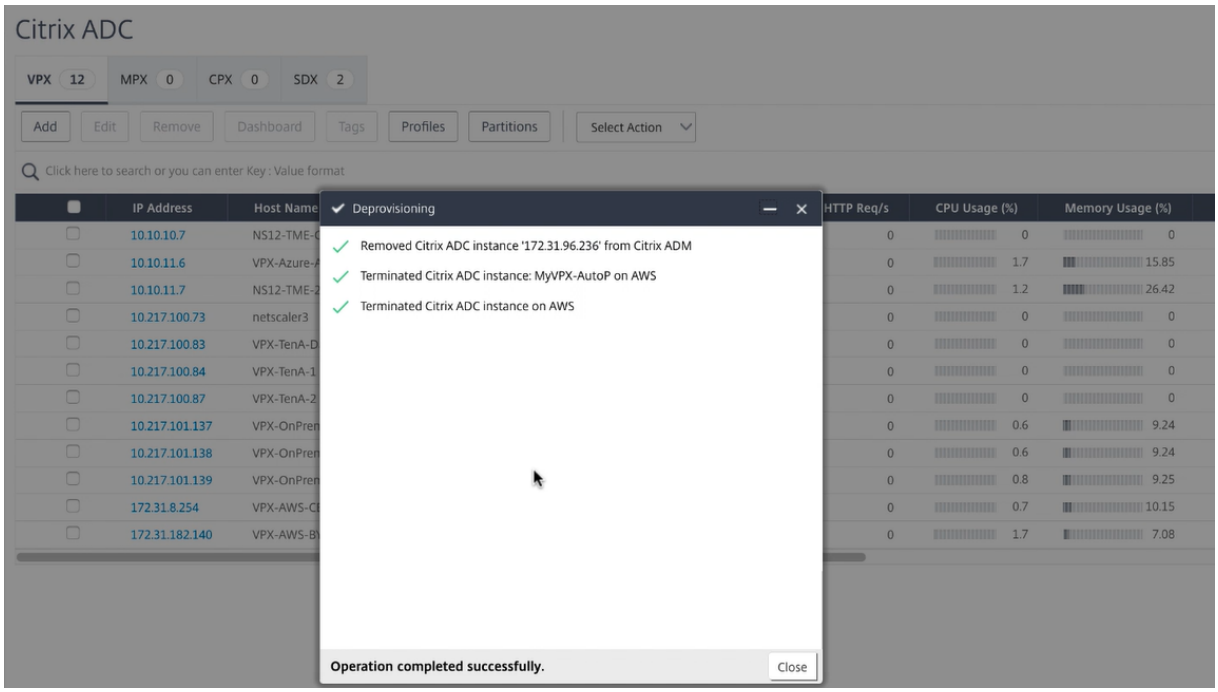


操作を確認するプロンプトが表示されます。続行するには、[**Yes**] を選択すると、すべての Provisioning が取り消されます。

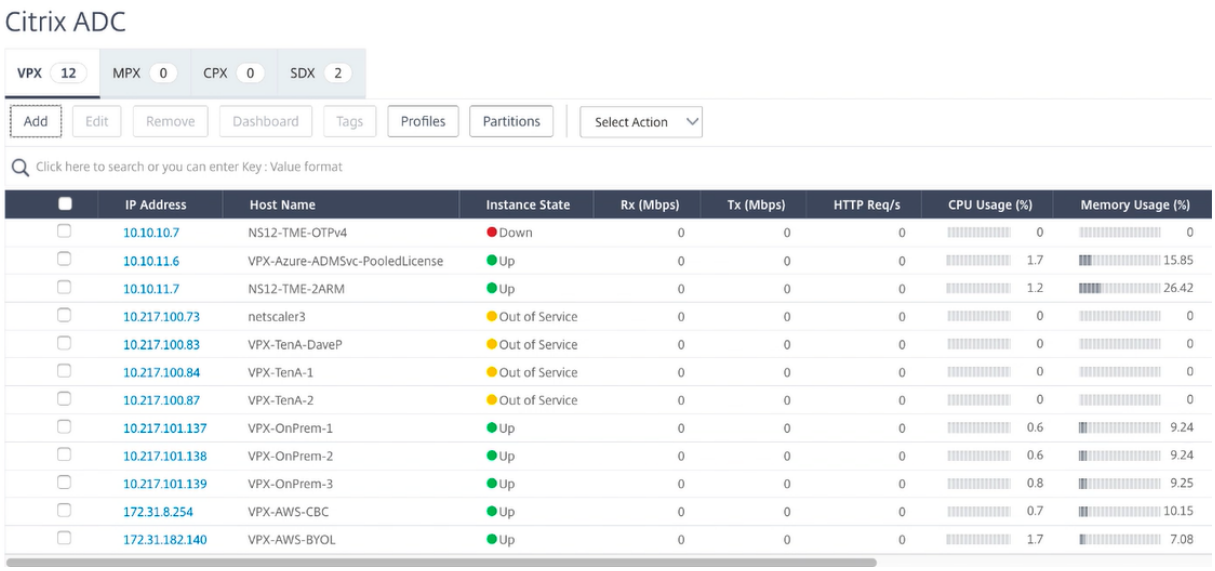
© 1999–2021 Citrix Systems, Inc. All rights reserved.



VPX インスタンスがプロビジョニング解除されたという確認メッセージを受け取ると、Citrix ADM コンソールにデバイスが表示されなくなります。



© 1999–2021 Citrix Systems, Inc. All rights reserved.



詳細情報の表示

- 実装ガイド:AWS での Citrix XenDesktop
- 一般的なエンタープライズアプリケーション用に Unified Gateway を設定する方法
- Amazon Web Services（AWS）で Citrix ソリューションを実行してビジネスを加速する
- AWS 向けクラウドネットワーキングおよびデスクトップ仮想化ソリューション
- 複数のアベイラビリティーゾーンにわたる AWS での Citrix ADC HA の使用
- NetScaler VPX と AWS AutoScale 統合

Citrix ADC 管理パーティション検証済みリファレンスデザイン

May 18, 2020

機能の概要

Citrix ADC 管理パーティションは、単一の Citrix ADC インスタンスでソフトウェアレベルでマルチテナント機能を有効にします。各パーティションには、独自のコントロールプレーンとネットワークプレーンがあります。

管理パーティションの主な利点は次のとおりです。

1. コントロールプレーン：分離された構成と管理
2. データプレーン：重要なパーティションデータとファイルは、パーティション境界内で厳しく制御されます。
3. ネットワークプレーン：トラフィックは独自のネットワーク構成で分離されます。同じ Citrix ADC 上の 2 つのパーティションは、各パーティションを通過する同じトラフィックを認識しません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

このドキュメントでは、管理パーティションによって有効になっている一般的なユースケースと、お客様の環境で管理パーティションを使用するためのガイドラインを詳しく説明します。

管理パーティションの使用例

管理パーティションのエンタープライズユースケース

Citrix ADC 管理者は、Citrix ADC を複数の ADC に分割し、そのパーティションを Microsoft SharePoint や Microsoft Lync などのさまざまなアプリケーション管理者に割り当てることができます。各アプリケーション管理者/所有者は、独自の構成を変更できます。

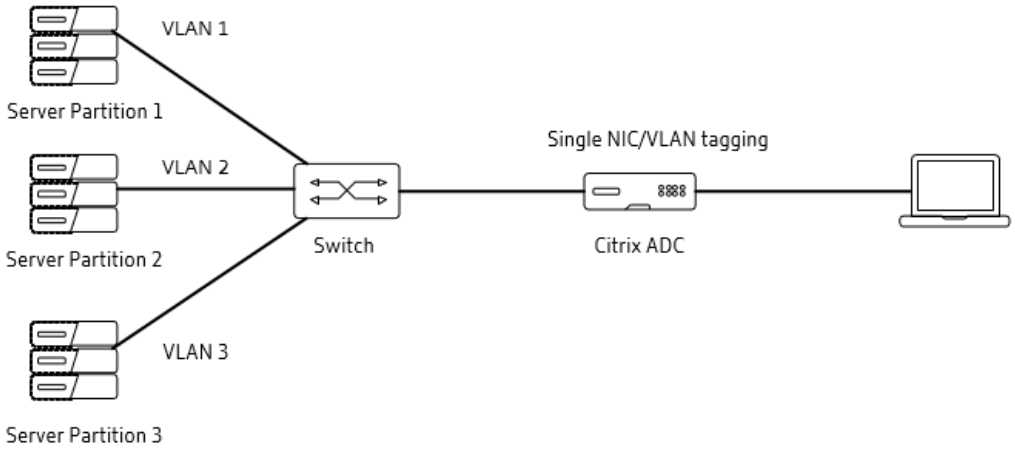
IP オーバーラップ**:** IP オーバーラップの主な利点は、IP の競合なしに、異なる管理パーティション間で同じ IP 範囲を使用できることです。バックエンドサーバーでは、同じプライベート IP アドレスのセットを使用できます。IP オーバーラッピングのシナリオでは、VLAN を共有できません。

仮想ルーティング：ルーティング構成は各パーティションに固有であり、各パーティションの所有者は独自のルーティングプロトコルを設定できます。

名前空間の分離**:** エンティティ名は異なるパーティション間で一意であるため、異なる管理パーティションで同じ名前を使用できます。

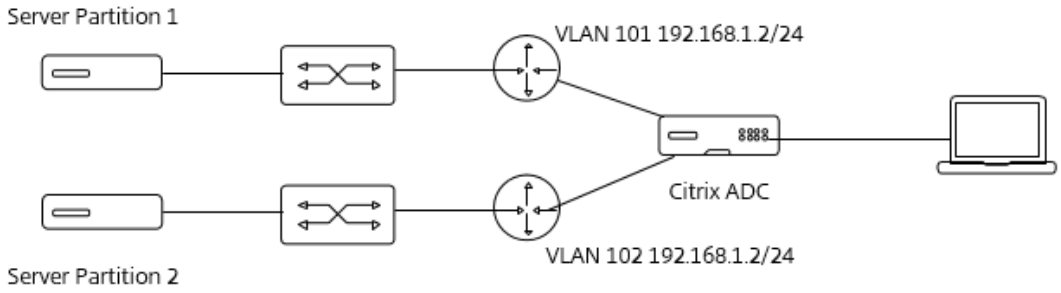
参照図**:**

単一 NIC – 複数の Vlans



IP オーバーラップ:

© 1999–2021 Citrix Systems, Inc. All rights reserved.



管理パーティションのサービスプロバイダーの使用例

サービスプロバイダは、Citrix ADC を分割し、帯域幅要件と同時接続数に基づいて個々のクライアントに割り当てることができます。

サービスプロバイダは、NITRO API を使用してオーケストレーションツールを開発し、個々のクライアントから帯域幅要件と同時接続に関する入力を取得し、パーティションを作成してクライアントに割り当てることができます。

以下は、サービスプロバイダを支援する分離のセットです。

ファイルシステム：各パーティションは、ファイルシステムの一部が割り当てられ、それぞれのパーティション領域に格納されているファイルは、他のパーティションには見えません。SSL 証明書/キーはそのパーティションに格納され、他のパーティション所有者には見えません。したがって、各パーティションは安全になります。

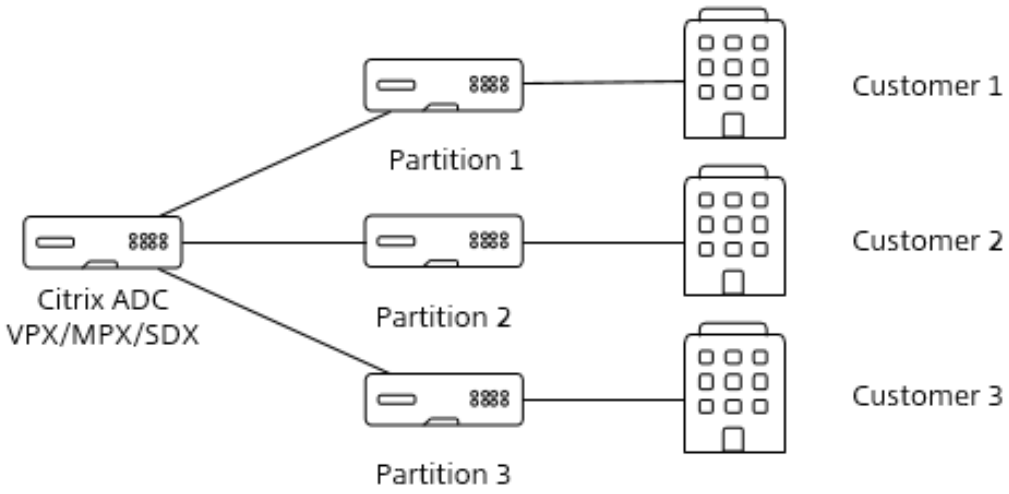
共有 **VLAN:** マルチテナント配置を使用する一般的なサービスプロバイダーでは、エンドカスタマーが着信トラフィック用に独立した VLAN を持っていない場合があります。共有 VLAN 機能は、専用 VLAN を使用できない場合に VLAN を共有します。

VLAN タギング： 1 つのインターフェイスを複数の管理パーティションで共有し、タグ付き VLAN を使用して分離できます。タグなし VLAN の場合は、共有 VLAN を使用します。

トラブルシューティングとデバッグ**:** 管理者は各パーティションのトラフィック統計を個別に確認し、パーティション ID でフィルタリングしてログを分離できます。トレース機能は、あるパーティションから起動されたトレースが別のパーティションからのパケットを認識しないため、パーティションの独立性を保証します。

参照図

© 1999–2021 Citrix Systems, Inc. All rights reserved.



管理パーティションを実装するためのガイドライン

管理パーティションにより、帯域幅、メモリ、同時接続などのリソースの共有が可能になり、ネットワーク、データ、管理プレーンでの分離が可能になります。

リソースのパーティション

ADC 管理者は、admin パーティションを構成するために次の詳細情報が必要です。

1. 接続:（TCP 接続の数）
2. メモリ
3. 帯域幅の要件

接続数と帯域幅の要件は、アプリケーションとそれぞれのパーティションによって処理されるトラフィックによって異なります。ADC 管理者は、アプリケーション管理者と協議して、パーティションの接続/帯域幅を取得します。

メモリ割り当てのガイドライン

デフォルトパーティションに割り当てられるメモリの量は、使用可能な合計メモリの 50% 以上である必要があります。理由は次のとおりです。

1. 制限に達した場合に備えて、他のパーティションのメモリを増やすために、将来お客様に柔軟性を提供します。
2. すべてのパーティションの統合キャッシュメモリは、既定のパーティションから取得されます。

PE で消費できる合計メモリは 4 GB です。したがって、2 GB の合計は、管理パーティションを除くすべてのパーティションに割り当てることができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

admin パーティションに割り当てられたメモリは、次の 2 つの目的で使用されます。

1. 静的オブジェクト（設定、SSL キー）の保存
2. 動的オブジェクト — 有効な機能のリストと接続数に応じて、動的オブジェクトに割り当てられるメモリは異なります。

ADC の管理者は、アプリの所有者からの接続と帯域幅の要件、および以下のガイドラインを使用して、メモリの見積もりを考え出します。

config に静的メモリを割り当てるためのガイドライン

表 1 に、一般的に使用される構成と必要なメモリを示します。

表 **1**

構成のタイプ	パケットエンジンあたりの割り当てメモリ（KB 単位）
SNIP の追加	255
IPv4 サーバーの追加	0.384
サービスの追加	5.253
サービスでの vServer の追加	11.157
VLAN をパーティションにバインドする	0.116
パーティションへのルートの追加	0.564
acl を追加	0.5
モニタの追加	4.34
サービスグループの追加	4.625
サーバーをサービスグループにバインドする	5.817
cs アクションを追加	4.532
add cs policy	2.548
add cs vserver	11.589
cs ポリシーを cs vServer にバインドする	7.348

設定は PE 間で複製されるため、上記の要件に PE の数を乗算する必要があります。

動的メモリのガイドライン

表 **2**

© 1999–2021 Citrix Systems, Inc. All rights reserved.

機能	メモリ要件
接続（Citrix ADC のバージョンが 12.0 以降の場合のみ適用）	1 K 接続あたり 2.4 MB
永続的なセッション	1 K セッションあたり 600 KB
GSLB 永続セッション	1 K セッションあたり 6 MB
SSL	SSL オフロードでは 1000 個の SSL 接続/セッションでは 6 MB、エンドエンド SSL では 1000 個の SSL 接続/セッションでは 9 MB
AAA：ユーザ数に依存する	ユーザー数 * 2 KB
書き換え — 書き換えポリシーによって解析される最大長を取得します。	接続数 * 最大長
レスポンダー — レスポンダーポリシーによって解析される最大長を取得します。	接続数 * 最大長さ
TCP バッファリング	接続の 20% * 構成された TCP バッファのサイズ

動的メモリ = 上記の表の上記の行のそれぞれから計算されたメモリの合計。

計算された合計メモリに 10 〜20% のバッファを追加します。

AppQoE のようないくつかの機能のメモリ要件は提供されません。パーティションメモリから消費されるメモリは、これらの機能では無視できるものであり、10 〜20% のバッファで処理するのに十分であるためです。

合計メモリ = 静的メモリ * PE のなし + 動的メモリ

必要なメモリが 1 GB、パケットエンジンの数が 4 であるという結論に達したと仮定しましょう。次に、その特定のパーティションについて、必要なメモリの量は、次の式によって導出されます。

管理パーティションのメモリ構成 =（必要なメモリ量/パケットエンジンの数）

管理パーティションのメモリ = 1 GB/4 = 250 MB

リソース制限に達したときの動作

1. 接続 — 新しい接続は切断されます
2. 帯域幅：新しいトラフィックはドロップされます。
3. メモリ：新しいトラフィックがドロップされる

特定のパーティションのリソースが枯渇した場合にトリガーされる SNMP アラートを設定できます。SNMP トラップのリストは、「その他のリソース」セクションに記載されています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ネットワークプレーン

VLAN：ネットワークレベルの分離を維持するために、異なる VLAN を設定して管理パーティションに割り当てます。

ルーティング: ルーティング設定はパーティションごとに一意です。

ADC 管理者は、ネットワーク管理者（アプリケーション管理者からの入力を含む）と協議して、ネットワークトポロジに基づいて VLAN およびルーティング関連の設定を定義します。

L3 パラメータ: パーティション固有です。L3 パラメータには、ドロップ DF パケット、ICMP エラーしきい値、オーバーライダーナットなどがあり、入力はネットワークまたは ADC 管理者から取得する必要があります。

コントロールプレーン**:** ユーザーエクスペリエンス

Admin Partitions はさまざまなレベルで分離できるため、分離された ADC インスタンスを安全に管理できます。

次のような分離レベルがあります。

1. UI ページ：パーティションに対してのみ表示される構成、統計情報
2. 診断 — トレース分離。トレースは、他のパーティションのトラフィックをキャプチャしません。
3. SNMP アラート：パーティションレベルで構成
4. ログレベルの分離

UI レベルの分離は、次の方法を使用して設定できます。

1. それぞれのパーティションで、1 つの SNIP に対して mgmt. アクセスを有効にし、その SNIP を使用して GUI にアクセスします。これにより、UI レベルの分離と可視性がそのパーティションのみに提供されます。

表 **3**

ログの種類	パーティション固有
ウェブログ	はい
Techsupport バンドル	はい
監査ログ	いいえ
/var/log	いいえ

エンタープライズユースケースの管理パーティション

この項では、Admin Partitions を使用する 4 つのアプリケーションを使用したエンタープライズカスタマーのユースケースについて説明します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

お客様の要件

- 4 つのアプリケーションをホストする必要がある
- 各アプリケーションには、独自の管理者と異なる ADC 要件のセットがあります。次の表に、アプリケーションとその固有の要件を示します。

表 **4**

アプリケーション	特性	要件/機能
SharePoint	ファイル、オーディオ、ファイルなどの共有	キャッシュ、圧縮、認証、SSL オフロード、SSL プロファイル
データベース	カスタム SQL ルール、認証、読み取りと書き込みの分割によるパフォーマンスの向上	コンテンツスイッチ、SQL 関連キーワードのポリシーインフラ
エンタープライズ Web サイト	パブリックアクセス-攻撃を受けやすい、アプリケーションファイアウォール	DDoS、アプリケーション品質、アプリケーション FW、SSL プロファイル
Outlook	AD、SSO との統合、HTTP でのパフォーマンスの向上	認証 SSO、SSL オフロード

上記の要件表から、Citrix ADC メリットをすべて実現するために、アプリケーションごとに異なる構成セットが必要であることは明らかです。Citrix ADC をパーティション分割し、それらのパーティションをそれぞれのアプリケーション所有者に割り当てることをお勧めします。

帯域幅と接続推定

Outlook と **SharePoint**

SharePoint、Exchange、Lync などのエンタープライズアプリケーションの帯域幅は、次の項目に依存します。

1. 同時ユーザー数
2. 使用タイプ
   a) Exchange：メッセージの平均サイズと数
   b) SharePoint：ファイルのタイプ、読み取りと書き込みの比率

アプリケーション管理者は、上記の 2 つの要素を使用して帯域幅要件を計算し、管理者パーティションの構成に関する情報を Citrix ADC admin に提供します。帯域幅の計算方法に関する広範なガイドラインについては、Microsoft TechNetおよびMSDN ブログを参照してください。

例：

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Outlook 2010 の帯域幅: ユーザーの種類 (ライト、ミディアム、ヘビーなど)。ミディアムユーザーの場合は、10 回の電子メールを送信し、40 回の電子メールを受信します。msg. サイズ 50 kb = 2.15 Kbps。1,000 ユーザの場合、必要な帯域幅は 2,150 Kbps です。

SharePoint の帯域幅: ユーザー数 = 1,000。ユーザーの 20% が任意の時点でアクティブであり、平均ページロードサイズは 100 KB で、1 時間以内に約 10 ページにアクセスすると仮定します。

= 100 KB * 200 * 10 per hour = 200000 KB/hr = 200000*8(8 bits per byte)/3600(no of seconds)

= 444 キロビット/秒

1 秒あたりの接続数 = アクティブユーザー数* 10

MSSQL

クエリの速度と応答のサイズに基づいて、帯域幅と接続を導出します。

エンタープライズ **Web** サイト

帯域幅要件：平均ページサイズ*任意の時点での最大ユーザー数* 2

接続: 最大ユーザー数 * ユーザーあたりの接続数

例:

帯域幅:4 KB*1000*2 = 48000 キロビット/秒

最大ユーザー数 = 1000、ユーザーあたりの接続数 = 10。接続数 = 10K

ほとんどのユーザーが HTTP/1.1 からのものである場合、ユーザーあたりの接続数は 2〜3 になりますが、ミックスが HTTP/1.0 に向かって傾いている場合、接続数は 10〜15 になります。ユーザーあたりの乗数係数の接続数は、トラフィックとクライアントの組み合わせに応じて 3 〜15 です。

構成するメモリは、次の条件によって異なります。

1. 各 admin パーティション（スタティックメモリ）内の設定のリスト。詳しくは、表 1 を参照してください。
2. 動的メモリ — 接続数と接続のタイプ (HTTP と SSL) — 詳しくは、表 2 を参照してください。
3. パケットエンジンの数。メモリ =（スタティックメモリ + ダイナミックメモリ）/（パケットエンジンの数）

ADC 管理の手順

1. 各アプリケーションの帯域幅と接続を収集する
2. それぞれ SharePoint、データベース、および Outlook 用の 3 つのパーティションを作成します。前の手順の帯域幅と接続を使用し、各パーティションに割り当てます。AppFW はデフォルトパーティションでのみサポートされているため、顧客が AppFW を必要とする場合、エンタープライズ Web サイトはデフォルトパーティションでホストできます。
3. 各パーティションのユーザーを作成し、資格情報を共有します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

4. 統合キャッシュを有効にし、キャッシュメモリを設定します。キャッシュメモリは、デフォルトパーティションで設定されたキャッシュメモリから取得されます。割当てについて詳しくは、IC の付録セクションを参照してください。

    a) ADC 管理者に相談した後、キャッシュメモリを割り当てます。システムの合計キャッシュメモリの 30～40% を割り当てます。割り当てた合計が 10 GB の場合は、SharePoint パーティションのキャッシュに約 3-4 GB を割り当てます。
    b) アプリケーションの所有者は、最初にキャッシュ統計を監視して、メリットのレベルをチェックする必要があります。
    c) キャッシュオブジェクトのヒット率を確認し、多数のキャッシュオブジェクトのヒット率が高い場合は、そのパーティションの IC メモリのサイズを増やします。

5. 圧縮を有効にする

    a) SharePoint は、異なる種類のファイル（Excel、PowerPoint、Word）を発行し、同じファイルを圧縮してクライアントに配信すると、帯域幅の使用量が減少します。

データベースユーザー

1. CS、VIP、およびバックエンドサーバーを設定します。
2. コンテンツスイッチを使用して、読み取り/書き込み要求を分割し、それぞれのサーバーセットにリダイレクトします。

エンタープライズ **Web** サイト

1. VIP サーバーとバックエンドサーバーを設定します。
2. 統合キャッシュを有効にします。

    a) 他のパーティションからの未使用のキャッシュメモリは、エンタープライズ Web サイトのために利用可能であるように、エンタープライズ Web サイトは、デフォルトのパーティションにあります。したがって、SharePoint と Outlook がそれぞれ 35%を消費すると仮定すると、消費された合計は 70%になり、残りの 30%はデフォルトパーティション（エンタープライズ Web サイト）に残ります。合計キャッシュメモリが 10 GB の場合、デフォルトパーティションには 3 GB のキャッシュメモリがあります。
    b) アプリケーションの所有者は、最初にキャッシュ統計を監視して、メリットのレベルをチェックする必要があります。
    c) キャッシュオブジェクトのヒット率を確認し、多数のキャッシュオブジェクトのヒット率が高い場合は、そのパーティションの IC メモリのサイズを増やします。

3. フロントエンドの最適化を有効にします。
4. AppFW を有効にします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サービスプロバイダーの管理パーティションの使用例

サービスプロバイダーは Microsoft アプリケーションをホストし、IIS、SharePoint、および MSSQL アプリケーションをサービスとして提供します。お客様には、通常、次の要件があります。

お客様の要件

- 顧客 1: データベースサーバーにアクセスし、読み取り/書き込みの分割は 90:10 で、エンドカスタマーは SQL 関連のカスタムフィルタの設定を希望しています。
- 顧客 2: SSL 経由で Web アプリにアクセスし、エンドカスタマーが SSL 証明書の管理を希望している
- お客様 3: サービスプロバイダーからホストされている SharePoint にアクセスする

サービスプロバイダは、顧客のためのポータルをホストします。

1. ホストするアプリケーションを選択します。
2. 帯域幅の要件

サービスプロバイダは、顧客のためのポータルをホストします。

1. ホストするアプリケーションを選択します。
2. 帯域幅の要件
3. 接続

この選択に基づいて、サービスプロバイダは、NITRO API を使用して、バックエンド内の特定のアプリケーションに関連する構成で適切なパーティションを設定できます。

お客様が選択したアプリケーションに基づいて、適切なオプションを選択します。

1. SSL を使用するウェブアプリ
    a) VIP にバインドされる SSL 証明書オプション
    b) HTTP から HTTPS へのリダイレクト
    c) SSL プロファイル関連パラメータ
2. SQL
    a) 顧客が設定する SQL 関連のフィルタ
3. SharePoint
    a) キャッシュメモリ制限とルール
    b) 圧縮ポリシー

サービスプロバイダは、管理パーティションの作成後に正確な要件を実装するために、2 つのオプションのいずれかに従います。

構成オプション **1:**

サービスプロバイダは、顧客からの要求を収集し、それぞれのパーティションで実行します。

構成オプション **2:**

© 1999–2021 Citrix Systems, Inc. All rights reserved.

NITRO API を使用して管理パーティションを自動化します。入力はフロントエンドポータルから収集することができ、バックエンドで NITRO API を実行してパーティションを構成することができます。

機能に関する考慮事項

機能のサポート：管理者パーティションは、ほとんどの機能でサポートされ、唯一のいくつかの機能のためにサポートされていません。正確なリストについては、Citrixを参照し、特定のソフトウェアリリースで確認してください。このテーブルには、サポートマトリックスをリストしたテーブルが含まれます。

設定の制限事項。管理パーティションは、ではサポートされていません。

1. クラスタリング
2. MPX-FIPS アプライアンス

結論

Admin Partitions の主な利点は、ADC をソフトウェアレベルで分離し、各パーティションの所有者に安全で分離されたユーザーエクスペリエンスを提供することです。

そのほかの情報の入手先

トラブルシューティングツール

管理者パーティションの一般的な問題：

ESX 上の **VPX** 上の管理者パーティション：

- カスタム MAC アドレスが設定されている場合、デフォルト以外のパーティションに到達できません。
- 解決方法: デフォルト以外のパーティションを動作させるには、ESX で無差別モードを有効にする必要があります。

構成エラー**:**

- 設定で、入力ファイルが存在しないというエラーをスローできないことがあります。
- 絶対パスではなく、相対パスを使用する必要があります。

VLAN の構成：

- 管理パーティション VLAN はタグ付き VLAN をサポートしているため、VLAN がタグ付けされている場合、Citrix ADC インターフェイスが接続されているスイッチを適切な VLAN で構成する必要があります。タグなし VLAN の場合は、共有 VLAN 設定を使用します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

キャッシュメモリ割り当ての統合

パーティション分割された Citrix ADC で統合キャッシュ（IC）を構成するには、デフォルトパーティションに IC メモリを定義した後、スーパーユーザーは各管理パーティションに IC メモリを構成して、すべての管理パーティションに割り当てられる IC メモリの合計がデフォルトパーティションに定義されている IC メモリを超えないようにできます。で指定します。admin パーティション用に構成されていないメモリは、デフォルトパーティションで引き続き使用できます。

たとえば、2 つの管理パーティションを持つ Citrix ADC アプライアンスで、デフォルトパーティションに 10 GB の IC メモリが割り当てられ、2 つの管理パーティションに対する IC メモリ割り当ては次のようになります。

- パーティション 1：4 GB
- パーティション 2：3 GB

次に、デフォルトのパーティションには 10-(4 + 3) = 3 GB の IC メモリが使用可能です。

> 注:
>
> すべての IC メモリが admin パーティションによって使用されている場合、デフォルトパーティションには IC メモリを使用できません。

メモリ使用量をチェックするコマンド

- パーティション内の Stat システムメモリには、パーティションのシステムレベルのメモリ割り当てが集約され、stat パーティション名は、パーティション内で使用されているメモリのパーセンテージを示します。

```
>add partition p1
Done
>switch partition p1
Done
p1> stat system memory
done

Citrix ADC Memory Information:
Maximum Memory Available (MB): 50
Memory Currently Available (MB): 50
Memory Allocated (MB) 7
Memory Allocated (%) 14.95
InUse Memory  (MB) 7
InUse Memory (%) 14.95
Free Memory (MB) 42

>stat partition p1

Partition(s) Summary
   MinBW MaxBW MaxConn MaxMem
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
21
22 p1 10240 10240  1024  10
23
24 Partition Stats:
25
26                        Rates (/s)   Total
27 Current Bandwidth         --          0
28 Current Connections       --          0
29 Memory Usage (%)          --          14
30 Total Packet Drops        0           7
31 Total Drops (KB)          0           0
32 Total Connection Drops    0           0
33 <!--NeedCopy-->
```

- 設定メモリ：各設定は、すべてのパケットエンジンで複製されているので、それに応じてメモリは、すべてのパケットエンジンの内部に割り当てられます。たとえば、「add lb vserver」コマンドがピーチパケットエンジンで約 10KB かかり、5 パケットエンジンシステムで 10MB のパーティションを作成した場合、合計で 50KB のパーティションメモリを消費します。
- 特定の構成に必要なメモリ要件の正確な値は、構成を適用し、Citrix ADC シェルで次のコマンドを実行することで測定できます。

```
1 root@ns# nsconmsg -s nsppeid=0 -s nspartid=1 -g mem_cur_usedsize -d
     current
2 Displaying performance information
3 Citrix ADC V20 Performance Data
4 Citrix ADC NS11.0: Build 65.572.nc, Date: Apr 7 2016, 10:32:51
5
6 reltime:mili second between two records Thu Feb 23 13:45:18 2017
7  Index rtime totalcount-val delta rate/sec symbol-name&device-no
8     0  22681     1597631     8965  5333     mem_cur_usedsize
          partition_ctx(p1) (PART-1)
9 <!--NeedCopy-->
```

この実験では、**PPE-0** でパーティション **ID 1** に約 **9KB** のメモリが使用されています。**Citrix ADC** 上で構成されたすべてのパーティションには、一意の **ID** が割り当てられます。

次のコマンドは、指定されたパーティションのための完全なシステム（すべてのパケットエンジンを含む）のメモリ推定を測定することを可能にします。

```
1 root@ns# nsconmsg -s nspartid=1 -g mem_cur_used -d current
2 Displaying performance information
3 Citrix ADC V20 Performance Data
4 Citrix ADC NS11.0: Build 65.572.nc, Date: Apr 7 2016, 10:32:51
5
6 reltime:mili second between two records Thu Feb 23 13:44:27 2017
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
Index rtime totalcount-val delta rate/sec symbol-name&device-no
 0   7000    7881865       6403    5333    mem_cur_usedsize
    partition_ctx(p1) (PART-1)
<!--NeedCopy-->
```

Citrix ADC 12.0 で導入された **SNMP** トラップのリスト

トラップ名	説明
パーティション接続制限を超えました	パーティションの接続制限がなくなり、新しい接続が切断される
パーティション接続制限標準	パーティションが新しい接続を受け入れるようになりました。
パーティション BW リミットを超えました	パーティションの BW 制限が使い果たされ、パケットがドロップされる
パーティション BWW しきい値に達しました	現在の帯域幅使用率 80% 以上
パーティション接続しきい値に達しました	現在のアクティブな接続数 80% 以上
パーティション接続しきい値 (標準)	現在のアクティブな接続数 60% 以下
パーティション MEM しきい値に達しました	PE の現在のメモリ使用率 80% 以上
パーティション MEM しきい値 (標準)	PE の現在のメモリ使用率 60% 以下
パーティション MEM リミット超過	PE の現在のメモリ使用率 95% 以上

その他の参考資料

Exchange クライアントネットワーク帯域幅計算ツール (ベータ版)

Microsoft オンラインサービスを実行するために必要な帯域幅

Citrix Gateway SaaS および **O365** クラウド **Citrix** 検証済みリファレンスデザイン

May 18, 2020

概要

Software as a Service（SaaS）は、ソフトウェアを Web ベースのサービスとしてリモートで配信するためのソフトウェア配布モデルです。一般的に使用される SaaS アプリ (Microsoft Office 365 サブスクリプションを含む)。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Gateway サービスを使用して、Citrix Workspace で SaaS アプリにアクセスできるようになりました。Citrix Gateway サービスと Citrix Workspace を組み合わせることで、構成済みの SaaS アプリケーション、構成済みの仮想アプリケーション、またはその他のワークスペースリソースに対する統一されたユーザーエクスペリエンスが提供されます。

Citrix Gateway サービスを使用した SaaS アプリの配信は、アプリを管理するための簡単で安全で堅牢でスケーラブルなソリューションを提供します。クラウド上で提供される SaaS アプリには、次のような利点があります。

シンプルな構成 - 操作、更新、使用が簡単です。
シングルサインオン — シングルサインオンで手間のかからないログオンが可能です。
さまざまなアプリの標準テンプレート — 一般的なアプリのテンプレートベースの構成。

Citrix Gateway SaaS アプリケーション

[アプリの詳細] セクションで、次のように入力します。

- 場所 = 社内ネットワーク外
- 名前 = オフィス 365* URL =`https://login.microsoftonline.com/login.srf`
- 関連ドメイン:*.login.com
- 説明 = (デフォルト)

[シングルサインオン**]** セクションで、次のように入力します。

- アサーション URL = `https://login.microsoftonline.com/login.srf`
- オーディエンス = urn:federation:MicrosoftOnline
- 名前 ID 形式 = 永続的
- 名前 ID = Active Directory GUID
- 高度な属性:
  - 属性名:`IDPEmail`
  - 属性形式: 未指定
  - 属性値: `Email`

Citrix Gateway への O365 SaaS アプリケーションのフェデレーション

PowerShell コマンドは、Microsoft Cloud 上で FEDERATED モードを構成します:

- PS> `connect-msolservice`

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注: msolserviceに接続するには、Microsoft クラウドアカウントを使用する必要があります。
>
> たとえば、*admin.user@onmicrosoft.com* のように指定します。

- PS> `Install-Module AzureAD -Force`
- PS> `Import-Module AzureAD -Force`
- PS> `Install-Module MSOnline -Force`
- PS> `Import-module MSOnline -Force`

Citrix Gateway カスタマーサブスクリプションに固有の フェデレーション設定を構成します。

- PS> `$dom = "ad-domain.com"`

> 注:
> *ad-domain.com* 名前空間は、ユーザー認証ドメインです。

- `PS> $fedBrandName = "CitrixNS(TME)"`
- `PS> $url = "https://customerID.cloud.com/cgi/tmlogout"`
- `PS> $uri = "https://citrix.com/customerID"`
- `PS> $ecpUrl = "https://customerID.cloud.com/saml/login"`

> 注:
> *customerID*は、*Citrix Workspace の URL* です。

Citrix Gateway から SAML IdP 証明書を指定します。

- `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\cert\saml_idp.crt")`
- `PS> $certData = [system.convert]::tobase64string($cert.rawdata)`

PS 文字列を実行して、Citrix Gateway へのmsolフェデレーションを完了します。

- `PS> Set-MsolDomainAuthentication -DomainName $dom -federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -SigningCertificate $certData -IssuerUri $uri -ActiveLogOnUri $ecpUrl -LogOffUri $url -PreferredAuthenticationProtocol SAMLP`

ドメインフェデレーションと設定が完了したことを検証します。

- `PS> Get-MsolDomainFederationSettings`

```
DomainName: customerID.com

ActiveLogOnUri https://customerID.cloud.com/saml/login

FederationBrandName customerID(TME)

IssuerUri https://citrix.com/customerID

LogOffUri https://customerID.cloud.com/cgi/tmlogout
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
PassiveLogOnUri https://citrix.comcustomerID

SigningCertificate MIIG3zCCBMegAwIBAgIJAMUTG1zqJgUZMA0GCSqGSIb3DQEBCwUAMIGcMQswCQYD
```

Office 365 Suite Applications

- Outlook https://outlook.office365.com/
- OneDrive for Business https://customerid.sharepoint.com/
- Word https://office.live.com/start/Word
- Excel https://office.live.com/start/Excel
- PowerPoint https://office.live.com/start/PowerPoint
- OneNote https://www.onenote.com/
- SharePoint https://customerid.sharepoint.com/
- Teams https://teams.microsoft.com/
- Yammer https://www.yammer.com/office365
- Dynamics 365 https://customerid.dynamics.com/
- Flow https://flow.microsoft.com/

参照リンク

Azure PowerShell モジュールリファレンス

Azure PowerShell コマンドリファレンス

Microsoft Azure で Office 365 ディレクトリ同期を展開する

Access Control 付き Citrix Gateway サービス SSO Citrix 検証済みリファレンスデザイン

May 18, 2020

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Gateway サービス

Citrix Gateway サービスは、認証、シングルサインオンを提供し、Citrix VDI および SaaS アプリケーションの高速かつ安全な配信を可能にする Citrix ソリューションです。

Citrix Gateway サービスでは、SaaS および Web アプリケーションへの SSO も提供されます。サービスとしてのソフトウェア（SaaS）SSO 機能は、Citrix Cloud のクラウドベースの完全管理型サービスです。パブリックにホストされている SaaS アプリケーションおよび企業でホストされている Web アプリケーションへのリモートアクセスとシングルサインオンを提供します。

ユーザーのワークスペースサブスクリプション内で、Citrix Gateway サービスを使用して SaaS アプリケーションにアクセスできるようになりました。Citrix Gateway サービスは、パブリックにホストされている外部 SaaS アプリケーションプロバイダーで実行されているサードパーティの SaaS アプリケーションへの認証アクセスを提供します。

Citrix Gateway サービスと Citrix Workspace を組み合わせることで、構成済みの SaaS アプリケーション、構成済みの仮想アプリケーション、またはその他のワークスペースリソースに対する統一されたユーザーエクスペリエンスが提供されます。

NetScaler Gateway Service を使用した SaaS アプリケーションの配信は、アプリを管理するための簡単で安全で堅牢でスケーラブルなソリューションを提供します。クラウド上で提供される SaaS アプリには、次のような利点があります。

- シンプルな構成 - 操作、更新、使用が簡単です。
- シングルサインオン — シングルサインオンで手間のかからないログオン。
- さまざまなアプリの標準テンプレート — 一般的なアプリのテンプレートベースの構成。

Citrix Gateway サービスの機能

- シンプルさ：クラウドベースのサービスを使用して、NetScaler の導入と管理の複雑さを軽減
- 常に最新の製品：常に最新の製品で Citrix Gateway の管理を簡素化
- セキュリティと高可用性:XenApp および XenDesktop サービスのセキュリティと可用性を向上
- スピード：Citrix Gateway の導入と管理を迅速かつ簡単に行えます。
- 利便性: Gateway サービスをまとめてパッケージ化および販売することで、IT 部門が最も一般的に直面しているユースケースへの対応をシンプル化

Citrix Gateway サービス安全なリモートアクセスにより、
コストを削減し、管理を簡素化し、ユーザーエクスペリエンスを向上させます。

アクセス制御サービスの概要

アクセス制御サービスを使用すると、管理者はシングルサインオン、リモートアクセス、コンテンツ検査を単一のソリューションに統合し、エンドツーエンドのアクセス制御を実現する一貫したエクスペリエンスを提供できます。IT

© 1999–2021 Citrix Systems, Inc. All rights reserved.

管理者は、承認された SaaS アプリへのアクセスを、シンプルなシングルサインオン環境で制御できます。アクセス制御サービスを使用すると、管理者は、特定の Web サイトや Web サイトカテゴリへのアクセスをフィルタリングすることで、マルウェアやデータ漏洩から組織のネットワークやエンドユーザーのデバイスを保護することもできます。アクセスに関するセキュリティの強化ポリシーを設定することで、SaaS アプリへのセキュアなアクセスが可能になります。一度認証されると、社内、自宅、または外出中のいずれの場合も、従業員は任意のデバイスから重要なすべてのアプリケーションにアクセスできます。

管理者は、次のようなユーザーアクティビティを監視できます。

- 悪意のある、危険な、または不明な Web サイトが訪問された
- 消費された帯域幅
- 危険なダウンロードとアップロードの動作。

アクセスされた Web サイトおよび Web サイトカテゴリを分析し、企業ネットワークを保護するための修正作業を行うことができます。同時に、エンドユーザーには、ホストされたすべてのアプリへのシームレスかつセキュアなアクセスが提供されます。

管理者は、印刷制限、ダウンロード、クリップボードへのアクセス（コピー/貼り付け）などの操作を制限することもできます。

次の図は、アクセス制御サービスを視覚的に示しています。

アクセス制御機能を備えた **Gateway** サービス

アクセス制御サービスを使用して完了できる主なタスクには、以下のものがあります：

- シングルサインオンでアクセスできる SaaS アプリを公開する
- SaaS アプリへのセキュリティ強化ポリシーを設定する（透かし、コピー/貼り付けの制限、ダウンロードの禁止など、）
- ブロックする Web サイトカテゴリと Web サイトへのアクセスポリシーを定義する
- Secure Browser サービスにリダイレクトする Web サイトカテゴリと Web サイトへのアクセスポリシーを定義する
- SaaS アプリのコンテキストでのユーザーと Web サイトのアクティビティを理解し、定義済みポリシーに関連付ける
- ポリシーを変更して Web サイトへのアクセスを許可またはブロックし、Secure Browser サービスセッションでのアクセスを有効にする

Citrix Gateway サービス **SaaS** 公開手順

Software as a Service Apps のサポート

© 1999–2021 Citrix Systems, Inc. All rights reserved.

4 つの簡単な手順で開始する

1. Citrix Cloud にサインアップ
2. NetScaler Gateway Service 試用版のリクエスト
3. NetScaler Gateway Service がプロビジョニングされている
4. NetScaler Gateway Service UI へのアクセス

Citrix Cloud の利用を開始する

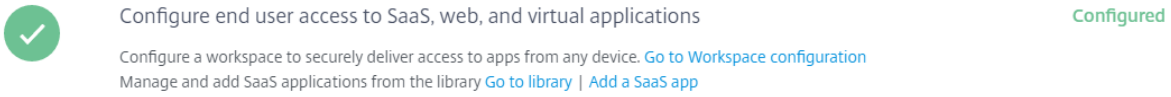
Citrix Workspace の利用を開始する

Citrix Gateway サービス **SaaS** アプリケーションの構成

この例では、SalesForce.com の SaaS アプリケーションを使用して Citrix Gateway サービスを構成するために必要な構成手順について説明します。

構成された **SaaS**、**Web**、および仮想アプリケーションへのエンドユーザーアクセスの構成

任意のデバイスからアプリへのアクセスを安全に配信するように Workspace を設定します。ワークスペース設定に移動
ライブラリからの SaaS アプリケーションの管理と追加ライブラリに移動 | SaaS アプリを追加する



Citrix Gateway サービスアプリケーションカタログから **SaaS** アプリケーションを追加するには、次の手順に従います

次の **URL** で **Citrix** サブスクリプションインスタンスにアクセスします

Citrix Cloud アカウントのログインで、組織のログイン認証情報を提供します。

1. Citrix Cloud 管理ポータルから **Citrix Gateway** サービスのタイルを起動します。
2. 「はじめに」リンクを起動して、SSO SaaS アプリケーションを設定します。
3. 「アプリケーションカタログ」リストから SaaS アプリケーションテンプレートを選択します。

   この例では、SSO 用の Salesforce を Workspace SaaS アプリケーションとして設定しようとしています。
4. 必要な SaaS アプリケーション固有のパラメータを入力します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> この例では、サードパーティのアプリケーションサブスクリプションによってホストされる SaaS アプリケーションであるため、「社内ネットワークの外側」を選択します。

5. ワークスペースの SaaS アプリケーションサブスクライバを管理します。
6. ユーザードメインから SaaS アプリケーションにユーザーを割り当てます。

> 注意:Workspace に対して認証
>
> するには、次の資格証明を使用します。
>
> - Windows Active Directory
> - Azure Active Directory

SaaS アプリケーション設定のアクセス制御

Citrix アクセス制御（CAC）: Gateway サービスに含まれる SSO および多要素認証（MFA）機能を基盤として構築され、SaaS および Web アプリケーションのアクセスと使用について、より詳細なポリシー制御を提供します。CAC は、ユーザーの行動分析とそのリスクスコアに基づく高度な分析とともに、セキュアなデジタルワークスペースを企業のエンドユーザーに提供する総合的なセキュリティ体制を強化します。

アクセス制御の強化されたセキュリティ設定

- セキュリティを強化する: Citrix 組み込みブラウザーで Web アプリケーションまたは SaaS アプリケーションを起動して監視し、未知のトラフィックをアクセス制御にルーティングします。
- クリップボードへのアクセスを制限する: アプリとシステムのクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
- 印刷を制限する: アプリブラウザ内から印刷する機能を無効にします。
- ナビゲーションを制限する: 次/後方アプリのブラウザボタンを無効にします。
- ダウンロードを制限する: ユーザーがアプリ内からダウンロードできないようにします。
- ウォーターマークの表示: ユーザーの画面にウォーターマークが表示され、ユーザーのマシンのユーザー名と IP アドレスが表示されます。

コンテンツアクセス設定のアクセス制御

Web フィルタリングを設定して、エンドユーザーのアクセスを許可/ブロックし、Citrix Secure Browser サービスにリダイレクトします。

- [コンテンツアクセスの設定] を選択します。
- [編集] を選択します。
- フィルタ Web サイトリストを有効にする

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- ブロックまたは許可された Web サイトを追加/削除する
- ブロックまたは許可された Web サイトのカテゴリを追加/削除する

アクセス制御を使用した **Citrix Workspace** アプリの起動

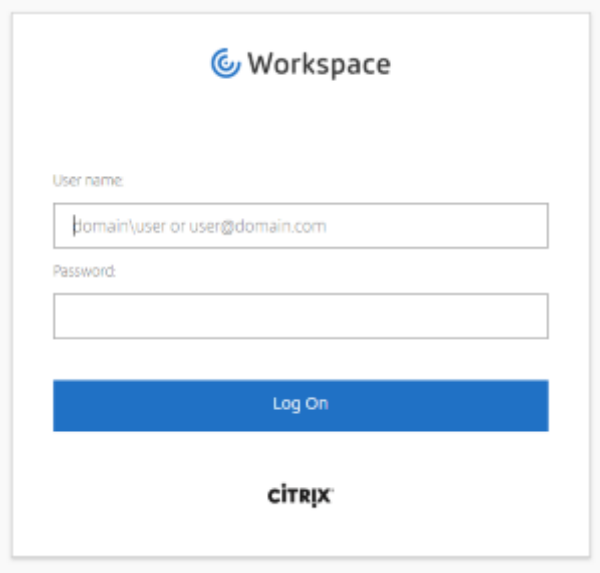
Workspace SaaS アプリケーションは、米国とアメリカでホストされるサブスクリプションの次の FQDN にあります。

Citrix Cloud アカウントのログイン

ワークスペースのエクスペリエンスは、Workspace アプリからアクセスできます。ワークスペースには、次の 3 つの種類があります。

- デスクトップ (Windows/Mac)
- モバイル (iOS/Android)
- Web (HTML5)

1. Web ブラウザーを使用して、ワークスペース URL に接続します。



2. ワークスペース内で SaaS アプリケーションタイルを選択します。
3. アプリケーションは、ネイティブ SSO を使用して、ブラウザーのタブでシームレスに起動されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

参照リンク

Azure Load Balancer フロントエンド IP 検証済みリファレンスデザインを使用した Citrix ADC 高可用性

March 2, 2021

概要

Azure ロードバランサー (ALB) をフロントエンド (FE) ロードバランサーとして使用して、Microsoft Azure で Citrix ADC の高可用性展開を実装します。

Azure のアクティブ-パッシブ高可用性 (高可用性) セットアップで、複数の NIC を持つ Citrix ADC 仮想アプライアンスのペアを展開できます。各 NIC に複数の IP アドレスを設定できます。

Azure サービス管理で高可用性モードで Citrix ADC VPX を構成する

アクティブ/パッシブモードでは、フェイルオーバー機能が提供されます。このモードの場合、VPX インスタンスは構成の状態と同期します。プライマリインスタンスが停止するとセカンダリアインスタンスが処理を引き継ぎます。

Citrix ADC アプライアンスの高可用性については、「高可用性」を参照してください

Microsoft Azure の展開では、Azure ロードバランサーを使用して、2 つの Citrix ADC 仮想マシンの高可用性構成を実現します。このロードバランサーは、両方の Citrix ADC インスタンスで構成された仮想サーバーにクライアントトラフィックを分散します。高可用性は、以下の 2 種類の Azure ロードバランサーによって実現します。

Azure 外部ロードバランサー: クライアントトラフィックがインターネットから発信される場合、クライアントトラフィックを分散するには、インターネットと Citrix ADC VPX インスタンスの間に外部ロードバランサーを展開する必要があります。

Azure 内部ロードバランサー: クライアントトラフィックがクラウドサービス内から発信される場合、またはクラウドサービス内の Gateway またはファイアウォールによって転送される場合、クライアントトラフィックを分散するために内部ロードバランサーを展開する必要があります。

Azure で高可用性を実現するには、2 つの Citrix ADC VM を負荷分散セットとして追加し、エンドポイントを構成する必要があります。

Citrix ADC アクティブ/パッシブ展開の前提条件

- 高可用性独立ネットワーク構成（INC）構成
- Direct Server Return（DSR）モードの Azure Load Balancer（ALB）
- すべてのトラフィックはプライマリノードを通過します。
- セカンダリノードは、プライマリノードが失敗するまでスタンバイモードを維持します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> Azure クラウド上の Citrix ADC 高可用性展開が機能するには、2 つの Citrix ADC 高可用性ノード間で移動できるフローティングパブリック IP（PIP）が必要です。Azure ロードバランサー (ALB) は、フローティング PIP を提供します。このフローティング PIP は、フェイルオーバーが発生した場合に自動的に第 2 ノードに移動されます。
>
> *Floating IP* 設定は、*ALB* 構成セクションの手順 ***4*** で定義された ***ALB*** 負荷分散ルールで構成します。

Citrix ADC ADC IPSET 機能の概要

IP アドレスセットは、Citrix ADC アプライアンス上でサブネット IP アドレス（SNIP）または仮想 IP アドレス（VIP）として構成される一連の IP アドレスです。IP セットには、そのセットに含まれる IP アドレスの用途を識別するためのわかりやすい名前を付けます。IP セットを作成するには、IP セットを追加し、Citrix ADC が所有する IP アドレスをバインドします。SNIP アドレスと VIP アドレスは、同じ IP セット内に存在できます。

Azure ロードバランサーの概要

Citrix ADC 12.1 高可用性（高可用性）Azure Resource Manager（ARM）テンプレートを使用して、Citrix ADC 高可用性インスタンスを展開します。

このテンプレートは、Citrix ADC 高可用性アクティブ-パッシブモードの展開について説明します。シームレスな高可用性エクスペリエンスを提供するために、コンポーネントと設定を含めるように事前構成されています。トポロジの詳細については、高可用性を参照してください。

展開が成功すると、Citrix ADC アプライアンスのペアが HA-INC モードで事前構成されます。Citrix ADC VPX 高可用性テンプレートは、バイオル、および VPX 10、VPX 200、VPX 1000、VPX 3000 などの時間単位のライセンスなど、さまざまな Citrix ADC SKU をサポートします。

> 注:
>
> Citrix ADC 用の ARM テンプレートには、特定の Azure ロードバランシング変数がリソースとして含まれています。

展開の構成の前提条件

- Azure ロードバランサーの構成
- Citrix ADC ADC の構成

Azure ロードバランサーの構成

1. Azure ロードバランサーで利用可能になる各 Citrix ADC サービスのフロントエンド IP アドレスを追加します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

2. アプリケーションごとに alb バックエンドプールを追加します。
3. アプリケーションごとに alb ヘルスプローブを追加します。
4. alb 負荷分散ルールを追加します。
5. 1 つ以上の受信セキュリティルールをネットワークセキュリティグループ (NSG) に追加する

Citrix NetScaler の構成

NetScaler では、Citrix ADC リソースを Azure フロントエンド IP 構成にマッピングするために、IPSETS を追加する必要があります。

> 注:
>
> ALB からのフロントエンドのパブリック IP を必要とするすべての VIP に対して、次の手順を繰り返します。

1. Azure フロントエンドのパブリック IP アドレスを Citrix ADC に追加する

   ```
   add ns ip 23.99.xx.xx 255.255.255.255 -type vip (Azure Frontend Ip)
   ```

2. Azure フロントエンド IP 用の Citrix ADC SET を作成してバインドする

   ```
   add ipset net_1
   bind ipset net_1 23.99.xx.xx
   ```

3. IPSET を使用して Citrix ADC の VIP をアップデートします

   ```
   set lb vserver net_1 -ipset net_1
   ```

ALB へのポート接続の確認

https://ping.eu/port-chk/などのツールを使用して、ALB および Citrix ADC サービスが利用可能であることを確認します。

```
IP address or host name:
23.99.xx.xx
Port number:"80, 443. etc"
23.99.xx.xx:80 port is open
<!--NeedCopy-->
```

トラブルシューティング

- nstcpdump -Citrix ADC フロントエンドの IP 構成を確認します。
- nstrace -ALB ヘルスプローブの確認

© 1999–2021 Citrix Systems, Inc. All rights reserved.

XenDesktop 7 のデータベースサイズ設定ツール

May 18, 2020

現在、XenDesktop 7 のデータベースのサイジングは、データベースのサイジングに関するサポート技術情報の記事CTX139508を解釈して理解できることに依存しています。リストされた環境にバリエーションがあることがわかっている場合、これは役に立ちません。この支援のために、当社の主要なソフトウェアエンジニアである Chris Gilbert は、カスタムサイズ情報の生成に役立つシンプルなツールを作成しました。

ツールが選ばれる理由

多くの人は、データベースのサイズを決定するために Excel ファイルまたは簡単な数式を求めていますが、これらの方法は複雑さと関係する要因のレベルに基づいて最適ではありません。

このツールは、計算の複雑さを隠し、XenDesktop 7.5 と 7.6 の違いを考慮します。それが消費して表示するデータはむしろ生ですが、改善のためのフィードバックは歓迎されます。

ダウンロード情報

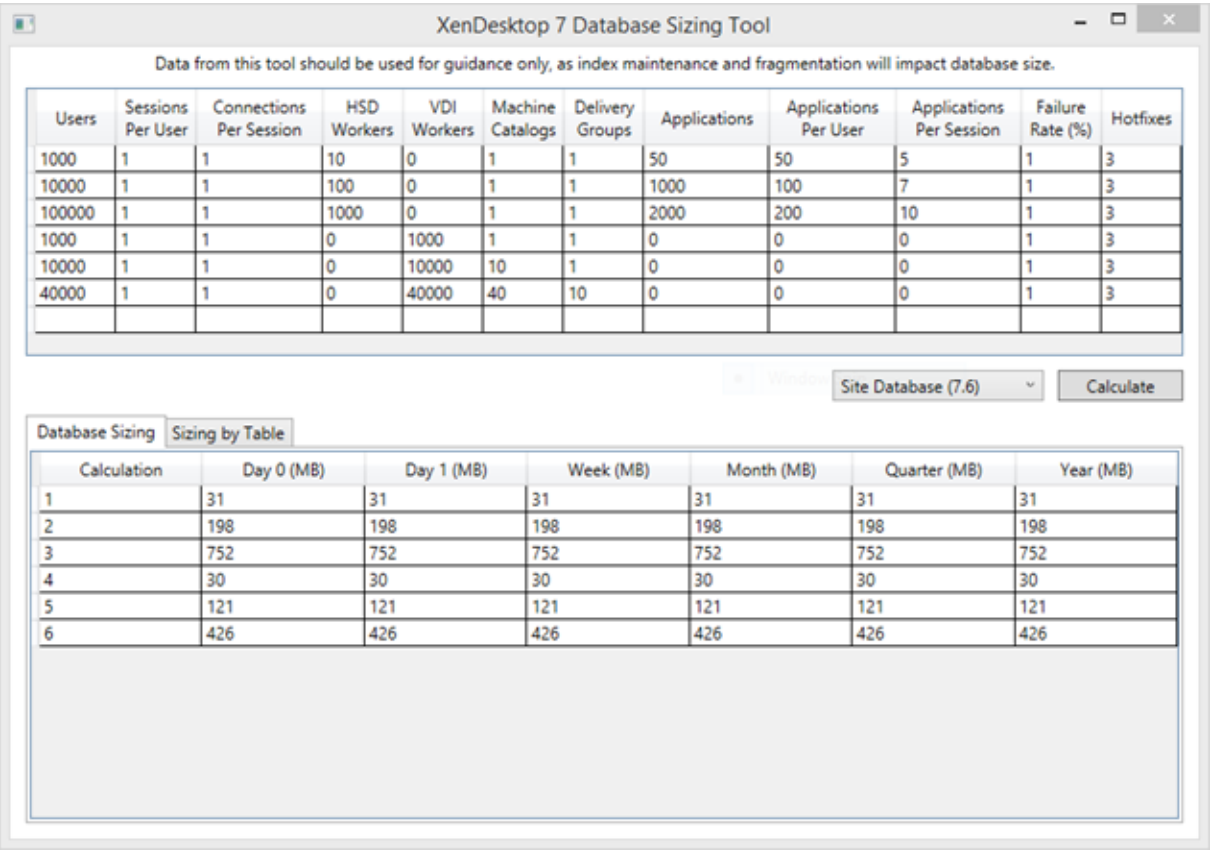
このツールは圧縮された MSI ファイルであるため、インストールとアンインストールは簡単です。このツールが持つ唯一の依存関係は、.NET 4.0 のみです。XenDesktop の一部は必要ありません。

CTX209080からツールをダウンロードします。

ツールの使い方

ツールを起動すると、ウィンドウの上部にセクションが表示され、予想される環境に関するパラメーターを入力できます。既定のセットは、さまざまなサイズの VDI と HSD で、次のスクリーンショットのようになります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



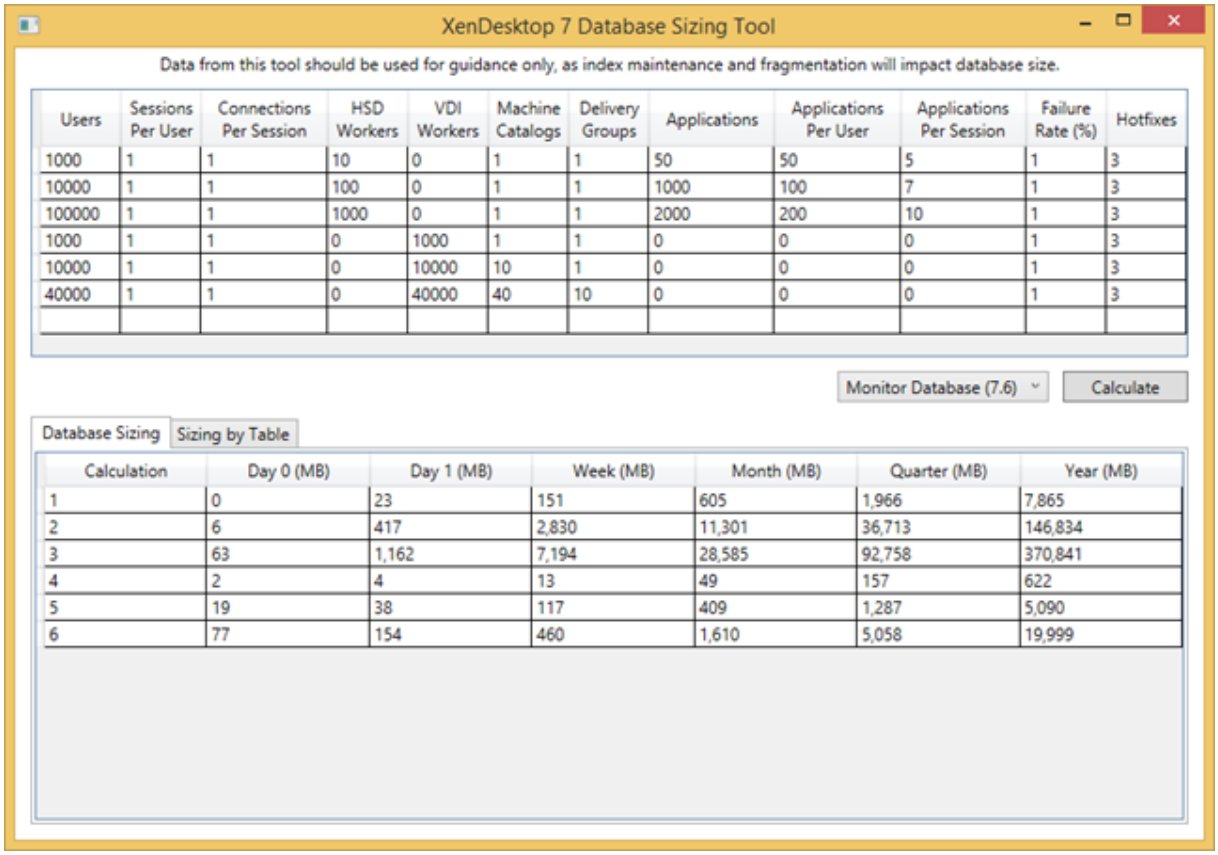
いずれかの行を更新するか、空白の一番下の行に数字を入力し始めると、より多くの行が追加されます。

その後、データベースの種類と XenDesktop のバージョンを選択して **[計算]** をクリックすると、計算が実行され、上のスクリーンショットの下部に表示されるサイズ設定ガイダンスが生成されます。

生成されたデータには、上部のセクションに入力された各行の行が含まれます。列には、さまざまな時点でのおおよそのサイズが表示されます。サイトデータベースの場合、データは蓄積されないため、サイズが最大サイズに達してそこに留まる傾向があります。監視の場合、監視用に構成されたグルーミング設定に応じて、データベースは時間の経過とともに大きくなります。これはライセンスにも依存することに注意してください（たとえば、プラチナのお客様だけがグルーミング間隔を 7 日以上に設定することができます）。

したがって、監視のために、データは次のようになります。

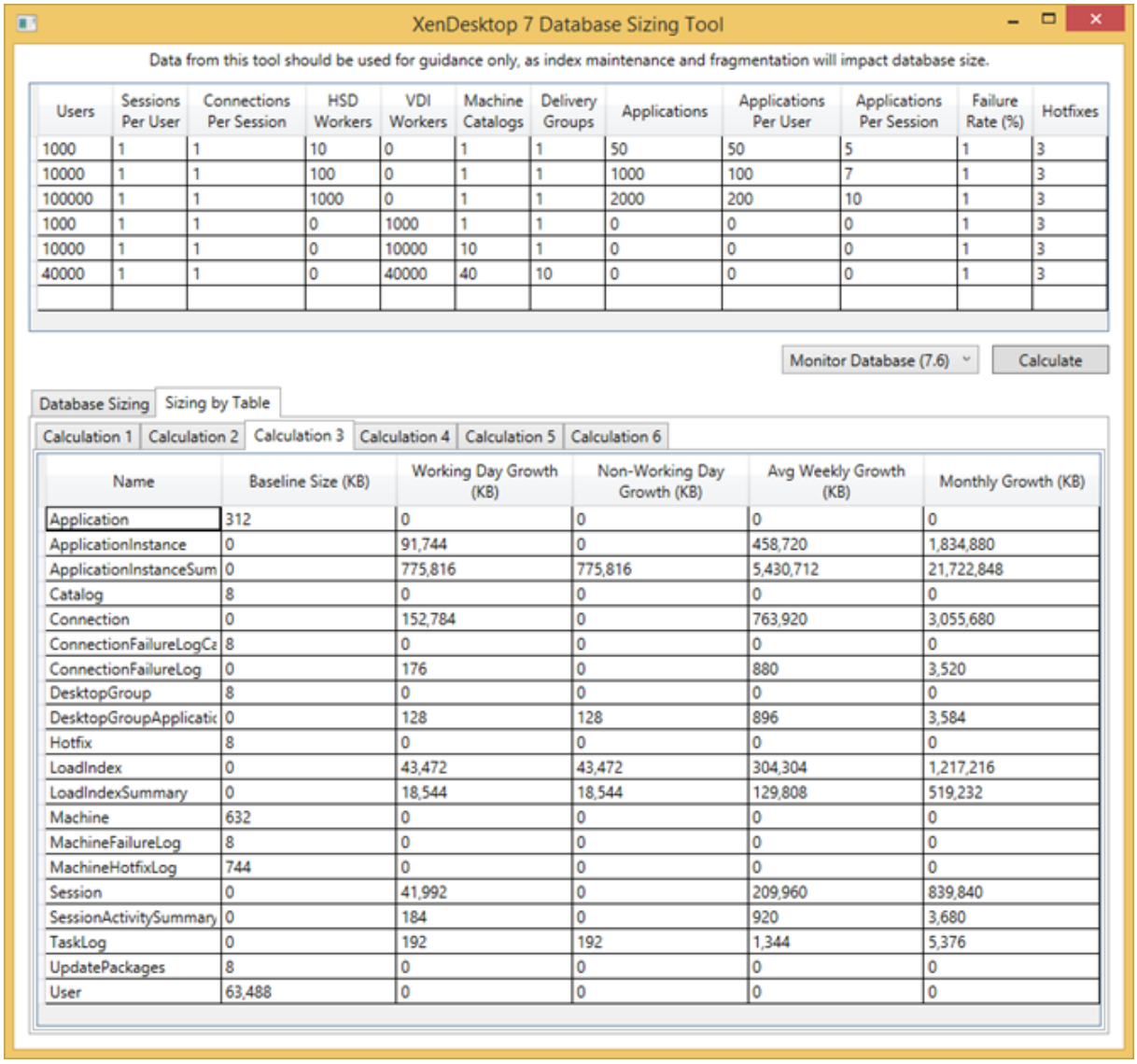
© 1999–2021 Citrix Systems, Inc. All rights reserved.



テーブルの詳細

実際にスペースを消費しているテーブルの詳細については、「テーブルによるサイジング」タブをクリックしてください。このタブには、各計算用のタブがあります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



Users	Sessions Per User	Connections Per Session	HSD Workers	VDI Workers	Machine Catalogs	Delivery Groups	Applications	Applications Per User	Applications Per Session	Failure Rate (%)	Hotfixes
1000	1	1	10	0	1	1	50	50	5	1	3
10000	1	1	100	0	1	1	1000	100	7	1	3
100000	1	1	1000	0	1	1	2000	200	10	1	3
1000	1	1	0	1000	1	1	0	0	0	1	3
10000	1	1	0	10000	10	1	0	0	0	1	3
40000	1	1	0	40000	40	10	0	0	0	1	3

Name	Baseline Size (KB)	Working Day Growth (KB)	Non-Working Day Growth (KB)	Avg Weekly Growth (KB)	Monthly Growth (KB)
Application	312	0	0	0	0
ApplicationInstance	0	91,744	0	458,720	1,834,880
ApplicationInstanceSum	0	775,816	775,816	5,430,712	21,722,848
Catalog	8	0	0	0	0
Connection	0	152,784	0	763,920	3,055,680
ConnectionFailureLogCa	8	0	0	0	0
ConnectionFailureLog	0	176	0	880	3,520
DesktopGroup	8	0	0	0	0
DesktopGroupApplicatic	0	128	128	896	3,584
Hotfix	8	0	0	0	0
LoadIndex	0	43,472	43,472	304,304	1,217,216
LoadIndexSummary	0	18,544	18,544	129,808	519,232
Machine	632	0	0	0	0
MachineFailureLog	8	0	0	0	0
MachineHotfixLog	744	0	0	0	0
Session	0	41,992	0	209,960	839,840
SessionActivitySummary	0	184	0	920	3,680
TaskLog	0	192	192	1,344	5,376
UpdatePackages	8	0	0	0	0
User	63,488	0	0	0	0

このより詳細なビューでは、どのテーブルが大きくなるかを示すため、監視グルーミングを調整して特定の領域を小さくすることができます。ブレークダウンは、ベースラインサイズ（固定サイズなど）をカバーします。一般に、ユーザーまたはマシンに基づくテーブルは毎日増加し（履歴負荷分散情報）、稼働日（接続とセッション）にのみ増加します。これらは、週単位の成長列 (7 日間の週で 5 営業日を想定しています) にロールされ、次に月単位の列にロールされます。

データを **Excel** にエクスポートする

テーブルを Excel にエクスポートするには、テーブル内をクリックし、すべてのコンテンツを選択してコピーし、Excel に貼り付けます。

この記事は、*Chris Gilbert* によって書かれたブログ記事から変更されました。元の投稿を見つけたり、コメントを読んだり、フィードバックを投稿したりすることができます: *https://www.citrix.com/blogs/2014/11/20/database-sizing-tool-for-xendesktop-7/*。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

実装と構成

March 2, 2021

ネットワーク

Citrix ADC と OpenShift 4 ソリューション概要

SC2S での VPX Amazon マシンイメージ（AMI）の作成

Citrix Gateway と Microsoft Azure の多要素認証

Azure DNS プライベートゾーンでの Citrix ADC 展開ガイド

Workspace

データベースの無停止アップグレードのためのローカルホストキャッシュの使用

AWS の Linux 踏み台ホスト経由で RDP 経由で Citrix インフラストラクチャに接続する

SQL サーバーと Citrix データベース

Citrix フェデレーション認証サービスのスケーラビリティ（PDF ダウンロード）

XenApp および XenDesktop のグループポリシー管理テンプレートの更新

XenApp および XenDesktop 7.11 から現在のバージョンまで：遅延および SQL ブロッキングクエリの改善

XenDesktop 7.6 のデータベースサイズ設定ガイダンス

SQL Server 高可用性ソリューションを使用するときにデータベース接続文字列を更新する

ローカルホストキャッシュのサイズ設定とスケーリング

XenApp および XenDesktop 7.9 での Citrix ユニバーサルプリントサーバーの負荷分散

Citrix Endpoint Management

展開

最新かつ完全な XenMobile Server ドキュメントについては、XenMobile Serverを参照してください。

Citrix ADC と OpenShift 4 ソリューション概要

May 18, 2020

© 1999–2021 Citrix Systems, Inc. All rights reserved.

OpenShift が解決する問題と **OpenShift** の概要

Red Hat OpenShift 4 は Kubernetes プラットフォームで、オンプレミス、ハイブリッド、マルチクラウドの展開にエンタープライズグレードの基盤を提供します。

OpenShift Container Platform は、Kubernetes にエンタープライズ対応の拡張機能を提供します。これには、次のようなものがあります。

ハイブリッドクラウドの展開

OpenShift Container Platform クラスターは、さまざまなパブリッククラウドプラットフォームまたはデータセンターにて展開できます。

統合された **Red Hat** テクノロジー

OpenShift Container Platform の主なコンポーネントは、Red Hat Enterprise Linux および関連する Red Hat テクノロジーから来ています。OpenShift Container Platform は、Red Hat のエンタープライズ品質ソフトウェアに対する厳しいテストと認定イニシアチブからメリットを得ています。

オープンソース開発モデル

開発はオープンで完了し、ソースコードは公開ソフトウェアリポジトリから入手できます。このオープンなコラボレーションは、迅速なイノベーションと開発を促進します。

より詳細なリファレンスについては、OpenShift コンテナプラットフォームアーキテクチャを参照してください。

外部ロードバランサーの **OpenShift4** 要件

外部ロードバランサーにより、Kubernetes ノードはクラスター外のサブネットと通信できるようになります。Pod とクラスターは、異なるコンテナーを正しくスケールアップおよびスケールダウンするには、受信トラフィックについて知っておく必要があります。また、適切な受信トラフィックを対応するコンテナーに送信するには、明らかな必要性があるため、これは OpenShift の展開の操作性にとって重要です。OpenShift は、Citrix が提供する外部ロードバランサーを効果的に動作させる必要があります。

つまり、当社のテクノロジー、具体的には、コンテナ化されたアプリケーション Delivery Controller（CPX）と Citrix Ingress Controller（CIC）を組み合わせることで、完全に機能し最適化された OpenShift の展開と、VPX などの自動化された外部 Citrix ADC フォームファクタをサポートできます。MPX、BLX。

Citrix ADC と **OpenShift** 統合のメリット

本番グレードの進入

Citrix ADC は、高度な負荷分散、TLS 終端、L3-L7 プロトコルの最適化、冗長性ソリューションなどの機能を、インターネット最大の Web プロパティと数千の企業に提供します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

柔軟性

Citrix ADC によるアーキテクチャの柔軟性 — Citrix は、クラスター内外のあらゆる環境に対応する ADC フォームファクタの完全な配列を備えています。

可視性とトラブルシューティング

Citrix ADM with Service Graphs は、アプリケーションの正常性とパフォーマンスに関する実用的な洞察を提供し、あらゆる問題に対するプロアクティブなトラブルシューティングを提供します。

より詳細なリファレンスについては、Citrix および Red Hat OpenShift によるマイクロサービスベースのアプリケーションおよび配信を参照してください。

OpenShift の実装

現在 OpenShift '4.x' をお使いの場合は、展開にネットワークトポロジーの要件があることがわかります。以下のセクションでは、Citrix および OpenShift の展開を開始するために必要な構成の前提条件について説明します。

Openshift4 では、以下のセクションで説明するように、各サービスに対して負荷分散サービスと対応する DNS マッピングの両方が必要です。

外部ロードバランシングサービスの前提条件

OpenShift Container Platform をインストールする前に、2 つの Layer-4 負荷分散サービスをプロビジョニングする必要があります。1 つ目は API サーバーによって要求され、2 つ目は、アプリケーションへの入力を提供するために必要です。

また、ネットワークトポロジ要件のためにアクセス可能でなければならない特定のポートもあります。

1. まず、ブートストラップとコントロールプレーン用のポート 6443 (Kubernetes API サーバー) と 22623 (マシン構成サーバー) を開く必要があります。コントロールプレーンの初期化後に、ロードバランサーからブートストラップマシンを削除してください。また、ルーター Pod、コンピューティング、ワーカーでポート 443 (HTTPS トラフィック) と 80 (HTTP トラフィック) を開く必要があります。

   詳しくは、OpenShift4 コンテナプラットフォームのドキュメントの「ネットワークトポロジの要件」を参照してください。

2. 外部 DNS マッピングの前提条件:

クラスターノード:

```
master1.openshift4.example.com +short    10.217.101.X
master2.openshift4.example.com +short    10.217.101.X
master3.openshift4.example.com +short    10.217.101.X
worker1.openshift4.example.com +short    10.217.101.X
worker2.openshift4.example.com +short    10.217.101.X
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
6     bootstrap.openshift4.example.com +short  10.217.101.X
7    <!--NeedCopy-->
```

ETCD ノード:

```
1     etcd-0.openshift4.example.com +short     10.217.101.X
2     etcd-1.openshift4.example.com +short     10.217.101.X
3     etcd-2.openshift4.example.com +short     10.217.101.X
4    <!--NeedCopy-->
```

API エンドポイント:

```
1     api.openshift4.example.com +short        10.217.101.X
2     api-int.openshift4.example.com +short    10.217.101.X
3    <!--NeedCopy-->
```

ワイルドカード DNS エントリ:

```
1     *.apps.openshift4.example.com +short     10.217.101.X
2    <!--NeedCopy-->
```

SRV レコード:

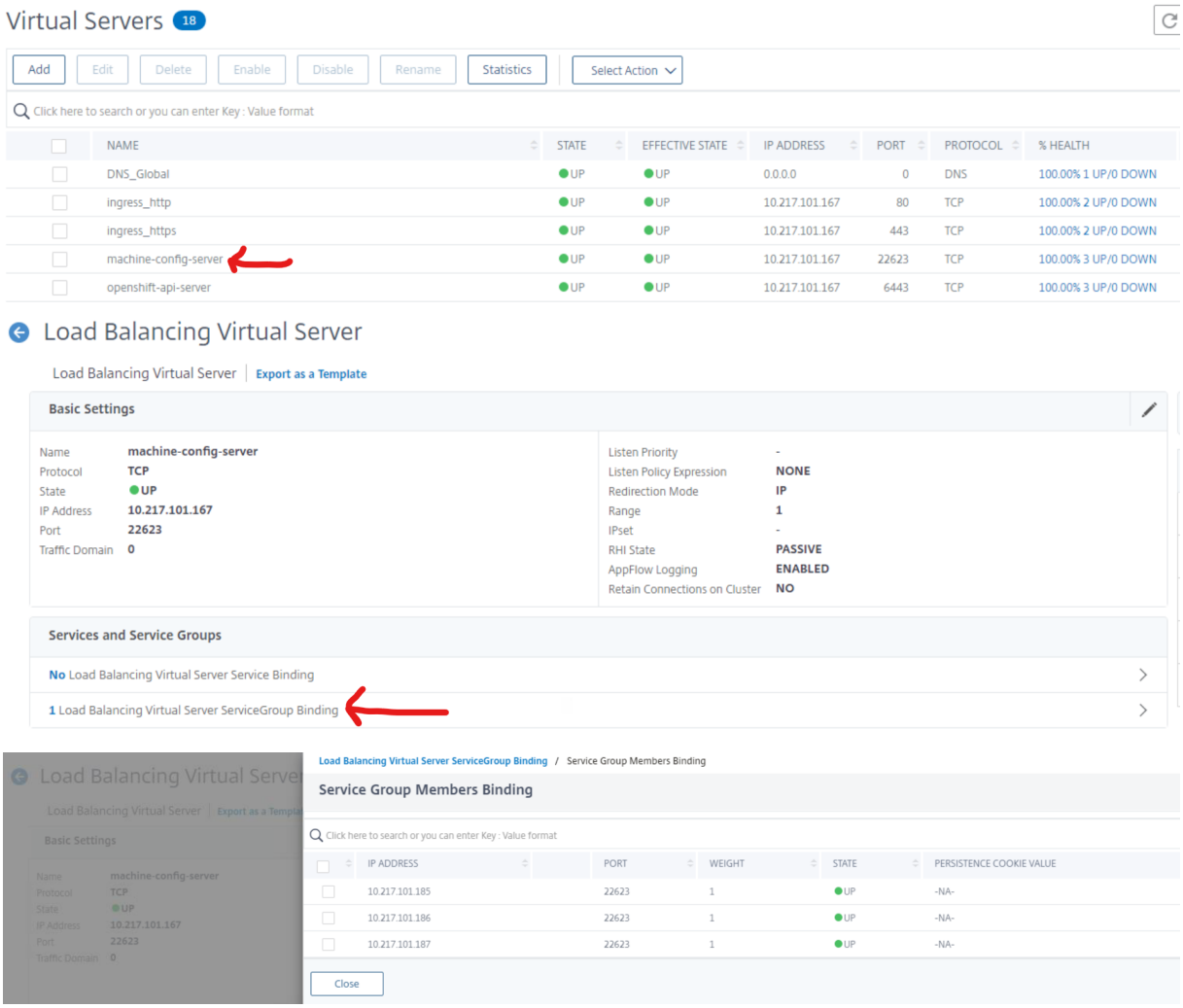
```
1     $ dig _etcd-server-ssl._tcp.openshift4.example.com SRV +short
2
3     0 10 2380 etcd-0.openshift4.example.com
4     0 10 2380 etcd-1.openshift4.example.com
5     0 10 2380 etcd-2.openshift4.example.com
6    <!--NeedCopy-->
```

Citrix ADC の実装

Citrix ADC 構成の概要

正しい仮想 IP が正しいサービスグループメンバーに対応していることを確認したいと考えています。次に示すように、一意の IP アドレス（10.217.101.185、10.217.101.186、10.217.101.187）を持つ 3 つのメンバーを持つサービスグループを指すようにmachine-config-serverを設定しました。

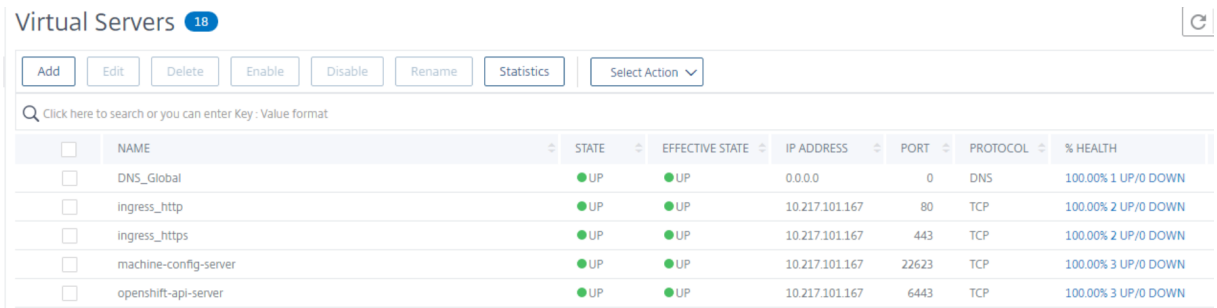
© 1999–2021 Citrix Systems, Inc. All rights reserved.



ADC の仮想サーバーとサービス

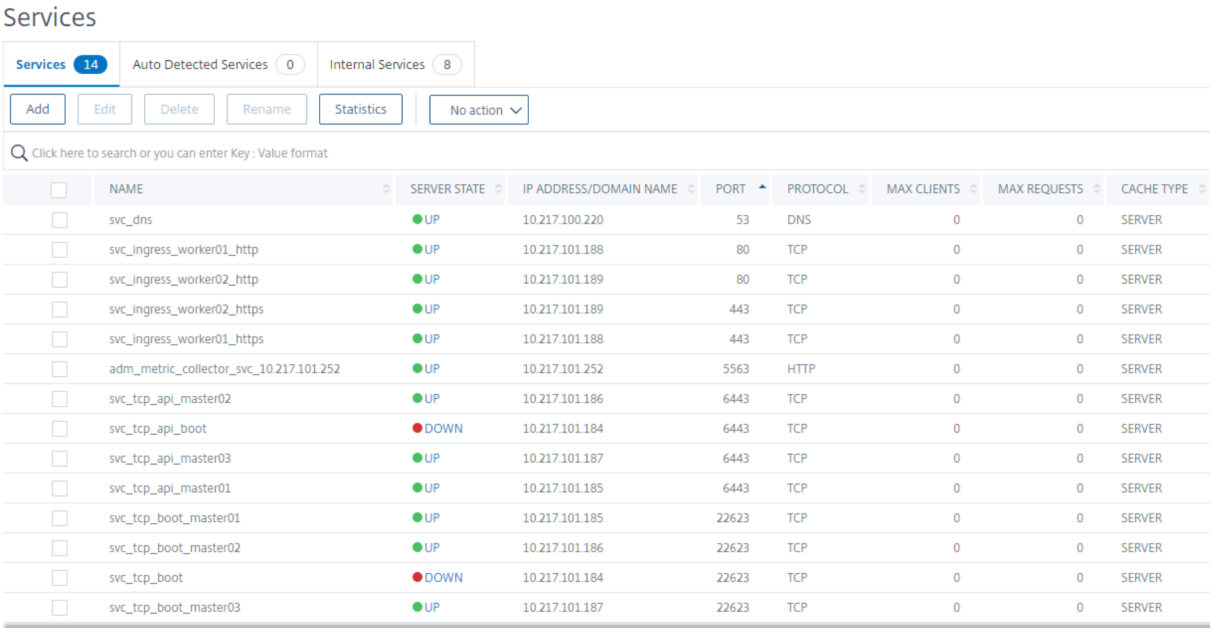
次のイメージを参照として使用して、適切な仮想サーバーおよびサービスが適切なポートで実行されていることを確認します。

仮想サーバ:



サービス:

© 1999–2021 Citrix Systems, Inc. All rights reserved.



概要

Citrix ADC は、OpenShift 4 クラスターにシームレスに統合でき、OpenShift4 のインストール要件に応じて高可用性と DNS サポートを実現するために、クラスターノードコンポーネントに統合された外部負荷分散サービスを提供します。さらに、Citrix CPX および Citrix Ingress Controller を使用して、OpenShift 4 クラスター内に Citrix ADC を統合して、すべてのコンテナ化された展開に対して OpenShift4 と統合することができます。

Citrix Cloud ネイティブソリューションの詳細については、を参照してください Citrix ADC プラットフォーム。

SC2S での VPX Amazon マシンイメージ（AMI）の作成

May 18, 2020

協力者

著者：ジル・フェッシャー、建築家

SC2S は、AWS Marketplace にアクセスできないエアギャップの AWS インスタンス化です。すべての Amazon マシンイメージ（AMI）は、`vmimport` ツールを使用して環境に手動でアップロードする必要があります。Citrix ADC VPX アプライアンスの性質上、イメージファイルが大きすぎて `vmimport` ツールを使用できません。VPX AMI は、将来の使用に備えて起動できるように作成する必要があります。SC2S 専用に次のメソッドを作成しましたが、マーケットプレイスが存在しない場合や、マーケットプレイスで VPX AMI オファリングが利用できない場合など、この性質の将来のユースケースに使用できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

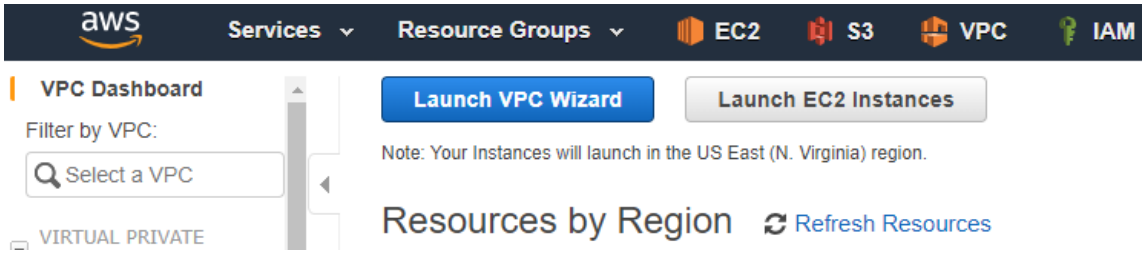
SC2S で VPX を作成する：ローサイドのステップ（商用 AWS）

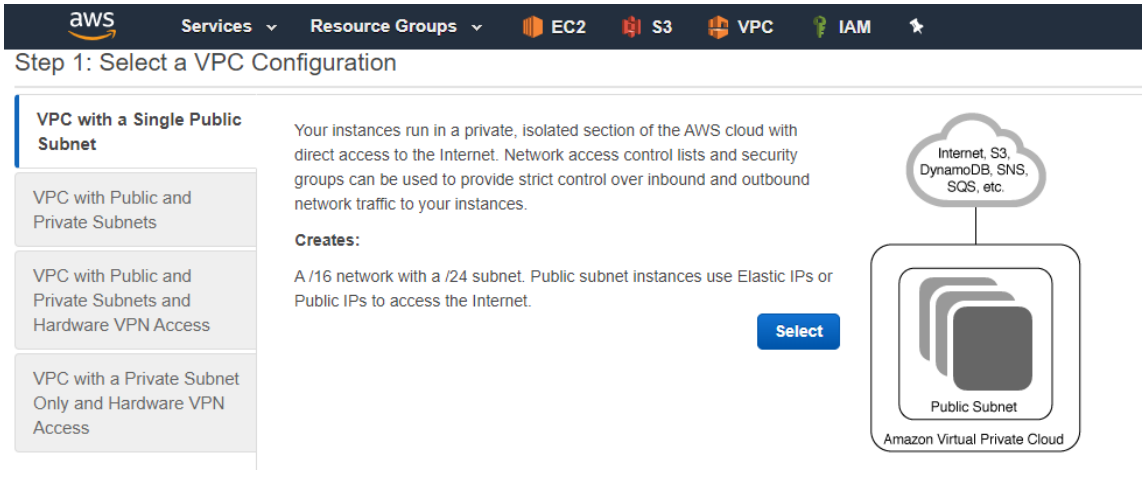
1. Citrix ADC C が SC2S に存在する VPC と同じ CIDR ブロックを使用して、UC2S（商用）に VPC とサブネットを作成します。（たとえば、VPC ウィザードを使用して、サイズが 10.0.0.0/16 の VPC を作成し、サイズが 10.0.0.0/24 の単一のパブリックサブネットを作成します）。

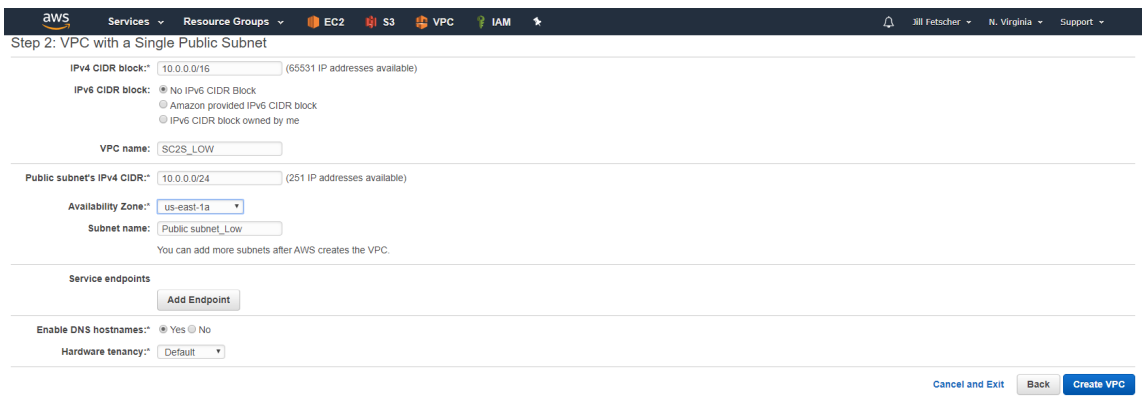
   これは、次の 2 つの方法のいずれかを実行できます。

   - 基本的な CIDR とサブネットを使用して SC2S でテスト VPC を作成する
   - SC2S で使用されている CIDR とサブネットをコピーします。

   > 注:C2S
   >
   > の場合、VPC の作成はサービスを通じて行われ、スーパーネットから IP スペースが自動的に割り当てられます。この場合、第 2 の方法が必要である。GovCloud については、詳細な手順を待つか、マーケットプレイスから最新バージョンの VPX をダウンロードしてください。

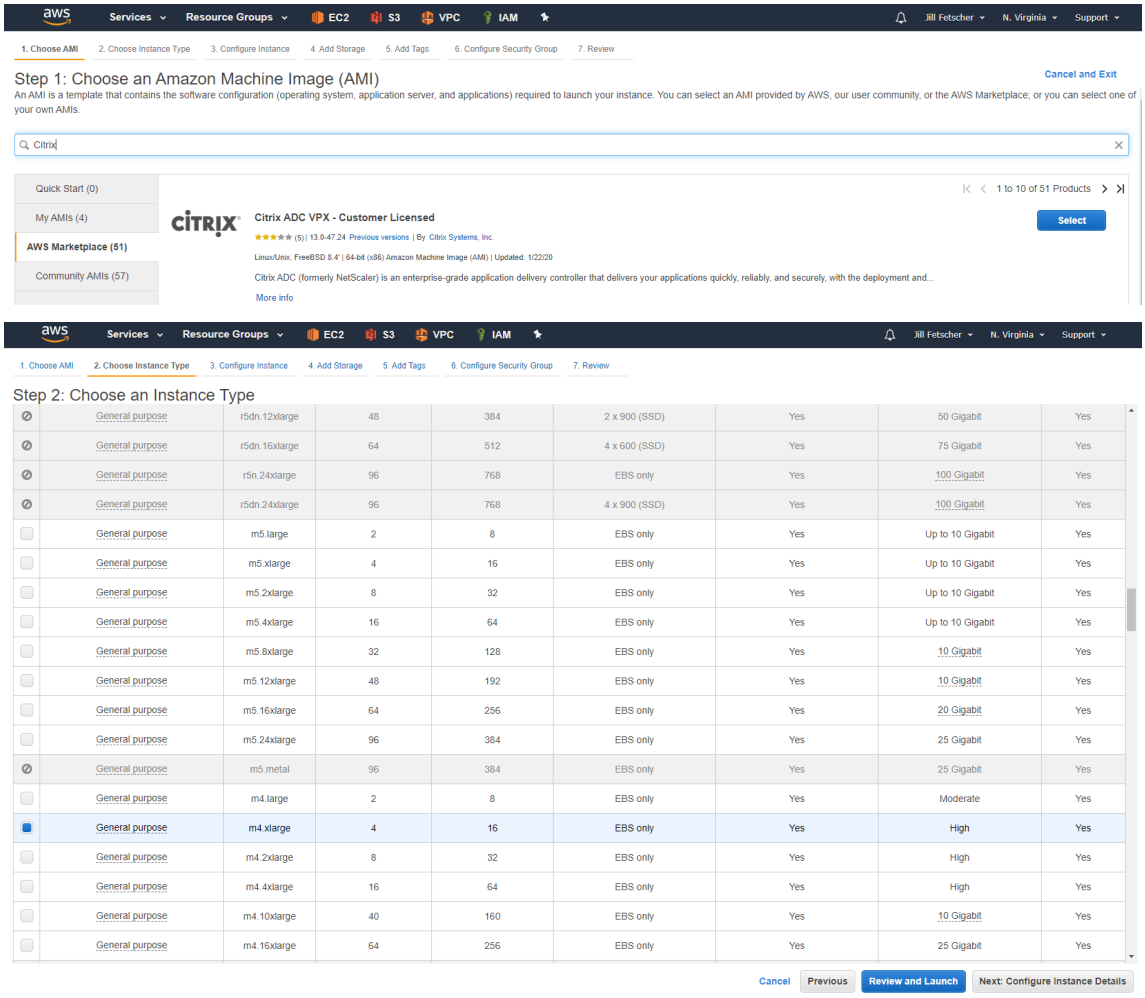






© 1999–2021 Citrix Systems, Inc. All rights reserved.

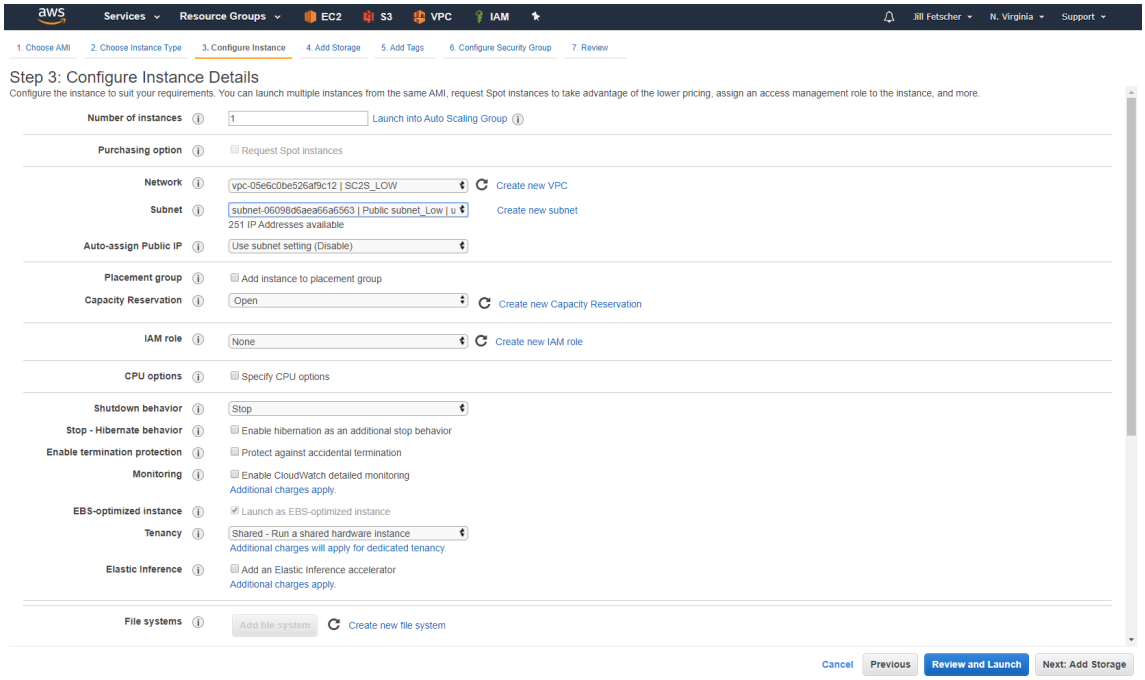
2. AWS マーケットプレイスの Citrix ADC AMI から EC2 インスタンスを展開します。インスタンスは カスタマーライセンスが必要です。非 Nitro ベースのインスタンス (`m4.xlarge`など) を使用します。



⊘	General purpose	r5dn.12xlarge	48	384	2 x 900 (SSD)	Yes	50 Gigabit	Yes
⊘	General purpose	r5dn.16xlarge	64	512	4 x 600 (SSD)	Yes	75 Gigabit	Yes
⊘	General purpose	r5n.24xlarge	96	768	EBS only	Yes	100 Gigabit	Yes
⊘	General purpose	r5dn.24xlarge	96	768	4 x 900 (SSD)	Yes	100 Gigabit	Yes
☐	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
☐	General purpose	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
☐	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
☐	General purpose	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
☐	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
⊘	General purpose	m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes
☐	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
☑	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
☐	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
☐	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes
☐	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit	Yes
☐	General purpose	m4.16xlarge	64	256	EBS only	Yes	25 Gigabit	Yes

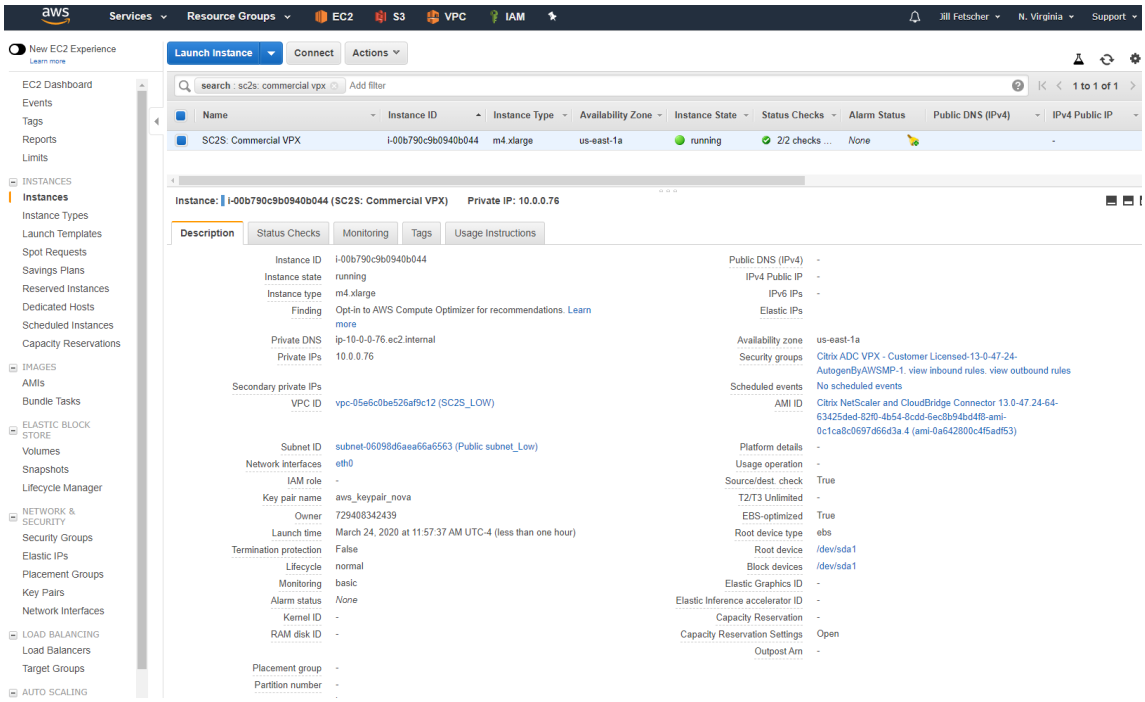
前のステップで作成した VPC を選択します。パブリック **IP** の自動割り当てを無効にします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



わかりやすい名前で、インスタンスに名前を付けます。以下の手順で多数のインスタンスを作成し、さらに設定するには、各インスタンスを特定する必要があります。

セキュリティグループが自動入力されます。インスタンスの起動の残りの手順は、**[次へ]** をクリックします。



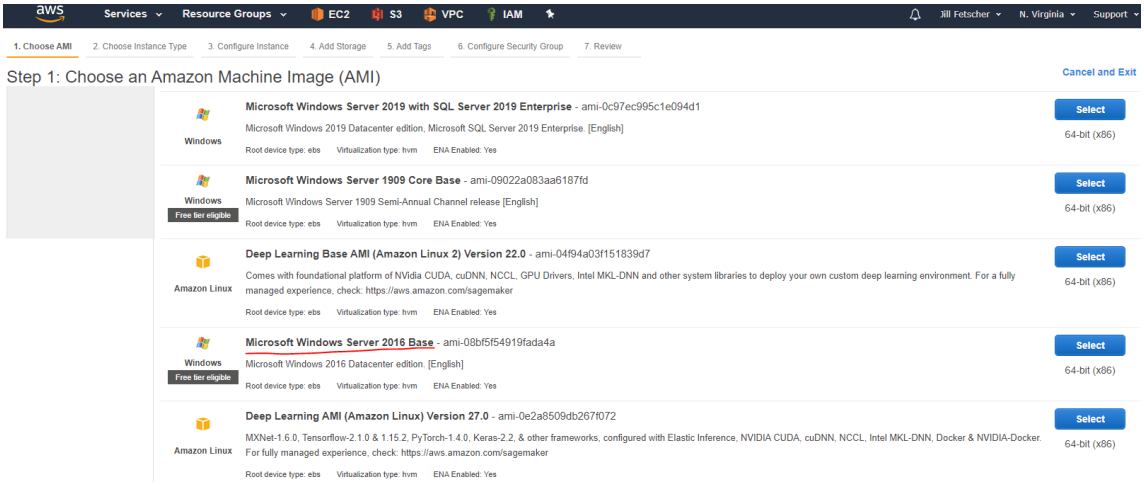
3. Windows Server 2019 または 2016 ベース踏み台ホストを作成して、VPX インスタンスに到達します。

   このインスタンスは`m4.xlarge`にすることができ、自動割り当てられたパブリック IP を使用して、Citrix ADC と同じ VPC および AZ に構築する必要があります。ルートボリュームには最低 45 GiB の汎用 SSD

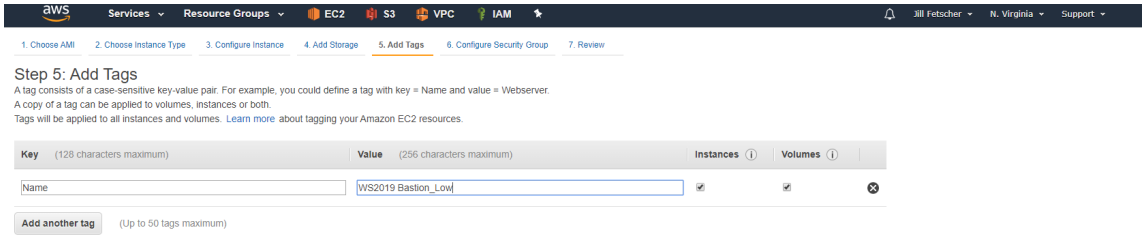
© 1999–2021 Citrix Systems, Inc. All rights reserved.

(gp2) が必要です。

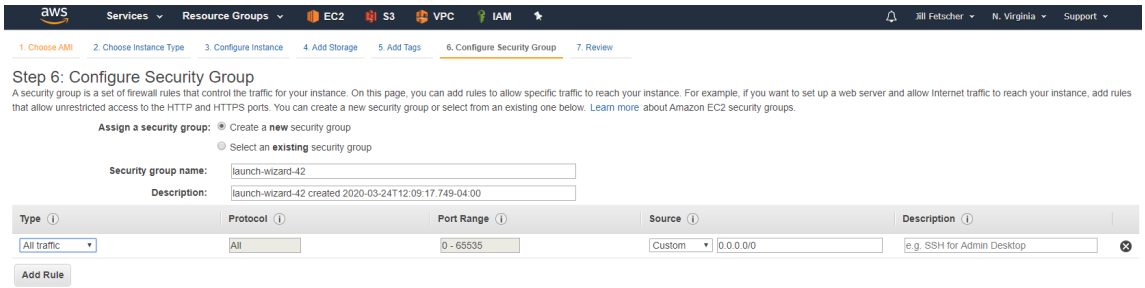
> 注:
>
> 環境で Elastic IP（EIP）の作成が許可されている場合は、踏み台ホストの作成をスキップできます。VPX インスタンスはネットワークまたはインターネットから直接接続できます。セキュリティ上の目的で、踏み台ホストの使用を推奨します。また、エアギャップのある環境では EIP の可用性が欠如しています。



インスタンスに認識可能な名前を付けます (たとえば、SC2S: WS2016 Bastion Low)。



簡単にするために、すべてのトラフィックを許可するセキュリティグループを作成します。このセキュリティグループは後でロックダウンできます。



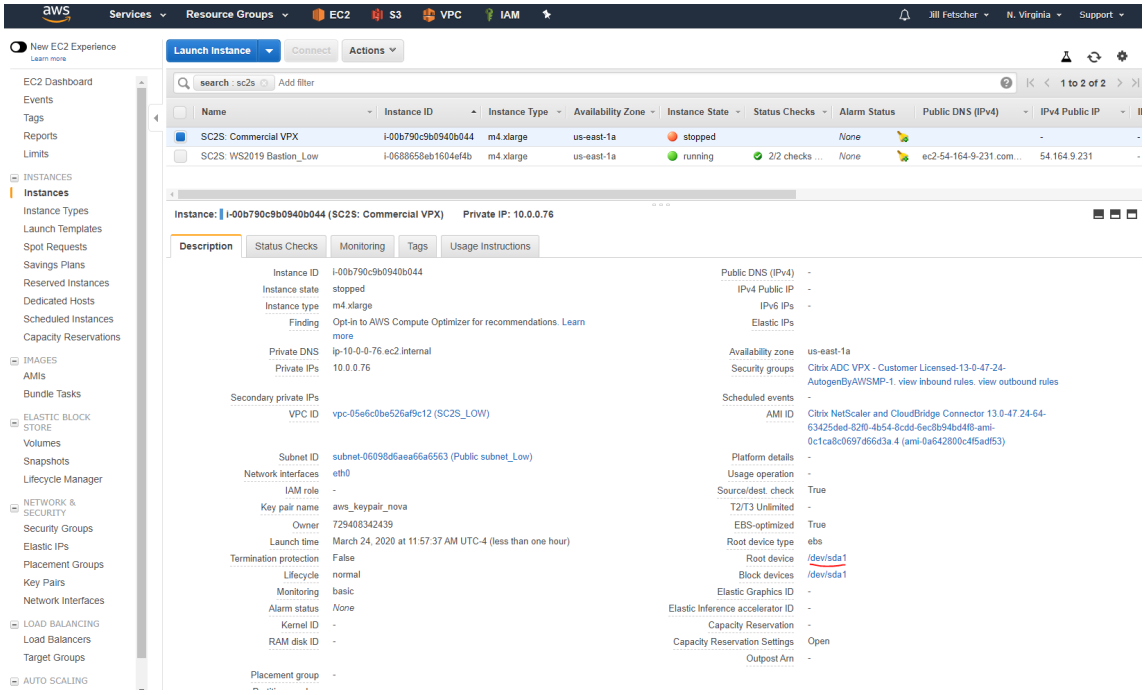
インスタンスの準備ができたら、パブリック IP を使用してマシンに RDP インします。次に、PuTTY と WinSCP をダウンロードし、VPX インスタンスの作成に使用されたキーペアをコピーします。これには、PuttyGen を使用して.pem を.ppk に変換する必要があります。サーバーマネージャーで、Windows ファイアウォールと Internet Explorer セキュリティ強化を無効にします。PuTTY を使用して、新しくデプロイ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

した Citrix ADC アプライアンスに SSH 接続できることを確認します。インスタンスの `nsroot` パスワードをメモします。デフォルトでは、これは AWS インスタンス ID です。後のステップで必要になるように、インスタンスのプライベート IP を書き留めておきます。この段階では、Citrix ADC アプライアンスが動作しています。

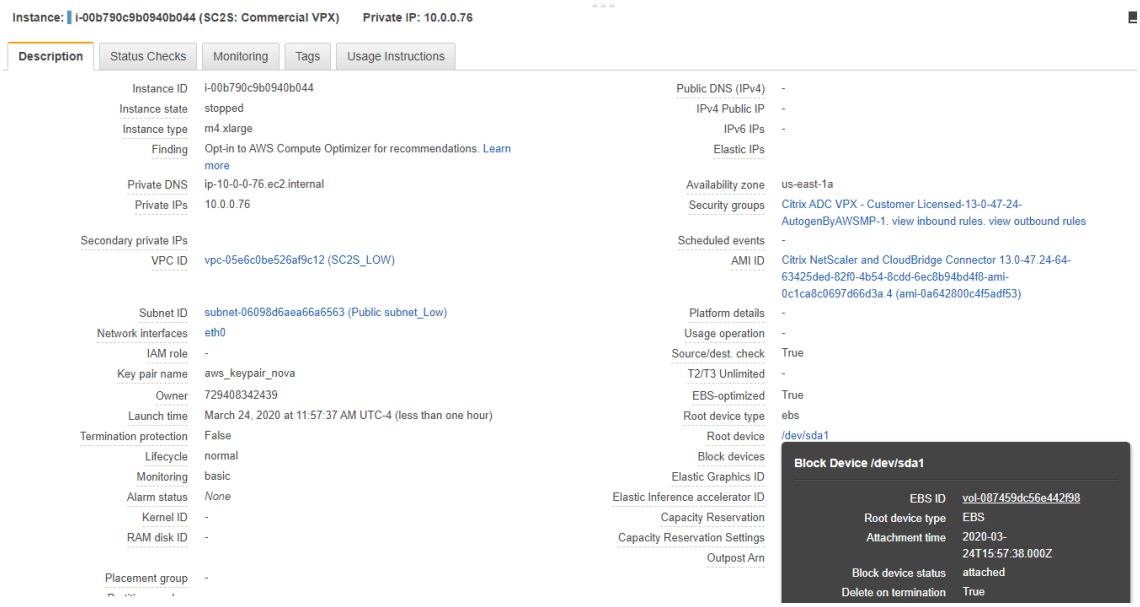
> 注：この VPX を設定
>
> しないでください！ログインするだけで、`nsroot` 機能を検証できます。

4. AWS コンソールから Citrix ADC インスタンスをパワーオフします。Citrix ADC インスタンスからルート EBS ボリュームをデタッチします。

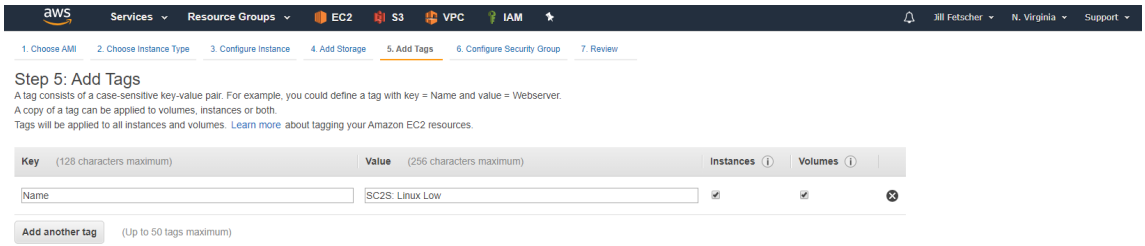


ルートボリュームをデタッチするには、ルートデバイスをクリックし `/dev/sda1`、ボリューム ID をクリックします。[ボリューム] タブで、ボリュームを選択し、認識可能な名前を付けて (たとえば、**SC2S: Commercial Root Vol**)、ボリューム ID を書き留めます。[** アクション] > [ボリュームのデタッチ] > [OK]** をクリックします。これで、ボリュームの状態が [**Available]** になります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

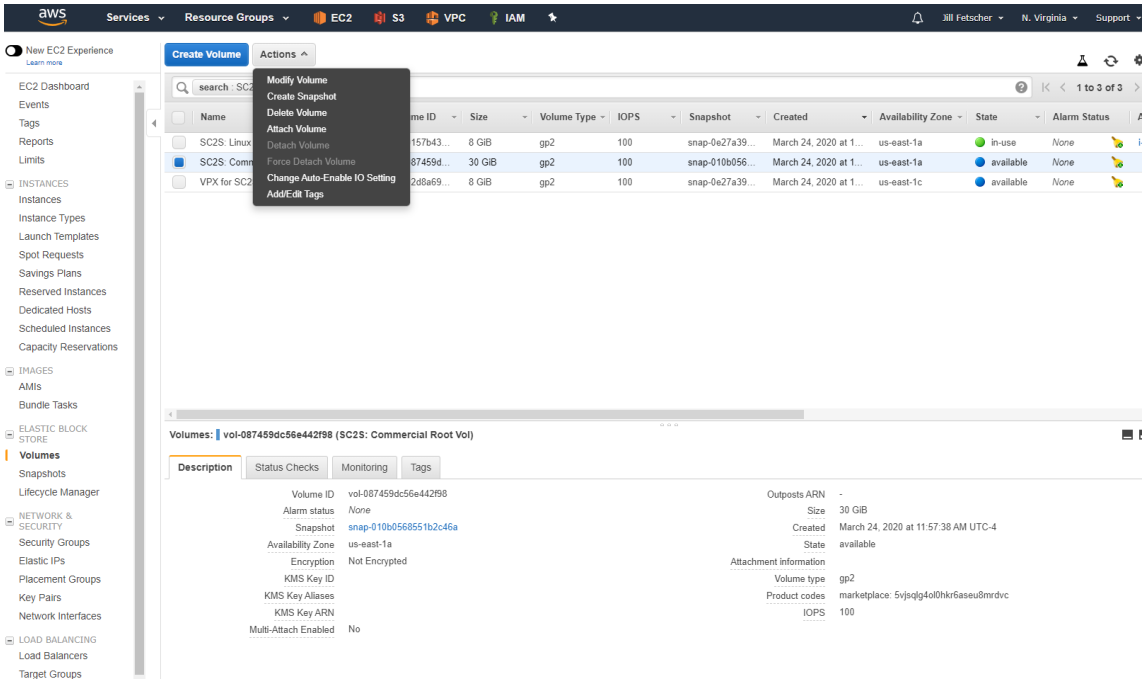


5. 新しい Amazon Linux EC2 インスタンス（Amazon Linux 2 AMI（HVM）、SSD ボリュームタイプ、64 ビット、EBS バックアップ、ENA 対応）をデプロイします。このインスタンスは、以前にデプロイした VPX インスタンスと同じインスタンスタイプ（たとえば `m4.xlarge`）で、同じ VPC とサブネットに存在し、「パブリック IP の自動割り当て」設定を無効にする必要があります。インスタンスに認識可能な名前を付けます (たとえば、**SC2S: Linux Low**)。すべてのトラフィックを許可するようにセキュリティグループを設定します。インスタンスが起動したら、電源を切ります。

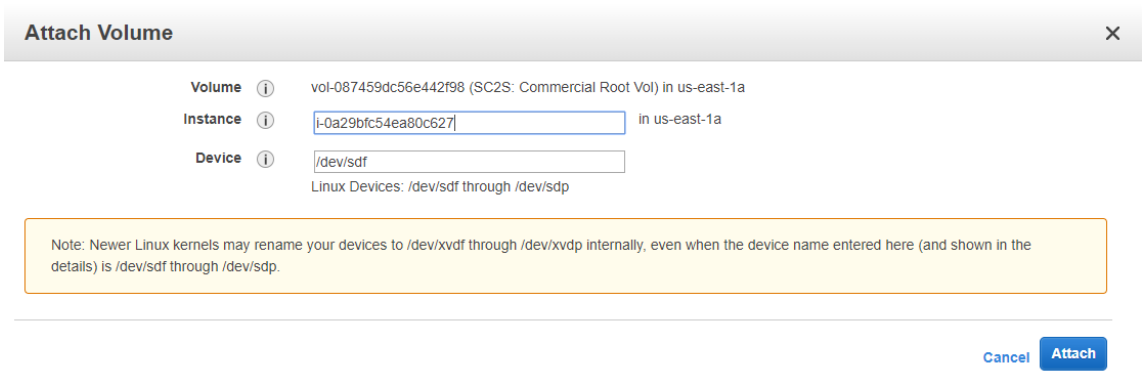


6. VPX から切り離されたルート EBS ボリュームを Linux EC2 インスタンスにアタッチします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

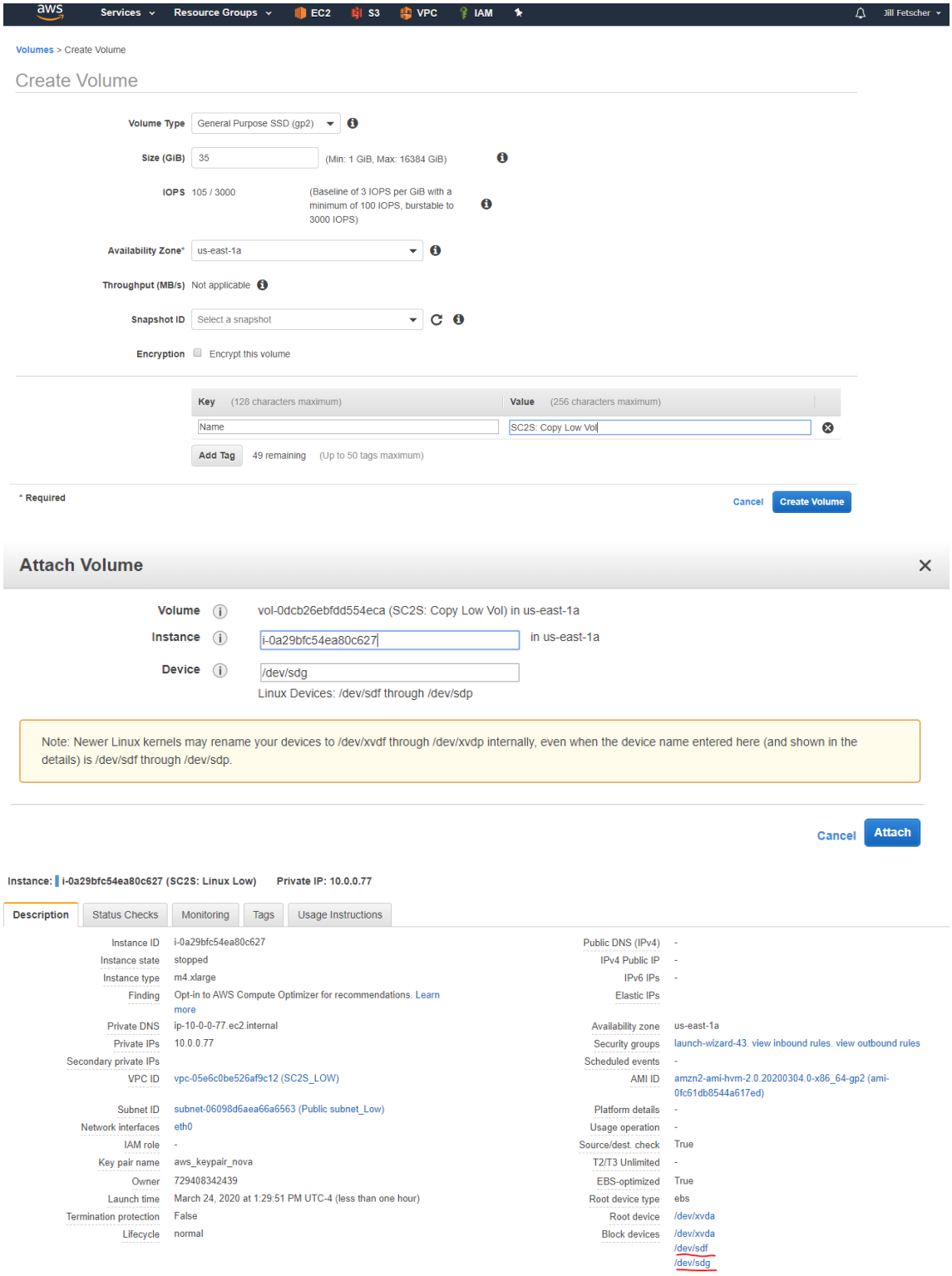


[インスタンス] > [アタッチ] をクリックして、作成した Linux インスタンスを選択します。



7. ルート VPX ボリュームよりも容量の大きいボリュームを作成します。VPX ボリュームのルートボリューム容量は 30 GiB です。容量が 35 GiB のボリュームを作成します。ボリュームタイプを General Purpose SSD (gp2) に設定し、認識可能な名前を付けます (**SC2S: Copy Low Vol**)。新しいボリュームを Linux インスタンスにアタッチします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



8. Linux インスタンスをパワーオンし、プライベートキーファイルを使用して踏み台ホストから SSH インスタンスに接続します。としてログイン `ec2-user*`します。

9. NEW EBS ボリュームにパーティションを作成します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> この例では、VPX ルートボリューム **SC2S:** 商用ルートボリュームは /dev/sdf 、新しく作成された 35 GiB ボリューム **SC2S:** コピー低ボリュームはです /dev/sdg。パーティションは、**SC2S:** 低ボリュームコピーのみで作成されます。AWS コンソールでは、これらのブロックデバイスはシンボリックリンクで示されます。Linux インスタンスでは、/dev/sdf および /dev/sdg がそれぞれ /dev/xvdf および /dev/xvdg として参照されます。

Linux CLI で、ファイルシステムがないことを確認します。応答は データのみである必要があります。

```
sudo file  -s /dev/xvdg
<!--NeedCopy-->
```

ファイルシステムを作成します。

```
sudo mkfs -t xfs /dev/xvdg
<!--NeedCopy-->
```

マウントポイントを作成し、デバイスをマウントします。

```
sudo mkdir /copy
<!--NeedCopy-->
```

```
sudo mount  /dev/svdg /copy
<!--NeedCopy-->
```

デバイスがマウントされていること、および 3 つのデバイス（xvdaxvdf、など xvdg）があることを確認します。

```
lsblk
<!--NeedCopy-->
```

を使用して fdisk、n パーティションを作成します。新しいパーティション、プライマリパーティ p ション、パーティション番号、および 1 最初と最後のセクタ (ENTER、ENTER)。終了するには、CRTL+C キーを押します。

```
sudo fdisk /dev/xvdg
>n
>p
>1
>enter
>enter
>CTRL+C
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

10. VPX ルートボリュームを新しい EBS ボリュームにブロックレベルでコピーします（たとえば、**SC2S:** 商用ルートボリュームを **SC2S:** コピー低ボリューム)。ここで作成したファイルは `citrixADC.img`、SC2S 環境に移動できます。

```
sudo dd if=/dev/xvdf of=/copy/citrixADC.img status=progress
<!--NeedCopy-->
```

このコピーには数時間かかる場合があります。

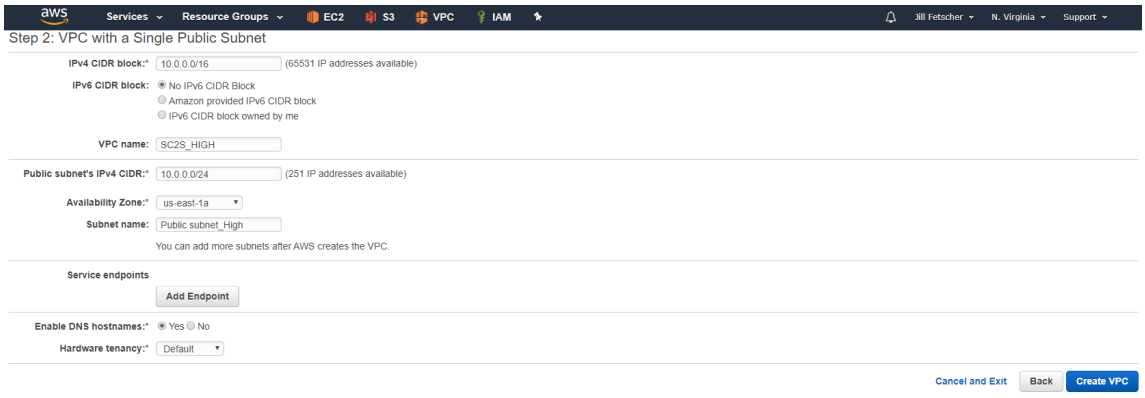
ファイルのコピーが完了したら、ファイルが /copy ディレクトリにあることを確認し、読み取り、書き込み、実行を許可するようにファイルのアクセス許可を変更します。

```
ls /copy
sudo chmod 777 /copy/citrixADC.img
<!--NeedCopy-->
```

11. WinSCP は、ハイサイドまで DTO できる場所に `citrixADC.img` ファイルを移動します。必要な場合、踏み台は、イメージファイルをにコピーするのに十分な大きさです。

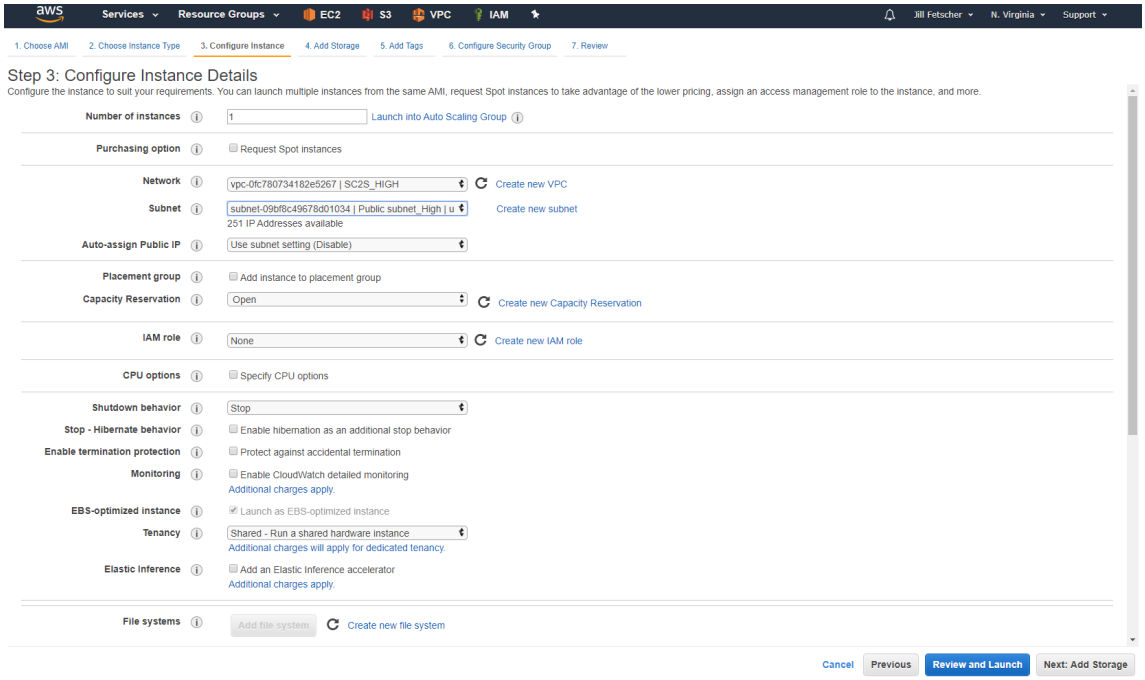
SC2S での **VPX** の作成-ハイサイドでのステップ

1. Low 側のステップ 1 と同じ CIDR ブロックとサブネットを持つ VPC を作成するか、既存の VPC を使用します。この例では、VPC の CIDR は 10.0.0.0/16 で、サブネット IP スペースは 10.0.0.0/16 です。作成される最終的な VPX は、商用マーケットプレイスのオリジナルと同じ IP でなければならないため、これは非常に重要です。



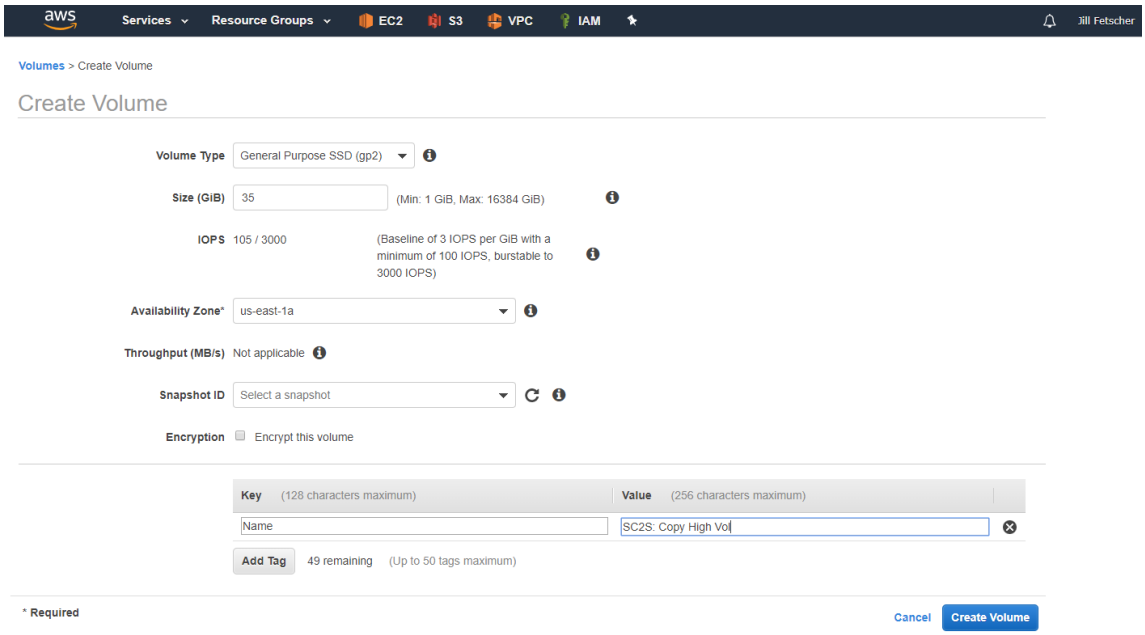
2. 新しい VPC およびサブネットで、ローサイドにデプロイされた Citrix ADC インスタンスと同じインスタンスタイプの Amazon Linux（Amazon Linux 2 AMI（HVM)、SSD ボリュームタイプ、EBS-backed、ENA 対応、64 ビット）のインスタンスを起動します（例: `m4.xlarge`)。インスタンスに認識可能な名前を付けます (たとえば、SC2S: Linux High)。インスタンスの準備ができたら、電源を切ります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



3. 転送されたファイルサイズよりも大きい容量の EBS ボリュームを 2 つ追加します（例：35 GiB）。これらのボリュームは、ローサイドで作成されたものと同じ SSD タイプ (gp2) でなければなりません。

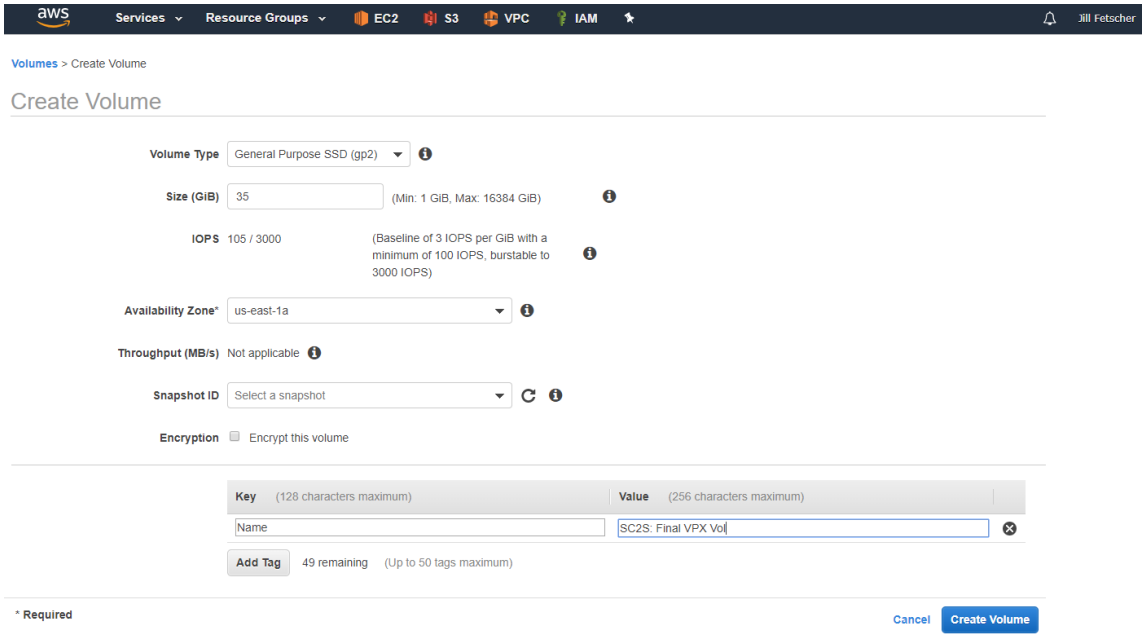
   a) 第 1 巻はローサイドからのコピー用です。ボリュームに認識可能な名前を付けます (「SC2S: コピー高ボリューム」など)。このボリュームを SC2S の新しい Linux インスタンスに/dev/sdfとしてアタッチします。これは、インスタンスの /dev/xvdf のシンボリックリンクです。



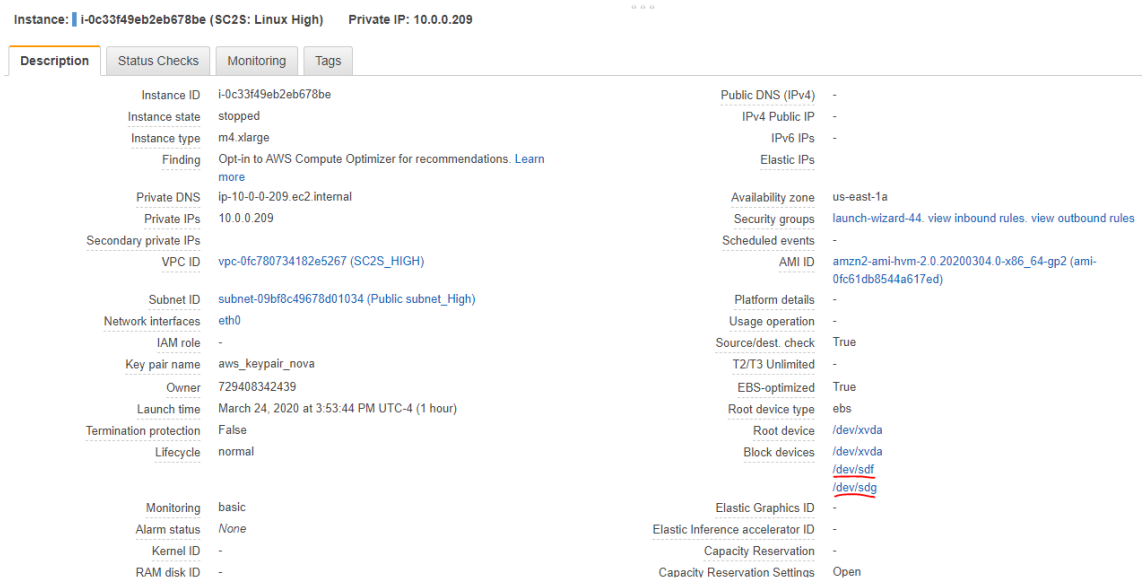
   a) 2 番目のボリュームが新しい VPX のルートボリュームになります。ボリュームに認識可能な名前を付けます (「SC2S: Final VPX Vol」など)。このボリュームを SC2S の新しい Linux インスタンスに/dev/sdgとしてアタッチします。これは、インスタンスの /dev/xvdg のシンボリックリンクで

© 1999–2021 Citrix Systems, Inc. All rights reserved.

す。



これで、インスタンスには、ルートデバイスを含む 3 つのブロックデバイスがアタッチされました。インスタンスをパワーオンします。



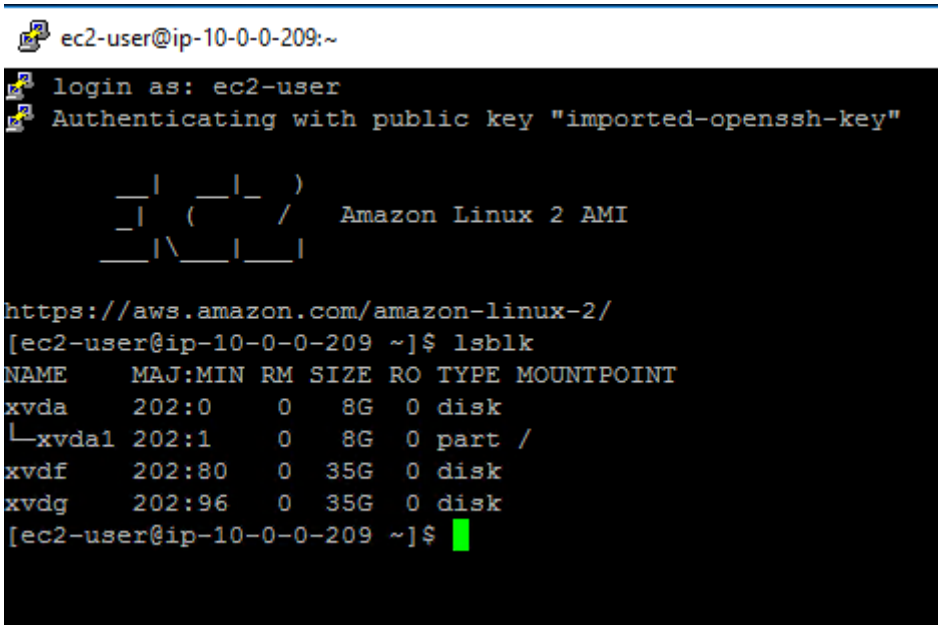
4. ハイサイドの Windows Server 2019 または 2016 ベース踏み台ホストを、ローサイド踏み台と同じ方法で作成します。このインスタンスは、新しく作成された VPC とサブネットにあり、ファイル転送には少なくとも 45 GiB である必要があります。「パブリック IP の自動割り当て」を有効に設定します。インスタンスに認識可能な名前（「SC2S: WS2016 Bastion_High」など）を指定し、セキュリティグループに「すべてのトラフィック」を許可するように設定します。

5. 踏み台ホストの準備ができたら、パブリック IP を使用してマシンに RDP インし、PuTTY と WinSCP をダウンロードし、VPX インスタンスの作成に使用されたキーペアにコピーします。これには、PuttyGen を使

© 1999–2021 Citrix Systems, Inc. All rights reserved.

用して.pem を.ppk に変換する必要があります。サーバーマネージャーで、Windows ファイアウォールと Internet Explorer のセキュリティ強化を無効にします。

6. CitrixADC.img ファイルを新しい踏み台ホストにコピーします。
7. AWS プライベートキーとユーザー名を使用して、踏み台ホストから新しい Linux インスタンス（「SC2S: Linux High」など）への PuTTY セッションを開始します `ec2-user`。
8. `lsblk` を使用して、すべてのデバイスがインスタンスに存在することを確認します。



9. `/dev/xvdf` デバイスにファイルシステムがないことを確認してから、ファイルシステムを作成します。

> 注:
>
> `/dev/xvdg` デバイス上にファイルシステムを作成しないでください。

```
sudo file -s /dev/xvdf
sudo mkfs -t xfs /dev/xvdf
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

10. デバイスのマウントポイントを作成し、デバイスをマウントして、ボリュームマウントポイントが/copyであることを確認します。

```
sudo mkdir /copy
sudo mount /dev/xvdf /copy
lsblk
<!--NeedCopy-->
```

```
[ec2-user@ip-10-0-0-209 ~]$ sudo mkdir /copy
[ec2-user@ip-10-0-0-209 ~]$ sudo mount /dev/xvdf /copy
[ec2-user@ip-10-0-0-209 ~]$ lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   8G  0 disk
└─xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  35G  0 disk /copy
xvdg    202:96   0  35G  0 disk
```

11. を使用してパーティションを作成します fdisk。

```
sudo fdisk /dev/xvdf
 >n
 >p
 >1
 >enter
 >enter
 >CTRL+C
<!--NeedCopy-->
```

```
[ec2-user@ip-10-0-0-209 ~]$ sudo fdisk /dev/xvdf

Welcome to fdisk (util-linux 2.30.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

The old xfs signature will be removed by a write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xaa805ecb.

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-73400319, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-73400319, default 73400319):

Created a new partition 1 of type 'Linux' and of size 35 GiB.

Command (m for help): ^C
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

12. /copy ディレクトリの権限を変更します。

```
sudo chmod 777 /copy
<!--NeedCopy-->
```

```
[ec2-user@ip-10-0-0-209 ~]$ sudo chmod 777 /copy
```

13. 踏み台ホストで WinSCP を使用して、Linux インスタンスに接続します。CitrixADC.img ファイルを /copy ディレクトリにコピーします。ファイルがコピーされたら、WinSCP コンソールから読み取り、書き込み、および実行を許可するようにアクセス許可を変更します。

14. Linux CLI で、次のコマンドを使用してイメージファイルを /dev/xvdg デバイスにコピーします。

```
sudo dd if=/copy/citrixADC.img of=/dev/xvdg status=progress
<!--NeedCopy-->
```

```
[ec2-user@ip-10-0-0-209 ~]$ sudo dd if=/copy/citrixADC.img of=/dev/xvdg status=progress
62337536 bytes (62 MB) copied, 5.000519 s, 12.5 MB/s
```

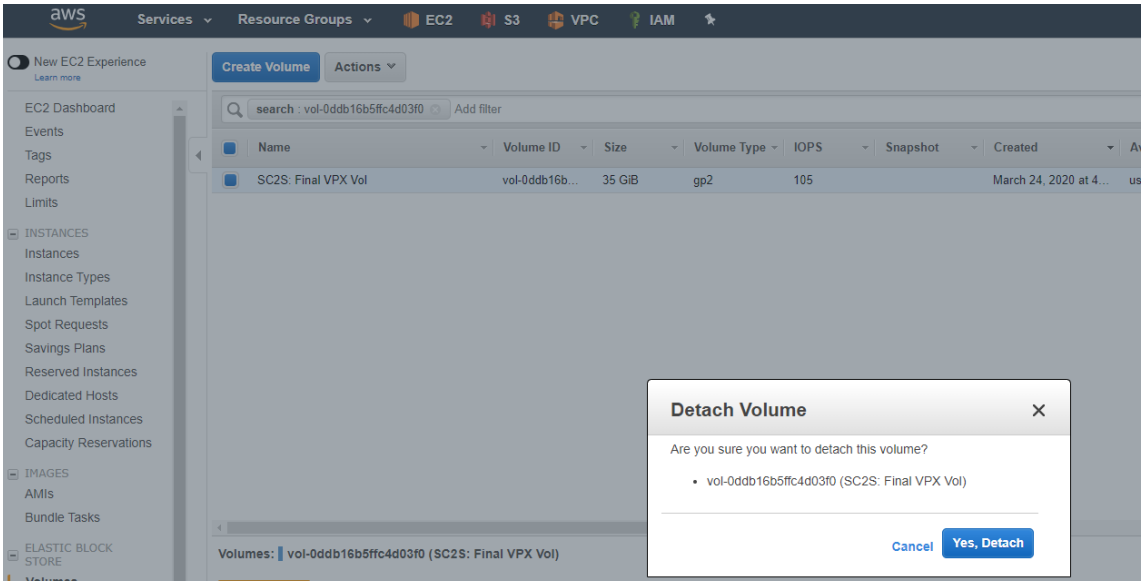
15. コピーが完了したら、`lsblk` コマンドを実行して、Citrix ADC パーティションが/dev/xvdg デバイスに表示されていることを確認します。

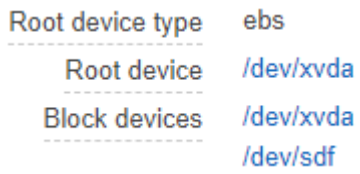
```
lsblk
<!--NeedCopy-->
```

```
[ec2-user@ip-10-0-0-209 ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
└─xvda1 202:1    0    8G  0 part /
xvdf    202:80   0   35G  0 disk /copy
xvdg    202:96   0   35G  0 disk
├─xvdg1 202:97   0   20G  0 part
├─xvdg5 202:101  0  1.5G  0 part
├─xvdg6 202:102  0  4.4G  0 part
├─xvdg7 202:103  0    5M  0 part
├─xvdg8 202:104  0 13.7G  0 part
└─xvdg9 202:105  0  5.9M  0 part
```

16. Linux インスタンスの電源を切り、/dev/xvdg (/dev/sdg) ボリューム (「SC2S: 最終的な VPX ボリューム」など) をデタッチします。

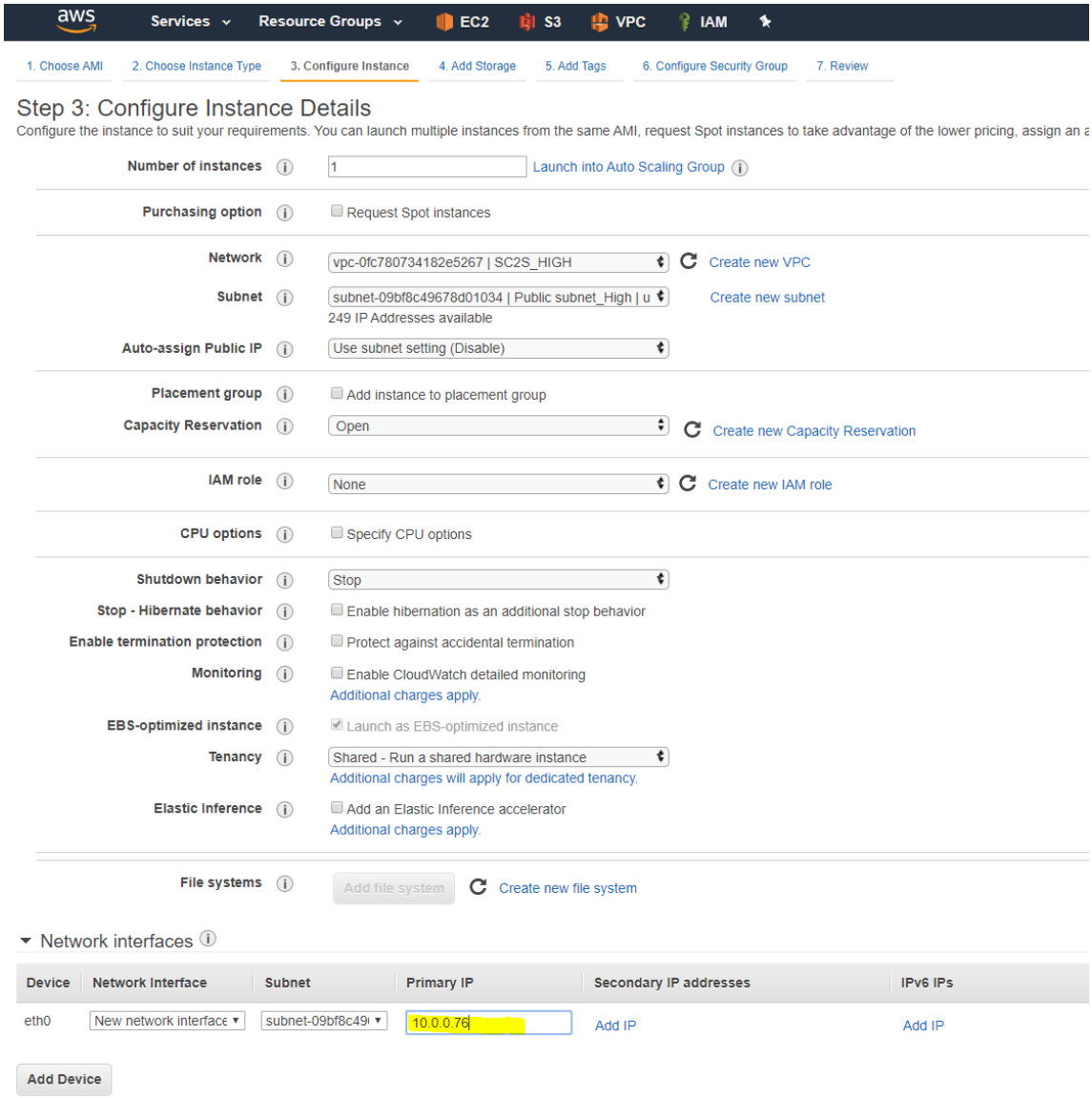
© 1999–2021 Citrix Systems, Inc. All rights reserved.



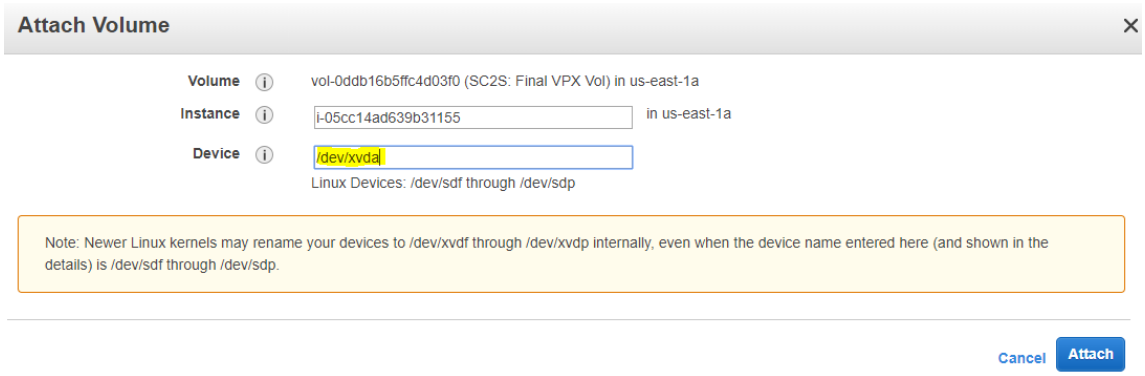


17. ハイサイド（Amazon Linux 2 AMI（HVM）、SSD ボリュームタイプ、EBS-backed、ENA 対応、64 ビット、セキュリティグループ）で作成された VPC およびサブネットに、低側の VPX とまったく同じインスタンスタイプの新しい Linux インスタンスをデプロイします。`m4.xlarge`Traffic」）。セットアップ中に、このドキュメントの前のセクションで説明した低側の VPX と同じ IP を設定します。インスタンスの準備ができたら、インスタンスの電源をオフにします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



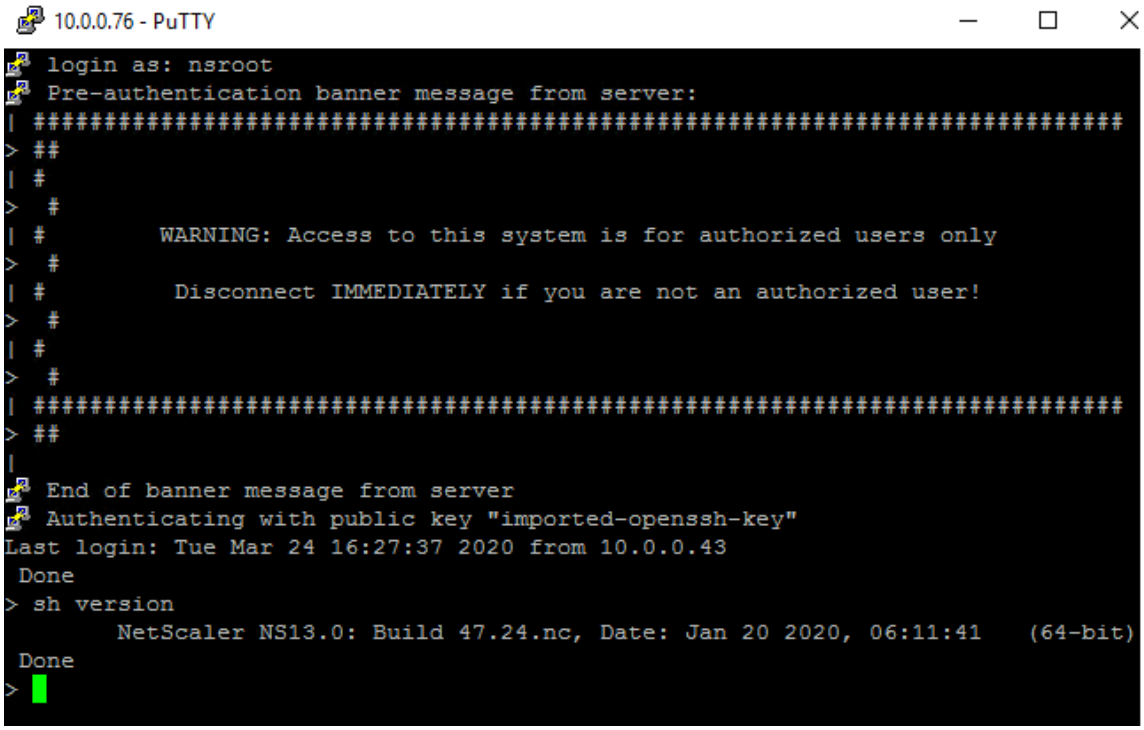
18. 新しくデプロイされた Linux インスタンスのルートボリュームをデタッチし、デタッチされたインスタンス（「SC2S: Final VPX Vol」など）をアタッチします。アタッチ時に、デバイスをルートボリューム（つまり `/dev/xvda`）として指定します。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

19. インスタンスをパワーオンします。ハイサイド踏み台ホストを使用して、インスタンスに PUTTY/SSH を実行して、VPX の機能を検証します。このドキュメントの前のセクションで説明 `nsroot` したインスタンス ID パスワードを使用してログインし、簡単なコマンドを実行します。

```
sh version
<!--NeedCopy-->
```

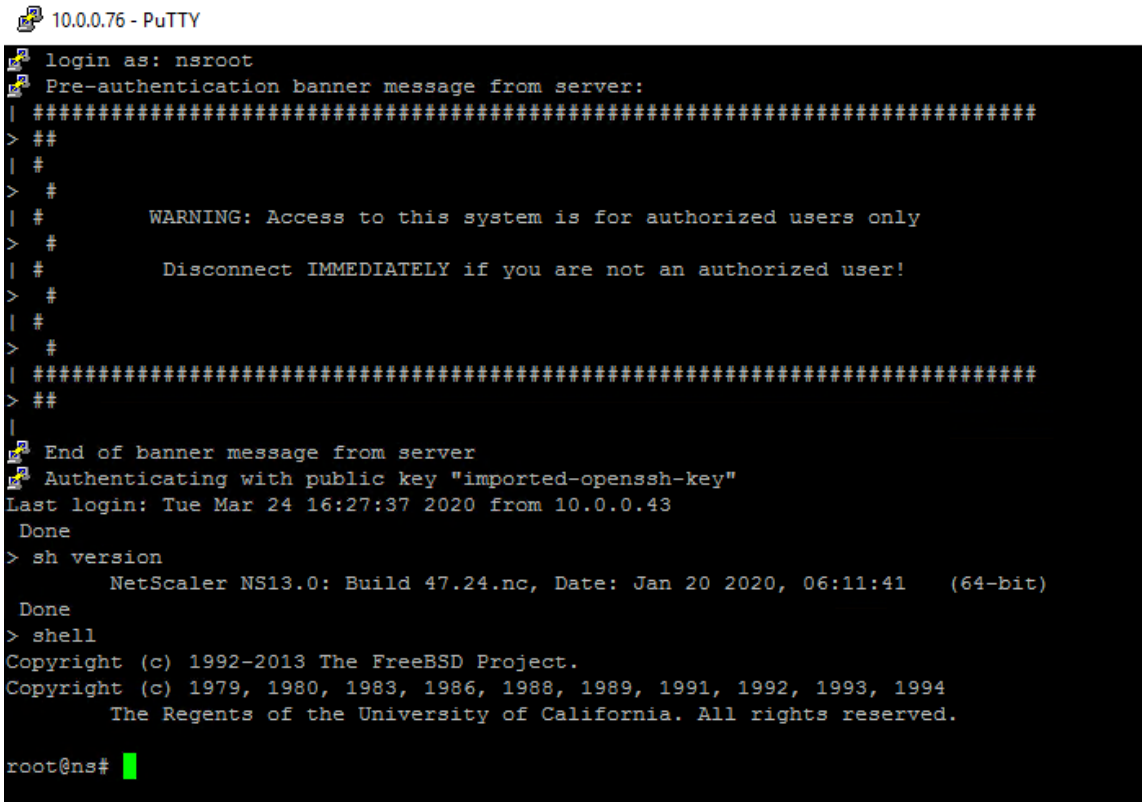


起動した **VPX** インスタンスからの **AMI** の作成

1. Citrix ADC インスタンスにログインします。シェルに移動して、root として必要な変更を実行します。

```
shell
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.



2. ADC ソフトウェアから次のディレクトリとファイルを強制的かつ再帰的に削除します。ファイルとディレクトリを手動で削除するには、それぞれの前に rm —rf を追加します。

   '/nsconfig/ns.conf'
   '/nsconfig/ssh/'
   '/nsconfig/ssl/'
   '/nsconfig/aws_bootstrap'
   '/nsconfig/rainman.conf'
   '/var/nslog'
   '/var/log/messages'
   '/var/log/*.log*'
   '/var/core/'
   '/nsconfig/.AWS/'
   '/var/db'
   '/etc/resolv.conf'
   '/flash/BUILD'
   '/mpsconfig/pgxl/.ssh/id_rsa.pub'
   '/var/pubkey/nsroot/.ssh/authorized_keys'
   '/var/pubkey/root/.ssh/authorized_keys'

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
root@ns# rm -rf /nsconfig/ns.conf*
root@ns# rm -rf /nsconfig/ssh/*
root@ns# rm -rf /nsconfig/ssl/*
root@ns# rm -rf /nsconfig/aws_bootstrap
root@ns# rm -rf /nsconfig/rainman.conf
root@ns# rm -rf /nsconfig/.AWS/
root@ns# rm -rf /var/nslog
root@ns# rm -rf /var/log/messages*
root@ns# rm -rf /var/log/*.log
root@ns# rm -rf /var/core/*
root@ns# rm -rf /var/db
root@ns# rm -rf /etc/resolv.conf
root@ns# rm -rf /mpsconfig/pgxl/.ssh/id_rsa.pub
root@ns# rm -rf /var/pubkey/nsroot/.ssh/authorized_keys
root@ns# rm -rf /var/pubkey/root/.ssh/authorized_keys
```

または次のスクリプトを実行します。

```
#!/bin/sh -x
rm -rf    /nsconfig/ns.conf*
rm -rf    /nsconfig/ssh/*
rm -rf    /nsconfig/ssl/*
rm -rf    /nsconfig/aws_bootstrap
rm -rf    /nsconfig/rainman.conf
rm -rf    /var/nslog
rm -rf    /var/log/messages*
rm -rf    /var/log/\*.log
rm -rf    /var/core/\*
rm -rf    /nsconfig/.AWS/
rm -rf    /var/db
rm -rf    /etc/resolv.conf
rm -rf    /flash/BUILD
rm -rf    /mpsconfig/pgxl/.ssh/id_rsa.pub
rm -rf    /var/pubkey/nsroot/.ssh/authorized_keys
rm -rf    /var/pubkey/root/.ssh/authorized_keys
<!--NeedCopy-->
```

3. /flash/nsconfig ディレクトリの権限を 755 に変更します。

```
chmod 755 /flash/nsconfig
<!--NeedCopy-->
```

```
root@ns# chmod 755 /flash/nsconfig
```

4. 残りのキーが残っていないことを確認します。存在する場合は、強制的に再帰的に削除します。

```
find / -type f -name  “authorized*”
rm -rf <filename>
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
3 <!--NeedCopy-->
```

```
root@ns# find / -type f -name "authorized*"
/var/python/lib/python2.6/site-packages/ansible-2.1.1.0-py2.6.egg/ansible/modules/core/system/authorize
d_key.py
/var/python/lib/python2.6/site-packages/ansible-2.1.1.0-py2.6.egg/ansible/modules/core/system/authorize
d_key.pyc
/var/python/lib/python2.7/site-packages/ansible-2.1.1.0-py2.7.egg/ansible/modules/core/system/authorize
d_key.py
/var/python/lib/python2.7/site-packages/ansible-2.1.1.0-py2.7.egg/ansible/modules/core/system/authorize
d_key.pyc
root@ns# rm -rf /var/python/lib/python2.6/site-packages/ansible-2.1.1.0-py2.6.egg/ansible/modules/core/
system/authorized_key.py
root@ns# rm -rf /var/python/lib/python2.6/site-packages/ansible-2.1.1.0-py2.6.egg/ansible/modules/core/
system/authorized_key.pyc
root@ns# rm -rf /var/python/lib/python2.7/site-packages/ansible-2.1.1.0-py2.7.egg/ansible/modules/core/
system/authorized_key.py
root@ns# rm -rf /var/python/lib/python2.7/site-packages/ansible-2.1.1.0-py2.7.egg/ansible/modules/core/
system/authorized_key.pyc
```

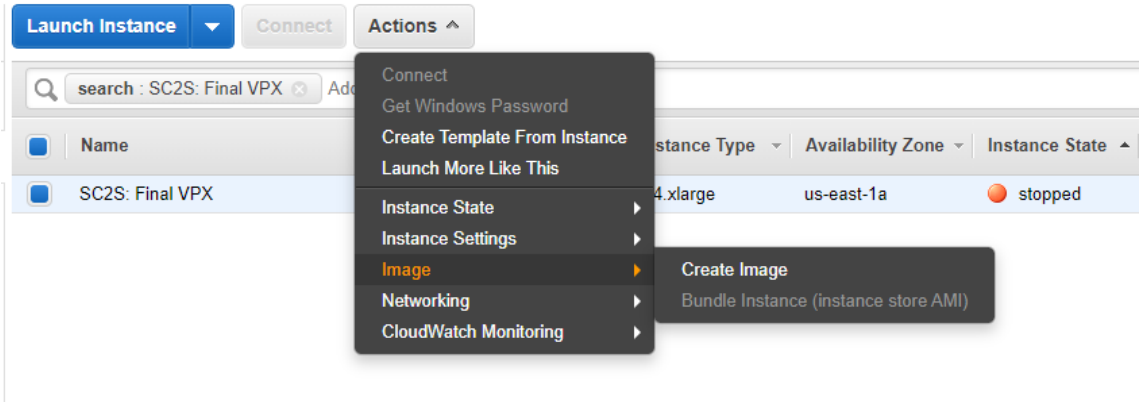
5. /nsconfig/license にライセンスが残っていないことを確認します。存在する場合は、強制的に再帰的に削除します。

   > 注:
   >
   > このフォルダーには他のディレクトリとファイル (SSL や XML など) があり、ライセンスファイルが存在する場合のみ削除してください。

```
1 ls /nsconfig/license
2 ls /nsconfig/license/ssl
3 ls /nsconfig/license/xml
4 <!--NeedCopy-->
```

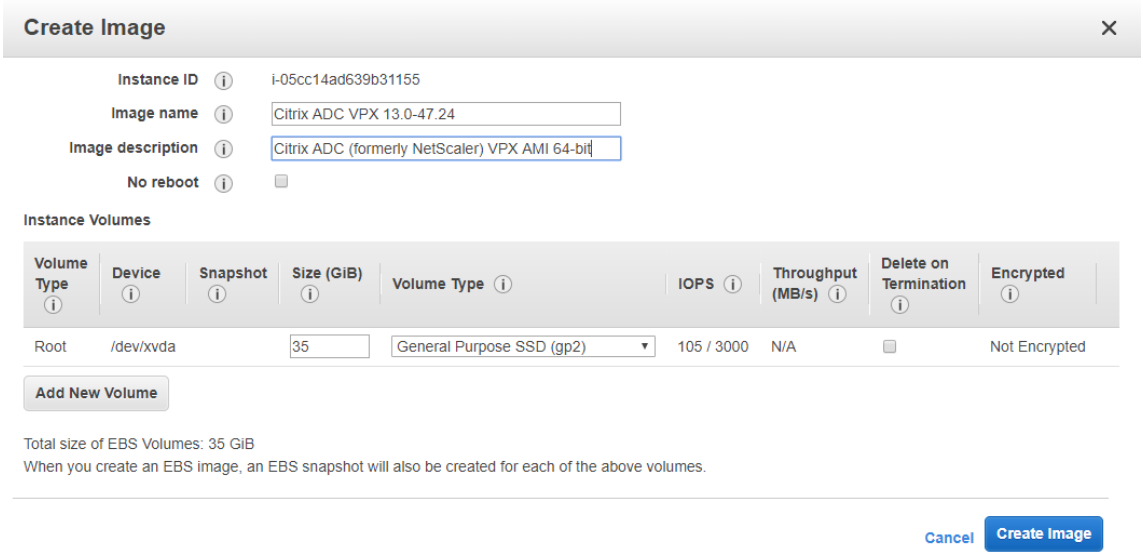
```
root@ns# ls /nsconfig/license/
ssl     xml
root@ns# ls /nsconfig/license/ssl
BaltimoreCyberTrustRoot.cert    BaltimoreCyberTrustRoot_CH.cert
root@ns# ls /nsconfig/license/xml
manifest.xml    report.xml
```

6. AWS コンソールからマシンの電源を切ります。インスタンスが停止したら、インスタンスから AMI を作成します。

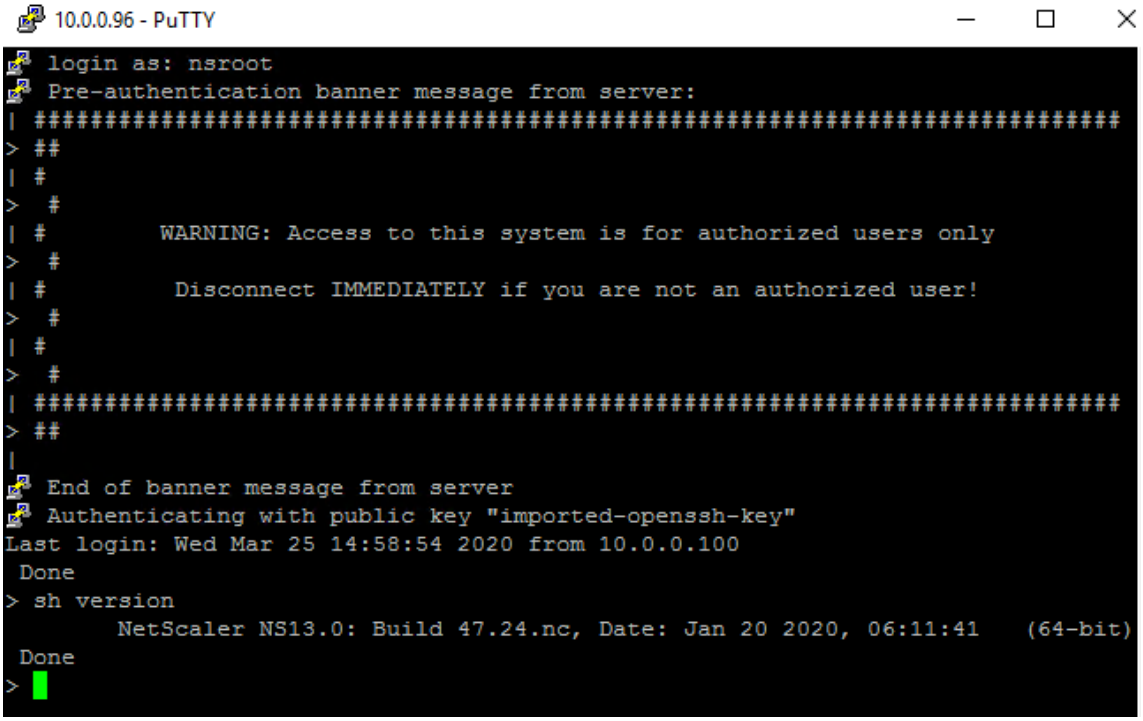


© 1999–2021 Citrix Systems, Inc. All rights reserved.

インスタンスに ALL が認識できる名前を付けます。これは、SC2S のすべての管理者に対してパブリックに共有されます (例:「Citrix ADC VPX 13.0〜47.24」)。



7. AMI の準備ができたら、そこからインスタンスをデプロイして機能を検証します。



8. AMI のアクセス許可を`Public`に設定します。これにより、SC2S のすべての管理者が使用できるようになります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

新しいリリースにアップグレードするには

- SC2S 内の既存の Citrix ADC VPX の場合: 利用可能なアップグレードソフトウェアを使用して VPX をアップグレードします https://citrix.com/downloads, ファイルをハイサイドに DTO します. のガイダンス Citrix ADC スタンドアロンアプライアンスのアップグレード に従ってインストールします。推奨されるアップグレード方法は、コマンドラインを使用することです。
- SC2S の新しい Citrix ADC VPX の場合: AMI を作成してパブリックに共有します。既存の AMI からインスタンスを起動し、前のセクションのようにマシンをアップグレードし、このドキュメントの「起動した VPX インスタンスから AMI を作成する」セクションの手順を実行します。

Citrix Gateway と Microsoft Azure の多要素認証

March 2, 2021

Citrix Gateway は、すべてのホストされたアプリケーション、SaaS/Web アプリケーション、エンタープライズアプリケーション、モバイルアプリケーションを、あらゆるデバイスやブラウザーのユーザーに提供します。nFactor 認証を使用して、オンプレミスの Microsoft AD に対してユーザーを認証し、Azure 多要素認証 (MFA) に Microsoft AD FS を活用します。

概要

Citrix Gateway

Citrix Gateway では、データセンターやクラウドに展開されたビジネスアプリケーションやデータに対して、1 つのアクセスポイントとシングルサインオン（SSO）をユーザーに提供します。ノートパソコン、デスクトップ、シンクライアント、タブレット、スマートフォンなど、さまざまなデバイスで SaaS として提供されます。Citrix Gateway は、統合、リモートアクセスインフラストラクチャの設置面積の削減、コストの削減、管理の容易さ、エンドユーザーエクスペリエンスの向上を実現します。Citrix Gateway は、IT をハイブリッドクラウドおよび SaaS 環境に移行するのに役立ちます。

- フェデレーションとシングルサインオン

Citrix Gateway はフェデレート ID を提供し、SAML 2.0、OAuth、OpenID をサポートしているため、Web、VDI、エンタープライズ、SaaS アプリケーションなど、すべてのアプリケーションでシングルサインオンを実現します。

- オンプレミスのユーザーディレクトリ

Citrix Gateway は、Office 365 や Salesforce などの SaaS アプリケーションに対して SSO を提供し、ユーザーディレクトリをオンプレミスで保持します。これは、Active Directory フェデレーションサービス (AD FS) の IdP またはプロキシとして実装できます。

- 多要素（**nFactor**）認証

© 1999–2021 Citrix Systems, Inc. All rights reserved.

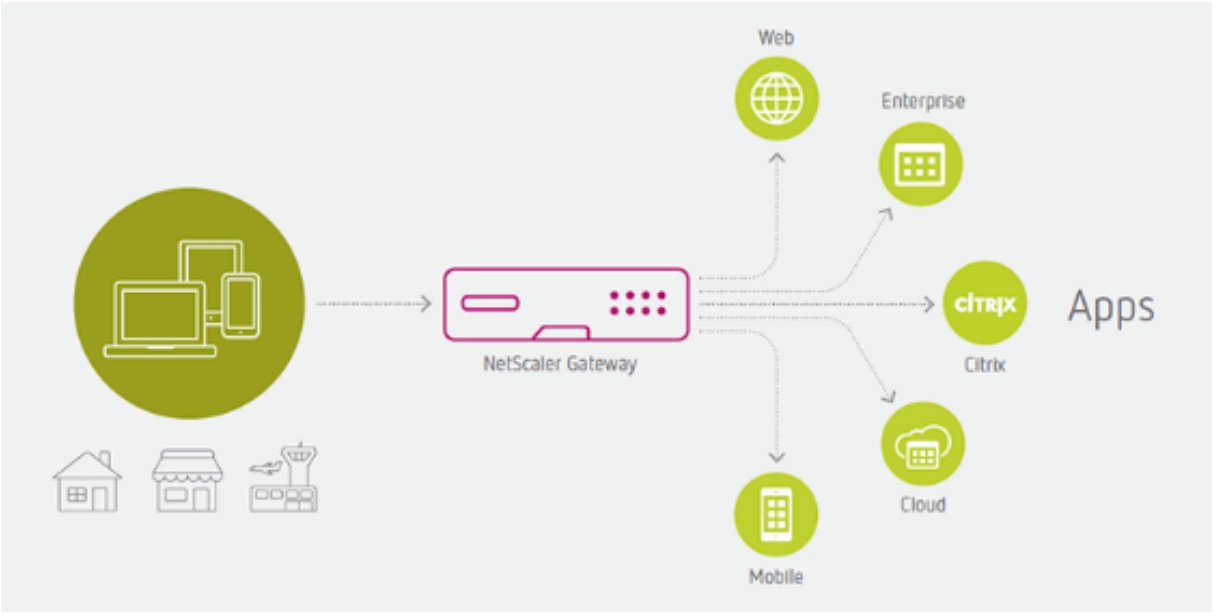
Citrix Gateway は、nFactor 認証メカニズムを提供し、ネットワークにアクセスするユーザー、アクセス内容、アクセス方法とアクセス時期をきめ細かく制御できます。これは、このような RADIUS、タカス、NTLM、直径、SAML 2.0、OAuth 2.0、および OpenID
2.0 などのすべての認証メカニズムをサポートしています。

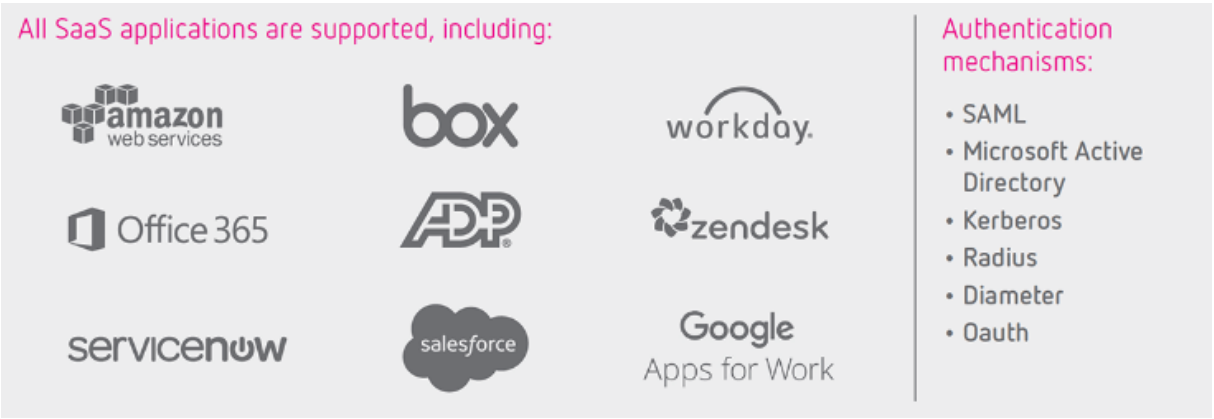
- コンテキストに基づくアクセス制御ポリシー

Citrix Gateway では、エンドユーザーデバイス、ユーザー、ユーザーの場所などのデータの状態に基づいて、ビジネスアプリケーションへのきめ細かいアクセス制御が可能です。IT 管理者は、アプリケーション環境でデータに安全にアクセスするためのポリシーを作成、管理、および適用できます。これらのポリシーは、VDI、Web、モバイル、エンタープライズ、SaaS アプリケーションに対して実装できます。

- 可視性とモニタリング

Citrix Application Delivery Management には、Citrix Gateway を介してアクセスされるすべてのアプリケーションのエンドツーエンドのユーザーエクスペリエンスを可視化するためのゲートウェイインサイトが含まれています。EPA チェックの失敗やシングルサインオンの失敗など、認証の失敗に関する問題のトラブルシューティングを行うために、アプリケーションサポートチームが情報を提供します。





© 1999–2021 Citrix Systems, Inc. All rights reserved.

Microsoft Azure MFA

人々はますます複雑化するシナリオで、組織のリソースに接続しています。企業は、スマートフォン、タブレット、PC、ラップトップを使用して、企業ネットワーク内外で、組織所有のデバイス、個人用デバイス、公共デバイスから接続できます。多くの場合、複数のプラットフォームを使用します。この常時接続、マルチデバイス、マルチプラットフォームの世界では、ユーザーアカウントのセキュリティがこれまで以上に重要になっています。デバイス、ネットワーク、プラットフォーム間で使用されるパスワードは、複雑さに関係なく、ユーザーアカウントのセキュリティを確保するのに十分ではありません。特に、ユーザーがアカウント間でパスワードを再利用する傾向がある場合は特にそうです。高度なフィッシングやその他のソーシャルエンジニアリング攻撃により、暗い Web 上でユーザー名とパスワードが投稿され、販売される可能性があります。

2 段階検証プロセスのセキュリティは、階層化されたアプローチにあります。複数の認証要素が侵害されることは、攻撃者にとって大きな課題となります。攻撃者がユーザーのパスワードを習得しても、追加の認証方法を所有することなく役に立たない。これは、次の認証方法の 2 つ以上を要求することによって機能します。

- あなたが知っているもの（通常はパスワード）
- あなたが持っているもの（電話のように簡単に複製できない信頼できるデバイス）
- あなたが何か（生体認証）

Azure 多要素認証は、データとアプリケーションへのアクセスを保護するのに役立ちます。これは、認証の第二の形式を使用して、セキュリティの余分な層を提供します。組織は、条件付きアクセスを使用して、ソリューションを特定のニーズに合わせることができます。

Microsoft Azure MFA の展開方法

Azure MFA を認証の 2 番目の要素として活用するには、さまざまな方法があります。ここでは、それぞれの長所と短所を簡単に説明します。

Azure MFA サーバー

Microsoft Azure の多要素認証サーバーは、元の方法であり、廃止される予定です。そのため、新しい実装での使用は考慮しないでください。

- この方法については、今後 Microsoft からの更新はありません。
- SSPR および Azure MFA クラウドベースとの統合はありません。
- MFA サーバーから MFA クラウドベースのソリューションへのシームレスな移行ツールはありません。

Azure MFA ネットワークポリシーサーバー拡張

Azure MFA 用のネットワークポリシーサーバー (NPS) 拡張機能は、NPS アダプターを使用して Azure MFA クラウドベースに接続するためにサポートされているソリューションです。オンプレミスの RADIUS サーバーとして使用できます。

- NPS アダプタ（RADIUS）は、MFA 規則内外またはオン/オフのネットワークロケーションを提供します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- SAML 統合方法と同様、Azure AD 条件付きアクセスポリシーと互換性がありません。条件付きアクセスポリシーは、より豊かで優れたユーザーエクスペリエンスを提供します。
- ユーザーは、NPS アダプターを使用する前に MFA に登録する必要があります。Azure MFA クラウドベースおよび条件付きアクセスとは異なり、ユーザーが登録されていない場合、NPS 拡張機能はユーザーの認証に失敗し、ヘルプデスクへの呼び出しが増えます。
- NPS アダプターが MFA を起動すると、ユーザーが登録したデフォルトオプションにヒットします。ユーザーには、MFA が必要であり、これから来るという視覚的な通知はありません。ゲート処理中にユーザーが MFA メソッドを変更するための UI はありません。ユーザーがデフォルトのデバイスを持っていない場合、失敗します。ユーザーは、セルフサービスポータルに戻り、デフォルトオプションをリセットしてから、もう一度接続を試みる必要があります。

Microsoft AD FS と **Azure MFA**

組織が Azure AD とフェデレートされているがパスワードハッシュが Azure AD と同期されていない場合は、Lightweight Directory Access Protocol（LDAP）にオンプレミス AD を使用し、AD FS の証明書利用者のアクセスポリシーの一部として Azure MFA を有効にできます。Windows Server 2016 以降、プライマリ認証用に Azure MFA を構成できるようになりました。

- Azure MFA アダプターは Windows Server 2016 に組み込まれており、追加のインストールは必要ありません。
- Azure MFA アダプターは Azure AD と直接統合され、オンプレミスの Azure MFA サーバーは必要ありません。
- ユーザーが MFA に登録されていない場合は、次回のサインイン時にプロセスを案内します。これにより、ヘルプデスクへの呼び出しが少なくなり、ユーザーにとってより良いプロセスが実現されます。
- ユーザーは、MFA が必要であり、今後予定されているという視覚的な通知を受け取ります。ユーザーは、UI のゲート処理中に Gateway オプションを変更できます。

Azure AD と **Azure MFA**

組織がパスワードハッシュを Azure AD に同期している場合は、条件付きアクセスポリシーによって Azure MFA を活用して、ユーザーに第 2 要素認証をチャレンジできます。

- この方法では、オンプレミスで追加のインストールは必要ありません。
- ユーザーが MFA に登録されていない場合は、次回のサインイン時にプロセスを案内します。これにより、ヘルプデスクへの呼び出しが少なくなり、ユーザーにとってより良いプロセスが実現されます。
- ユーザーは、MFA が必要であり、今後予定されているという視覚的な通知を受け取ります。ユーザーは、UI のゲート処理中に Gateway オプションを変更できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Azure AD パススルー認証と **Azure MFA**

Azure AD パススルー認証 (PTA) を使用すると、ユーザーは同じパスワードを使用して、オンプレミスアプリケーションとクラウドベースの両方のアプリケーションにサインインできます。ユーザーが Azure AD を使用してサインインすると、この機能はユーザーのパスワードをオンプレミスの Active Directory に対して直接検証します。Azure AD PTA は、Azure AD パスワードハッシュ同期の代替手段であり、組織にクラウド認証の同じ利点を提供します。

- Azure AD PTA では、軽量エージェントをオンプレミスにインストールする必要があります。
- Azure AD PTA は、Azure MFA を含む Azure AD 条件付きアクセスポリシーとシームレスに連携することで、ユーザーアカウントを保護します。
- ユーザーは、セルフサービスのパスワード管理タスクをクラウドで完了できます。
- オンプレミスのパスワードは、どのような形式でもクラウドに保存されることはありません。
- エージェントは、ネットワーク内からのみアウトバウンド接続を行います。したがって、境界ネットワーク (DMZ とも呼ばれる) にエージェントをインストールする必要はありません。

現在の状況

次の特性を持つ環境では、認証の 2 番目の要素として Azure MFA を活用する必要があります。

- Azure AD 同期を使用するオンプレミス AD が構成されています。
- Azure AD パスワードハッシュ同期が無効になっています。
- O365 アプリケーションへのアクセスが必要です。
- Citrix Virtual Apps and Desktops をオンプレミスでアクセスする必要があります。
- 最新の認証方法（SAML、OAuth）を使用したアプリケーションへのアクセスが必要です。
- レガシー認証方式を使用するアプリケーションへのアクセスが必要です。

デザイン面の考慮事項

提案されたソリューションのデザイン面での考慮事項は次のとおりです。

- ホストされたアプリケーション、SaaS アプリケーション、エンタープライズアプリケーション、Web アプリケーションに 1 つのポータルで安全にアクセスする必要があります。
- ユーザーは、認証プロセス中に資格情報の入力を 1 回だけ要求される必要があります。
- シングルサインオンは、ホスト型、SaaS 型、エンタープライズ、Web のすべてのアプリケーションに提供する必要があること。

提案されたソリューション

概要

提案されたソリューションは、次のコンポーネントに基づいています。

- オンプレミスの Citrix Gateway

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- オンプレミスの Microsoft AD
- オンプレミスの AD FS
- AD FS プロキシとしてのオンプレミスの Citrix ADC
- Microsoft Azure MFA

Citrix Gateway では、認証、承認、監査機能 (Citrix ADC AAA) および nFactor 認証メカニズムを利用して、LDAP ポリシーを使用してユーザーを認証し、AD FS 証明書利用者のアクセスポリシーを利用して Azure MFA 検証プロセスをトリガーします。Azure MFA がユーザーを検証した後、AD FS は SAML アサーション (SAML 応答) を生成し、ユーザーを Citrix Gateway にリダイレクトします。この時点で、ユーザーは認証され、Citrix Gateway はそのユーザーが使用を許可されているすべてのアプリケーションを表示します。

このソリューションには、2 つのパブリック DNS レコードと 2 つのパブリック IP アドレスが必要です。

説明	値
Citrix Gateway FQDN	access.ctxdemos.com
Citrix の認証、承認、および監査 FQDN の	aaa.ctxdemos.com

このソリューションでは、1 つのパブリック SSL 証明書を使用します。

説明	値
共通名	access.ctxdemos.com
サブジェクトの別名	sts.ctxdemos.com
サブジェクトの別名	aaa.ctxdemos.com

このソリューションは、内部の Microsoft 認証局サービスによって発行されたワイルドカード SSL 証明書も使用します。

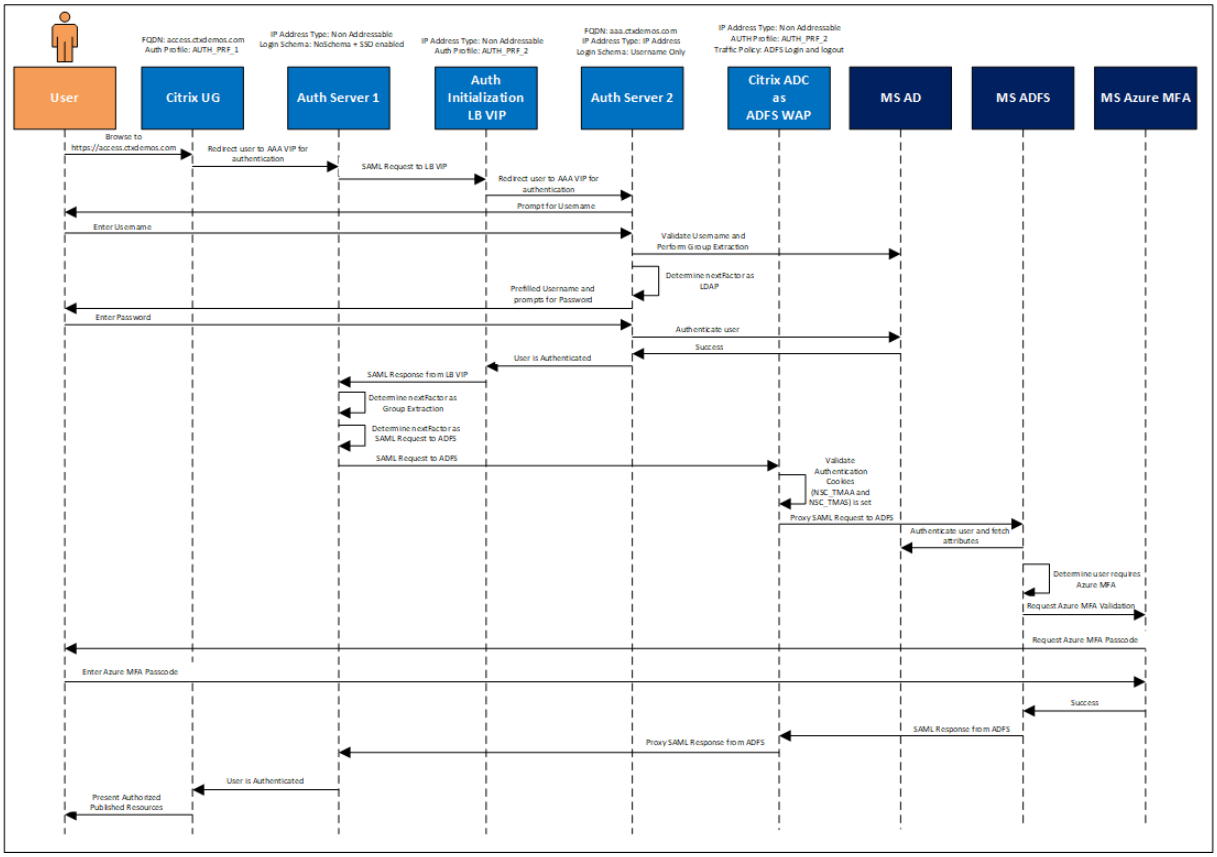
説明	値
共通名	*.ctxdemos.com

認証フロー

シーケンス図

次のシーケンス図は、ソリューションの認証フローを示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



認証手順

認証手順は次のとおりです。

1. ユーザーがhttps://access.ctxdemos.comに移動します。
2. Citrix Gateway は、最初の Citrix ADC AAA VIP（アドレス指定不可）にユーザーをリダイレクトします。
3. 最初の Citrix ADC AAA VIP は、シングルサインオンで構成されたスキーマなしのログオンを使用します。次に、高度な認証ポリシーの処理を開始します。
4. 最初の認証ポリシーは、認証クッキーを生成するために、アドレス指定できない LB VIP への SAML SP です。
5. ヘルパー LB VIP は、認証に 2 番目の Citrix ADC AAA VIP（アドレス可能）を使用するように構成されています。したがって、ユーザは 2 番目の認証、認可、および監査 VIP にリダイレクトされます。
6. 2 つ目の Citrix ADC AAA VIP は、ユーザー名の入力を求める`Username Only`ログオンスキーマを使用します。次に、高度な認証ポリシーの処理を開始します。
7. 最初の認証ポリシーは、オンプレミス AD でユーザー名を照会し、ユーザーが AzureMFACAUsers セキュリティグループに属しているかどうかを検証するグループの抽出です。検証結果が成功すると、次の認証要素（LDAP ポリシー）の処理が開始されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

8. LDAP ポリシーは、UsernameAndPasswordログインスキーマと事前に入力されたユーザー名フィールドを使用して、AD パスワードの入力をユーザーに要求します。
9. 2 つ目の Citrix ADC AAA VIP での認証が正常に完了すると、ヘルパー LB VIP に戻り、最初の認証、承認、および監査 VIP の SAML 応答を生成します。
10. 最初の Citrix ADC AAA VIP は次の要素の処理を開始します。これは、ユーザーのグループが AD から抽出され、認証、承認、および監査変数に格納され、プロセスの後半で使用できるようになります。
11. まず、Citrix ADC AAA VIP は、次の要因の処理を開始します。これは、Citrix ADC 上の AD FS プロキシ VIP への SAML SP です。

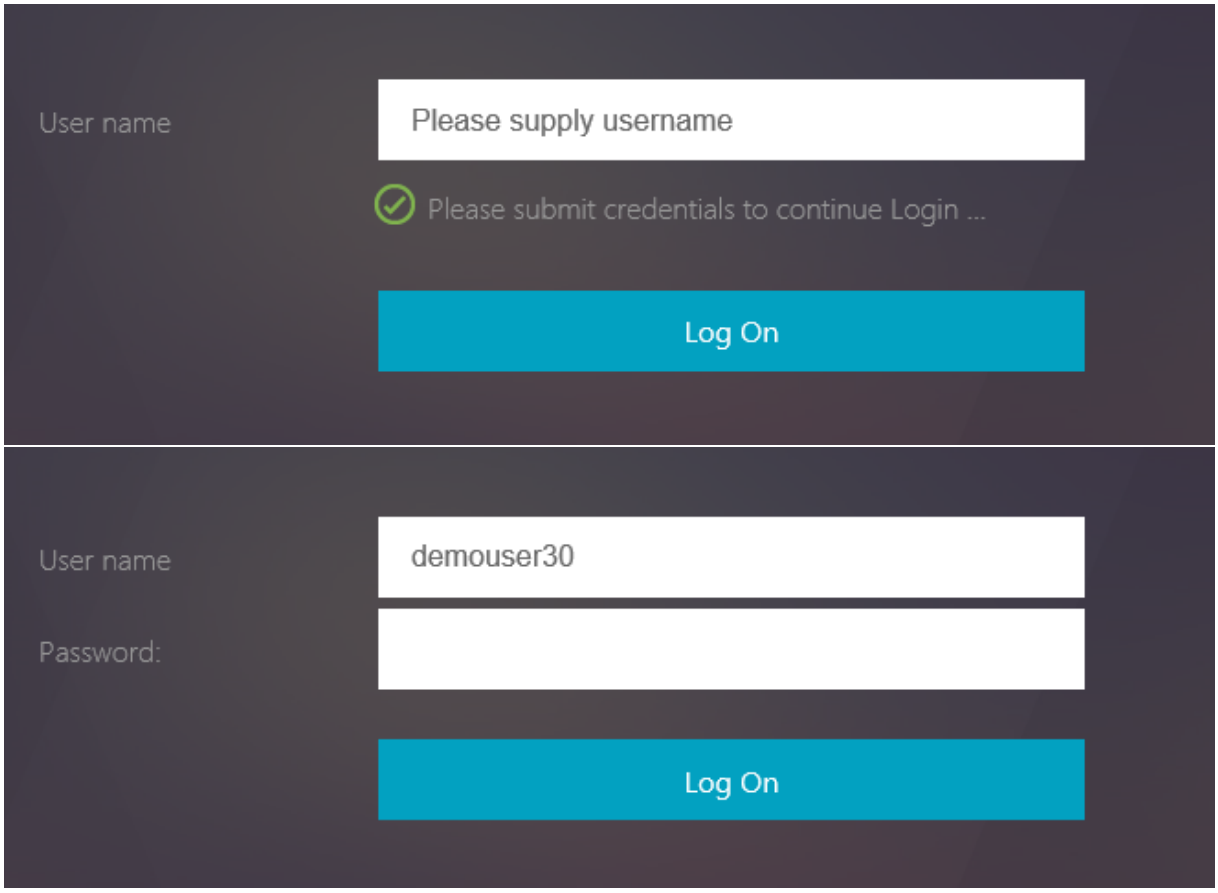
    > 注:
    >
    > Citrix ADC は AD FS ファームとフェデレートされます。詳細な手順については、後のセクションで説明します。

12. AD FS プロキシ VIP は、認証クッキー (NSC_TMAA および NSC_TMAS) が設定されていることを検証します。次に、SAML 要求をバックエンド AD FS サーバーに送信します（高可用性とサービスの復元性を実現するために、バックエンド AD FS サーバーは内部 Citrix ADC で負荷分散される必要があります)。
13. AD FS サーバーは SAML 要求を処理します。証明書利用者のアクセスポリシーが「すべてのユーザーを許可し、認証に MFA を要求する」に設定されているため、Azure MFA 認証プロセスがトリガーされます。
14. Azure MFA はユーザー名を処理します。すでに登録されている場合は、設定された方法でユーザにチャレンジします。そうでない場合は、プライマリ認証方式とセカンダリ認証方式を登録して設定するよう求められます。
15. Azure MFA 認証プロセスが正常に完了すると、AD FS は、Citrix Gateway (最初の Citrix ADC AAA VIP) の SAML 応答を生成します。
16. まず、Citrix ADC AAA VIP が SAML 応答を受信し、ユーザーの認証プロセスが完了したことを確認します。
17. Citrix Gateway は認証情報を Citrix StoreFront に送信します。この情報は、ユーザーが使用を許可されているすべてのアプリケーションとデスクトップを列挙します。また、ユーザーのグループメンバーシップを処理して、Citrix Gateway に公開されたブックマークを表示します。

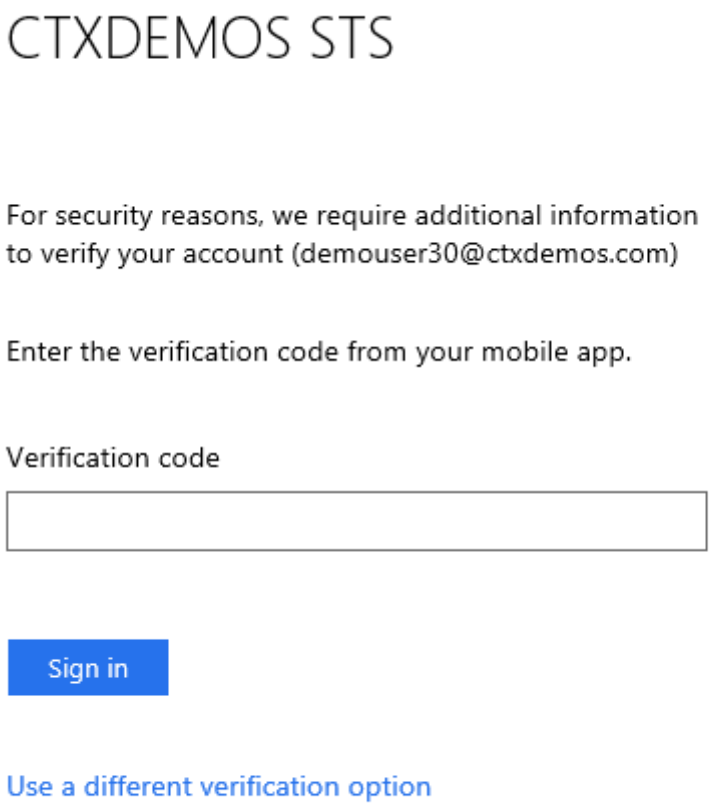
認証画面

上記の手順のほとんどは、Citrix ADC 上のさまざまな VIP 間で内部的に発生するため、ユーザーにとってシームレスです。ユーザーエクスペリエンスを以下に示します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



© 1999–2021 Citrix Systems, Inc. All rights reserved.



実装

Microsoft AD FS

証明書の要件

フェデレーションサーバーには、次の表に示す証明書が必要です。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

証明書の種類	説明	展開する前に知る必要があること
Secure Sockets Layer (SSL) 証明書	これは、フェデレーションサーバーとクライアント間の通信をセキュリティで保護するために使用される標準のセキュアソケットレイヤー (SSL) 証明書です。	この証明書は、フェデレーションサーバーまたはフェデレーションサーバープロキシのインターネットインフォメーションサービス (IIS) の既定の Web サイトにバインドする必要があります。フェデレーションサーバープロキシの場合、フェデレーションサーバープロキシ構成ウィザードを正常に実行する前に、IIS でバインドを構成する必要があります。推奨事項: この証明書は AD FS のクライアントによって信頼される必要があるため、パブリック (サードパーティ) 証明機関 (CA) によって発行されたサーバー認証証明書を使用します。たとえば、ベリサイン。ヒント: この証明書のサブジェクト名は、展開する AD FS の各インスタンスのフェデレーションサービス名を表すために使用されます。このため、パートナーにとって会社または組織の名前を最もよく表す新しい CA 発行の証明書で、サブジェクト名を選択することを検討してください。
サービス通信証明書	この証明書により、フェデレーションサーバー間の通信をセキュリティで保護するための WCF メッセージセキュリティが有効になります。	デフォルトでは、SSL 証明書がサービス通信証明書として使用されます。これは、AD FS 管理コンソールを使用して変更できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

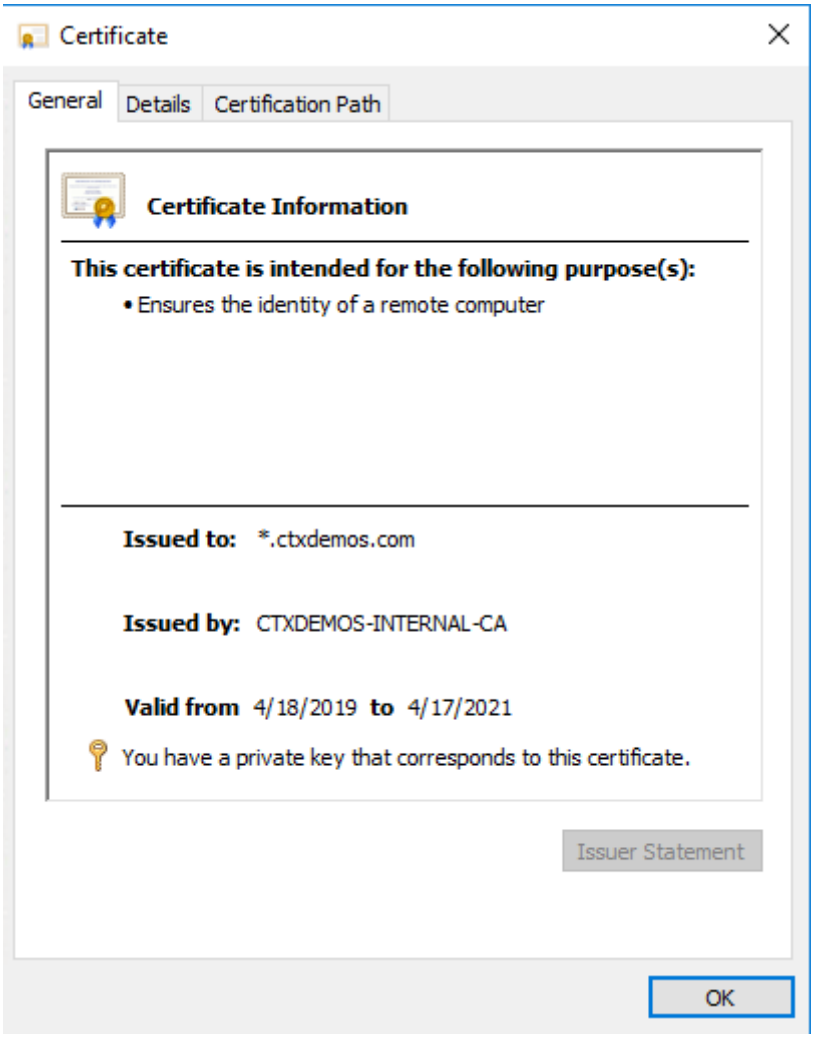
証明書の種類	説明	展開する前に知る必要があること
トークン署名証明書	これは、フェデレーションサーバーが発行するすべてのトークンに安全に署名するために使用される標準の X509 証明書です。	トークン署名証明書には秘密キーが含まれていなければならず、フェデレーションサービスの信頼されたルートにチェーンする必要があります。既定では、AD FS は自己署名証明書を作成します。ただし、組織のニーズに応じて、AD FS の管理スナップインを使用して、後で CA 発行の証明書に変更できます。
トークン暗号化解除証明書	これは、パートナーフェデレーションサーバーによって暗号化された受信トークンの復号化に使用される標準 SSL 証明書です。また、フェデレーションメタデータにも公開されます。	既定では、AD FS は自己署名証明書を作成します。ただし、組織のニーズに応じて、AD FS の管理スナップインを使用して、後で CA 発行の証明書に変更できます。

デモ環境の構成

証明書の種類	デモ環境の構成
Secure Sockets Layer (SSL) 証明書	AD FS サーバー上の内部発行 CA によって発行された内部証明書。Citrix ADC 上の信頼できる公開証明書。
サービス通信証明書	AHS 内部発行認証局によって発行された内部証明書。
トークン署名証明書	AD FS サービスによって自動生成されます。
トークン暗号化解除証明書	AD FS サービスによって自動生成されます。

デモ環境では、ワイルドカード証明書が登録され、サーバーにインストールされます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



サービスアカウントの要件

サービスアカウントを作成するか、グループ管理サービスアカウント（gMSA）を活用できます。gMSA を使用するには、キー配布サービスのルートキーを作成する必要があります。そのため、PowerShell を起動し、次のコマンドを実行します。

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
<!--NeedCopy-->
```

このコマンドは、Active Directory に格納されたキー配布サービスのルートキーを作成します。これにより、後で作成する AD FS サービスアカウントとして、グループ管理サービスアカウント (gMSA) を作成できます。ドメイン管理者権限でこのコマンドを実行します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
PS C:\> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))

Guid
----
c75b3af1-229f-6d0a-f62a-361976348390


PS C:\> _
```

DNS レコードの要件

内部および外部の AD FS フェデレーションサービス名の DNS A レコードが必要です。デモ環境では、内部 DNS レコードは AD FS サーバーの IP を指し、外部 DNS レコードは Citrix Gateway のパブリック IP を指しています。

レコード名	スコープ	種類	IP アドレス
sts.ctxdemox.com	内部	A	22.22.22.6
sts.ctxdemox.com	外部	A	40.85.225.175

AD FS の役割の追加 AD FS ファームの構成

AD FS の役割の追加

AD FS の役割を Windows Server 2016 に追加するには、PowerShell を起動し、次のコマンドを実行します。

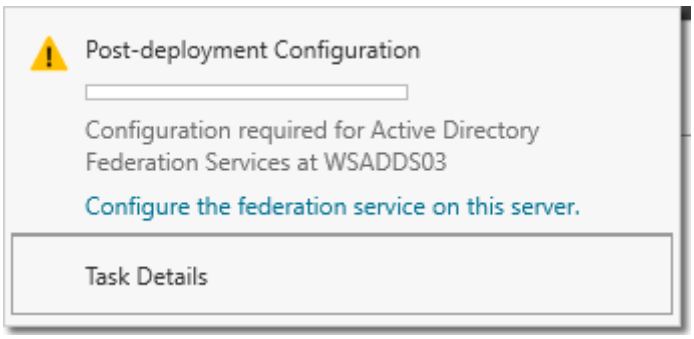
```
1 Install-WindowsFeature AD FS-Federation -IncludeManagementTools
2 <!--NeedCopy-->
```

```
PS C:\> Install-WindowsFeature ADFS-Federation -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Federation Services}
WARNING: To finish configuring this server for the federation server role using Windows PowerShell, see
http://go.microsoft.com/fwlink/?LinkId=224868.


PS C:\> _
```

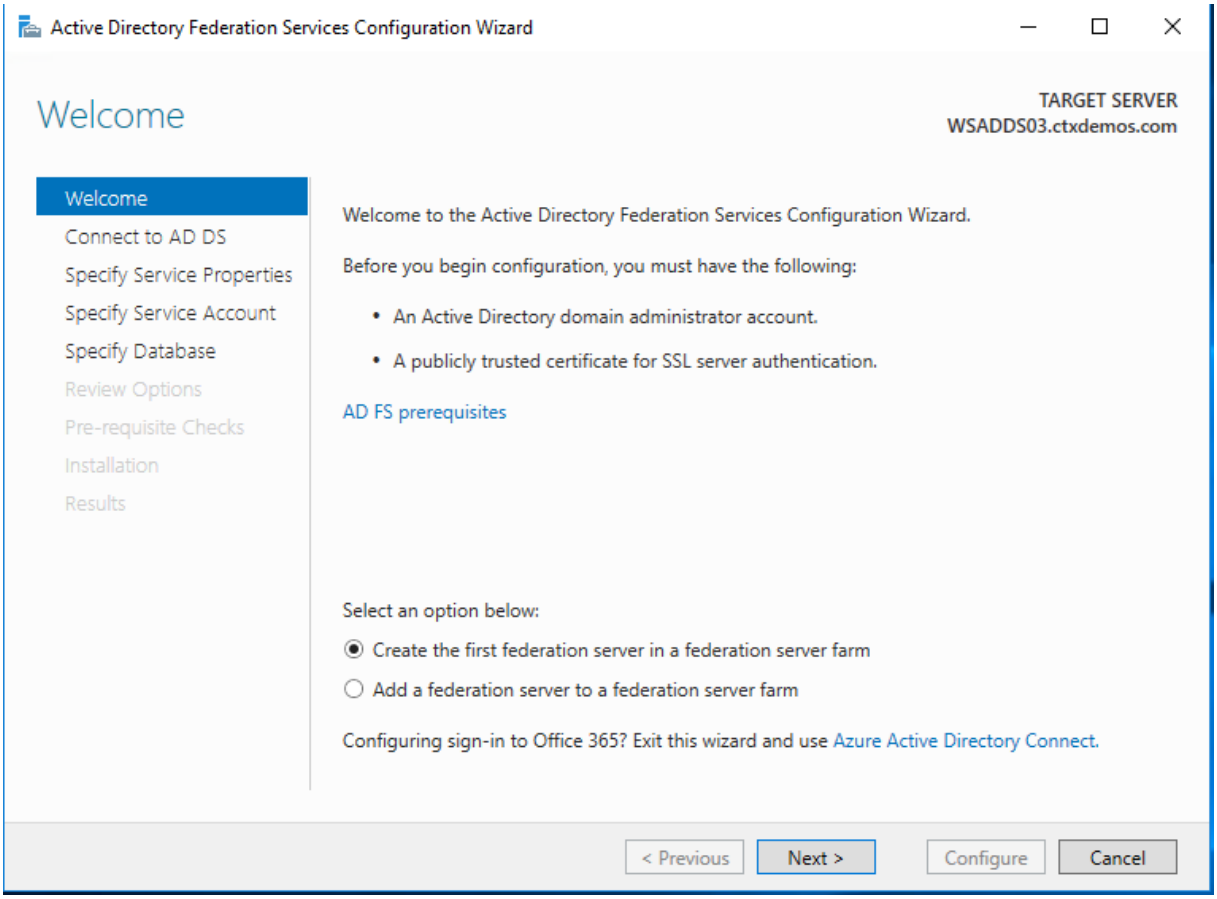
AD FS ファームの構成

これで、サーバーマネージャーから AD FS の展開後の構成を開始できます。[このサーバーでフェデレーションサービスを構成する] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

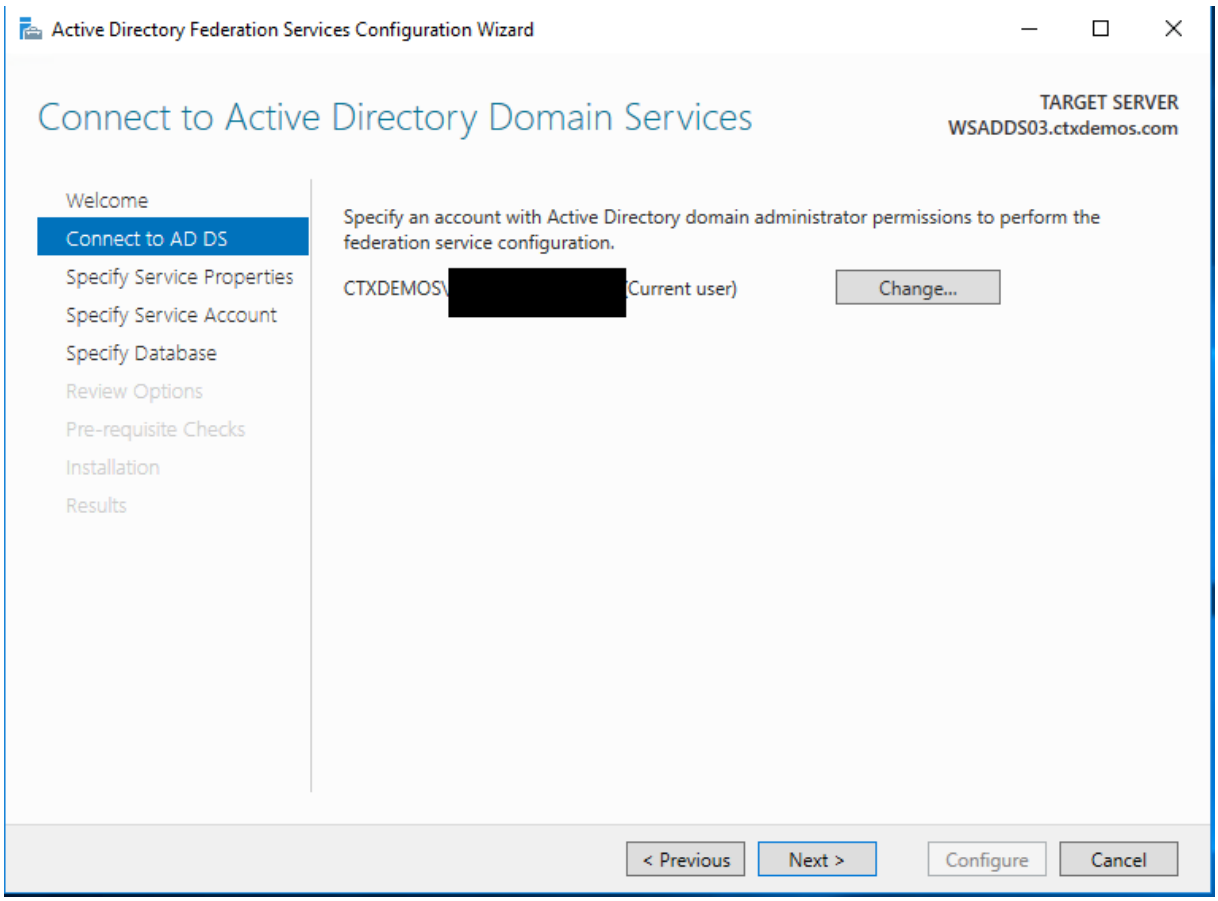


[ようこそ**]** ページで、**[**フェデレーションサーバーファームに最初のフェデレーションサーバーを作成する**]** を選択し、**[**次へ**]** をクリックします。



[Active Directory ドメインサービスへの接続**]** ページで、ドメイン管理者アカウントが指定されていることを確認し、**[**次へ**]** をクリックします。

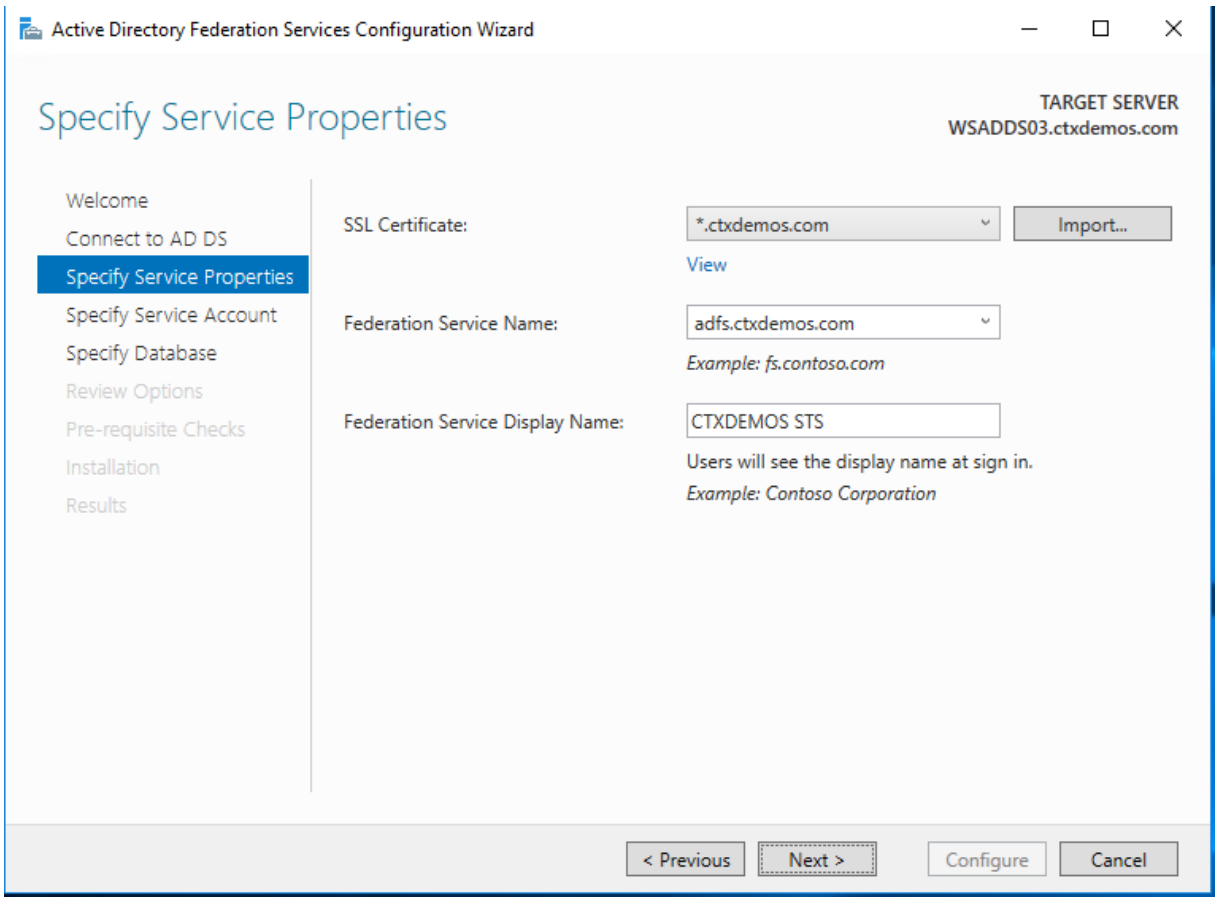
© 1999–2021 Citrix Systems, Inc. All rights reserved.



[サービスのプロパティの指定] ページで、次の手順を完了し、**[次へ]** をクリックします。

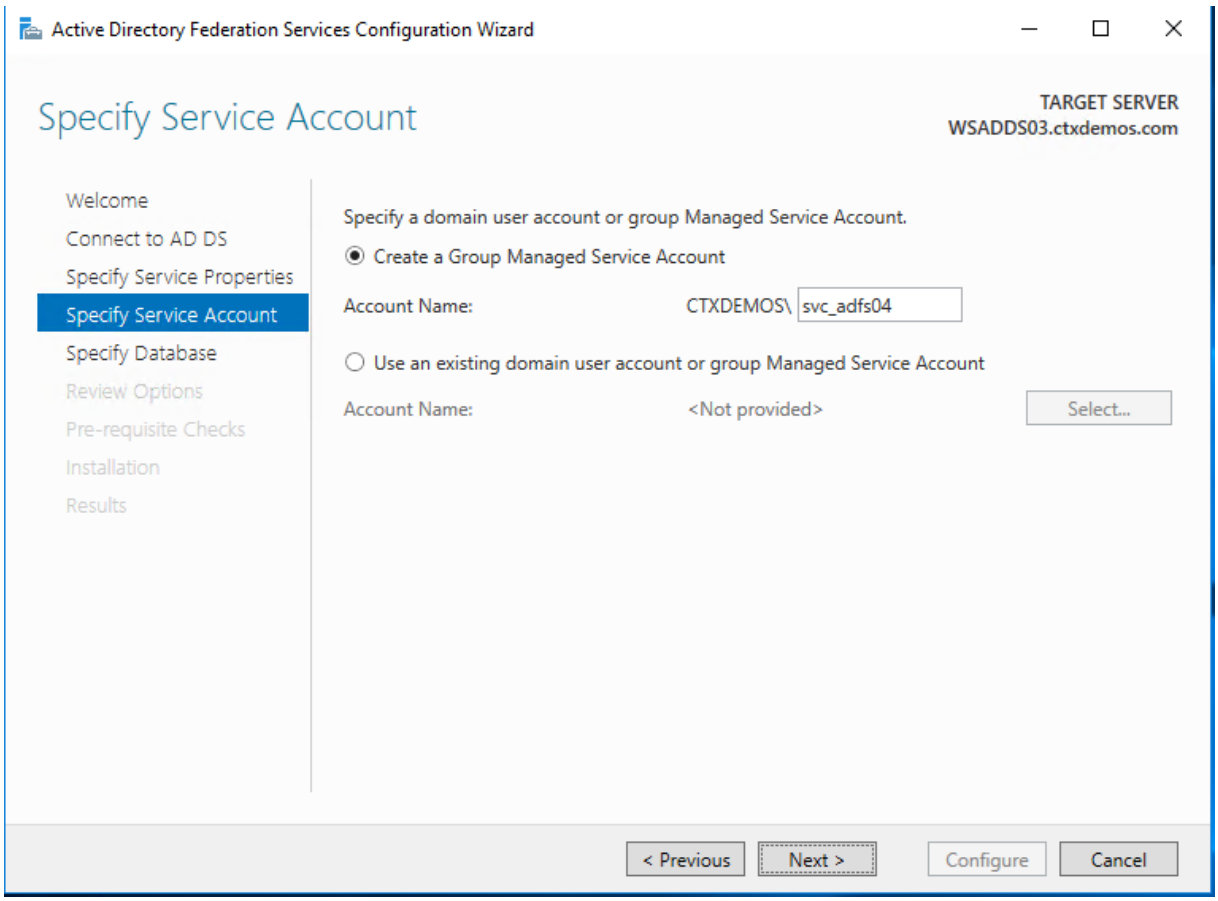
- 前の手順でサーバーにインストールされた証明書を選択します。
- フェデレーションサービス名は、証明書のサブジェクト名に基づいて自動的に設定されます。
- フェデレーションサービスの表示名を入力します。たとえば、「**CTXDEMOS STS**」などです。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



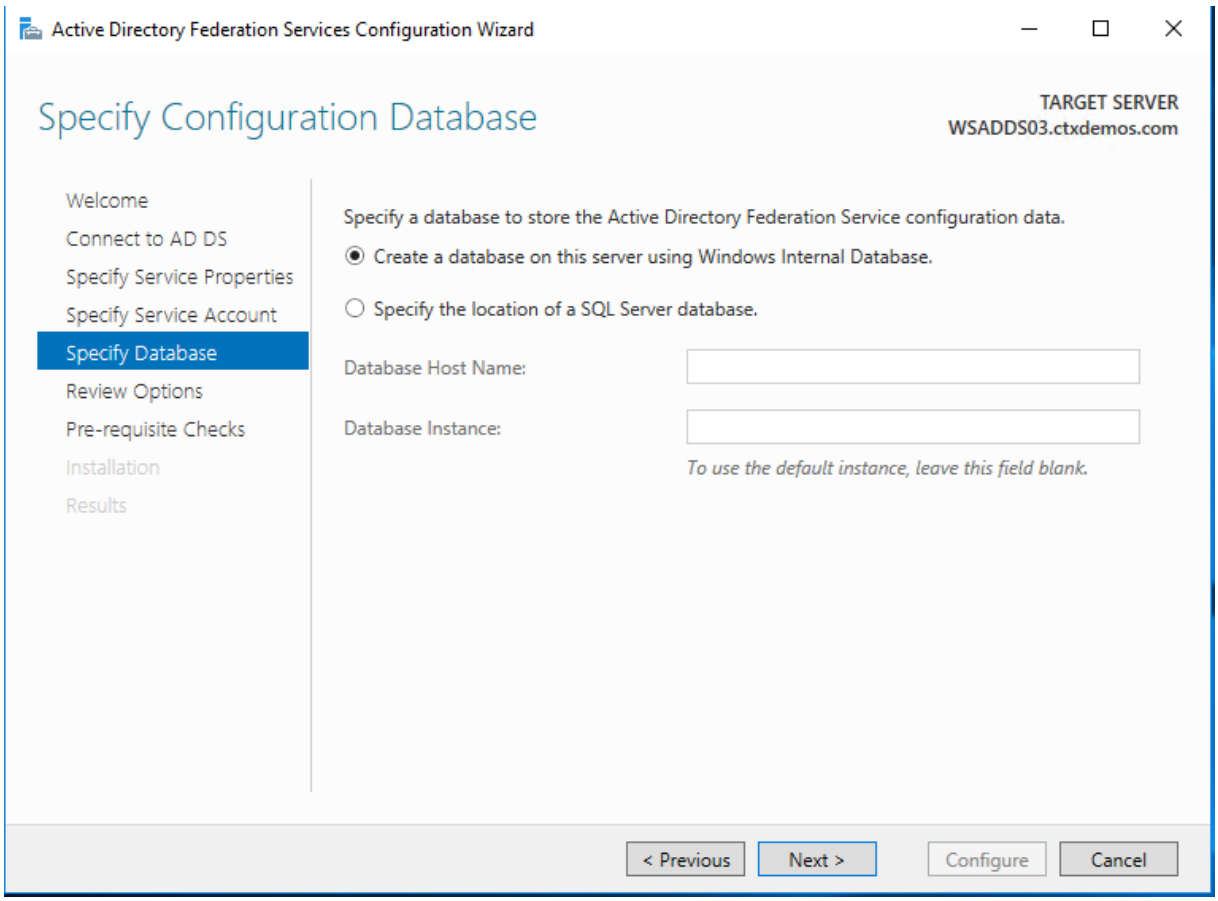
[サービスアカウントの指定] ページで、[グループ管理サービスアカウントの作成] を選択し、このアカウントの一意の名前を入力します。グループ管理サービスアカウントは、Windows Server 2012 以降でサポートされており、30日ごとに自動的に変更される厳密な複雑なパスワードが付属しています。［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



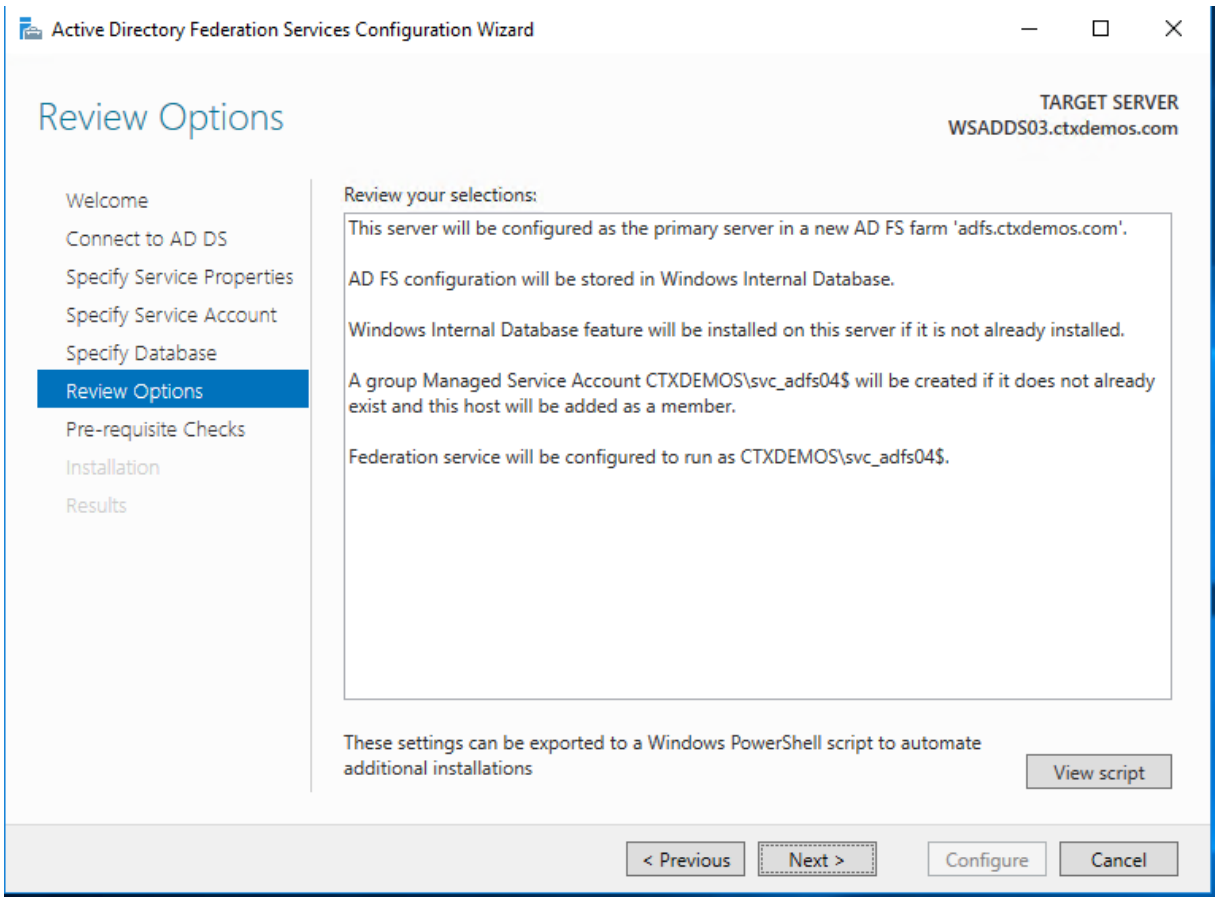
[構成データベースの指定**]** ページで、SQL Server データベースの場所を指定します。［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



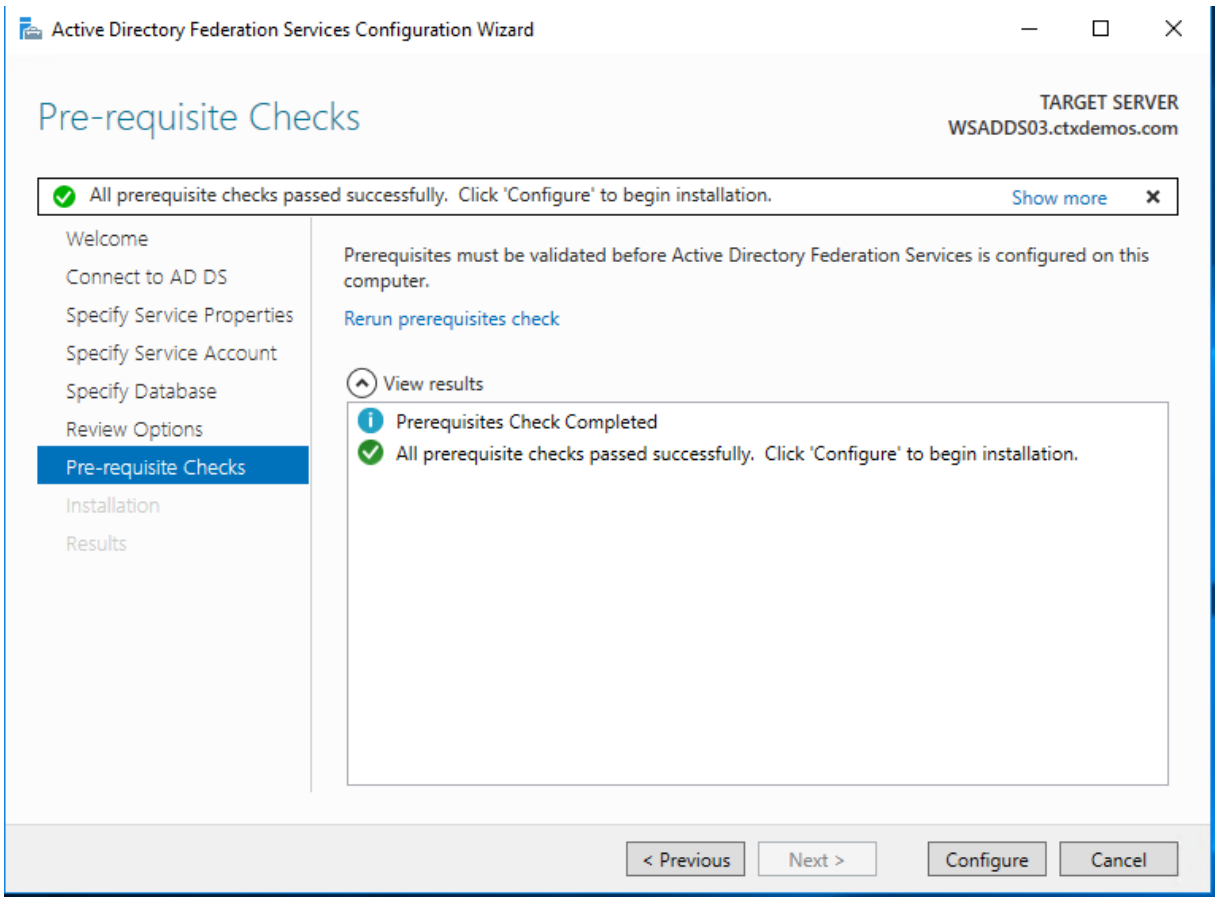
[確認オプション] ページで、構成の選択を確認し、[次へ] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



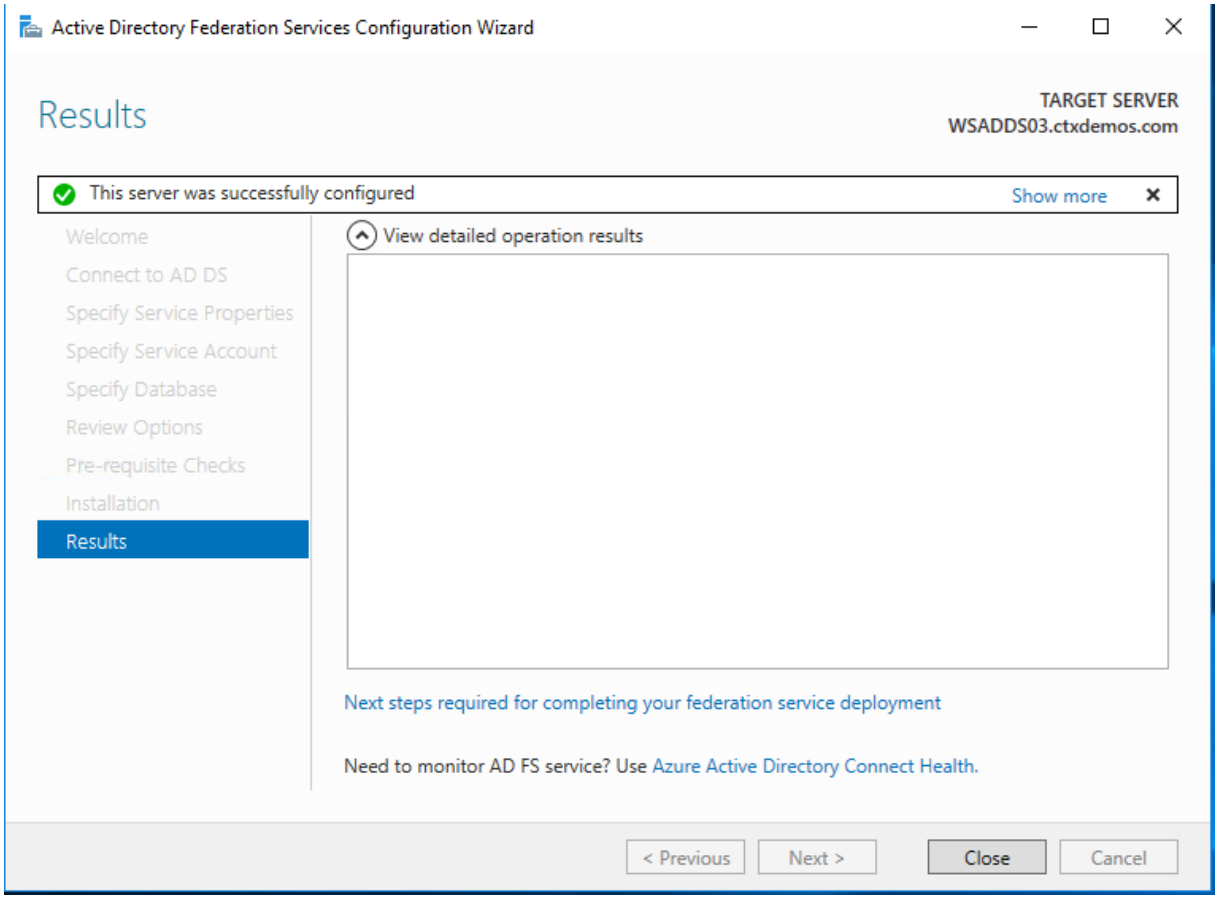
[前提条件のチェック] ページで、すべての前提条件のチェックが正常に完了していることを確認し、[構成] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



[結果] ページで、インストールが正常に完了していることを確認します。［閉じる］をクリックしてウィザードを終了します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



> 注:
>
> 次の手順を完了するには、Azure テナント ID が必要です。
>
> Azure テナント ID を取得するには、Microsoft のドキュメント記事「Get AzureID Tenant Detail」の手順に従います。
>
> Microsoft のドキュメント記事「Configure AD FS 2016 and Azure MFA」に、Azure MFA クライアント GUID に関する情報も記載されています。

AD FS ファームの構成-自動化

次の PowerShell スクリプトを実行できます。

```
#
# Windows PowerShell script for AD FS Deployment
#
Import-Module ADFS
Install-AdfsFarm `
-CertificateThumbprint:"BD02F30D90A96EEE4A5934F2EA979E7A052584AE" `
-FederationServiceDisplayName:"CTXDEMOS STS" `
-FederationServiceName:"adfs.ctxdemos.com" `
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
-GroupServiceAccountIdentifier:"C
<!--NeedCopy-->
```

Azure MFA を使用した AD FS の構成

AD FS サーバーを構成する

各 AD FS サーバーで PowerShell を起動し、次のコマンドを実行します。

```
# Install Windows PowerShell MSOnline Module
Install-Module MSOnline

# Import Windows PowerShell MSOnline Module
Import-Module MSOnline

# Get the Azure Global Administrator credential
$credential = Get-Credential

# Sign in to your Azure Active Directory environment
Connect-MsolService -Credential $credential

# Set a variable for the Azure Tenant name
$azureTenantID = "ctxdemos.onmicrosoft.com"

# Set a variable for the Azure MFA Client GUID
$azureMFAClientGUID = "981f26a1-7f43-403b-a875-f8b09b8cd720"

# Generate a certificate for the Azure MFA on AD FS server
$azureMFACertificate = New-AdfsAzureMfaTenantCertificate -TenantId
    $azureTenantID

# Add the new credentials to the Azure MFA Client Service Principal
New-MsolServicePrincipalCredential -AppPrincipalId $azureMFAClientGUID
    -Type asymmetric -Usage verify -
Value $azureMFACertificate
<!--NeedCopy-->
```

AD FS ファームを構成する

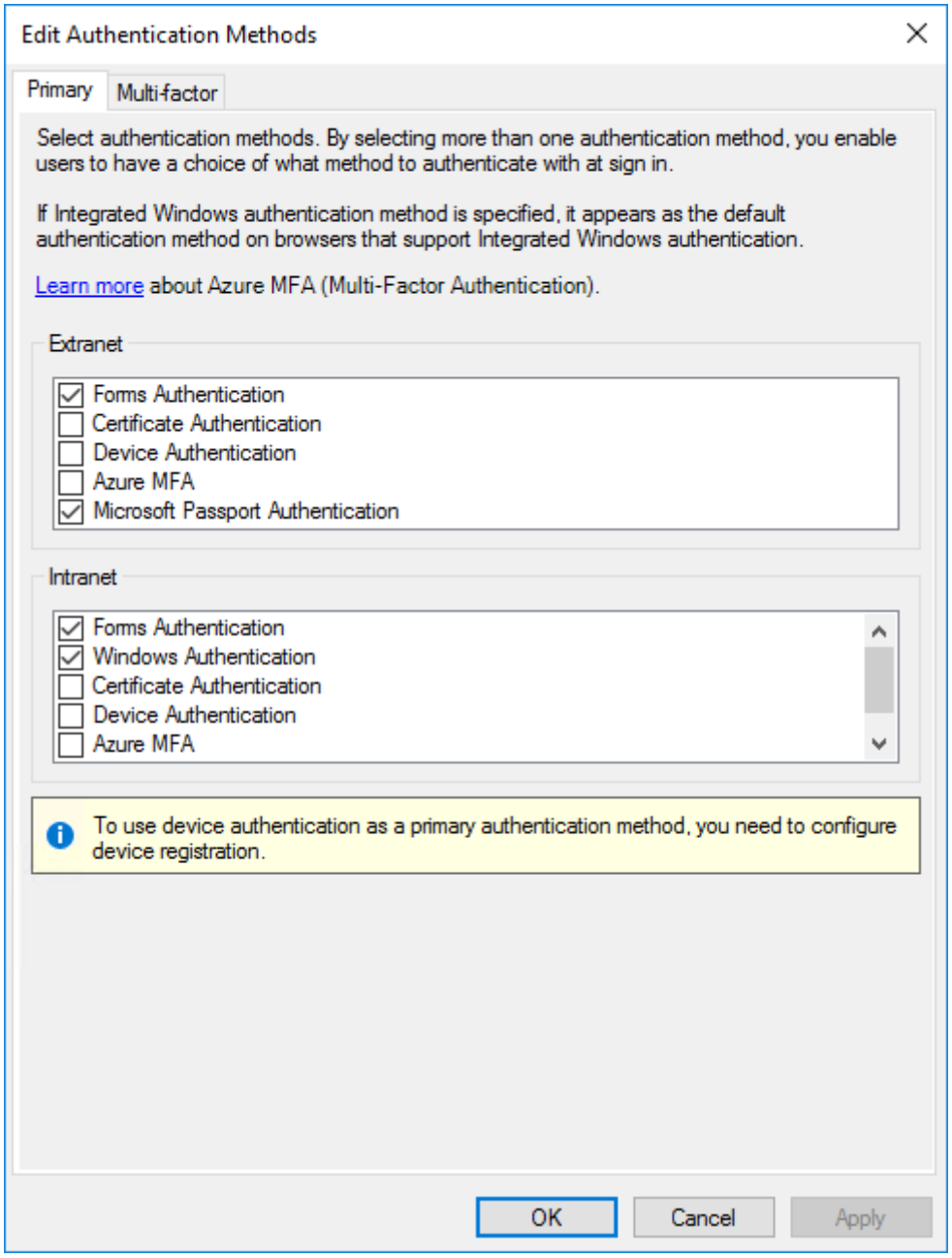
AD FS サーバーの 1 つだけで、次のコマンドを実行します。

```
Set-AdfsAzureMfaTenant -TenantId $azureTenantID -ClientId
    $azureMFAClientGUID
```

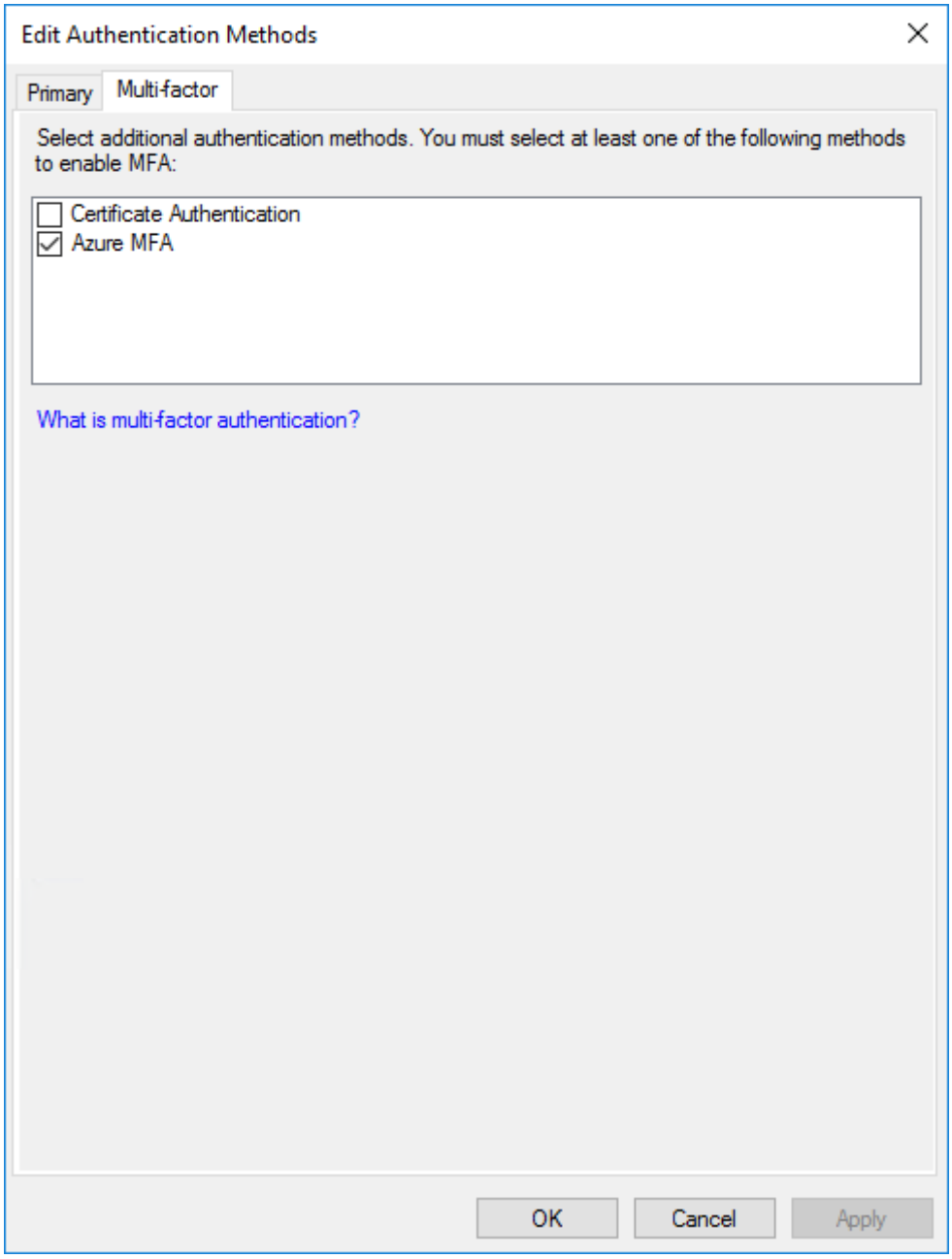
© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
<!--NeedCopy-->
```

各サーバーで AD FS サービスを再起動します。次に、Azure MFA がイントラネットとエクストラネットのプライマリおよび多要素認証方法として使用できることがわかります。



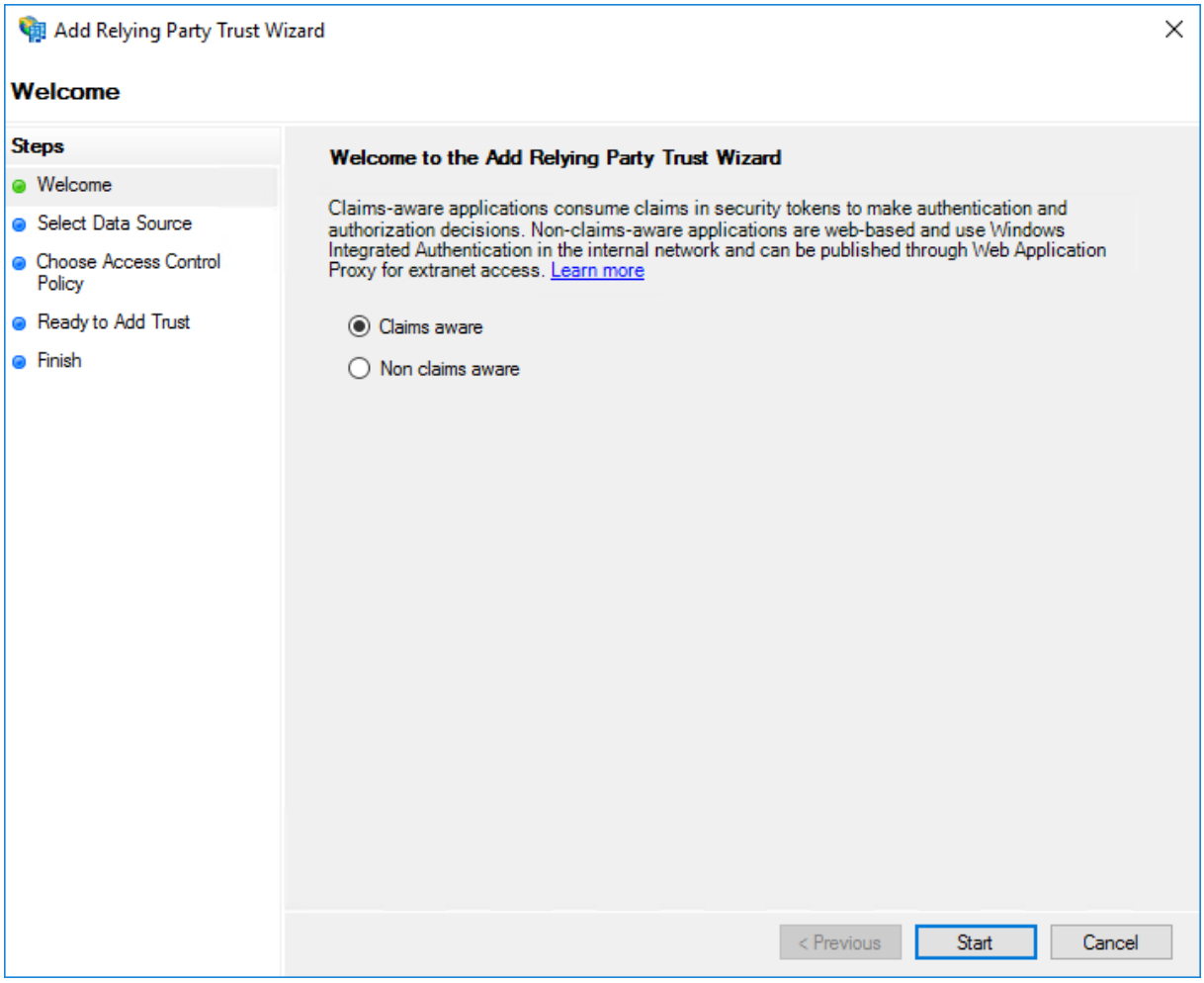
© 1999–2021 Citrix Systems, Inc. All rights reserved.



Citrix ADC を使用して **AD FS** を構成する

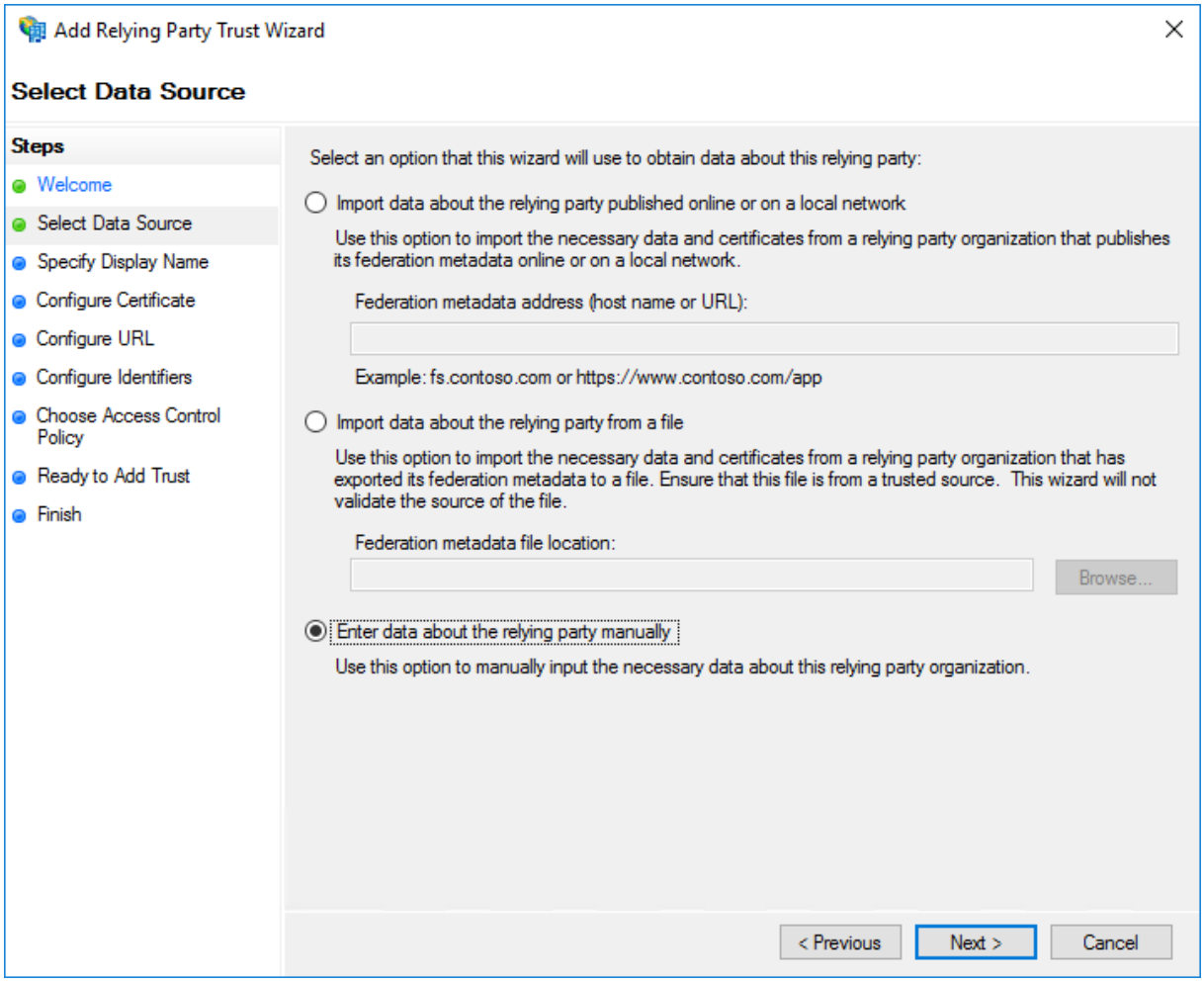
AD FS と Citrix ADC の間にフェデレーション信頼を作成する必要があります。AD FS 管理コンソールで、**[**証明書利用者の信頼**]** に移動し、**[**証明書利用者の信頼の追加**]** を選択します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



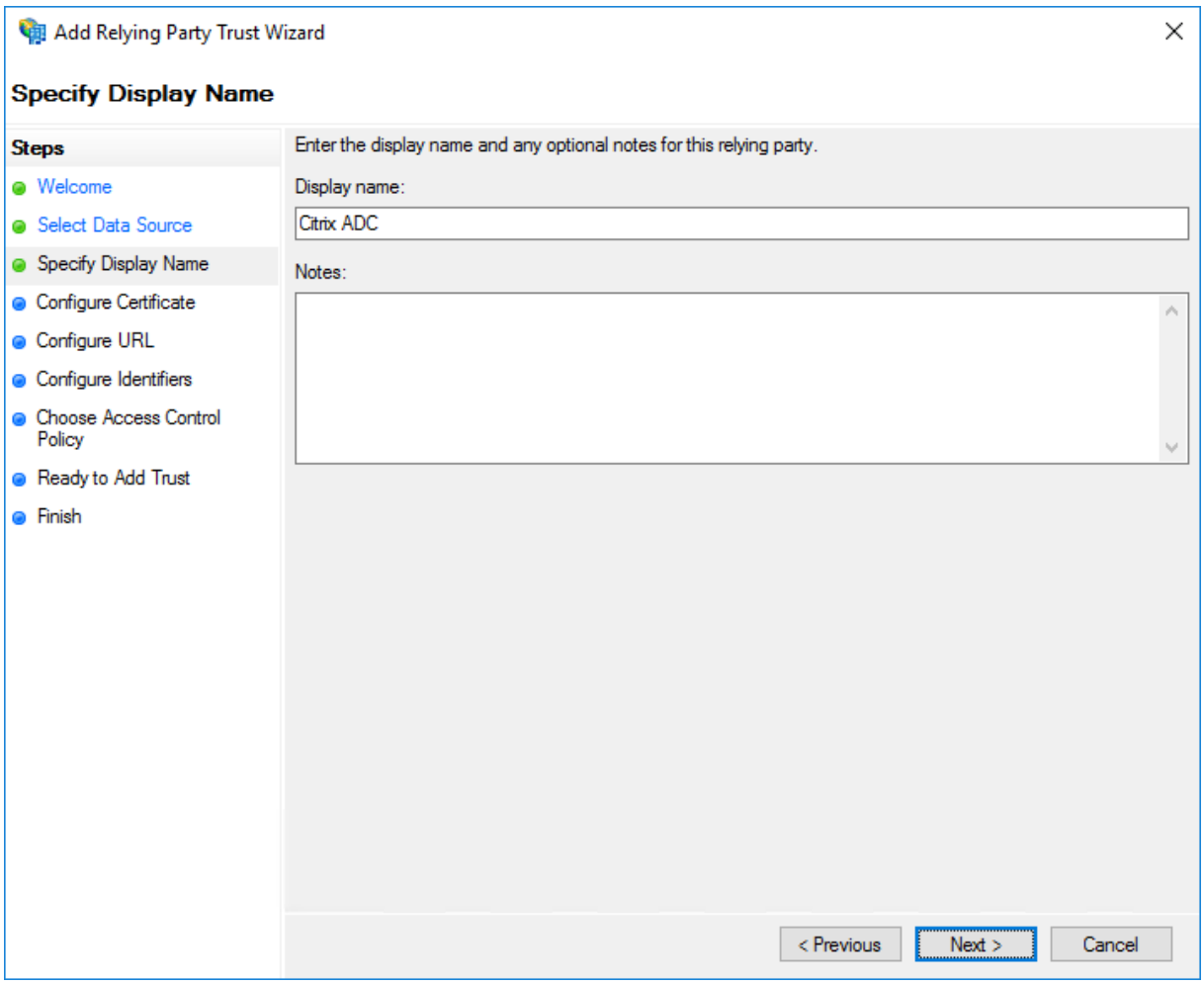
[証明書利用者に関するデータを手動で入力する] を選択し、[次へ] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



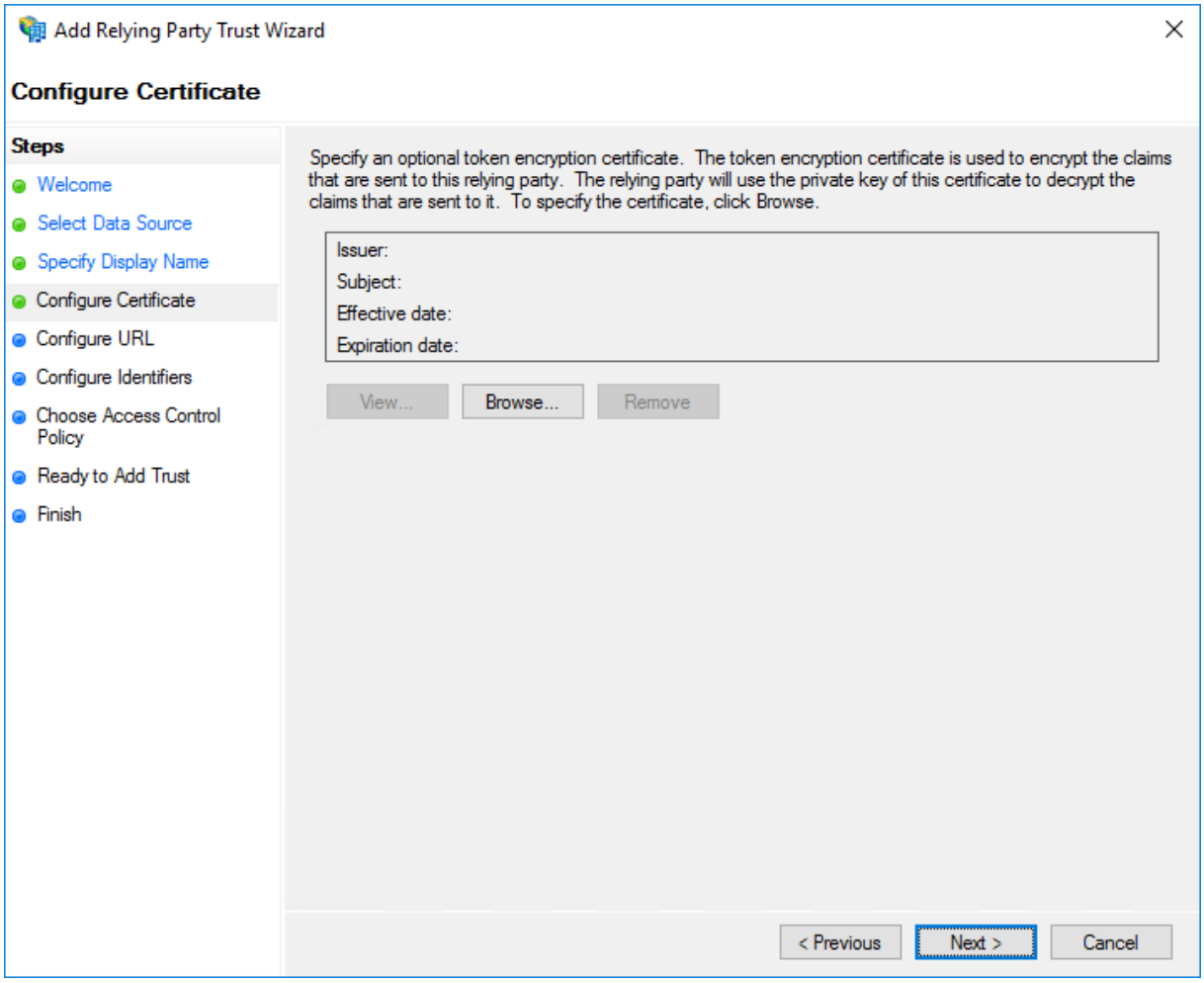
わかりやすい表示名およびオプションの注記を入力します。［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



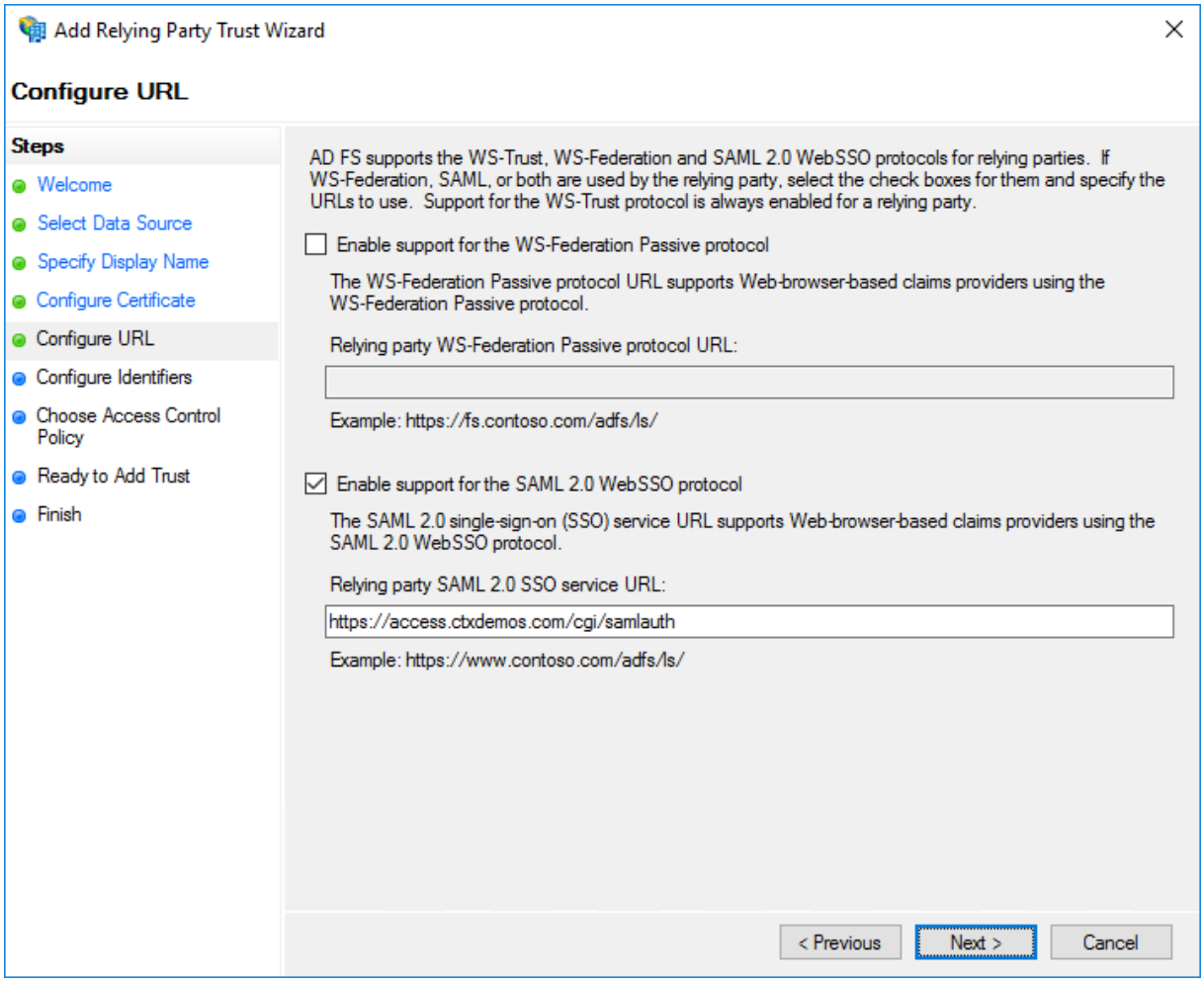
[次へ] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



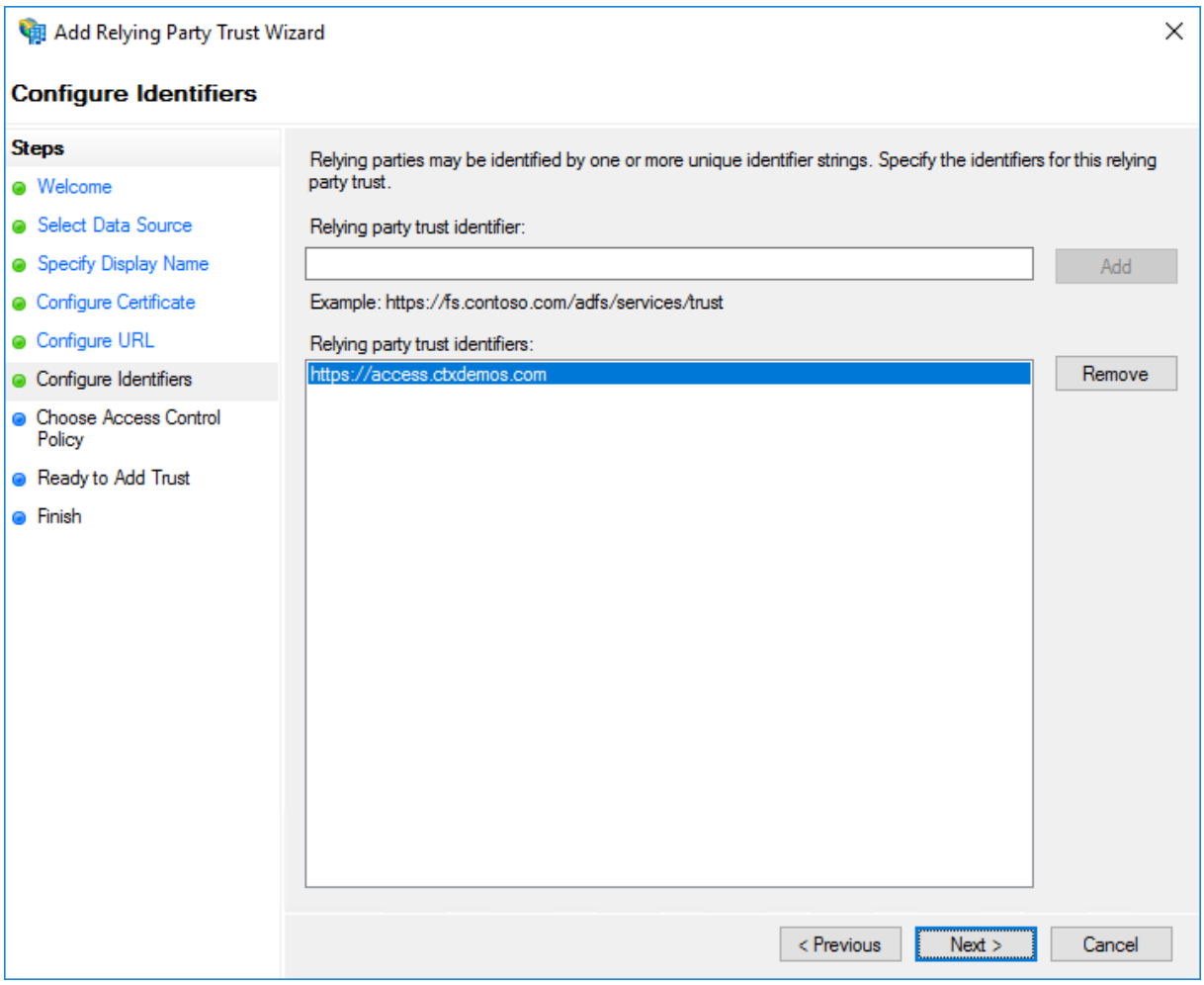
[SAML 2.0 WebSSO プロトコルのサポートを有効にする**]** を選択し、`https://CitrixGatewayFQDN/cgi/samlauth`と入力します。デモ環境では、`https://access.ctxdemos.com/cgi/samlauth`です。［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



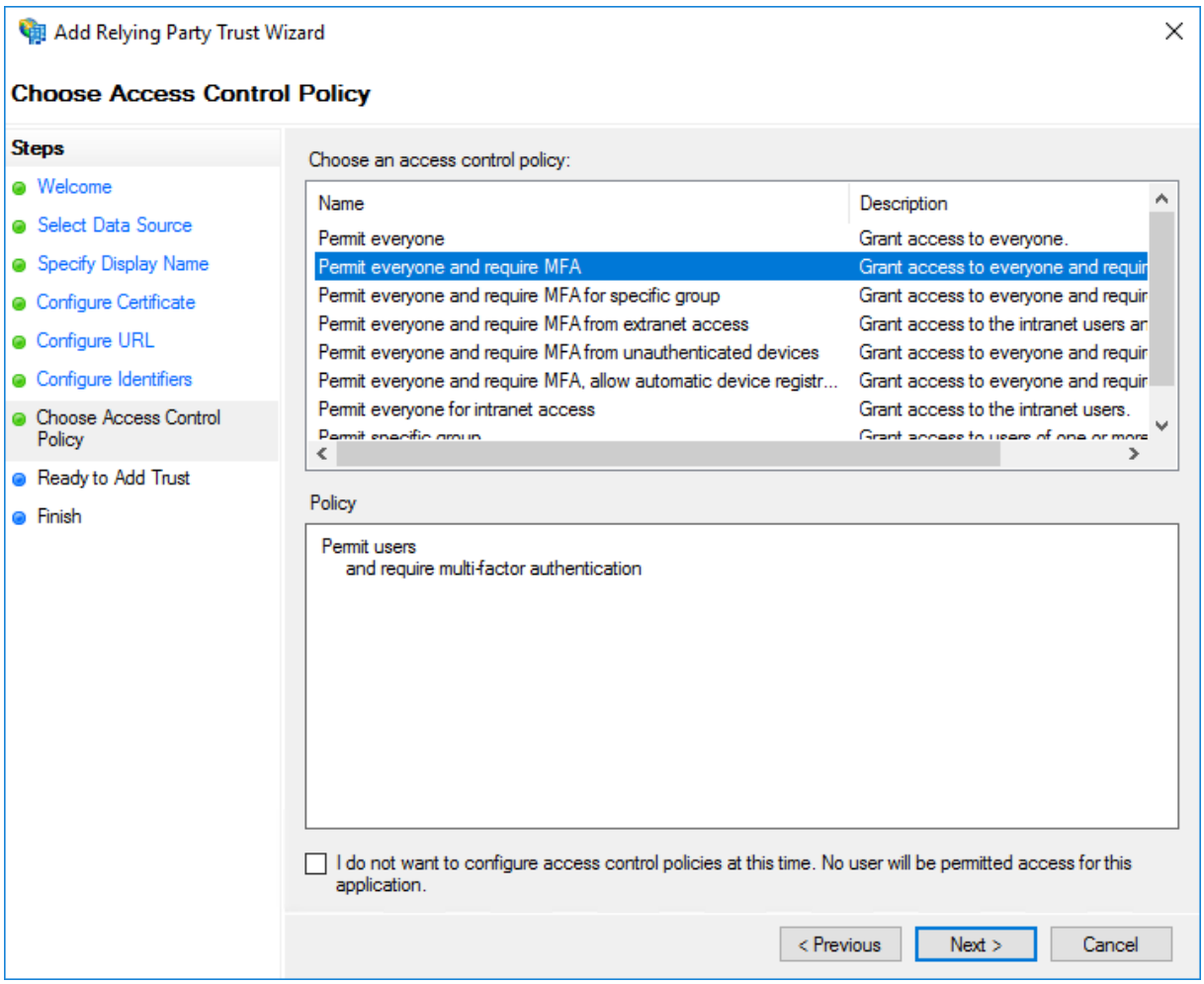
証明書利用者信頼の一意の識別子文字列を入力します。デモ環境では、`https://access.ctxdemos.com`です。この識別子は、Citrix ADC SAML プロファイルの発行者 URL として使用されます。［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



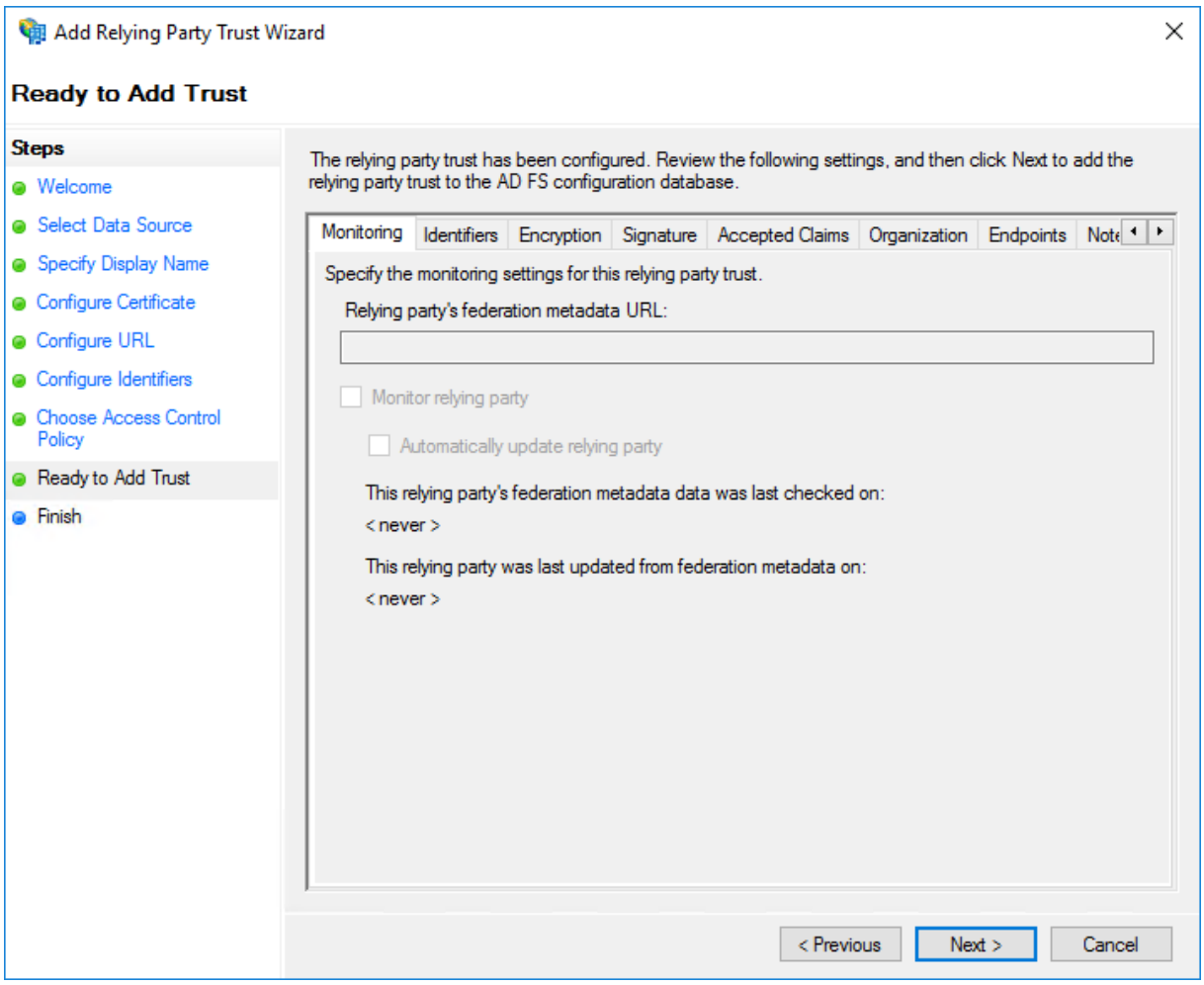
[アクセス制御ポリシーの選択**]** ページで、**[**全員を許可し、**MFA** を要求する**]** を選択します。［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



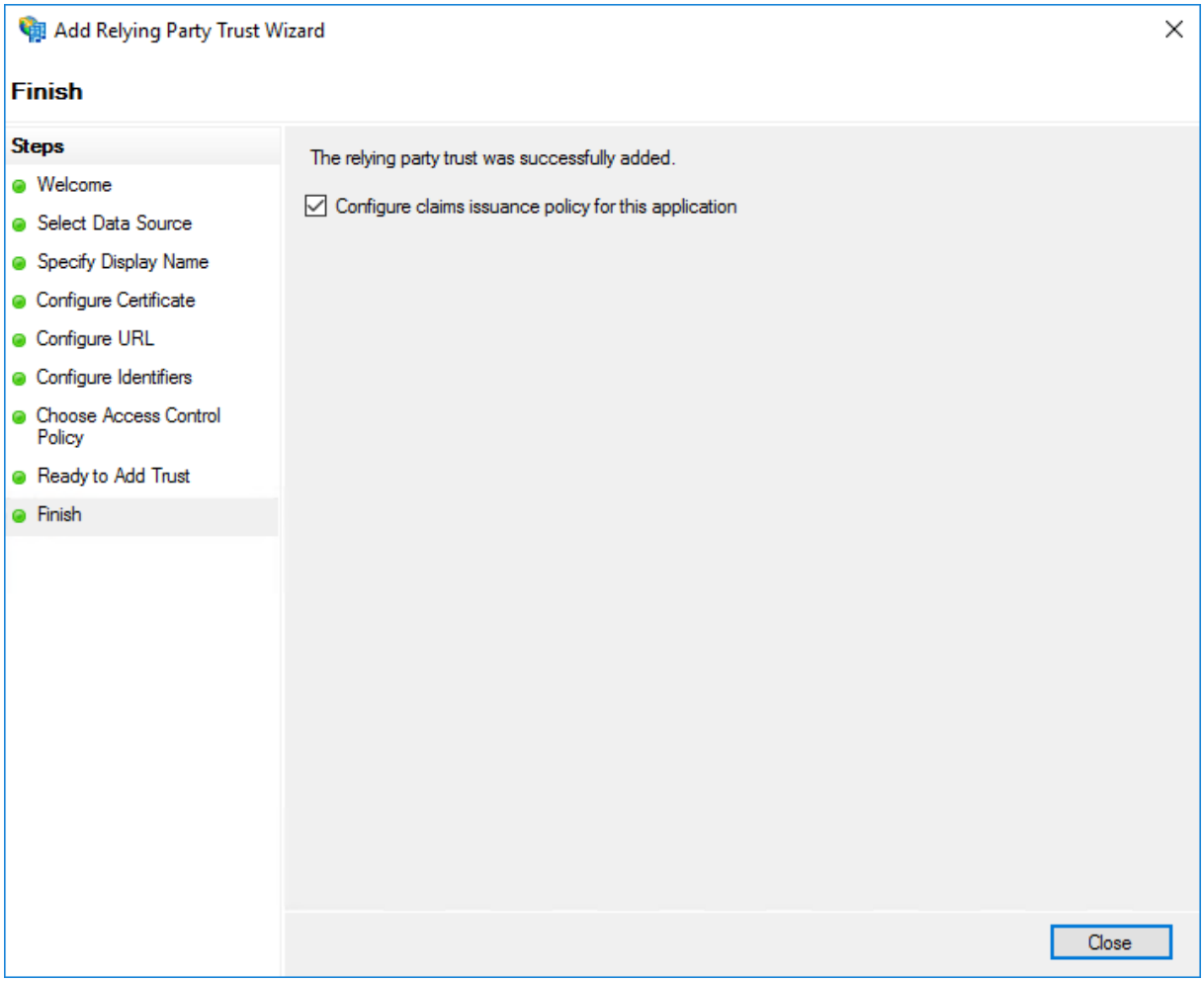
[次へ] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



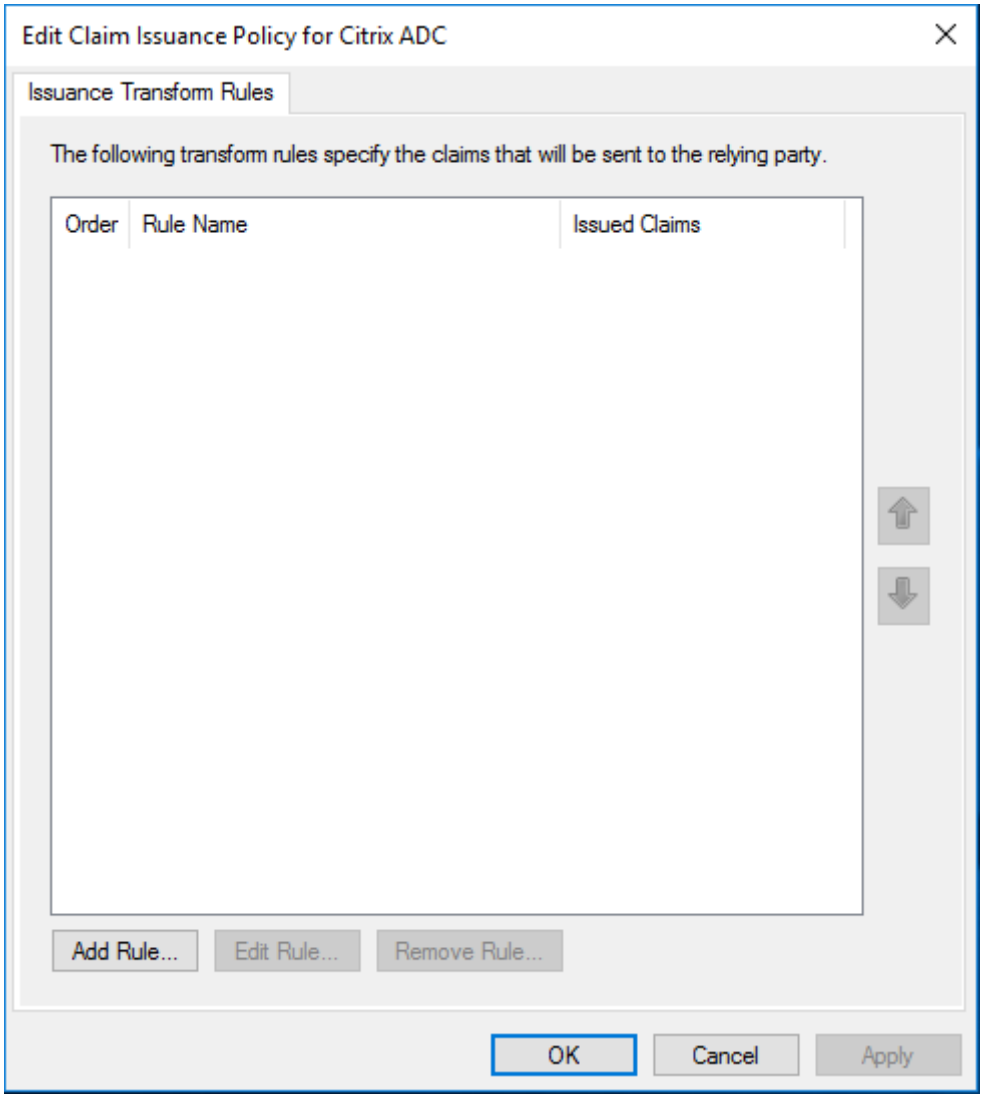
[完了] ページで、[このアプリケーションの要求発行ポリシーを構成する] を選択します。[閉じる] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



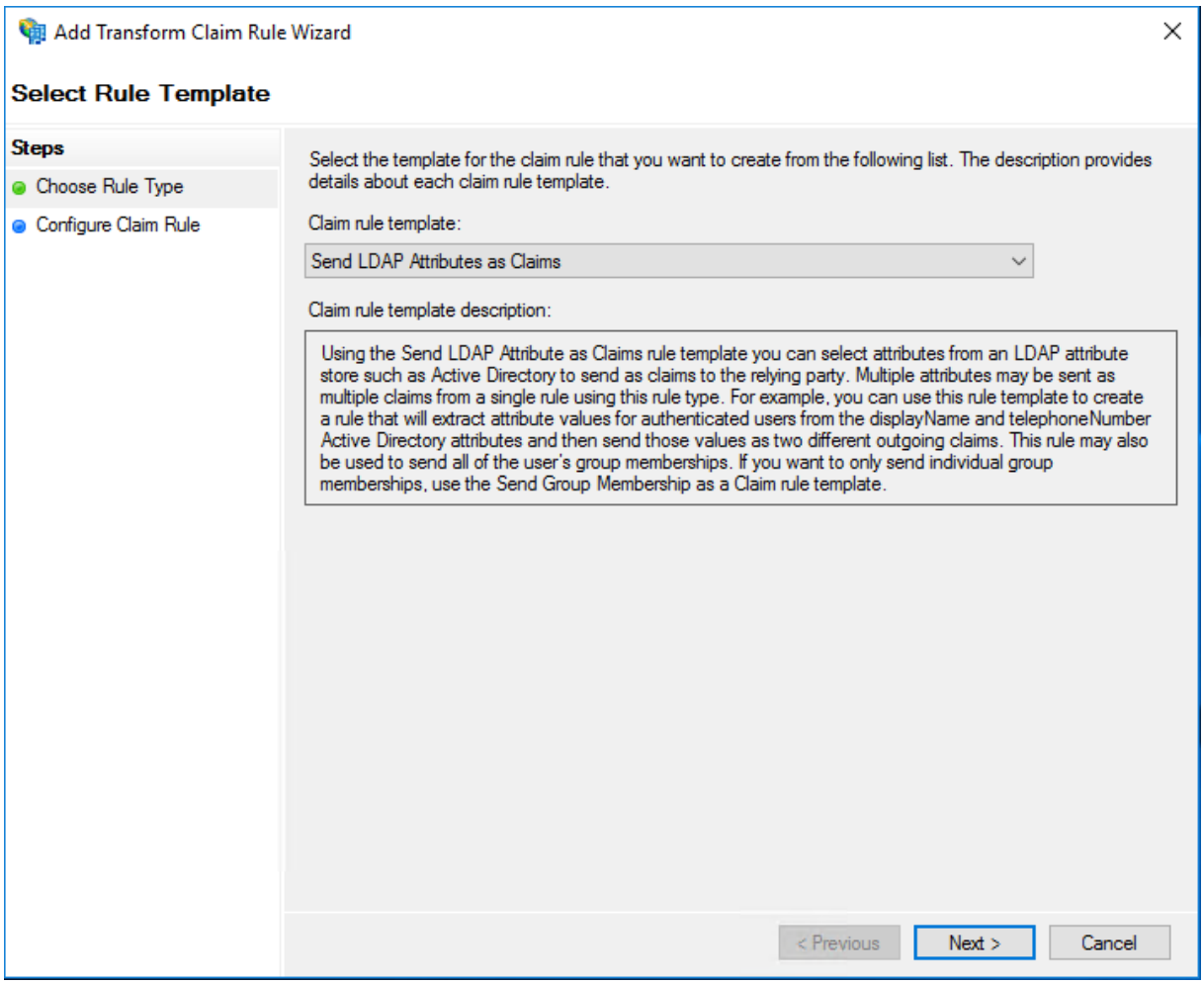
[発行変換規則] ページで、[規則の追加] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



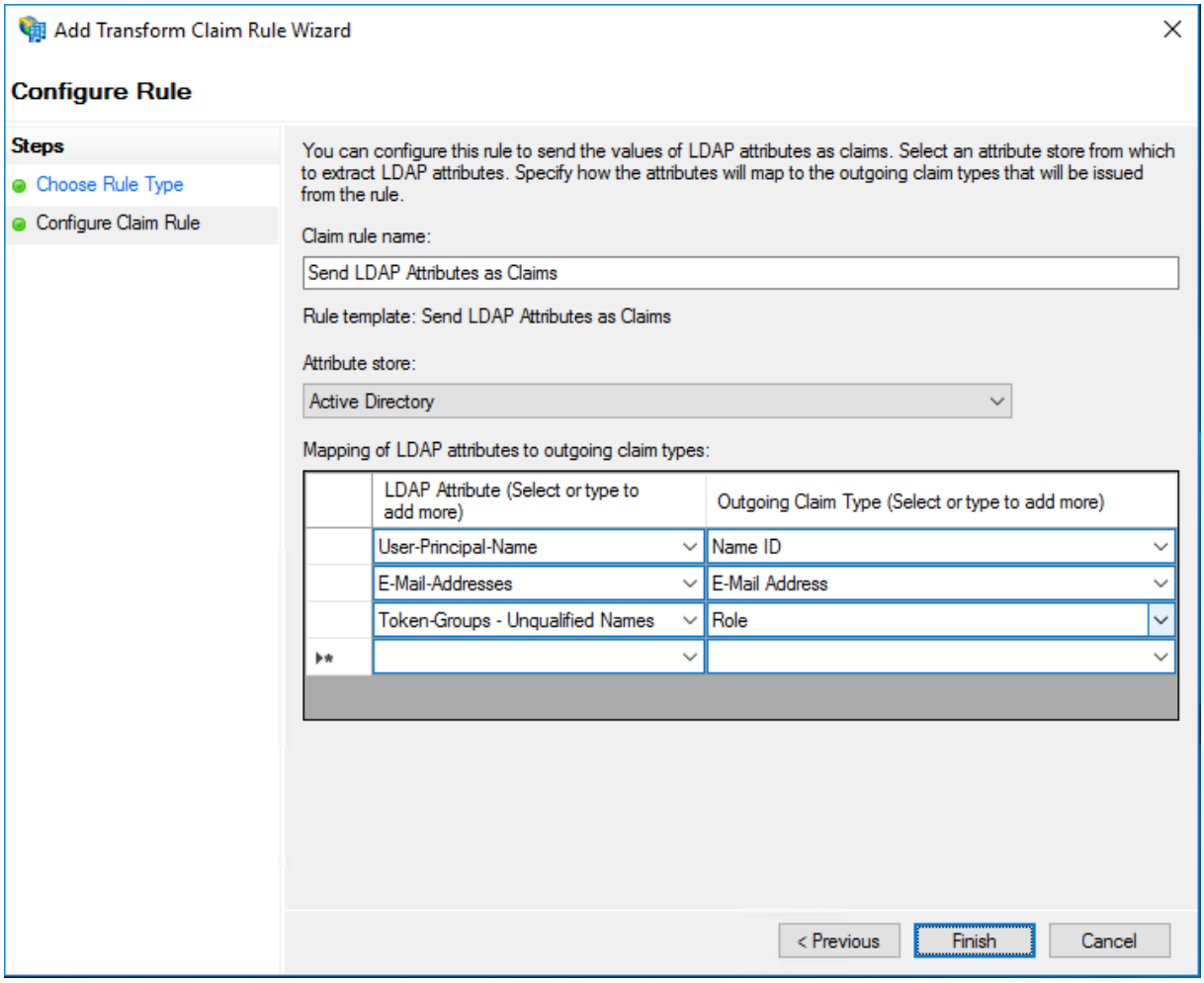
［次へ］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



[要求規則名**]** フィールドにわかりやすい名前を入力します。**[**属性ストア**]** で、**[Active Directory]** を選択します。次に、**[LDAP** 属性**]** と **[**送信要求タイプ**]** を選択します。

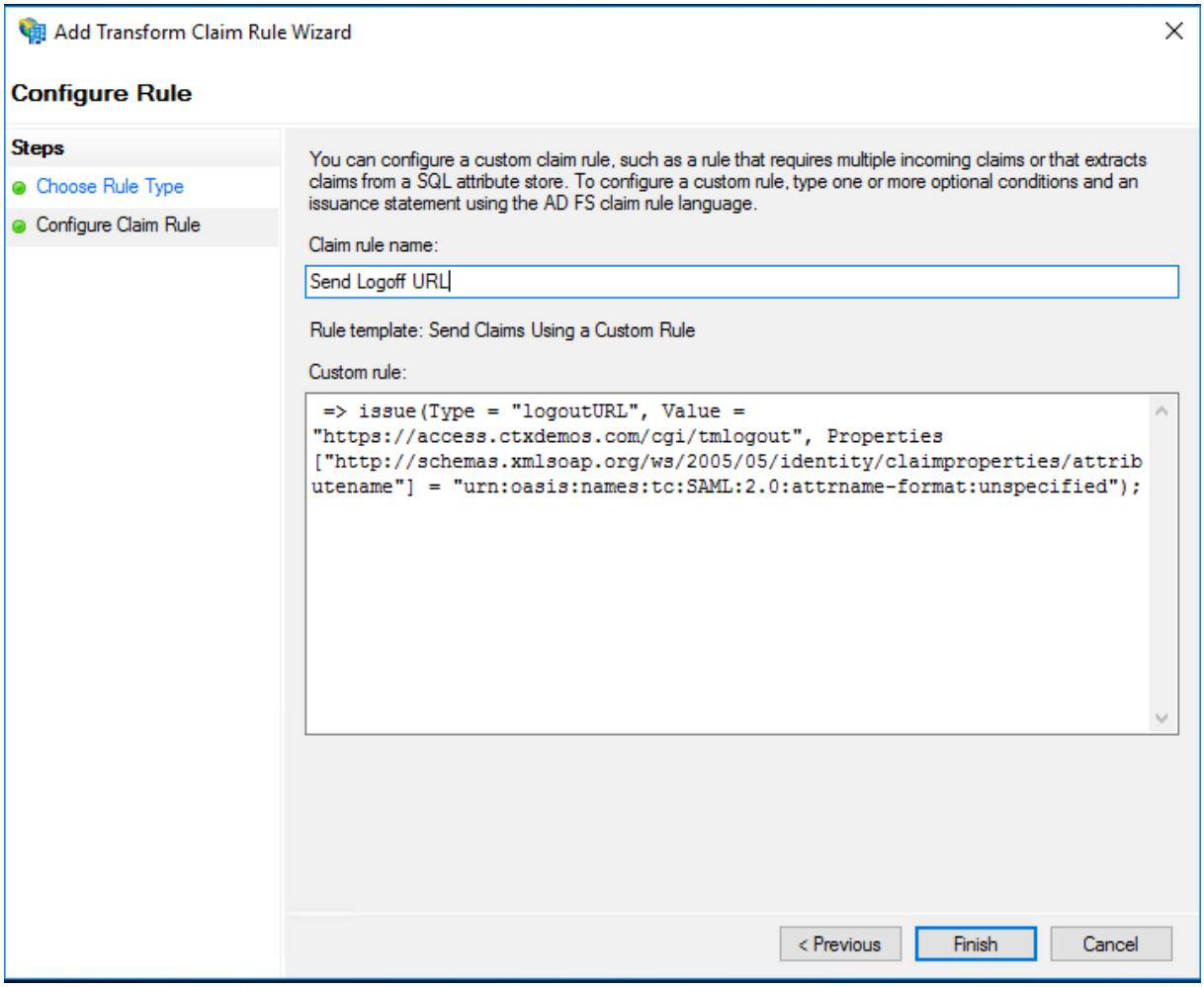
© 1999–2021 Citrix Systems, Inc. All rights reserved.



新しい規則を作成し、[規則テンプレートとして要求] として、[カスタム規則を使用して要求を送信する] を使用します。[要求規則名] にわかりやすい名前を入力し、[カスタム規則] に次の文字列を入力します。

```
1 => issue(Type = "logoutURL", Value = "https://access.ctxdemos.com/cgi/
    tmlogout", Properties["http://schemas.xmlsoap.org/ws/2005/05/
    identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML
    :2.0:attrname-format:unspecified");
2 <!--NeedCopy-->
```

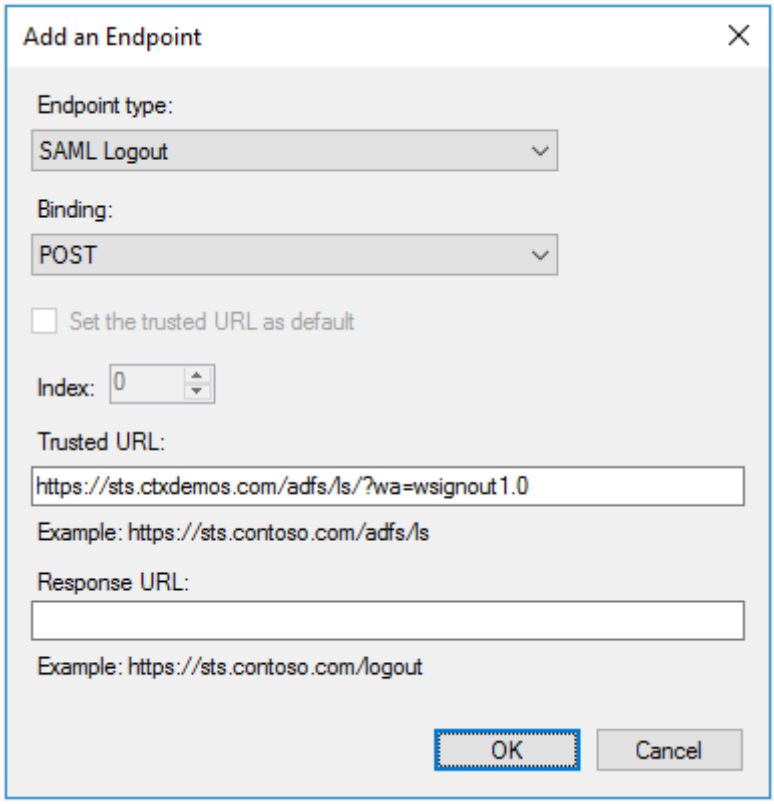
© 1999–2021 Citrix Systems, Inc. All rights reserved.



要求発行ポリシーが作成されたら、**[OK]** をクリックします。

[証明書利用者の信頼] > [Citrix ADC] を右クリックし、**[プロパティ]** を選択します。**[エンドポイント]** を選択し、**[ログアウト用の SAML を追加]** をクリックしてエンドポイントを追加します。**[エンドポイントタイプ]** リストから **[SAML ログアウト]** を選択します。**[バインド]** で **[POST]** を選択し、**[信頼済み URL]** に`https://sts.ctxdemos.com/adfs/ls/?wa=wsignout1.0`と入力します。これは、Citrix ADC からログアウトするときのログアウト URL として機能します。[**OK**] をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



[証明書利用者の信頼**] > [Citrix ADC]** を右クリックし、**[**プロパティ**]** を選択します。［暗号化］を選択し、Citrix Gateway にインストールされているパブリック SSL 証明書を追加します。この証明書は、Citrix ADC からの受信 SML リクエストの復号化に使用されます。[署名] タブでも同じ操作を繰り返します。この証明書は、着信 SAML リクエストの署名を確認するために使用されます。［**OK**］をクリックします。

IdP 開始サインオンページの有効化

AD FS IdP が開始するサインオンページを有効にできます。IdP が開始したサインオンを使用して、未登録の MFA ユーザーにカスタムエラーページを表示します。有効にするには、次のコマンドを実行します。

```
1 Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
2 <!--NeedCopy-->
```

AD FS ファームのテスト

Web ブラウザーを開き、次の場所に移動します。

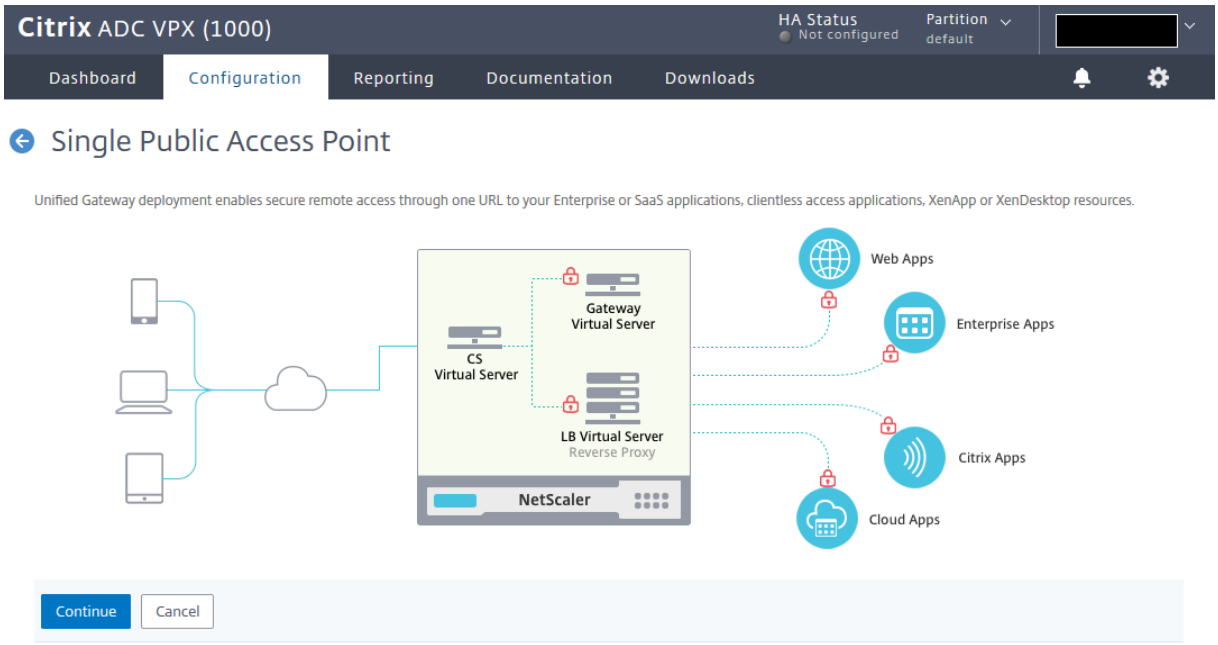
- https://sts.ctxdemos.com/FederationMetadata/2007-06/FederationMetadata.xml
- https://sts.ctxdemos.com/adfs/fs/federationserverservice.asmx
- https://sts.ctxdemos.com/adfs/ls/idpinitatedsignon.aspx

© 1999–2021 Citrix Systems, Inc. All rights reserved.

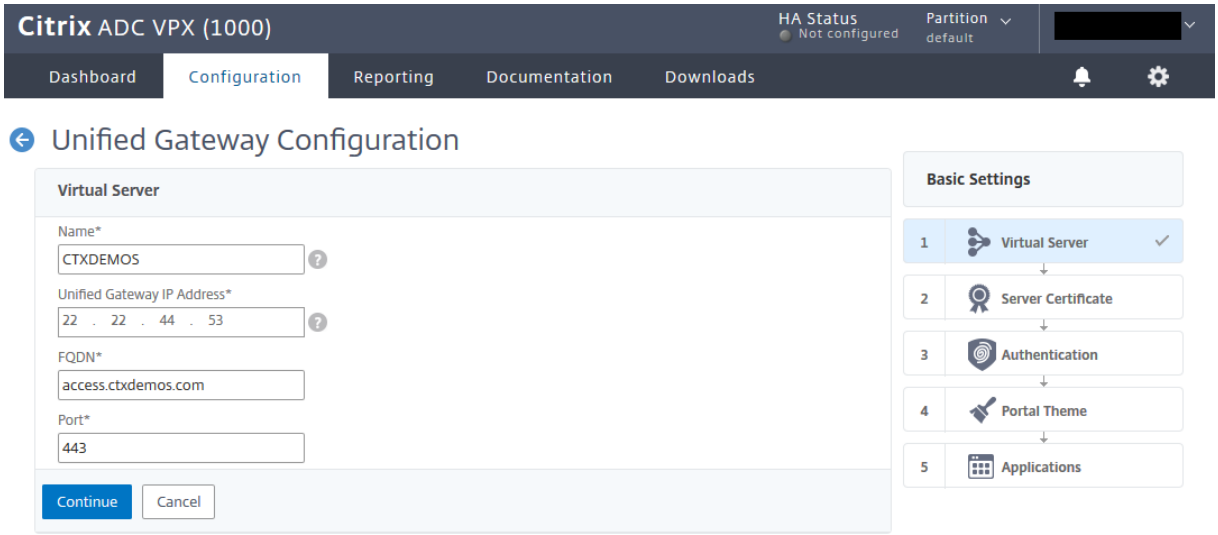
Citrix ADC および Citrix Gateway

Citrix Gateway の構成

ウィザードを使用して Citrix Gateway を構成できます。Citrix ADC 管理 GUI にログオンし、**Unified Gateway** に移動し、［新しいゲートウェイの作成］をクリックします。次に、［続行］をクリックします。

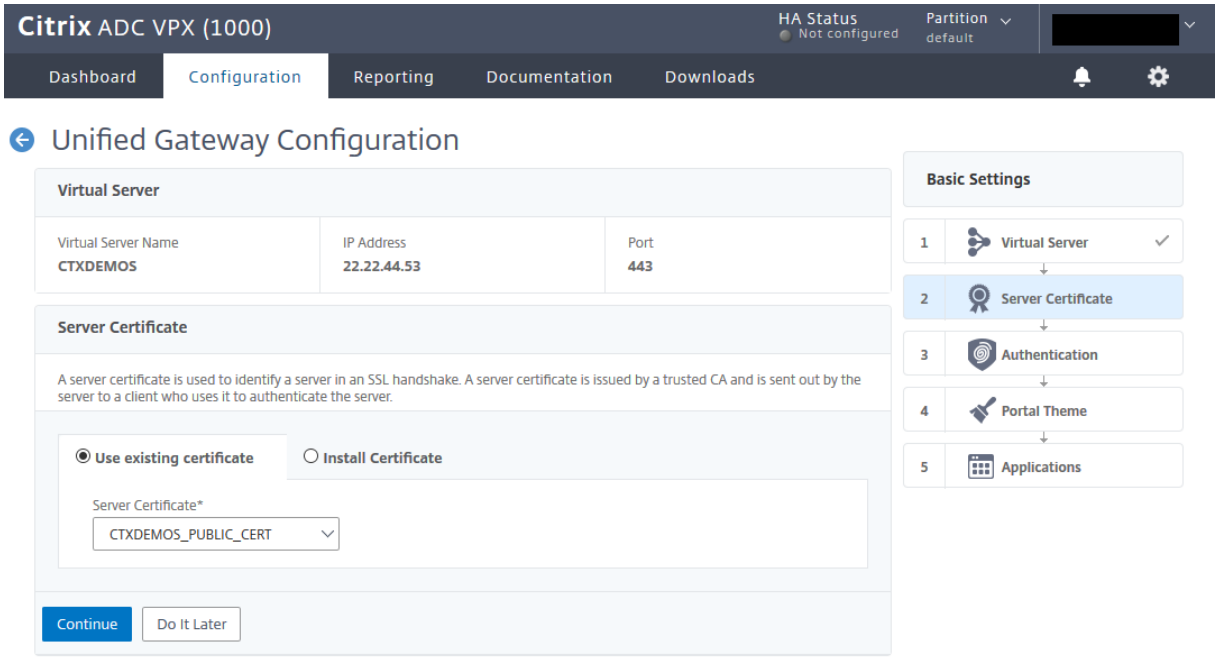


Unified Gateway の名前、IP、および FQDN を入力し、［続行］をクリックします。



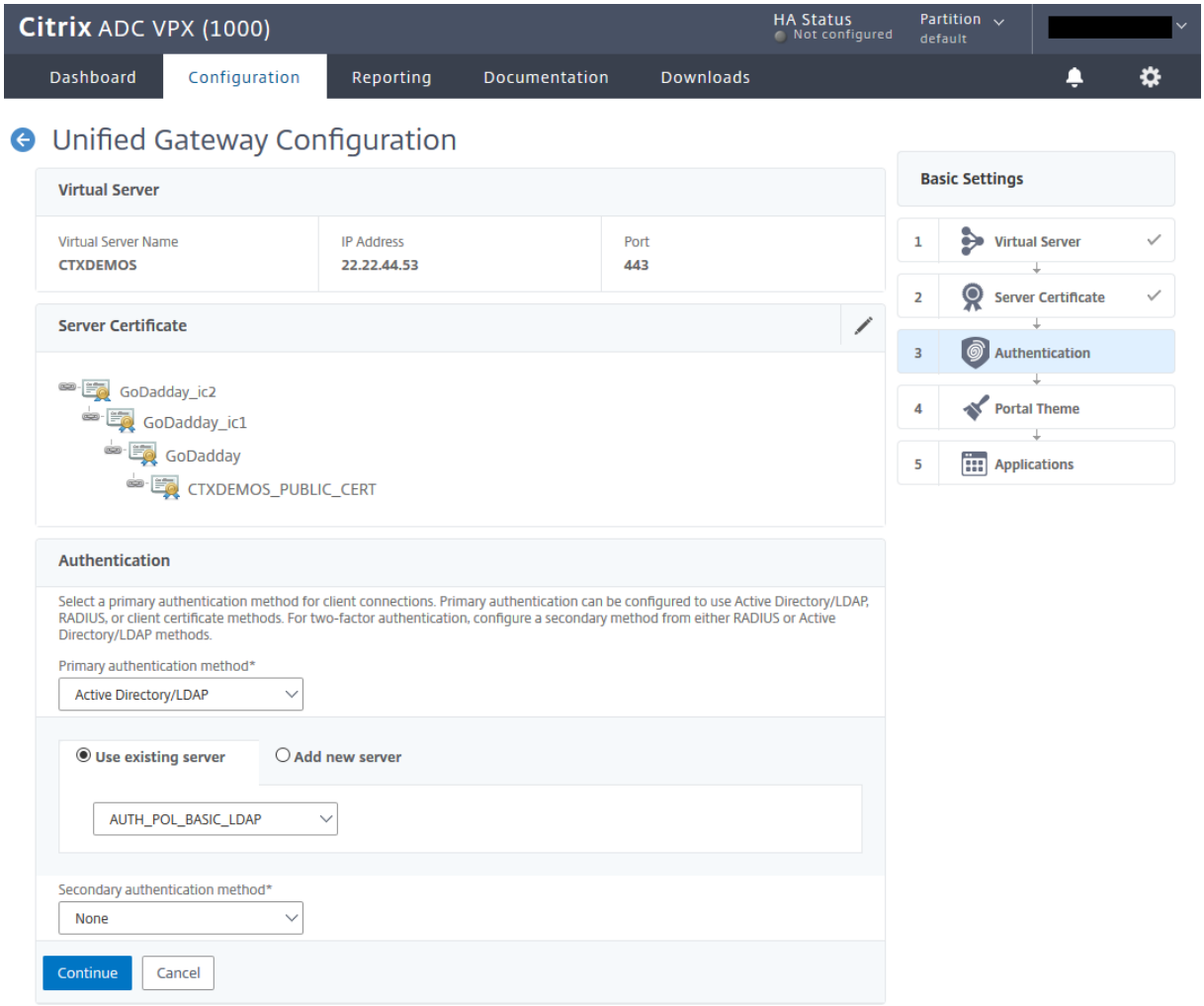
パブリック SSL 証明書を選択し、［続行］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



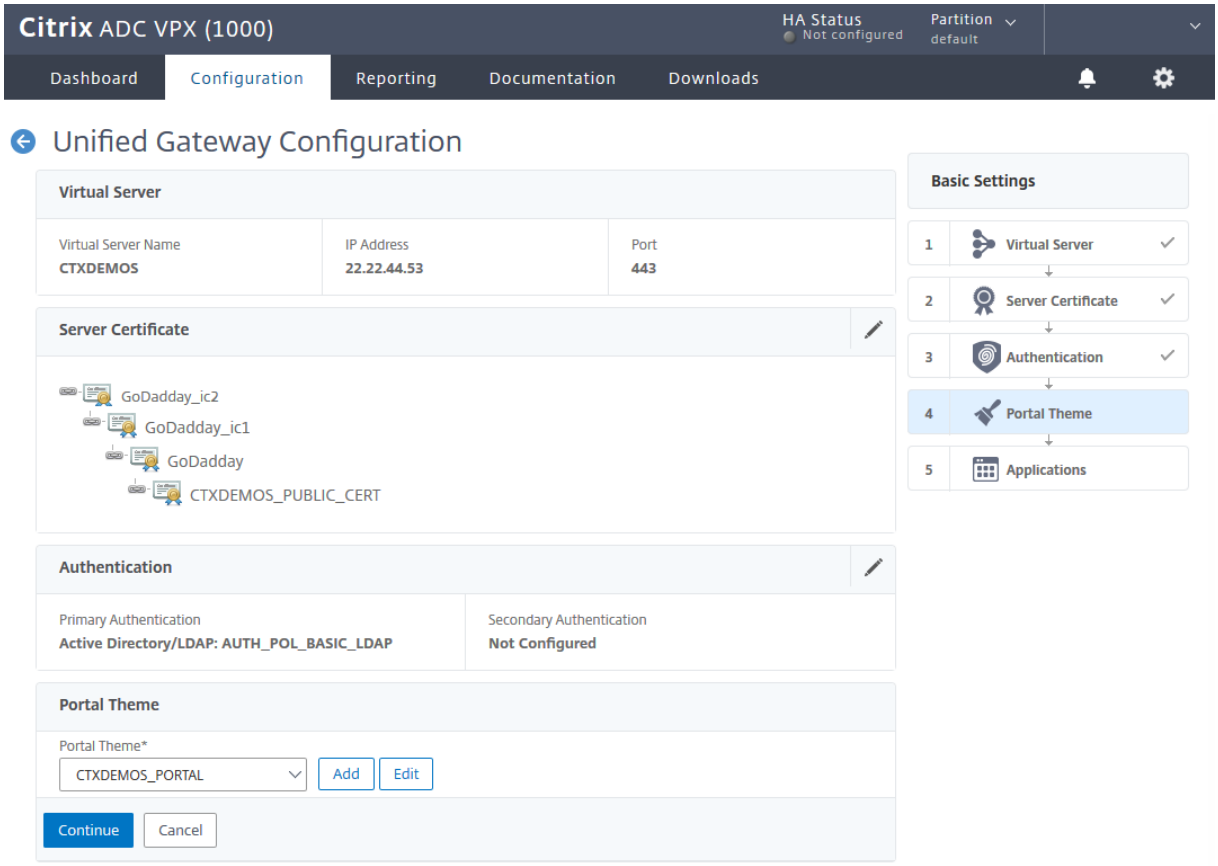
基本的な LDAP ポリシーを作成し、**Unified Gateway** にバインドします。［続行］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



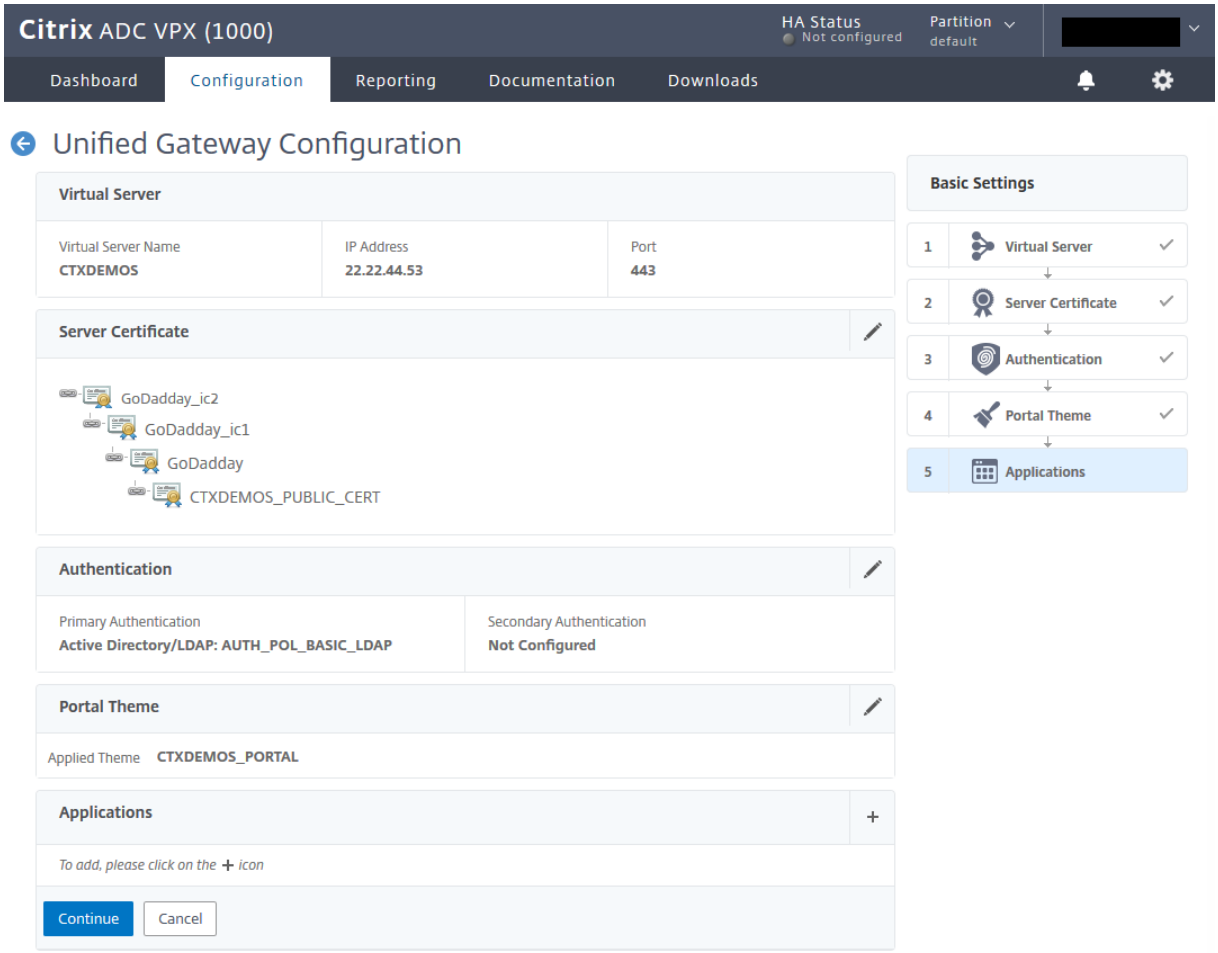
RfWebUI に基づいてポータルテーマを作成し、**Unified Gateway** にバインドします。［続行］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



Citrix Gateway と StoreFront を統合するアプリケーションの前にあるプラス記号（+）を選択します。

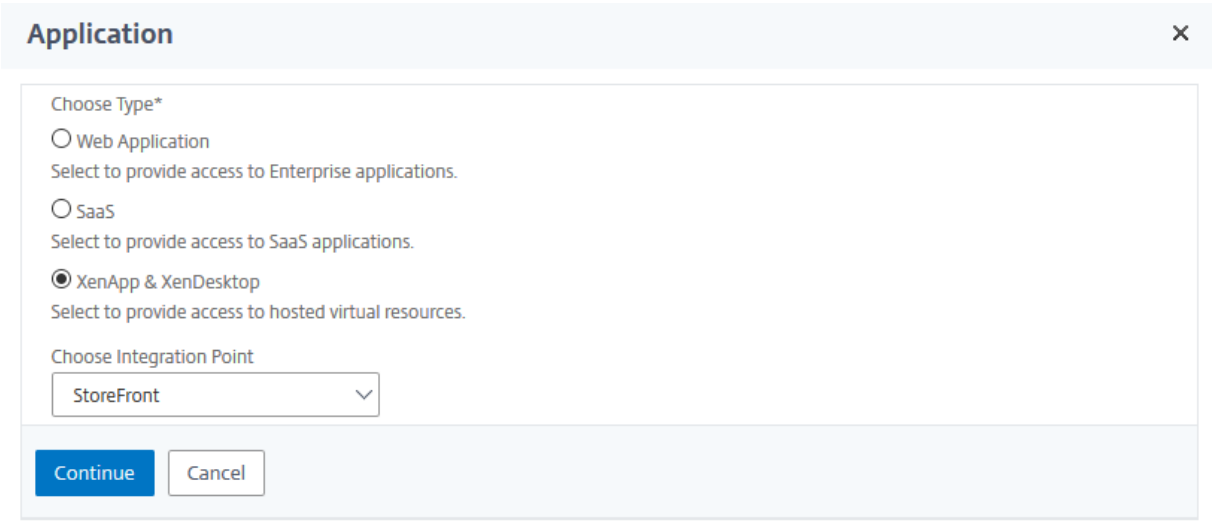
© 1999–2021 Citrix Systems, Inc. All rights reserved.



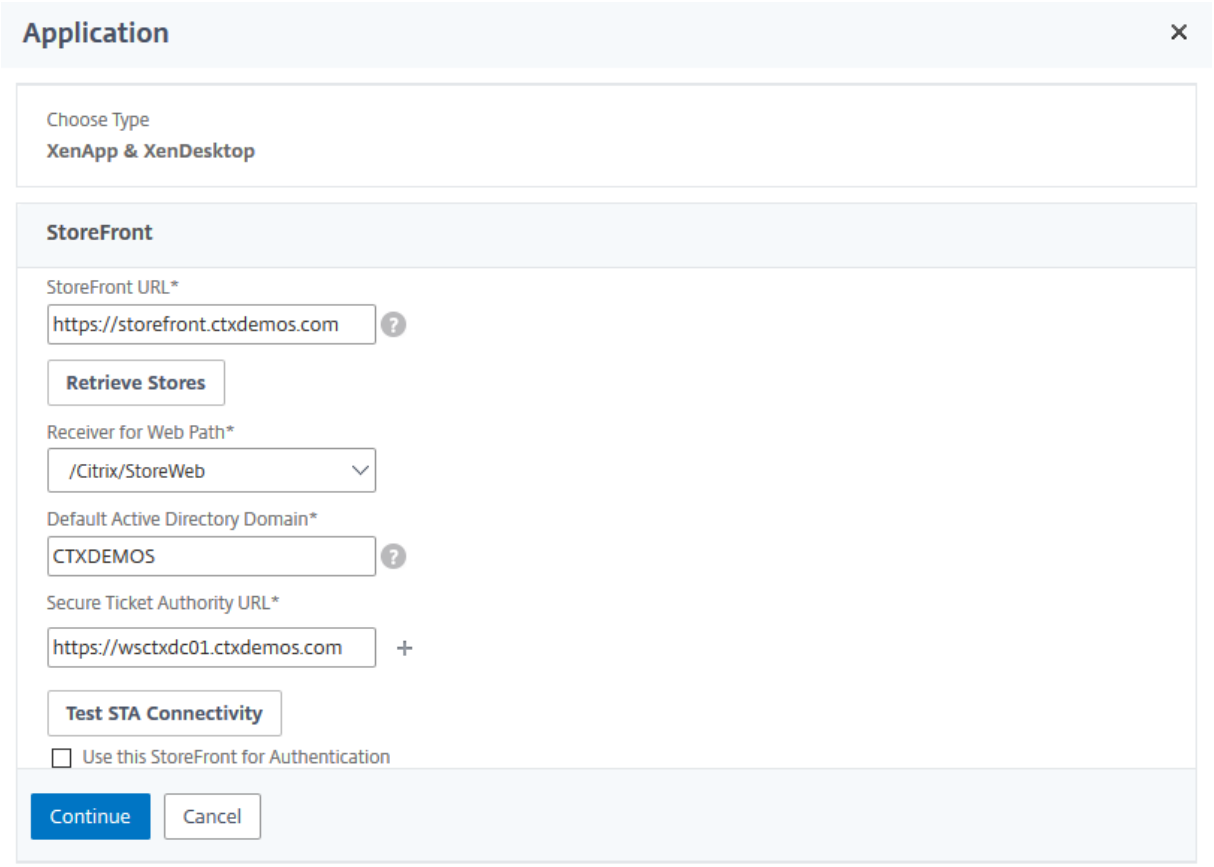
Citrix StoreFront と **Citrix Gateway** の統合

[アプリケーション]ページで [**XenApp & XenDesktop**]を選択し、[統合ポイントの選択]リストから [**StoreFront**] を選択します。［続行］をクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

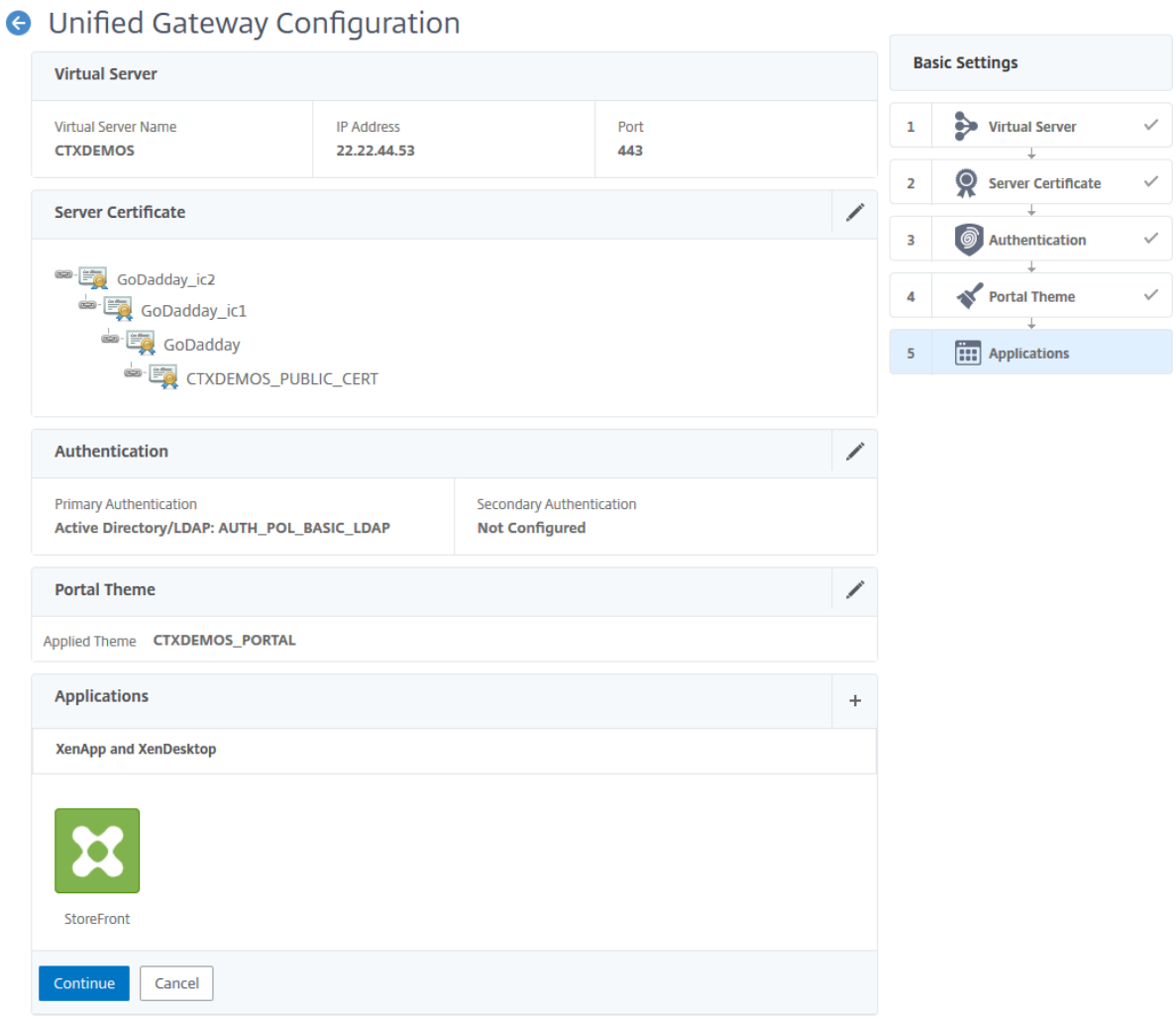


StoreFront URL を入力し、［ストアの取得］をクリックします。次に、［デフォルトの **Active Directory** ドメイン］と ［**Secure Ticket Authority URL**］設定を入力します。［**STA** 接続のテスト］、［続行］の順にクリックします。



［完了］、［続行］の順にクリックします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



Citrix Gateway の構成と **StoreFront** の統合 **— CLI**

```
# Create Session Policy and Action for Citrix Receiver
add vpn sessionAction AC_OS_22.22.44.50 -transparentInterception OFF -
    defaultAuthorizationAction ALLOW -SSO ON -icaProxy ON -wihome "https
    ://access.ctxdemos.com/Citrix/ExternalWeb" -ClientChoices OFF -
    ntDomain CTXDEMOS -clientlessVpnMode OFF -storefronturl "https://
    access.ctxdemos.com"
add vpn sessionPolicy PL_OS_22.22.44.50 "HTTP.REQ.HEADER("User-Agent").
    CONTAINS("CitrixReceiver") && HTTP.REQ.HEADER("User-Agent").CONTAINS
    ("CitrixVPN").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("
    NSGiOSplugin").NOT" AC_OS_22.22.44.50

# Create Session Policy and Action for Citrix Web Client
add vpn sessionAction AC_WB_22.22.44.50 -transparentInterception ON -
    defaultAuthorizationAction ALLOW -forceCleanup cookie -SSO ON -
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    ssoCredential PRIMARY -icaProxy OFF -wihome "https://storefront.
    ctxdemos.com/Citrix/ExternalWeb" -wiPortalMode COMPACT -
    ClientChoices OFF -ntDomain CTXDEMOS -clientlessVpnMode ON -
    clientlessPersistentCookie ALLOW
add vpn sessionPolicy PL_WB_22.22.44.50 "HTTP.REQ.HEADER("User-Agent").
    CONTAINS("CitrixReceiver").NOT" AC_WB_22.22.44.50

# Create Session Policy and Action for Citrix Gateway Client
add vpn sessionAction UG_VPN_SAct_22.22.44.50 -transparentInterception
    ON -defaultAuthorizationAction ALLOW -SSO ON -ClientChoices ON -
    clientlessVpnMode ON
add vpn sessionPolicy UG_VPN_SPol_22.22.44.50 true UG_VPN_SAct_22
    .22.44.50

# Create Responder Policy and Action for Gateway Logout
add responder action RESACT_GATEWAY_LOGOFF_REDIRECT redirect ""https://
    " + HTTP.REQ.HOSTNAME.HTTP_URL_SAFE" -responseStatusCode 302
add responder policy RESPOL_GATEWAY_LOGOFF_REDIRECT "HTTP.REQ.URL.
    CONTAINS("/cgi/logout")" RESACT_GATEWAY_LOGOFF_REDIRECT

# Create Citrix Gateway vServer
add vpn vserver UGVS_VPN_UGCTXDEMOS SSL 0.0.0.0 -loginOnce ON -
    Listenpolicy NONE -vserverFqdn access.ctxdemos.com
set ssl vserver UGVS_VPN_UGCTXDEMOS -ssl3 DISABLED -tls1 DISABLED -
    tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -
    maxage 157680000 -IncludeSubdomains YES
bind ssl vserver UGVS_VPN_UGCTXDEMOS -certkeyName CTXDEMOS_PUBLIC_CERT
bind ssl vserver UGVS_VPN_UGCTXDEMOS -cipherName
    CTXDEMOS_FRONTEND_APLUS
bind vpn vserver UGVS_VPN_UGCTXDEMOS -portaltheme CTXDEMOS_PORTAL
bind vpn vserver UGVS_VPN_UGCTXDEMOS -staServer "https://wsctxdc01.
    ctxdemos.com"
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy
    RESPOL_GATEWAY_LOGOFF_REDIRECT -priority 100 -gotoPriorityExpression
     END -type REQUEST
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy PL_OS_22.22.44.50 -
    priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy PL_WB_22.22.44.50 -
    priority 110 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy UG_VPN_SPol_22.22.44.50 -
    priority 58000 -gotoPriorityExpression NEXT -type REQUEST

# Create Content Switching Policy and Action for Citrix Gateway
add cs action CSACT_UGCTXDEMOS -targetVserver UGVS_VPN_UGCTXDEMOS
add cs policy CSPOL_UGCTXDEMOS -rule "is_vpn_url  ||  HTTP.REQ.URL.PATH
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    .SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Citrix/External")" -action
    CSACT_UGCTXDEMOS
32
33 # Create Content Switching vServer for Citrix Gateway
34 add cs vserver CSVS_UGCTXDEMOS SSL 22.22.44.50 443 -cltTimeout 180
35 set ssl vserver CSVS_UGCTXDEMOS -ssl3 DISABLED -tls1 DISABLED -tls11
    DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage
    157680000 -IncludeSubdomains YES
36 bind ssl vserver CSVS_UGCTXDEMOS -certkeyName CTXDEMOS_PUBLIC_CERT
37 bind ssl vserver CSVS_UGCTXDEMOS -cipherName CTXDEMOS_FRONTEND_APLUS
38 bind cs vserver CSVS_UGCTXDEMOS -policyName CSPOL_UGCTXDEMOS -priority
    63000
39
40 # Create Responder Policy and Action for HTTP to HTTPS Redirection
41 add responder action RESACT_HTTP_TO_HTTPS redirect ""https://" + HTTP.
    REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY.
    HTTP_URL_SAFE" -responseStatusCode 301
42 add responder policy RESPOL_HTTP_TO_HTTPS HTTP.REQ.IS_VALID
    RESACT_HTTP_TO_HTTPS
43
44 # Create Always On Server and Service
45 add server LBSRV_ALWAYS_UP 127.0.0.1
46 add service LBSVC_ALWAYS_UP LBSRV_ALWAYS_UP HTTP 80 -gslb NONE -
    maxClient 0 -maxReq 0 -cip ENABLED cip-header -usip YES -
    useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
    TCPB NO -CMP NO
47
48 # Create Always On vServer for Citrix Gateway
49 add lb vserver CSVS_UGCTXDEMOS_REDIRECT_HTTP_TO_HTTPS HTTP 22.22.44.50
    80 -persistenceType NONE -cltTimeout 180
50 bind lb vserver CSVS_UGCTXDEMOS_REDIRECT_HTTP_TO_HTTPS LBSVC_ALWAYS_UP
51 bind lb vserver CSVS_UGCTXDEMOS_REDIRECT_HTTP_TO_HTTPS -policyName
    RESPOL_HTTP_TO_HTTPS -priority 100 -gotoPriorityExpression END -type
     REQUEST
52 <!--NeedCopy-->
```

最初の認証サーバーの構成

```
1 # Create Initialization SAML SP Policy and Action and Bind it to Citrix
     ADC AAA Authentication vServer
2 add authentication samlAction AUTH_ACT_SAML_SP_VPN_TO_LB -
    samlIdPCertName CTXDEMOS_PUBLIC_CERT -samlSigningCertName
    CTXDEMOS_PUBLIC_CERT -samlRedirectUrl "https://access.ctxdemos.com/
    samltolb" -signatureAlg RSA-SHA256 -digestMethod SHA256 -samlBinding
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
      REDIRECT -groupNameField Groups
3 add authentication Policy AUTH_POL_SAMP_SP_VPN_TO_LB -rule TRUE -action
      AUTH_ACT_SAML_SP_VPN_TO_LB
4
5 # Create Authentication Policy and Action for SAML SP to ADFS
6 add authentication samlAction AUTH_ACT_SAML_SP_ADFS -samlIdPCertName
    CTXDEMOS_ADFS_TOKEN_SIGNING -samlSigningCertName
    CTXDEMOS_PUBLIC_CERT -samlRedirectUrl "https://sts.ctxdemos.com/adfs
    /ls/" -samlUserField "Name ID" -samlRejectUnsignedAssertion OFF -
    samlIssuerName "https://access.ctxdemos.com" -Attribute1 "E-Mail
    Address" -signatureAlg RSA-SHA256 -digestMethod SHA256 -logoutURL "
    https://sts.ctxdemos.com/adfs/ls/wa=wsignout1.0" -forceAuthn ON
7 add authentication Policy AUTH_POL_SAML_SP_ADFS -rule TRUE -action
    AUTH_ACT_SAML_SP_ADFS
8
9 # Create Authentication Policy Label for for SAML SP to ADFS
10 add authentication policylabel AUTH_POLLBL_ADFS_AZUREMFA -loginSchema
    LSCHEMA_INT
11 bind authentication policylabel AUTH_POLLBL_ADFS_AZUREMFA -policyName
    AUTH_POL_SAML_SP_ADFS -priority 100 -gotoPriorityExpression NEXT
12
13 # Create Authentication Policy and Action for Group Extraction
14 add authentication ldapAction AUTH_ACT_LDAP_GROUP_EXTRACTION_AZUREMFACA
     -serverIP 22.22.22.61 -serverPort 636 -ldapBase "DC=ctxdemos,DC=com
    " -ldapBindDn "CN=svc_ctxadc01,OU=Services,OU=Accounts,DC=ctxdemos,
    DC=com" -ldapBindDnPassword 0
    c4fe86d56a865ef514a15affd1429f3e079ce1089731d4a407772d21036f3c8 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    searchFilter "memberOf:1.2.840.113556.1.4.1941:=CN=AzureMFACAUsers,
    OU=Groups,OU=Authorizations,DC=ctxdemos,DC=com" -groupAttrName
    memberOf -subAttributeName cn -secType SSL -authentication DISABLED
    -nestedGroupExtraction ON -maxNestingLevel 5 -groupNameIdentifier
    sAMAccountName -groupSearchAttribute memberOf -
    groupSearchSubAttribute CN -Attribute1 mail -Attribute2 objectGUID
15 add authentication Policy AUTH_POL_LDAP_GROUP_EXTRACTION_AZURAMFACA -
    rule TRUE -action AUTH_ACT_LDAP_GROUP_EXTRACTION_AZUREMFACA
16
17 # Create Authentication Policy Label for Group Extraction
18 add authentication policylabel
    AUTH_POLLBL_LDAP_GROUP_EXTRACTION_AZURAMFACA -loginSchema
    LSCHEMA_INT
19 bind authentication policylabel
    AUTH_POLLBL_LDAP_GROUP_EXTRACTION_AZURAMFACA -policyName
    AUTH_POL_LDAP_GROUP_EXTRACTION_AZURAMFACA -priority 100 -
    gotoPriorityExpression NEXT -nextFactor AUTH_POLLBL_ADFS_AZUREMFA
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
20
21
22 # Create Login Schema Policy and Profile for First Citrix ADC AAA
       Authentication vServer
23 add authentication loginSchema LSCHEMA_PRF_NOSCHEMA -
       authenticationSchema noschema -SSOCredentials YES
24 add authentication loginSchemaPolicy LSCHEMA_POL_NOSCHEMA -rule TRUE -
       action LSCHEMA_PRF_NOSCHEMA
25
26 # Create First Citrix ADC AAA Authentication vServer
27 add authentication vserver AAAVS_CTXDEMOS_COM_FOR_VPN SSL 0.0.0.0
28 set ssl vserver AAAVS_CTXDEMOS_COM_FOR_VPN -ssl3 DISABLED -tls1
       DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS
       ENABLED -maxage 157680000 -IncludeSubdomains YES
29 bind ssl vserver AAAVS_CTXDEMOS_COM_FOR_VPN -certkeyName
       CTXDEMOS_PUBLIC_CERT
30 bind ssl vserver AAAVS_CTXDEMOS_COM_FOR_VPN -cipherName
       CTXDEMOS_FRONTEND_APLUS
31 bind authentication vserver AAAVS_CTXDEMOS_COM_FOR_VPN -policy
       LSCHEMA_POL_NOSCHEMA -priority 100 -gotoPriorityExpression END
32 bind authentication vserver AAAVS_CTXDEMOS_COM_FOR_VPN -policy
       AUTH_POL_SAMP_SP_VPN_TO_LB -priority 100 -nextFactor
       AUTH_POLLBL_LDAP_GROUP_EXTRACTION_AZURAMFACA -gotoPriorityExpression
        NEXT
33
34 # Create First Citrix ADC AAA Authentication Profile
35 add authentication authnProfile AAA_AUTH_PRF_VPN -authnVsName
       AAAVS_CTXDEMOS_COM_FOR_VPN -AuthenticationHost aaa.ctxdemos.com
36
37 # Set Authentication Profile on Gateway vServer
38 set vpn vserver UGVS_VPN_UGCTXDEMOS -authnProfile AAA_AUTH_PRF_VPN
39 <!--NeedCopy-->
```

2 番目の認証サーバーの構成

```
1 # Create Authentication Policy and Action for LDAP
2 add authentication ldapAction AUTH_ACT_LDAP -serverIP 22.22.22.61 -
      serverPort 636 -authTimeout 60 -ldapBase "DC=ctxdemos,DC=com" -
      ldapBindDn "CN=svc_ctxadc01,OU=Services,OU=Accounts,DC=ctxdemos,DC=
      com" -ldapBindDnPassword 273881819
      af883e70c33d83c0546eac84e81d6eeba904f2d65bbebf2819c025a -encrypted -
      encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
       memberOf -subAttributeName cn -secType SSL -passwdChange ENABLED -
      nestedGroupExtraction ON -maxNestingLevel 5 -groupNameIdentifier
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    sAMAccountName -groupSearchAttribute memberOf -
    groupSearchSubAttribute CN -Attribute1 userprincipalname -Attribute2
     mail -Attribute3 userParameters
add authentication Policy AUTH_POL_LDAP_USER_NAME_PASSWORD -rule TRUE -
    action AUTH_ACT_LDAP

# Create Login Schema Policy and Profile for Second Citrix ADC AAA
    Authentication vServer - Username (Pre-filled ) and Password
add authentication loginSchema LSCHEMA_USER_NAME_PASSWORD -
    authenticationSchema "/nsconfig/loginschema/CTXDEMOS_USER_NAME_PASS.
    xml" -SSOCredentials YES
add authentication loginSchemaPolicy LSCHEMA_POL_USER_NAME_PASSWORD -
    rule TRUE -action LSCHEMA_USER_NAME_PASSWORD

# Create Authentication Policy Label for LDAP Username and Password
add authentication policylabel AUTH_POLLBL_LDAP_USER_NAME_PASSWORD -
    loginSchema LSCHEMA_USER_NAME_PASSWORD
bind authentication policylabel AUTH_POLLBL_LDAP_USER_NAME_PASSWORD -
    policyName AUTH_POL_LDAP_USER_NAME_PASSWORD -priority 110 -
    gotoPriorityExpression NEXT

# Create Login Schema Policy and Profile for Second Citrix ADC AAA
    Authentication vServer - Username Only
add authentication loginSchema LSCHEMA_USER_NAME_ONLY -
    authenticationSchema "/nsconfig/loginschema/CTXDEMOS_USER_NAME_ONLY.
    xml"
add authentication loginSchemaPolicy LSCHEMA_POL_NOPASSWORD -rule TRUE
    -action LSCHEMA_USER_NAME_ONLY

# Create Citrix ADC AAA Session Policy and Profile
add tm sessionAction AAA_SESSION_PRF_CTXDEMOS -SSO ON -ssoDomain
    CTXDEMOS -persistentCookie ON -persistentCookieValidity 30
add tm sessionPolicy AAA_SESSION_POL_CTXDEMOS TRUE
    AAA_SESSION_PRF_CTXDEMOS

# Create Second Citrix ADC AAA Authentication vServer
add authentication vserver AAAVS_CTXDEMOS_COM SSL 22.22.44.51 443
set ssl vserver AAAVS_CTXDEMOS_COM -ssl3 DISABLED -tls1 DISABLED -tls11
     DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage
     157680000 -IncludeSubdomains YES
bind ssl vserver AAAVS_CTXDEMOS_COM -certkeyName CTXDEMOS_PUBLIC_CERT
bind ssl vserver AAAVS_CTXDEMOS_COM -cipherName CTXDEMOS_FRONTEND_APLUS
bind authentication vserver AAAVS_CTXDEMOS_COM -portaltheme
    CTXDEMOS_PORTAL
bind authentication vserver AAAVS_CTXDEMOS_COM -policy
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    AAA_SESSION_POL_CTXDEMOS -priority 100 -gotoPriorityExpression NEXT
28 bind authentication vserver AAAVS_CTXDEMOS_COM -policy
    LSCHEMA_POL_NOPASSWORD -priority 110 -gotoPriorityExpression END
29 bind authentication vserver AAAVS_CTXDEMOS_COM -policy
    AUTH_POL_LDAP_GROUP_EXTRACTION_AZURAMFACA -priority 140 -nextFactor
    AUTH_POLLBL_LDAP_USER_NAME_PASSWORD -gotoPriorityExpression NEXT
30
31 # Create Second Citrix ADC AAA Authentication Profile
32 add authentication authnProfile AAA_AUTH_PRF -authnVsName
    AAAVS_CTXDEMOS_COM -AuthenticationHost aaa.ctxdemos.com
33 <!--NeedCopy-->
```

Citrix ADC の AD FS WAP としての構成

Citrix ADC CLI で次のコマンドを実行して、Citrix ADC を AD FS Web アプリケーションプロキシ（WAP）として構成します。

```
1  # Pattern Set - ADFS Proxy Hostname
2  add policy patset PATSET_ADFS_HOSTNAME
3  bind policy patset PATSET_ADFS_HOSTNAME sts.ctxdemos.com -index 1 -
    charset ASCII
4  # Policy Expression - ADFS Proxy Hostname
5  add policy expression is_ADFS_HOSTNAME "HTTP.REQ.HEADER("Host").
    TO_LOWER.CONTAINS_ANY("PATSET_ADFS_HOSTNAME")"
6
7  # Pattern Set - ADFS Proxy Path for NoAuth
8  add policy patset PATSET_ADFS_PATH_NOAUTH
9  bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/services/trust" -
    index 1 -charset ASCII
10 bind policy patset PATSET_ADFS_PATH_NOAUTH "/federationmetadata
    /2007-06/federationmetadata.xml" -index 2 -charset ASCII
11 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/fs/
    federationserverservice.asmx" -index 3 -charset ASCII
12 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/ls/FormsSignIn.aspx"
    -index 4 -charset ASCII
13 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/services/trust/2005/
    usernamemixed" -index 5 -charset ASCII
14 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/services/trust/mex" -
    index 6 -charset ASCII
15
16 # Policy Expression - ADFS Proxy Path for NoAuth
17 add policy expression is_ADFS_PROXY_NOAUTH "HTTP.REQ.URL.PATH.TO_LOWER.
    CONTAINS_ANY("PATSET_ADFS_PATH_NOAUTH")"
18
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
# Pattern Set - ADFS Proxy Path for Passive Client
add policy patset PATSET_ADFS_PATH_ACTIVE_PASSIVE
bind policy patset PATSET_ADFS_PATH_ACTIVE_PASSIVE "/adfs" -index 1 -
    charset ASCII
bind policy patset PATSET_ADFS_PATH_ACTIVE_PASSIVE "/cgi/selfauth" -
    index 2 -charset ASCII

# Policy Expression - ADFS Proxy Path for Passive Client
add policy expression is_ADFS_PROXY_ACTIVE_PASSIVE "(HTTP.REQ.HEADER("
    Host").TO_LOWER.CONTAINS_ANY("PATSET_ADFS_HOSTNAME") && HTTP.REQ.URL
    .PATH.TO_LOWER.STARTSWITH_ANY("PATSET_ADFS_PATH_ACTIVE_PASSIVE"))"

# Rewrite Policies for ADFS PIP
add rewrite action RWACT_X_MS_Proxy insert_http_header X-MS-Proxy ""
    NETSCALER""
add rewrite policy RWPOL_X_MS_Proxy true RWACT_X_MS_Proxy

add rewrite action RWACT_X_MS_Forwarded_Client_IP insert_http_header X-
    MS-Forwarded-Client-IP CLIENT.IP.SRC
add rewrite policy RWPOL_X_MS_Forwarded_Client_IP true
    RWACT_X_MS_Forwarded_Client_IP

add rewrite action RWACT_X_MS_Endpoint_Absolute_Path insert_http_header
     X-MS-Endpoint-Absolute-Path HTTP.REQ.URL
add rewrite policy RWPOL_X_MS_Endpoint_Absolute_Path true
    RWACT_X_MS_Endpoint_Absolute_Path

add rewrite action RWACT_X_MS_Target_Role insert_http_header X-MS-
    Target-Role ""PrimaryComputer""
add rewrite policy RWPOL_X_MS_Target_Role true RWACT_X_MS_Target_Role

add rewrite action RWACT_X_MS_ADFS_Proxy_Client_IP insert_http_header X
    -MS-ADFS-Proxy-Client-IP CLIENT.IP.SRC
add rewrite policy RWPOL_X_MS_ADFS_Proxy_Client_IP true
    RWACT_X_MS_ADFS_Proxy_Client_IP

add rewrite action RWACT_X_MS_Client_User_Agent insert_http_header X-MS
    -Client-User-Agent "HTTP.REQ.HEADER("User-Agent")"
add rewrite policy RWPOL_X_MS_Client_User_Agent true
    RWACT_X_MS_Client_User_Agent

add rewrite action RWACT_ADFS_PROXYMEX replace HTTP.REQ.URL.
    PATH_AND_QUERY ""/adfs/services/trust/proxymex" + HTTP.REQ.URL.
    SET_TEXT_MODE(IGNORECASE).PATH_AND_QUERY.STRIP_START_CHARS("/adfs/
    services/trust/mex").HTTP_URL_SAFE"
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
add rewrite policy RWPOL_ADFS_PROXYMEX "is_ADFS_HOSTNAME && HTTP.REQ.URL.TO_LOWER.STARTSWITH("/adfs/services/trust/mex")" RWACT_ADFS_PROXYMEX

add rewrite policy RWPOL_ADFS_PROXY_HEADERS-NOACT TRUE NOREWRITE

add rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS http_req
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_Proxy 100 NEXT
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_Forwarded_Client_IP 110 NEXT
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_Endpoint_Absolute_Path 120 NEXT
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_Target_Role 130 NEXT
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_ADFS_Proxy_Client_IP 140 NEXT
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_Client_User_Agent 150 NEXT
bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_ADFS_PROXYMEX 160 NEXT

# Create ADFS Server and Service Group
add server LBSRV_ADFS wsadfs01.ctxdemos.com
add serviceGroup LBSVCGRP_ADFS_443 SSL -maxClient 0 -maxReq 0 -cip ENABLED X-MS-Forwarded-Client-IP -usip NO -useproxyport YES -sp ON -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
bind ssl serviceGroup LBSVCGRP_ADFS_443 -cipherName CTXDEMO_BACKEND
set ssl serviceGroup LBSVCGRP_ADFS_443 -ssl3 DISABLED -tls1 DISABLED -tls11 DISABLED
bind serviceGroup LBSVCGRP_ADFS_443 LBSRV_ADFS 443

# Create ADFS Proxy NoAuth Load Balancing vServer
add lb vserver LBVS_ADFS_PROXY_NOAUTH SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
set ssl vserver LBVS_ADFS_PROXY_NOAUTH -ssl3 DISABLED -tls1 DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage 157680000 -IncludeSubdomains YES
bind ssl vserver LBVS_ADFS_PROXY_NOAUTH -certkeyName CTXDEMOS-PUBLIC
bind ssl vserver LBVS_ADFS_PROXY_NOAUTH -cipherName CTXDEMO_BACKEND
bind lb vserver LBVS_ADFS_PROXY_NOAUTH LBSVCGRP_ADFS_443
bind lb vserver LBVS_ADFS_PROXY_NOAUTH -policyName RWPOL_ADFS_PROXY_HEADERS-NOACT -priority 100 -gotoPriorityExpression NEXT -type REQUEST -invoke policylabel RWPOLLBL_ADFS_PROXY_HEADERS

```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
# Create ADFS Proxy NoAuth Content Switching Policy and Action
add cs action CSACT_ADFS_PROXY_NOAUTH -targetLBVserver
    LBVS_ADFS_PROXY_NOAUTH
add cs policy CSPOL_ADFS_PROXY_NOAUTH -rule is_ADFS_PROXY_NOAUTH -
    action CSACT_ADFS_PROXY_NOAUTH

# Create ADFS Proxy Active-Passive Load Balancing vServer
add lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE SSL 0.0.0.0 0 -
    persistenceType NONE -cltTimeout 180 -Authentication ON -
    authnProfile AAA_AUTH_PRF
set ssl vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -ssl3 DISABLED -tls1
    DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS
    ENABLED -maxage 157680000 -IncludeSubdomains YES
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE LBSVCGRP_ADFS_443
bind ssl vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -certkeyName CTXDEMOS-
    PUBLIC
bind ssl vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -cipherName
    CTXDEMO_FRONTEND_APLUS
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -policyName
    RWPOL_ADFS_PROXY_HEADERS-NOACT -priority 100 -gotoPriorityExpression
     NEXT -type REQUEST -invoke policylabel RWPOLLBL_ADFS_PROXY_HEADERS

# Create ADFS Proxy Active-Passive Content Switching Policy and Action
add cs action CSACT_ADFS_PROXY_ACTIVE_PASSIVE -targetLBVserver
    LBVS_ADFS_PROXY_ACTIVE_PASSIVE
add cs policy CSPOL_ADFS_PROXY_ACTIVE_PASSIVE -rule
    is_ADFS_PROXY_ACTIVE_PASSIVE -action CSACT_ADFS_PROXY_ACTIVE_PASSIVE

# Bind Content Switching Policies to Citrix Gateway Content Switching
    vServer
bind cs vserver CSVS_UGCTXDEMOS -policyName CSPOL_ADFS_PROXY_NOAUTH -
    priority 100
bind cs vserver CSVS_UGCTXDEMOS -policyName
    CSPOL_ADFS_PROXY_ACTIVE_PASSIVE -priority 300

# Create Citrix ADC AAA Traffic Policies and Bind them to ADFS Proxy
    Active-Passive Load Balancing vServer
add tm formSSOAction AAATM_SSOPRF_ADFS_LOGIN -actionURL "/adfs/ls" -
    userField UserName -passwdField Password -ssoSuccessRule true -
    nameValuePair AuthMethod=FormsAuthentication -responsesize 15000 -
    submitMethod POST
add tm trafficAction AAATM_PRF_ADFS_LOGIN -appTimeout 1 -SSO ON -
    formSSOAction AAATM_SSOPRF_ADFS_LOGIN -persistentCookie OFF -
    InitiateLogout OFF -kcdAccount NONE -userExpression "HTTP.REQ.USER.
    ATTRIBUTE(3)" -passwdExpression "HTTP.REQ.USER.ATTRIBUTE(2)"
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
add tm trafficPolicy AAATM_POL_ADFS_LOGIN "HTTP.REQ.URL.TO_LOWER.STARTSWITH("/adfs/ls")" AAATM_PRF_ADFS_LOGIN
add tm trafficAction AAATM_PRF_ADFS_LOGOUT -appTimeout 1 -persistentCookie OFF -InitiateLogout ON -kcdAccount NONE
add tm trafficPolicy AAATM_POL_ADFS_LOGOUT "HTTP.REQ.URL.TO_LOWER.STARTSWITH("/adfs/ls") && HTTP.REQ.URL.QUERY.VALUE("wa").EQ("wsignout1.0")" AAATM_PRF_ADFS_LOGOUT
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -policyName AAATM_POL_ADFS_LOGIN -priority 100 -gotoPriorityExpression END -type REQUEST
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -policyName AAATM_POL_ADFS_LOGOUT -priority 110 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

初期認証フローの設定

```
# Pattern Set - Gateway and AAA Hostname
add policy patset PATSET_GATEWAY_HOSTHEADER
bind policy patset PATSET_GATEWAY_HOSTHEADER access.ctxdemos.com -index 1 -charset ASCII
bind policy patset PATSET_GATEWAY_HOSTHEADER aaa.ctxdemos.com -index 2 -charset ASCII
# Policy Expression - Gateway and AAA Hostname
add policy expression is_GATEWAY_HOSTNAME "HTTP.REQ.HEADER("Host").TO_LOWER.CONTAINS_ANY("PATSET_GATEWAY_HOSTHEADER")"

# Create Initialization Load Balancing vServer
add lb vserver LBVS_SAML_SP_INITIALIZATION SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180 -Authentication ON -authnProfile AAA_AUTH_PRF
set ssl vserver LBVS_SAML_SP_INITIALIZATION -ssl3 DISABLED -tls1 DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage 157680000 -IncludeSubdomains YES
bind lb vserver LBVS_SAML_SP_INITIALIZATION LBSVC_ALWAYS_UP
bind ssl vserver LBVS_SAML_SP_INITIALIZATION -certkeyName CTXDEMOS_PUBLIC_CERT
bind ssl vserver LBVS_SAML_SP_INITIALIZATION -cipherName CTXDEMOS_FRONTEND_APLUS

# Create Initialization Content Switching Policy and Action
add cs action CSACT_SAML_SP_INITIALIZATION -targetLBVserver LBVS_SAML_SP_INITIALIZATION
add cs policy CSPOL_SAML_SP_INITIALIZATION -rule "is_GATEWAY_HOSTNAME
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
    && HTTP.REQ.URL.PATH.TO_LOWER.STARTSWITH("/samltolb")" -action
    CSACT_SAML_SP_INITIALIZATION
18
19 # Bind Content Switching Policies to Citrix Gateway Content Switching
    vServer
20 bind cs vserver CSVS_UGCTXDEMOS -policyName
    CSPOL_SAML_SP_INITIALIZATION -priority 500
21
22 # Create Initialization Citrix ADC AAA Traffic Policy and Action and
    Bind it to Load Balancing vServer
23 add tm samlSSOProfile AAATM_SAMLSSOPRF_VPN_TO_LB -samlSigningCertName
    CTXDEMOS_PUBLIC_CERT -assertionConsumerServiceURL "https://access.
    ctxdemos.com/cgi/samlauth" -relaystateRule "HTTP.REQ.URL.QUERY.VALUE
    ("RelayState")" -signatureAlg RSA-SHA256 -digestMethod SHA256 -
    Attribute1 Password -Attribute1Expr AAA.USER.PASSWD -Attribute2
    Groups -Attribute2Expr AAA.USER.GROUPS -encryptAssertion ON -
    samlSPCertName CTXDEMOS_PUBLIC_CERT
24 add tm trafficAction AAATM_PRF_VPN_TO_LB -SSO ON -persistentCookie OFF
    -InitiateLogout OFF -kcdAccount NONE -samlSSOProfile
    AAATM_SAMLSSOPRF_VPN_TO_LB
25 add tm trafficPolicy AAATM_POL_VPN_TO_LB "HTTP.REQ.URL.STARTSWITH("/
    samltolb")" AAATM_PRF_VPN_TO_LB
26 bind lb vserver LBVS_SAML_SP_INITIALIZATION -policyName
    AAATM_POL_VPN_TO_LB -priority 100 -gotoPriorityExpression END -type
    REQUEST
27 <!--NeedCopy-->
```

暗号グループ

```
1 # Create Cipher Group for Backend vServers
2 add ssl cipher CTXDEMOS_BACKEND
3 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.3-AES256-GCM-SHA384 -
    cipherPriority 1
4 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.3-CHACHA20-POLY1305-
    SHA256 -cipherPriority 2
5 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.3-AES128-GCM-SHA256 -
    cipherPriority 3
6 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-RSA-AES256-
    GCM-SHA384 -cipherPriority 4
7 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-RSA-AES128-
    GCM-SHA256 -cipherPriority 5
8 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-ECDSA-AES256-
    GCM-SHA384 -cipherPriority 6
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 7

# Create Cipher Group for Frondend vServers
add ssl cipher CTXDEMOS_FRONTEND
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.3-AES256-GCM-SHA384 -cipherPriority 1
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.3-CHACHA20-POLY1305-SHA256 -cipherPriority 2
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.3-AES128-GCM-SHA256 -cipherPriority 3
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 4
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384 -cipherPriority 5
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES128-SHA256 -cipherPriority 6
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES256-SHA384 -cipherPriority 7
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-ECDSA-AES128-SHA -cipherPriority 8
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-ECDSA-AES256-SHA -cipherPriority 9
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 10
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 11
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256 -cipherPriority 12
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384 -cipherPriority 13
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-RSA-AES128-SHA -cipherPriority 15
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-RSA-AES256-SHA -cipherPriority 16
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256 -cipherPriority 17
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384 -cipherPriority 18
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-DHE-RSA-AES-128-CBC-SHA -cipherPriority 19
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-DHE-RSA-AES-256-CBC-SHA -cipherPriority 20

# Create Cipher Group for Frondend vServers - A+
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
add ssl cipher CTXDEMOS_FRONTEND_APLUS
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.3-AES256-GCM-SHA384 -cipherPriority 1
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.3-CHACHA20-POLY1305-SHA256 -cipherPriority 2
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.3-AES128-GCM-SHA256 -cipherPriority 3
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384 -cipherPriority 4
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 5
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305 -cipherPriority 6
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES256-SHA384 -cipherPriority 7
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES128-SHA256 -cipherPriority 8
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 9
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 13
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 -cipherPriority 14
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384 -cipherPriority 15
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256 -cipherPriority 16
<!--NeedCopy-->
```

ログインスキーマ **XML** ファイル

CTXDEMOS_USER_NAME_PASS.XML

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
    <Status>success</Status>
    <Result>more-info</Result>
    <StateContext/>
    <AuthenticationRequirements>
        <PostBack>/nf/auth/doAuthentication.do</PostBack>
        <CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate</CancelPostBack>
        <CancelButtonText>Cancel</CancelButtonText>
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
10          <Requirements>
11              <Requirement>
12                  <Credential>
13                      <ID>login</ID>
14                      <SaveID>ExplicitForms-Username</SaveID>
15                      <Type>username</Type>
16                  </Credential>
17                  <Label>
18                      <Text>User name</Text>
19                      <Type>plain</Type>
20                  </Label>
21                  <Input>
22                      <AssistiveText>Please supply username</
                            AssistiveText>
23                      <Text>
24                          <Secret>false</Secret>
25                          <ReadOnly>false</ReadOnly>
26                          <InitialValue>${
27  AAA.USER.NAME }
28  </InitialValue>
29                          <Constraint>.+</Constraint>
30                      </Text>
31                  </Input>
32              </Requirement>
33              <Requirement>
34                  <Credential>
35                      <ID>passwd</ID>
36                      <SaveID>ExplicitForms-Password</SaveID>
37                      <Type>password</Type>
38                  </Credential>
39                  <Label>
40                      <Text>Password:</Text>
41                      <Type>plain</Type>
42                  </Label>
43                  <Input>
44                      <Text>
45                          <Secret>true</Secret>
46                          <ReadOnly>false</ReadOnly>
47                          <InitialValue/>
48                          <Constraint>.+</Constraint>
49                      </Text>
50                  </Input>
51              </Requirement>
52              <Requirement>
53                  <Credential>
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
                    <ID>saveCredentials</ID>
                    <Type>savecredentials</Type>
                </Credential>
                <Label>
                    <Text>Remember my password</Text>
                    <Type>plain</Type>
                </Label>
                <Input>
                    <CheckBox>
                        <InitialValue>false</InitialValue>
                    </CheckBox>
                </Input>
            </Requirement>
            <Requirement>
                <Credential>
                    <ID>loginBtn</ID>
                    <Type>none</Type>
                </Credential>
                <Label>
                    <Type>none</Type>
                </Label>
                <Input>
                    <Button>Log On</Button>
                </Input>
            </Requirement>
        </Requirements>
    </AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

CTXDEMOS_USER_NAME_ONLY.XML

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
    <Status>success</Status>
    <Result>more-info</Result>
    <StateContext/>
    <AuthenticationRequirements>
        <PostBack>/nf/auth/doAuthentication.do</PostBack>
        <CancelPostBack>/Citrix/Authentication/ExplicitForms/
           CancelAuthenticate</CancelPostBack>
        <CancelButtonText>Cancel</CancelButtonText>
        <Requirements>
            <Requirement>
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
12                  <Credential>
13                      <ID>login</ID>
14                      <SaveID>ExplicitForms-Username</SaveID>
15                      <Type>username</Type>
16                  </Credential>
17                  <Label>
18                      <Text>User name</Text>
19                      <Type>plain</Type>
20                  </Label>
21                  <Input>
22                      <AssistiveText>Please supply username</
                           AssistiveText>
23                      <Text>
24                          <Secret>false</Secret>
25                          <ReadOnly>false</ReadOnly>
26                          <InitialValue/>
27                          <Constraint>.+</Constraint>
28                      </Text>
29                  </Input>
30              </Requirement>
31              <Requirement>
32                  <Credential>
33                      <Type>none</Type>
34                  </Credential>
35                  <Label>
36                      <Text> Please submit credentials to continue Login
                           ...</Text>
37                      <Type>confirmation</Type>
38                  </Label>
39                  <Input/>
40              </Requirement>
41              <Requirement>
42                  <Credential>
43                      <ID>saveCredentials</ID>
44                      <Type>savecredentials</Type>
45                  </Credential>
46                  <Label>
47                      <Text>Remember my password</Text>
48                      <Type>plain</Type>
49                  </Label>
50                  <Input>
51                      <CheckBox>
52                          <InitialValue>false</InitialValue>
53                      </CheckBox>
54                  </Input>
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
            </Requirement>
            <Requirement>
                <Credential>
                    <ID>loginBtn</ID>
                    <Type>none</Type>
                </Credential>
                <Label>
                    <Type>none</Type>
                </Label>
                <Input>
                    <Button>Log On</Button>
                </Input>
            </Requirement>
        </Requirements>
    </AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

参照ドキュメント

Authentication to NetScaler using AD FS 4.0 on Server 2016, Citrix FAS, and Azure MFA in Azure Cloud. (2018). Retrieved from https://www.jgspiers.com/authentication-to-netscaler-using-ad-fs-4-0-server-2016-citrix-fas-azure-mfa-azure-cloud/

Configure Azure MFA as authentication provider with AD FS. (2019). Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa

Deploying a Federation Server Farm. (2017). Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/deploying-a-federation-server-farm

Federated Authentication Service ADFS deployment. (2018). Retrieved from https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/secure/federated-authentication-service/fas-architectures/fas-adfs.html

Guide to deploying NetScaler as an Active Directory Federation Services Proxy. (n.d.). Retrieved from https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/guide-to-deploying-netscaler-as-an-active-directory-federation-services-proxy.pdf

How it works: Azure Multi-Factor Authentication. (2018). Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Planning a cloud-based Azure Multi-Factor Authentication deployment. (2019). Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

Tijl Van den Broeck. (Dec 7, 2017). ADFS v3 on Windows Server 2012 R2 with NetScaler. Retrieved from https://www.citrix.com/blogs/2015/05/29/adfs-v3-on-windows-server-2012-r2-with-netscaler/

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Transition to hybrid cloud and SaaS with Citrix Gateway. (n.d.). Retrieved from https://www.citrix.com/products/citrix-gateway/resources/netscaler-unified-gateway.html

User sign-in with Azure Active Directory Pass-through Authentication. (2018). Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Written by Saman Salehian, Lead Networking Sales Engineer.

データベースの無停止アップグレードのためのローカルホストキャッシュの使用

May 18, 2020

ローカルホストキャッシュ（LHC）機能を使用すると、停止状態が発生しても、XenApp または XenDesktop サイトの接続仲介操作を続行できます。以下の手順では、セカンダリゾーンがない場合に、LHC を使用してサイトの無停止アップグレードを実行する方法を示します。Citrix はこのガイドを拡張して、複数のゾーンを持つ環境のための手順を含めることを検討しているため、今後のアップデートを確認してください。

続行する前に、ローカルホストキャッシュ機能、その要件、および制限を確認することをお勧めします。https://docs.citrix.com/ja-jp/xenapp-and-xendesktop/7-15-ltsr/manage-deployment/local-host-cache.html

ローカルホストキャッシュのサイズ設定とスケーリングに関する高度なコンセプトガイドもここにあります。https://docs.citrix.com/ja-jp/advanced-concepts/implementation-guides/local-host-cache-sizing-scaling.html

免責事項**:** これらの手順は、実稼働環境に実装する前にテスト環境で実行し、そのプロセスに精通していることを確認し、発生する可能性のある環境固有の問題や疑問に備えます。また、LHC に関連するいくつかの修正があるので利用可能な最新の LTSR 累積的な更新 (CU) を使用することをお勧めします。

概要

1. この手順の環境を設定します。
2. 選出されたプライマリブローカーを決定します。
3. 強制的に停止し、ローカルホストキャッシュ機能をトリガーします。
4. VDA が選出されたセカンダリブローカーに再登録できるようにします。
5. 選択されていないセカンダリブローカで製品のアップグレードを実行します。
6. データベースのアップグレードを含む、必須のサイトアップグレードを実行します。
7. 選択されていない残りのセカンダリブローカーで製品のアップグレードを実行します。
8. 停止とローカルホストキャッシュモードを終了します。
9. 新しくアップグレードした Delivery Controller への VDA の再登録を許可します。
10. 最後に残った Delivery Controller（以前に選択されたセカンダリブローカー）で製品のアップグレードを実行します。
11. 環境をデフォルト設定に戻します。

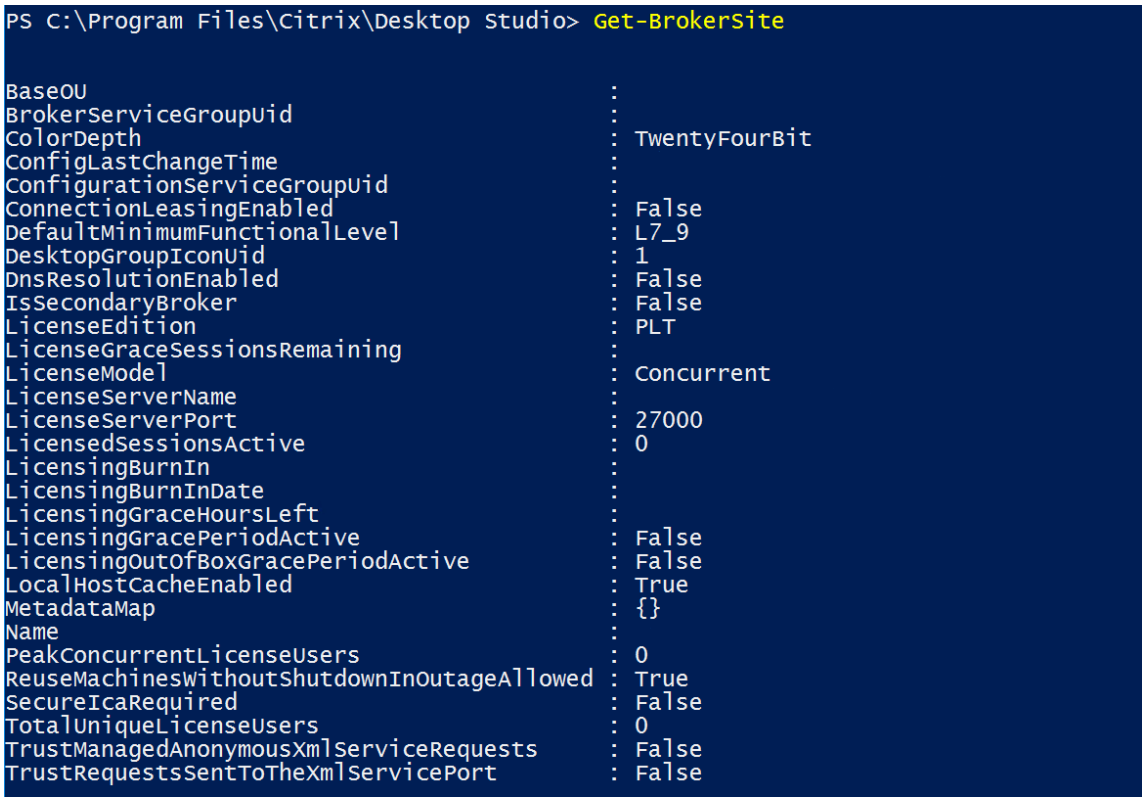
© 1999–2021 Citrix Systems, Inc. All rights reserved.

手順

1. 次の PowerShell コマンドレットを使用して、ローカルホストキャッシュが有効になっているかどうかを確認します。

   ```
   Get-BrokerSite
   ```

   ```
   LocalHostCacheEnabled : Trueを探します
   ```



```
PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSite


BaseOU                                       :
BrokerServiceGroupUid                        :
ColorDepth                                   : TwentyFourBit
ConfigLastChangeTime                         :
ConfigurationServiceGroupUid                 :
ConnectionLeasingEnabled                     : False
DefaultMinimumFunctionalLevel                : L7_9
DesktopGroupIconUid                          : 1
DnsResolutionEnabled                         : False
IsSecondaryBroker                            : False
LicenseEdition                               : PLT
LicenseGraceSessionsRemaining                :
LicenseModel                                 : Concurrent
LicenseServerName                            :
LicenseServerPort                            : 27000
LicensedSessionsActive                       : 0
LicensingBurnIn                              :
LicensingBurnInDate                          :
LicensingGraceHoursLeft                      :
LicensingGracePeriodActive                   : False
LicensingOutOfBoxGracePeriodActive           : False
LocalHostCacheEnabled                        : True
MetadataMap                                  : {}
Name                                         :
PeakConcurrentLicenseUsers                   : 0
ReuseMachinesWithoutShutdownInOutageAllowed  : True
SecureIcaRequired                            : False
TotalUniqueLicenseUsers                      : 0
TrustManagedAnonymousXmlServiceRequests      : False
TrustRequestsSentToTheXmlServicePort         : False
```

   false の場合は、ローカルホストキャッシュを有効にします。

   ```
   Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled
   $false
   ```

   このコマンドレットは、接続リース機能も無効化します。ローカルホストキャッシュと接続リースの両方を有効化しないでください。

2. デフォルトでは、停止状態が発生した場合、「ShutdownDesktopsAfterUse」プロパティが有効になっているデリバリーグループにプールされた、電源管理されたデスクトップ VDA は保守モードになります。デフォルトの動作を上書きするには、サイト全体で、影響を受けるデリバリーグループごとに、これを有効にする必要があります。次の PowerShell コマンドレットを実行します。

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

   ```
   Set-BrokerDesktopGroup -Name "<Delivery Group Name>"- ReuseMachinesWithoutShutdow
    $true
   ```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

3. ブローカサービスがカスタム VDA、StoreFront または StoreFront TLS ポートを使用するように構成されている場合は、次の手順を実行して、高可用性（HA）サービスが正しいカスタムポートで構成されていることを確認します。

   - 次のコマンドを実行して、各ブローカーの現在のブローカーサービスポート設定を確認します: `%programfiles%\Citrix\Broker\Service\BrokerService.exe -show`

     ```
     C:\Program Files\Citrix\Broker\Service>BrokerService.exe -show
     SDK Port: 80
     VDA Port: 80
     StoreFront Port: 80
     StoreFront TLS Port: 443
     Log File:
     ```

   - 次のコマンドを実行して、各ブローカーの現在の HA サービスポート設定を確認します: `%programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -show`

     ```
     C:\Program Files\Citrix\Broker\Service>HighAvailabilityService.exe -show
     SDK Port: 89
     VDA Port: 80
     StoreFront Port: 80
     StoreFront TLS Port: 443
     Log File:
     ```

   - HA サービス用にリストされている VDA、StoreFront、または StoreFront TLS ポートがブローカーサービスと一致しない場合は、以下に示す適切なコマンドラインスイッチを使用して、それに応じて HA サービスのポート設定を設定します。

```
1 %programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -
     VdaPort <port>
2 %programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -
     StoreFrontPort <port>
3 %programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -
     StoreFrontTlsPort <port>
4 <!--NeedCopy-->
```

```
C:\Program Files\Citrix\Broker\Service>HighAvailabilityService.exe -VdaPort 80
Stopping service: CitrixHighAvailabilityService
Starting service: CitrixHighAvailabilityService
Command completed successfully
```

> 注:
> ブローカーサービスと HA サービスでは、SDK ポートが異なることが予想されます。
>
> ブローカーサービスの StoreFront ポートを変更すると、HA サービスの StoreFront ポートが自動的

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> に一致するように更新されます。ただし、新しいポートの使用を開始するには、自動更新を受信するサービスを手動で再起動する必要があります。

4. 停止中は、選択されたセカンダリブローカーがすべての接続を処理します。停止状態の開始時に、セカンダリブローカーにはその時点の VDA 登録データがありませんが、VDA との通信が始まるとすぐに再登録処理がトリガーされます。その処理中、セカンダリブローカーは、その VDA に関する現在のセッション情報も取得します。VDA の再登録をデフォルトの 5 分間隔から 1 分間隔に高速化するには、サイト内のすべての Controller にこの設定を適用する必要があります。

   ```
   New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
   HeartbeatPeriodMs -PropertyType DWORD -Value 60000
   ```

5. VDA の再登録を監視するには、Citrix Studio を起動し、「構成」>「コントローラー」ノードをクリックし、プライマリブローカに登録されている VDA の数を表示します。Citrix Studio を開いたままにして、停止中に VDA が選出されたセカンダリブローカーに再登録されると、カウントがゼロになるようにします。Citrix Studio を使用して、セカンダリブローカに登録されている VDA の数を表示することはできません。

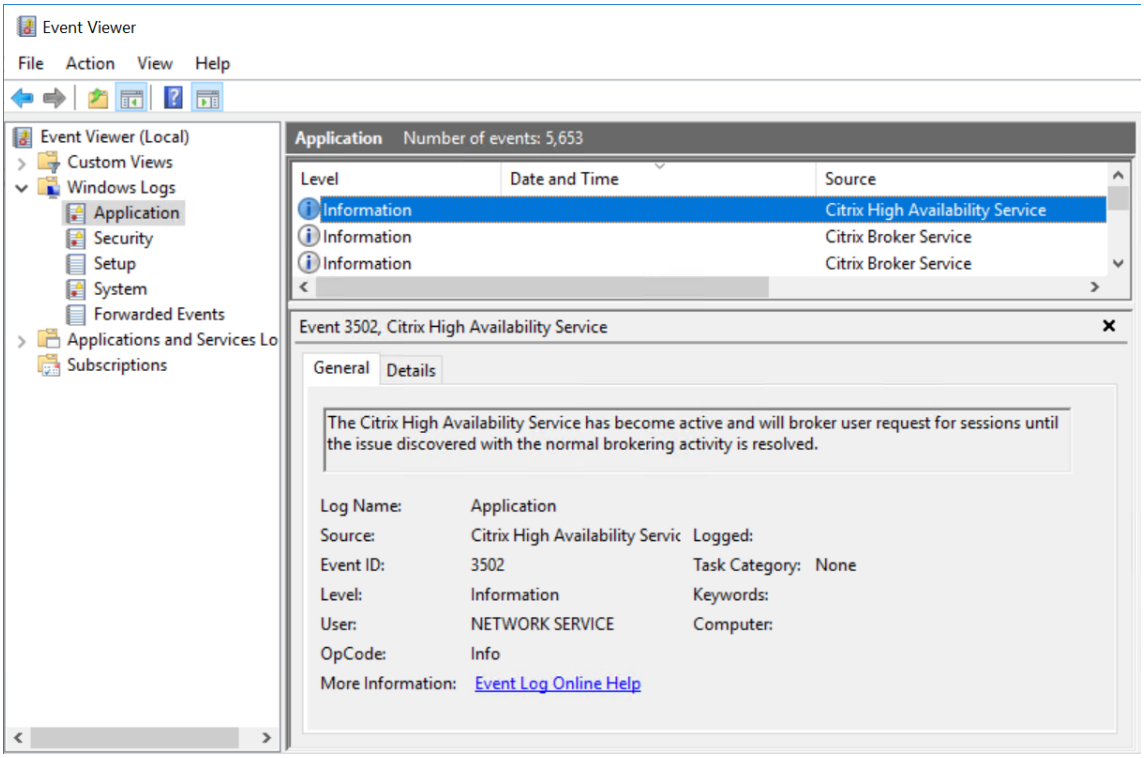
6. 強制的に停止して LHC モードにするには、各 Delivery Controller のレジストリを編集します。

   ```
   New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
   OutageModeForced -PropertyType DWORD -Value 1
   ```

7. 停止がトリガーされ、各プライマリブローカが LHC モードになったかどうかを判断するには、各コントローラのイベントログの「アプリケーション」ノードに移動し、Citrix 高可用性サービスから次のイベントを探します。

   3502：Citrix 高可用性サービスはアクティブになり、通常の仲介活動で検出された問題が解決されるまで、ユーザーからのセッション要求を仲介します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

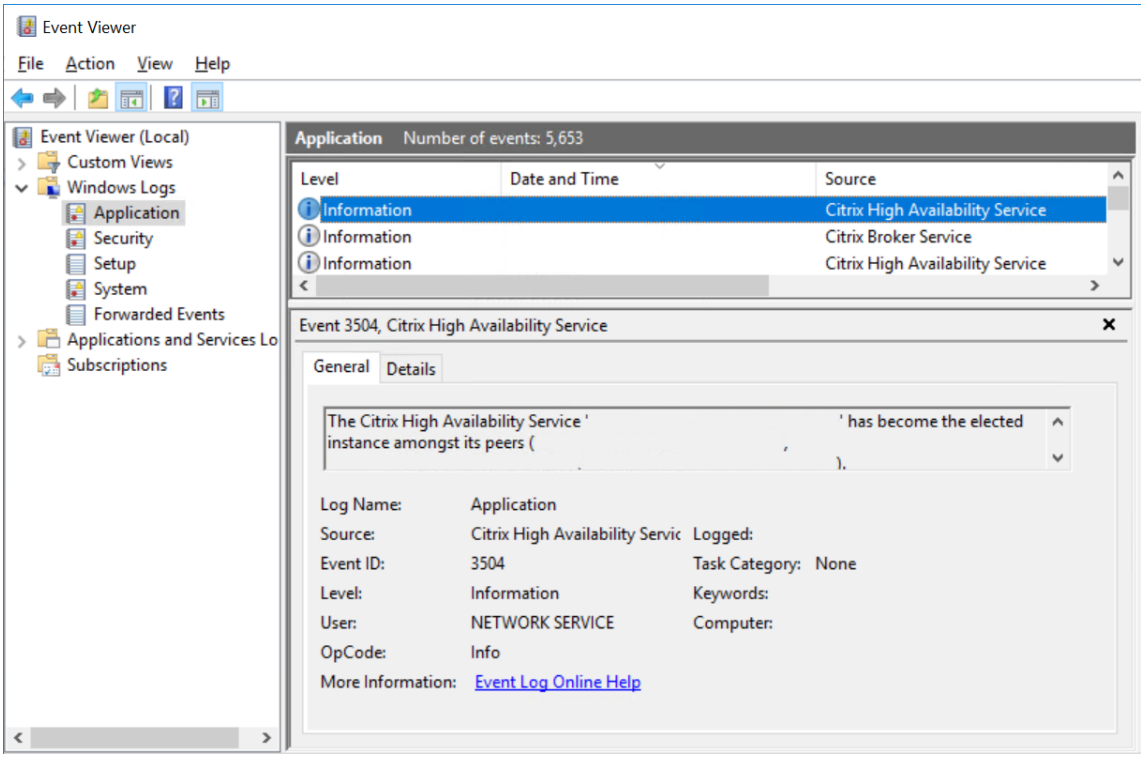


8. Citrix Studio の Controller ノードを更新して、選択したセカンダリブローカにすべての VDA が再登録されていることを確認します。プライマリブローカがゼロの登録済み VDA を示すと、すべての VDA が再登録されている可能性があります。

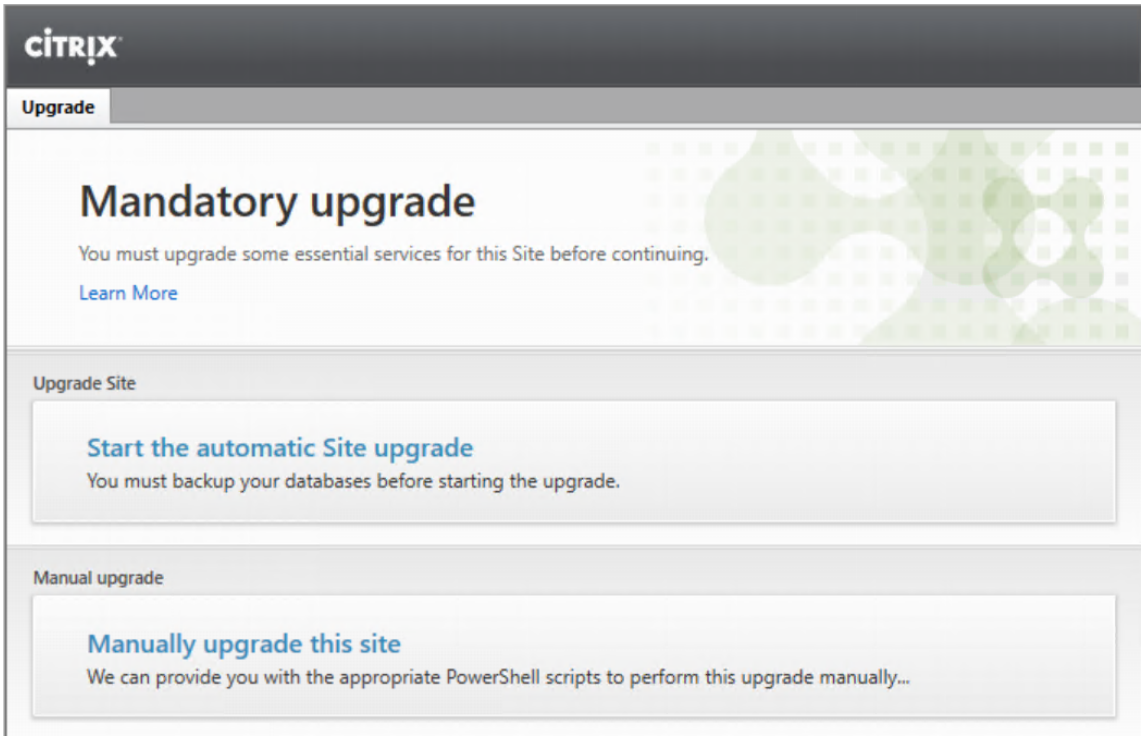
9. セカンダリブローカーは、停止が発生した場合にどのセカンダリブローカーがゾーン内で仲介操作を担当するかを決定（選択）するために、実行中のマシンの FQDN のアルファベット順のリストを使用します。どのセカンダリブローカが選出されたかを確認するには、Windows イベントログで Citrix 高可用性サービスから次のイベントを探します。

   3504：Citrix 高可用性サービス「選択されたコントローラの FQDN」が、ピア間で選択されたインスタンスになりました（ピアコントローラ *FQDN* のリスト）。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



10. 選択されていないピアコントローラの 1 つを選択し、選択されていないコントローラで製品のアップグレードを実行します。
11. 新しくアップグレードした Controller から Citrix Studio を起動し、データベースのアップグレードを含む必須サイトアップグレードを実行します。



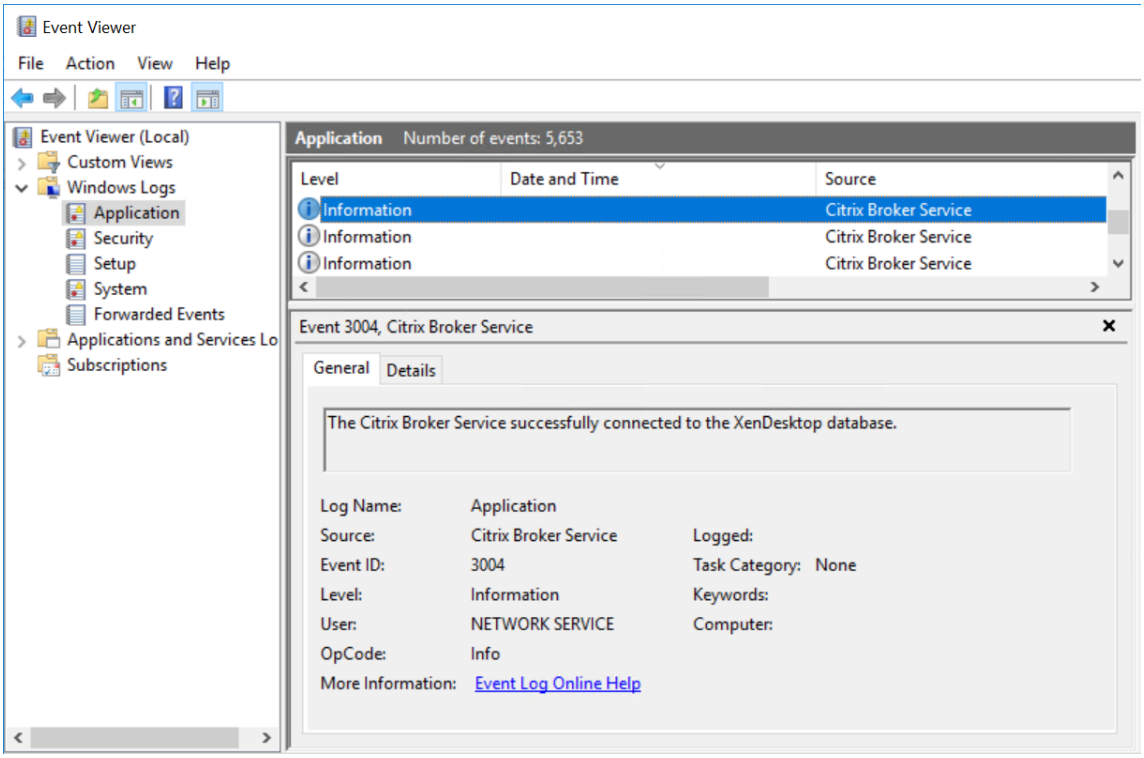
© 1999–2021 Citrix Systems, Inc. All rights reserved.

12. 選択されていない残りのピアコントローラで製品のアップグレードを実行します。選択されたコントローラは、環境内の新規およびアクティブな接続をすべて管理している中断しないようにしてください。
13. 選択されていないすべての Controller をアップグレードしたら、サイトの停止を解除し、LHC モードから移行します。強制停止トリガーを削除するには、各コントローラのレジストリを編集します。必要に応じて、キーを削除することもできます。

    ```
    Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
    OutageModeForced -Value 0
    ```

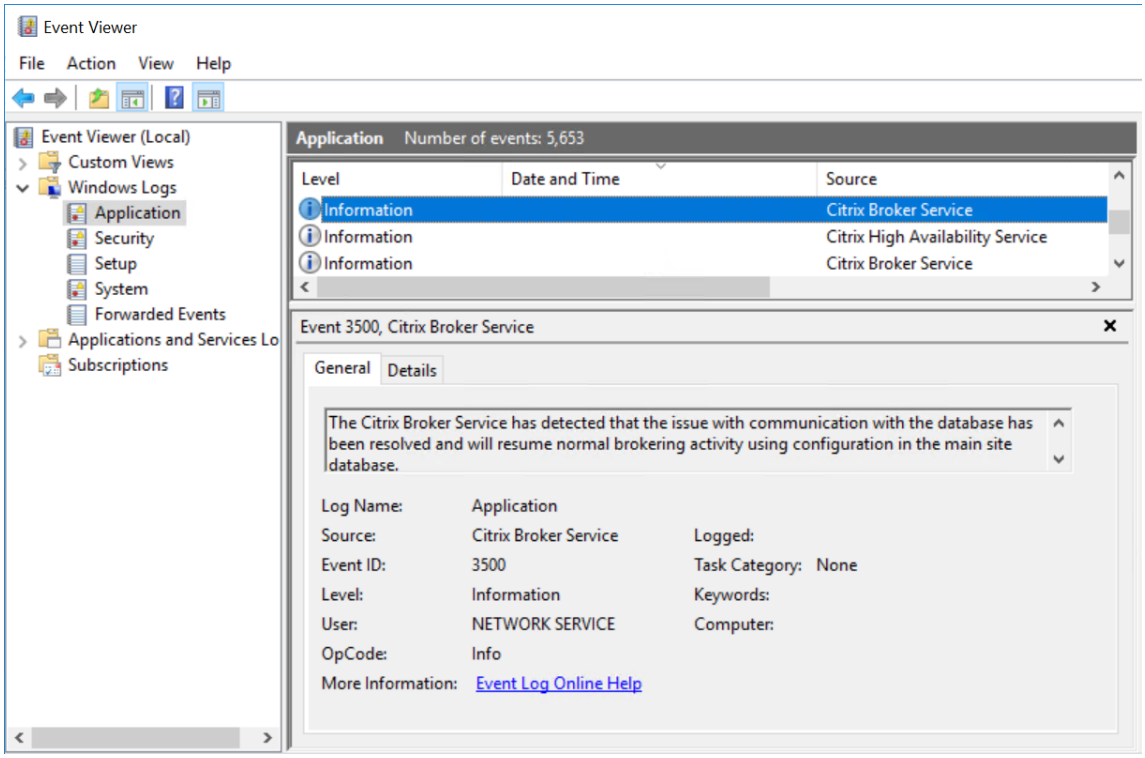
14. サイトが停止モードから外れているかどうかを確認するには、各 Controller で、アプリケーションイベントログで Citrix Broker Service から次のイベントを探します。

    3004：Citrix ブローカサービスが、XenDesktop データベースに正常に接続しました。



    3500：Citrix Broker Service は、データベースとの通信に関する問題が解決されたことを検出し、メインサイトデータベースの構成を使用して通常の仲介活動を再開します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



15. Citrix Studio からコントローラーノードを更新して、アップグレードされたコントローラーへの VDA の再登録を監視します。すべての VDA が正常に再登録されたことを確認します。
16. 停止中に選出されたセカンダリブローカーとして機能していた最後の残りの Controller で、製品のアップグレードを実行します。
17. 各 Controller のレジストリを変更して、VDA 登録間隔をデフォルト値 5 分に戻します（必要に応じてキーも削除できます）。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD -Value 300000
```

18. 電源管理デリバリーグループのデフォルトの動作に戻す場合は、次のコマンドレットを使用します。

```
1 Set-BrokerSite  -ReuseMachinesWithoutShutdownInOutageAllowed
     $false
2 Set-BrokerDesktopGroup -Name "<Delievery Group Name>" -
     ReuseMachinesWithoutShutdownInOutage $false
3 <!--NeedCopy-->
```

これで、ローカルホストキャッシュを使用した無停止アップグレードが完了します。

ローマのシリク、シニアによって寄与製品開発マネージャおよびジョセフ・ウ・シニア品質エンジニア

© 1999–2021 Citrix Systems, Inc. All rights reserved.

AWS の Linux 踏み台ホスト経由で RDP 経由で Citrix インフラストラクチャに接続する

May 18, 2020

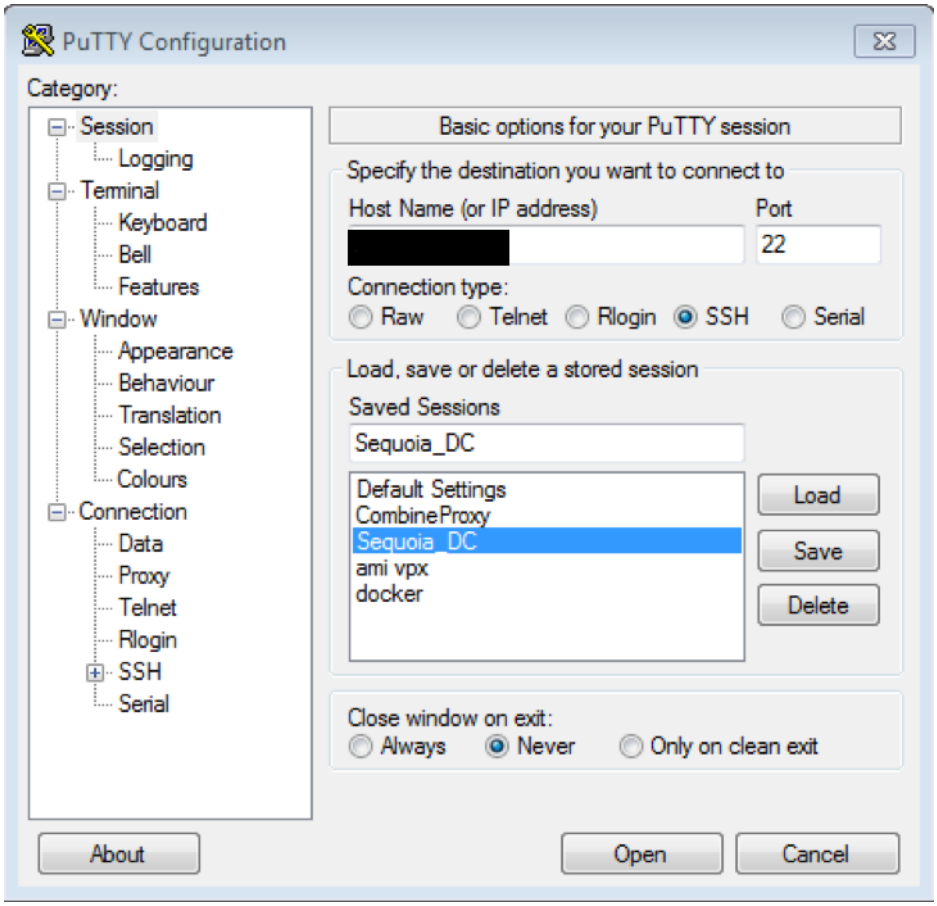
AWS で Citrix Virtual Apps and Desktops 環境をセットアップする場合、セキュリティ上の考慮事項を念頭に置いておくことが重要です。踏み台ホストは、通常、セキュリティを強化し、外部ネットワークと内部ネットワークを分離するために使用されます。通常、プロキシサーバーをホストする取り除かれた Linux インスタンスです。AWS での Citrix 実装の場合、管理者は踏み台ホストにアクセスできますが、Citrix インフラストラクチャへの直接のネットワークアクセスは許可されません。Citrix インフラストラクチャは Windows ベースのインスタンスで構成され、GUI ベースのメタインストーラが含まれているため、Linux ベースの踏み台ホストを介した接続が問題になります。

踏み台ホストを介して AWS の Linux インスタンスに接続することは、踏み台に PuTTYing し、目的のインスタンスに SSHing するのと同じくらい簡単です。踏み台ホストを介して Windows インスタンスへの RDP セッションを作成するには、ポート転送を使用します。ポート転送は、宛先 IP とポート番号の再マッピングです。これにより、保護されたネットワーク上のサービス（ルータなど）を Gateway の反対側で使用できるようになります。この場合、優先する SSH/トンネリングユーティリティでトンネルを作成して、ポート転送を使用してローカルポートを目的のインスタンスの RDP ポートにマッピングします。

たとえば、PuTTY コンソールで SSH セッションを作成します。踏み台ホストのパブリック IP を入力し、[**Auth**] セクションにプライベートキーを指定して、トンネルを作成します。トンネルの送信元ポートは、localhost 5000 以上などの未使用のローカルポートである必要があります。IP アドレスは、RDP ポートが追加された宛先ホスト（到達しようとしている Windows インスタンス）の IP アドレスです（3389）。必ず設定を保存してください。踏み台ホストに接続し、ログインします。次に、ローカルポートの RDP セッションを開始します。

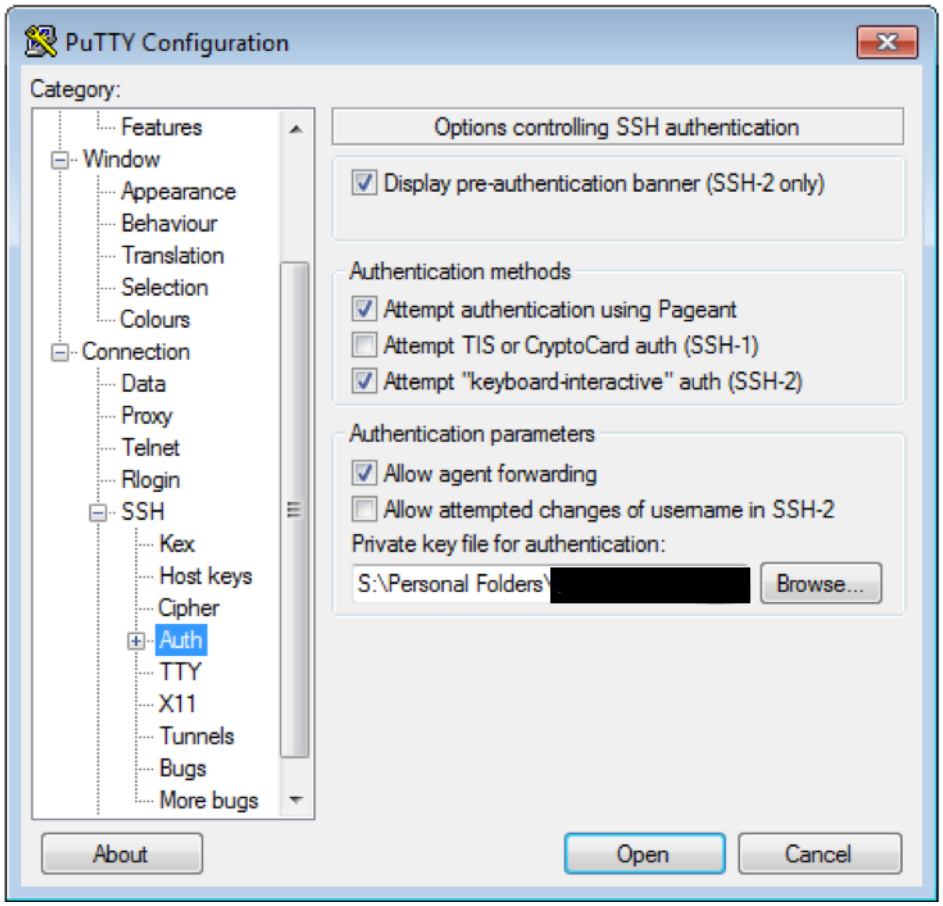
踏み台ホストのホスト名またはパブリック IP を設定します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



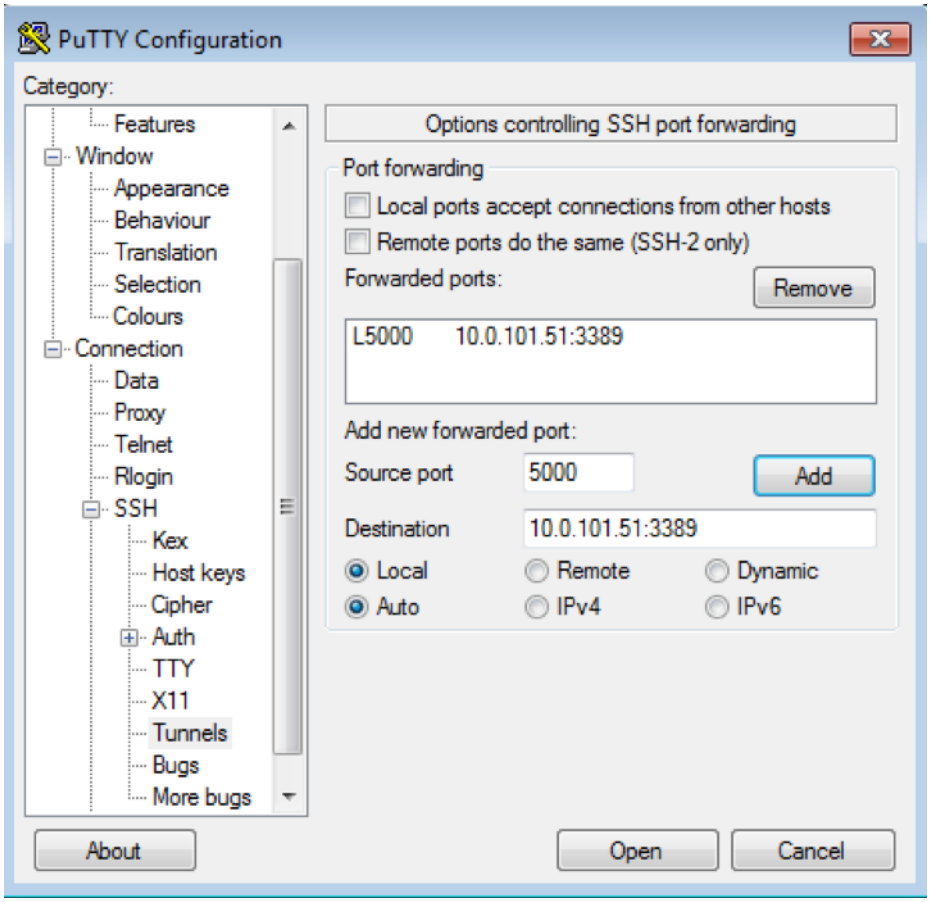
SSH > Auth で、秘密鍵ファイルを.ppk 形式で設定します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

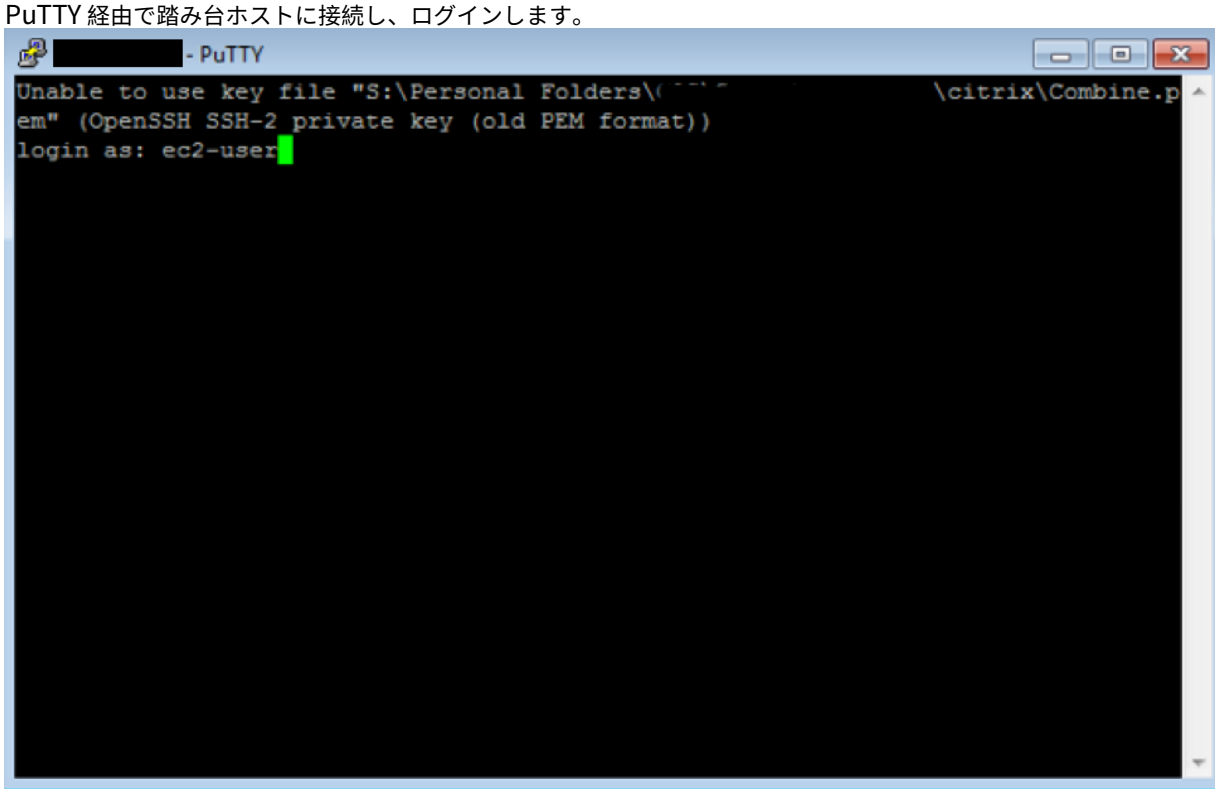


[**SSH**] > [トンネル] で、新しい転送ポートを追加します。**Source** ポートは任意の未使用のポートで、**Destination** は RDP ポートが追加された踏み台ホストの背後にある宛先サーバーの IP である必要があります。[**Source port**] フィールドで、[**Add**] をクリックして、新しい転送ポートを接続します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

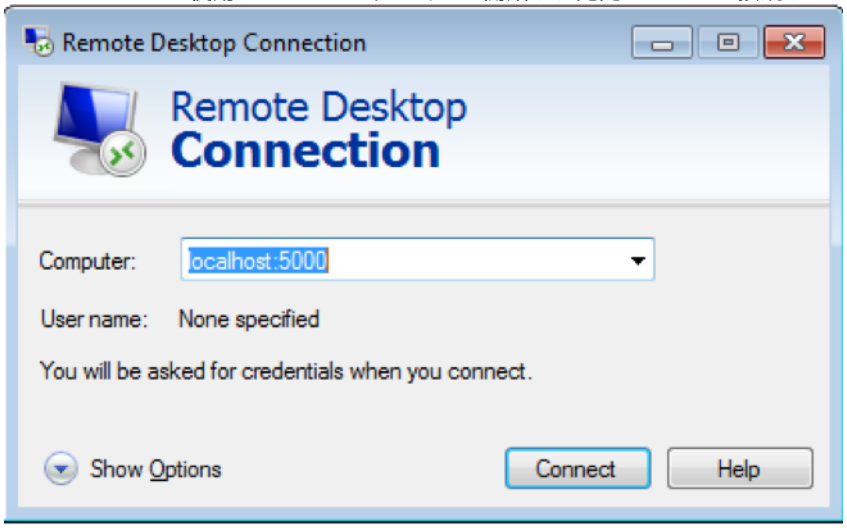


PuTTY 経由で踏み台ホストに接続し、ログインします。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

ローカルホストを使用して RDP セッションを開始し、宛先サーバーに接続します。



Citrix プリンシパルコンサルタント Jill Fetscher の寄稿

Azure DNS プライベートゾーンでの Citrix ADC 展開ガイド

May 18, 2020

はじめに

Citrix ADC は、以前は NetScaler と呼ばれていました。ADC（アプリケーションデリバリーコントローラー）領域で世界クラスの製品です。負荷分散、グローバルトラフィックの管理、圧縮、およびアプリケーションのセキュリティ保護が実証されています。

Azure DNS は、DNS ドメインをホストし、名前解決を提供するための Microsoft Azure インフラストラクチャ上のサービスです。

Azure DNS プライベートゾーンは、プライベートネットワーク内のドメイン名の解決に重点を置いたサービスです。プライベートゾーンでは、現在入手可能な Azure で提供されている名前ではなく、独自のカスタムドメイン名を使用できます。

Azure DNS の概要

ドメインネームシステム (DNS) は、サービス名をその IP アドレスに変換 (または解決) します。DNS ドメインのホスティングサービスである Azure DNS は、Microsoft Azure インフラストラクチャを使用して名前解決を提供します。インターネット向けの DNS ドメインのサポートに加えて、Azure DNS はプライベート DNS ドメインもサポートするようになりました。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Azure DNS は、カスタム DNS ソリューションを必要とせずに、仮想ネットワーク内のドメイン名を管理および解決するための、信頼性の高い、セキュリティで保護された DNS サービスを提供します。プライベート DNS ゾーンを使用すると、現在入手可能な Azure で提供されている名前ではなく、独自のカスタムドメイン名を使用できます。カスタムドメイン名を使用すると、組織のニーズに最も適した仮想ネットワークアーキテクチャを調整できます。仮想ネットワーク内および仮想ネットワーク間の仮想マシン (VM) の名前解決を提供します。また、スプリットホライズンビューを使用してゾーン名を構成することもできます。これにより、プライベート DNS ゾーンとパブリック DNS ゾーンで名前を共有できます。

なぜ **Azure** の **DNS** プライベートゾーンのための **Citrix** の **GSLB** ですか**?**

今日の世界では、企業はワークロードをオンプレミスから Azure クラウドに移行したいと考えています。クラウドへの移行により、市場投入までの時間、設備投資/価格、展開の容易さ、セキュリティを活用できます。Azure DNS プライベートゾーンサービスは、ワークロードの一部を Azure クラウドに移行している企業に対して、独自の提案を提供します。これらの企業は、プライベートゾーンサービスを使用するときに、オンプレミス展開で長年にわたって持っていたプライベート DNS 名を作成できます。イントラネットアプリケーションサーバーのこのハイブリッドモデルがオンプレミスにあり、Azure クラウドは安全な VPN トンネルを介して接続されているため、1 つの課題は、ユーザーがこれらのイントラネットアプリケーションにシームレスにアクセスする方法です。Citrix ADC は、アプリケーションのトラフィックをオンプレミスまたは Azure クラウド上で最適な分散ワークロード/サーバーにルーティングし、アプリケーションサーバーの正常性ステータスを提供するグローバル負荷分散機能によって、このユニークなユースケースを解決します。

使用例

オンプレミスネットワークと異なる Azure VNET のユーザーは、必要なコンテンツにアクセスするために内部ネットワークの最適なサーバーに接続できる必要があります。これにより、アプリケーションが常に利用可能になり、最適化されたコストとユーザーエクスペリエンスが良好です。Azure プライベートトラフィック管理 (PTM) が主な要件です。Azure PTM では、ユーザーの DNS クエリがアプリケーションサーバーの適切なプライベート IP アドレスに解決されます。

ユースケースソリューション

Citrix ADC には、Azure PTM 要件を満たすために役立つグローバルサーバー負荷分散（GSLB）機能が含まれています。GSLB は、DNS 要求を取得し、DNS 要求を提供するために、適切な IP アドレスに DNS 要求を解決する DNS サーバのように動作します。

- シームレスな DNS ベースのフェイルオーバー
- オンプレミスからクラウドへの段階的な移行
- A/B 新機能のテスト

サポートされる多くの負荷分散方式の中で、このソリューションでは次の方法が役に立ちます。

1. ラウンドロビン

© 1999–2021 Citrix Systems, Inc. All rights reserved.

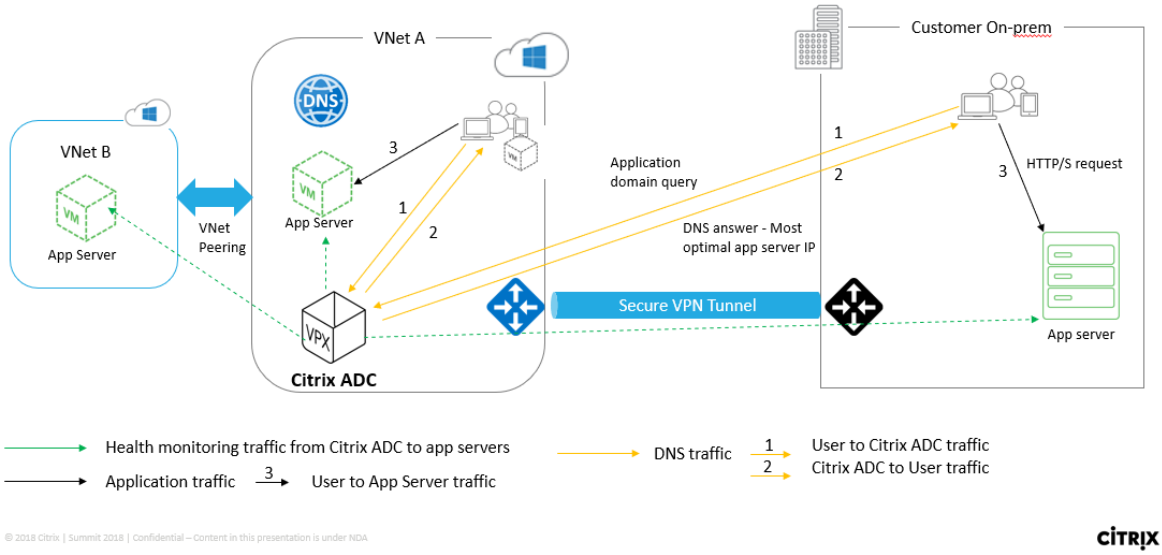
2. 静的近接（ロケーションベースのサーバー選択）：2 つの方法で展開できます

   a) Citrix ADC 上の EDNS クライアントサブネット（ECS）ベースの GSLB ベース

   b) すべての仮想ネットワークに DNS フォワーダを展開する

トポロジ

- Azure プライベート DNS ゾーン用の Citrix ADC GSLB 展開は、図 1 に論理的に示されています。



- ユーザーは、Azure または Azure のプライベート DNS ゾーンの Citrix ADC GSLB 負荷分散方式に基づいてオンプレミスで任意のアプリケーションサーバーにアクセスできます
- オンプレミスと Azure 仮想ネットワーク間のすべてのトラフィックは、セキュリティで保護された VPN トンネルのみを通過します。
- 前述のトポロジでは、アプリケーショントラフィック、DNS トラフィック、および監視トラフィックが示されています。
- 必要な冗長性に応じて、Citrix ADC および DNS フォワーダを仮想ネットワークおよびデータセンターに展開できます。簡単にするために、ここでは 1 つの Citrix ADC のみを示していますが、Azure リージョン用の Citrix ADC と DNS フォワーダーの少なくとも 1 つのセットをお勧めします。
- すべてのユーザー DNS クエリは、まず、クエリを適切な DNS サーバーに転送するためのルールが定義されている DNS フォワーダに送信されます。

Azure DNS プライベートゾーン用の **Citrix ADC** の構成

テスト済みの製品とバージョン

製品	バージョン
Azure	クラウドサブスクリプション

© 1999–2021 Citrix Systems, Inc. All rights reserved.

製品	バージョン
Citrix ADC VPX	BYOL (独自のライセンスを持参)

> 注：展開はテスト済みで、Citrix ADC バージョン 12.0 以降と同じままです。

前提条件と設定に関する注意事項

このガイドでテストされる一般的な前提条件と構成は次のとおりです。Citrix ADC を設定する前にクロスチェックしてください。

- 有効なサブスクリプションを持つ Microsoft Azure ポータルアカウント
- オンプレミスと Azure クラウド間の接続 (セキュアな VPN トンネル) を確実にします。Azure でセキュリティで保護された VPN トンネルをセットアップするには、ステップバイステップ:Azure とオンプレミスの間でサイト間 VPN ゲートウェイを構成するを参照してください

ソリューションの説明

お客様が、HTTP 上で実行され、ラウンドロビン GSLB 負荷分散方法に基づくイントラネットアクセスで Azure とオンプレミスで展開される 1 つのアプリケーションの Azure DNS プライベートゾーン (rr.ptm.mysite.net) をホストするとします。この展開を実現するには、Azure、オンプレミス、および Citrix ADC アプライアンスを構成する、Citrix ADC で Azure プライベート DNS ゾーンの GSLB を有効にする必要があります。

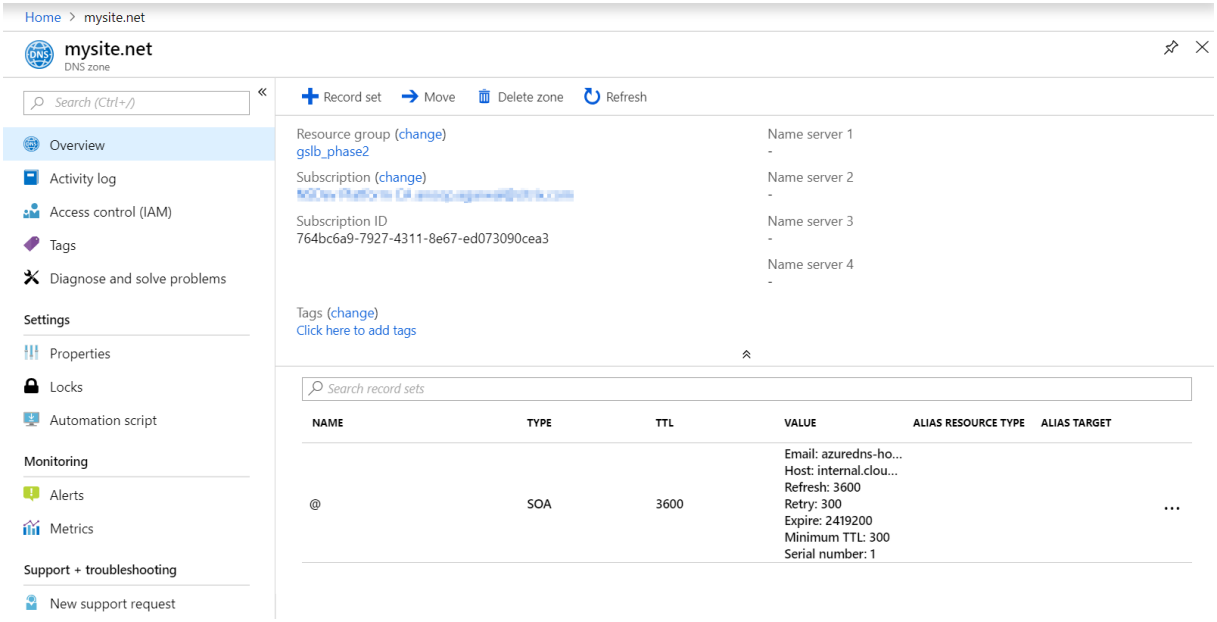
パート **1: Azure**、オンプレミスセットアップを構成する

トポロジに示すように、Azure 仮想ネットワーク (この場合は VNet A、VNet B) とオンプレミスのセットアップを設定します。
手順 1: ドメイン名 (mysite.net) で Azure プライベート DNS ゾーンを作成する
手順 2: Azure リージョンのハブアンドスポークモデルで 2 つの仮想ネットワーク (VNet A、VNet B) を作成する
手順 3: アプリケーションサーバー、DNS フォワーダー、Windows 10 Pro クライアント、および VNet A での Citrix ADC を展開する
手順 4: アプリケーションサーバーを展開し、クライアントが VNet B にある場合は DNS フォワーダーを展開する
手順 5: アプリケーションサーバー、DNS フォワーダー、および Windows 10 Pro クライアントをオンプレミスで展開する

Azure プライベート **DNS** ゾーン

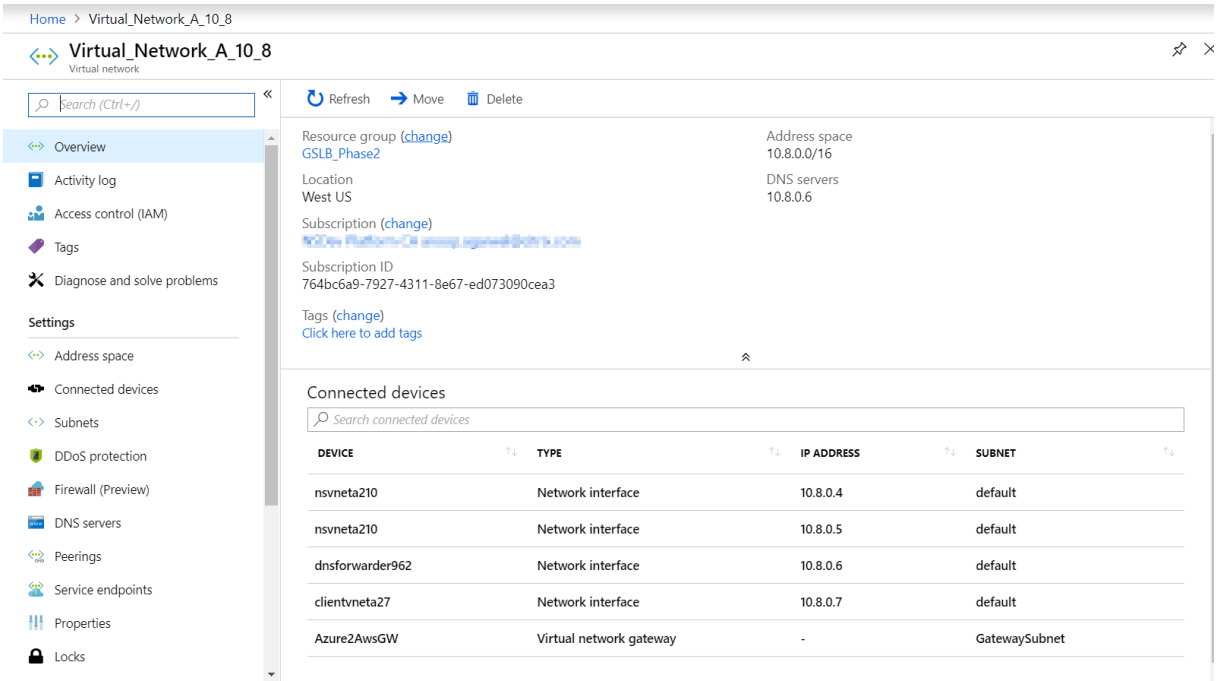
Azure Portal にログインし、ダッシュボードを選択または作成します。今 、リソースを作成し、次の図に示すように、**1**（この場合は **mysite.net**）を作成する **DNS** ゾーンを検索します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

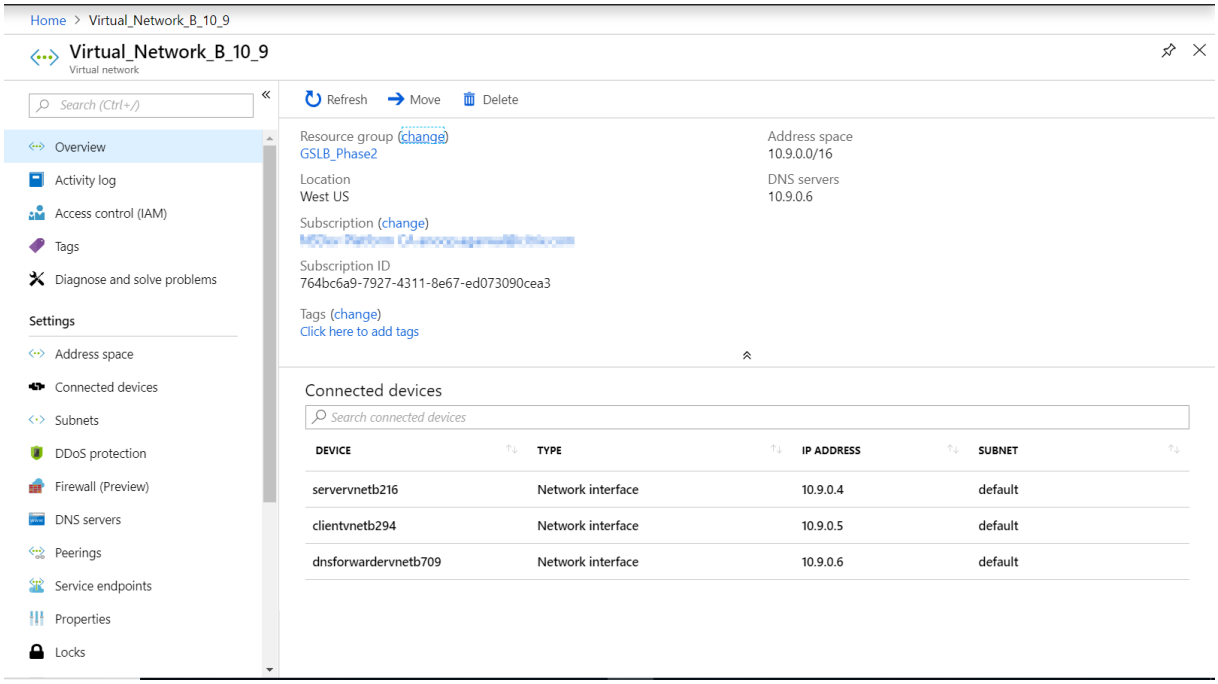


ハブモデルとスポークモデルの **Azure** 仮想ネットワーク **(VNet A**、**VNet B)**

同じダッシュボードを選択し、リソースを作成し、同じ領域内の **2** つの仮想ネットワーク、すなわち **VNet A**、**VNet B** を作成し、次の図に示すように、ハブとスポークモデルを形成するためにそれらをピアリングする仮想ネットワークを検索します。ハブアンドスポークトポロジの設定方法については、Azure でのハブスポークネットワークトポロジの実装を参照してください。



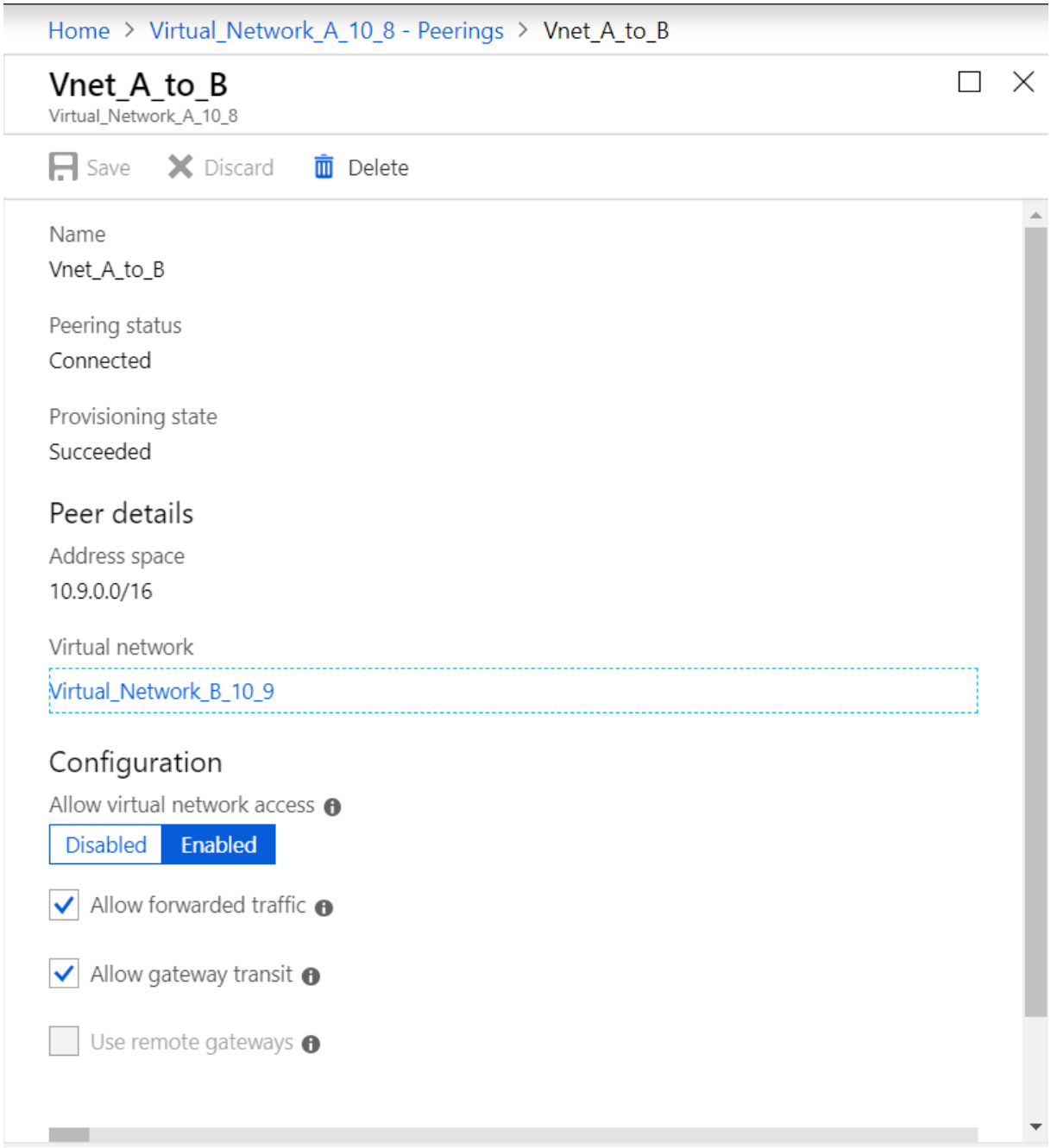
© 1999–2021 Citrix Systems, Inc. All rights reserved.



VNet A から **VNet B** へのピアリング

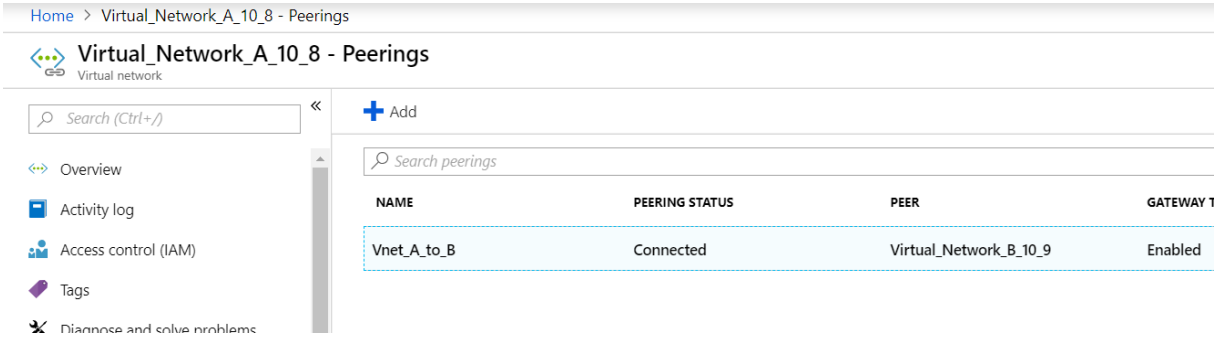
VNet A と VNet B をピアリングするには、VNet A とピア VNet B の設定メニューからピアリングをクリックします。次の図に示すように、[転送されたトラフィックを許可する] と [Gateway の通過を許可する] を有効にします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ピアリングが成功すると、次の図のように表示されます。

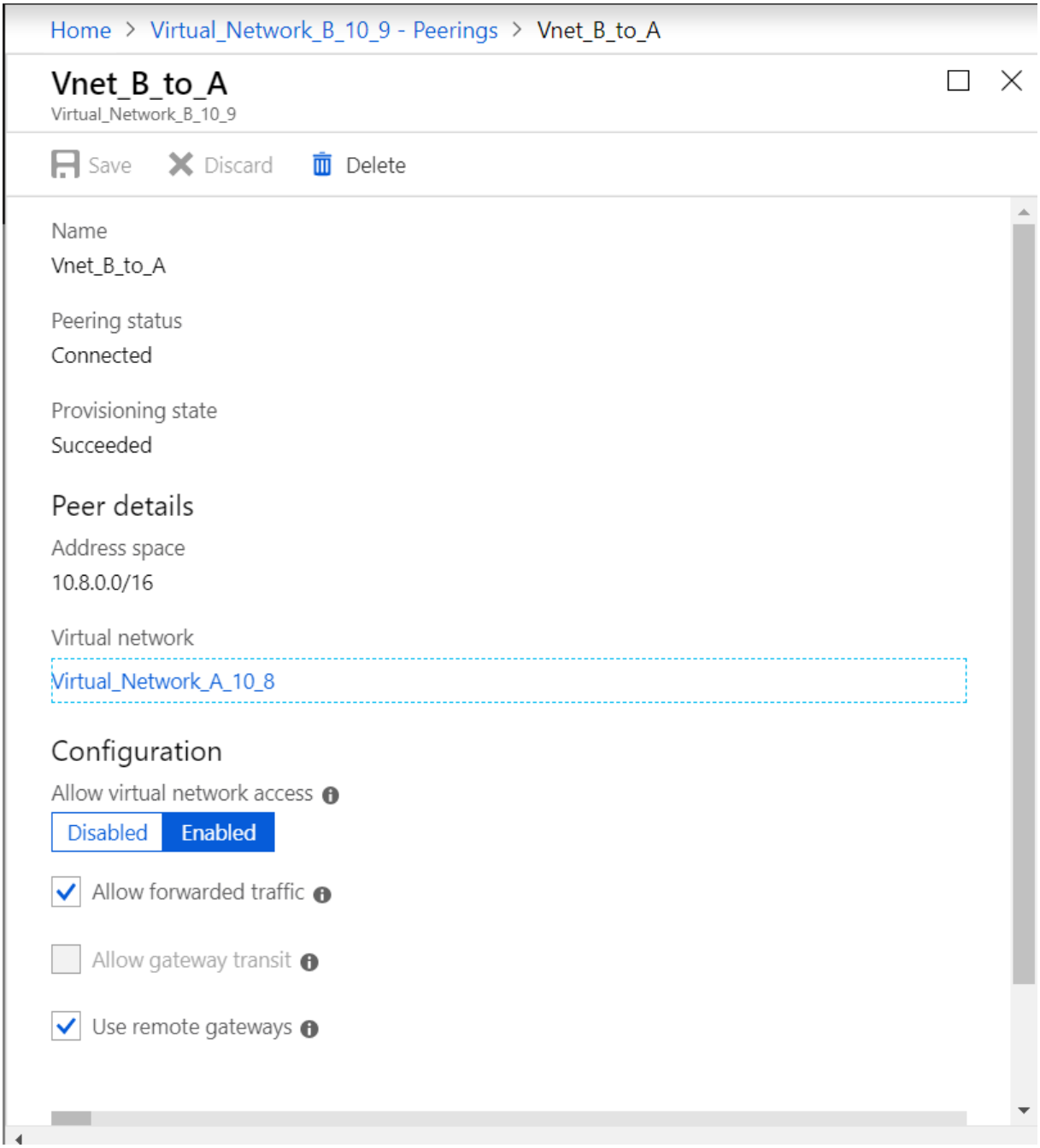
© 1999–2021 Citrix Systems, Inc. All rights reserved.



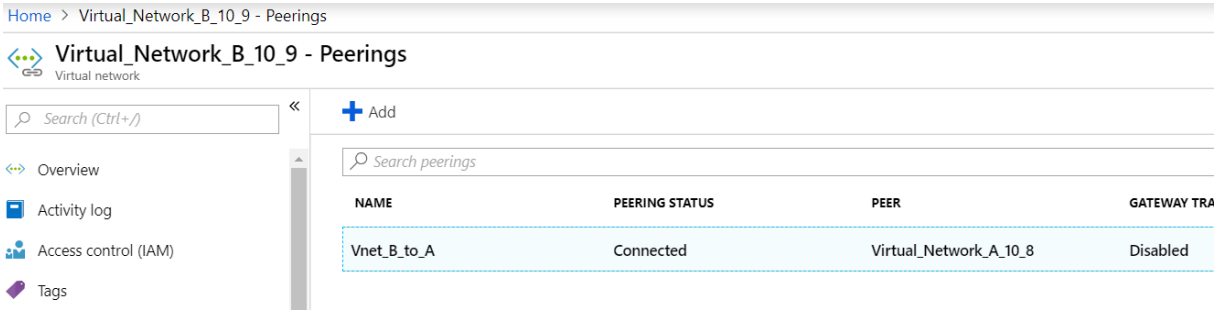
VNet B から **VNet A** へのピアリング

VNet B と VNet A をピア リングするには、VNet B とピア VNet A の設定メニューからピアリングをクリックします。次の図に示すように、[転送トラフィックを許可する] と [リモートゲートウェイを使用する] を有効にします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ピアリングが成功すると、次の図のように表示されます。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

アプリケーションサーバー、**DNS** フォワーダー、**Windows 10 Pro** クライアント、**VNet A** での **Citrix ADC** の展開

私たちは、アプリケーションサーバー、DNS フォワーダ、Windows 10 プロクライアント、および VNet A 上の Citrix ADC について簡単に説明します。同じダッシュボードを選択し、リソースを作成し、それぞれのインスタンスを検索し、VNet A サブネットから IP を割り当てます

アプリケーションサーバー

アプリケーションサーバーは、Ubuntu サーバー 16.04 が Azure またはオンプレミス VM 上のインスタンスとして展開され、CLI コマンドを実行するウェブサーバー（HTTP サーバー）に他ならない：sudo の apache2 をインストールしてウェブサーバーとして作る

Windows 10 Pro クライアント

VNet A およびオンプレミスのクライアントマシンとして Windows 10 pro インスタンスを起動します。

Citrix ADC

Citrix ADC は、Citrix MAS のヘルスチェックと分析によって、Azure DNA のプライベートゾーンを補完します。あなたの要件に基づいて、Azure のマーケットプレイスから Citrix ADC を起動します, ここでは、Citrix ADC を使用しています (BYOL) この展開のために. Microsoft Azure に Citrix ADC を展開する方法の手順については、以下の URL を参照してください。展開後、Citrix ADC IP を使用して Citrix ADC GSLB を構成します。「Microsoft Azure で NetScaler VPX インスタンスを展開する」を参照してください。

DNS フォワーダー

これは、Citrix ADC GSLB（ADNS IP）にバインドされたホストされたドメインのクライアント要求を転送するために使用されます。Linux インスタンス（Ubuntu サーバー 16.04）として Ubuntu のサーバー 16.04 を起動し、DNS フォワーダーとしてそれを設定する方法については、以下の URL を参照してください。

> 注**:** ラウンドロビン GSLB 負荷分散方法では、Azure リージョンの DNS フォワーダーが 1 つだけ十分ですが、静的近接では、仮想ネットワークごとに 1 つの DNS フォワーダーが必要です。https://github.com/Azure/azure-quickstart-templates/tree/master/301-dns-forwarderからクイックスタートテンプレートをダウンロードします

フォワーダーを展開した後、次の図に示すように、仮想ネットワーク A の DNS サーバー設定を VNet A DNS フォワーダー IP を使用してデフォルトからカスタムに変更し、VNet A DNS フォワーダーの`named.conf.options`ファイルを変更して、ドメイン (mysite.net) の転送ルールを追加します。サブドメイン（ptm.mysite.net）を Citrix の GSLB の ADNSIP に割り当てます。ここで、DNS フォワーダーを再起動して、`named.conf.options`ファイルに加えられた変更を反映します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

VNet A DNS フォワーダーの設定

```
    zone "mysite.net" {

                type forward;
    forwarders {
  168.63.129.16;  }
;
     }
;
    zone "ptm.mysite.net" {

        type forward;
        forwarders {
  10.8.0.5;  }
;
     }
;
<!--NeedCopy-->
```

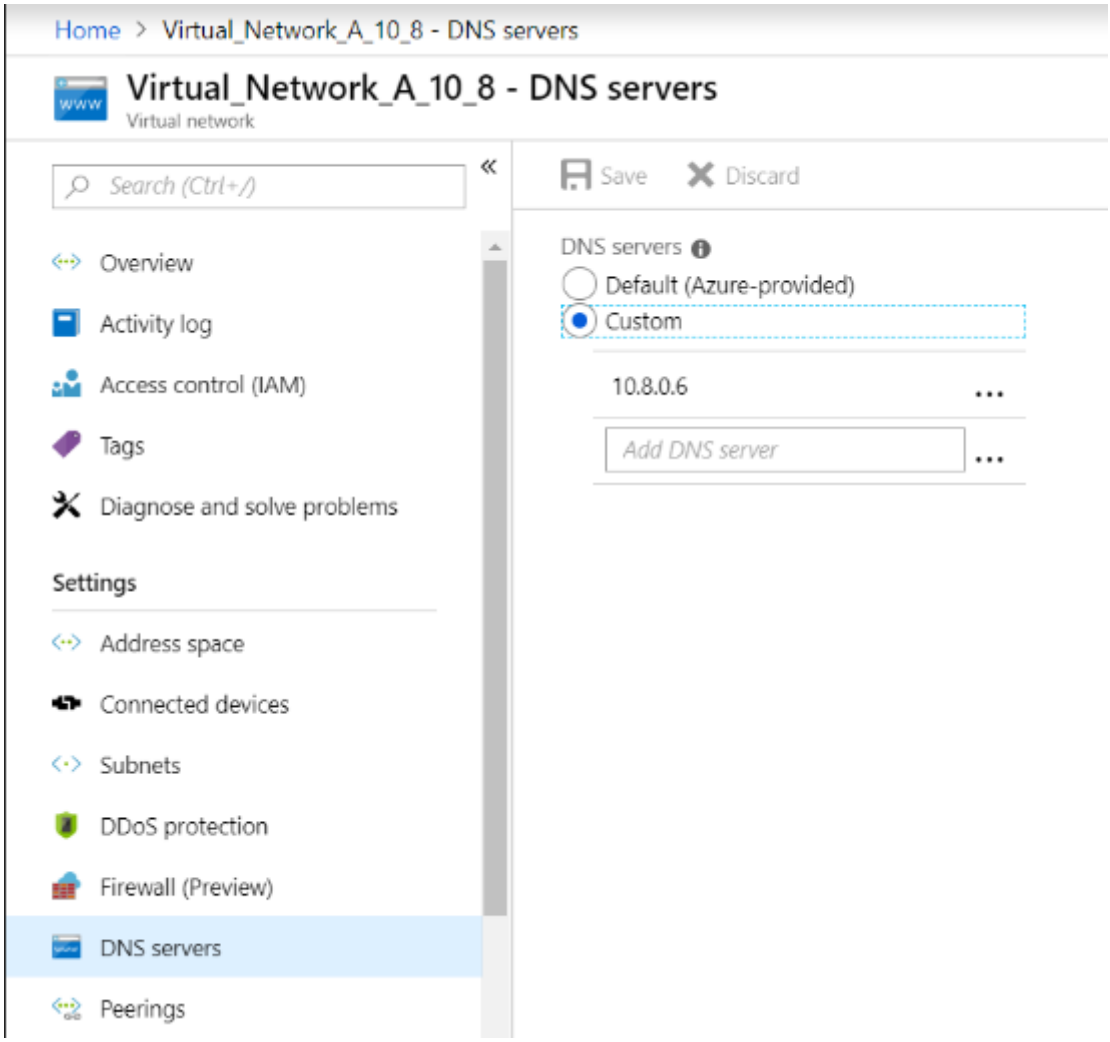
> **注:** ドメイン (「mysite.net」) ゾーンの IP アドレスには、Azure リージョンの DNS IP を使用します。サブドメイン (「ptm.mysite.net」) ゾーンの IP アドレスには、GSLB インスタンスのすべての ADNS IP アドレスを使用します。

VNet B にクライアントがある場合はアプリケーションサーバーを展開し、**DNS** フォワーダを展開する

仮想ネットワーク B で、同じダッシュボードを選択し、[リソースの作成] をクリックし、それぞれのインスタンスを検索して、VNet B サブネットから IP を割り当てます。VNet A に似た静的な近接性 GSLB ロードバランシングがある場合に、アプリケーションサーバーと DNS フォワーダを起動します。
次に示すように、`named.conf.options`の VNet B DNS Forwarder の設定を編集します。

```
    VNet B DNS Forwarder Settings:
    zone "ptm.mysite.net" {

        type forward;
        forwarders {
  10.8.0.5;  }
;
     }
;
<!--NeedCopy-->
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.



アプリサーバー、**DNS** フォワーダー、および **Windows 10** プロクライアントをオンプレミスで展開する

オンプレミスでは、ベアメタルで VM を起動し、VNet A に似たアプリケーションサーバー、DNS フォワーダー、および Windows 10 Pro クライアントをもたらします。
次の例に示すように、`named.conf.options`でオンプレミスの DNS Forwarder 設定を編集します。

オンプレミスの **DNS** フォワーダ設定

```
    zone "mysite.net" {

                type forward;
                forwarders {
 10.8.0.6;  }
;
     }
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
8   ;
9      zone "ptm.mysite.net" {
10
11          type forward;
12          forwarders {
13    10.8.0.5;  }
14  ;
15       }
16  ;
17 <!--NeedCopy-->
```

ここでは、mysite.netで Azure のプライベート DNS ゾーンサーバーの IP の代わりに VNet A の DNS フォワーダ IP が指定されています。これはオンプレミスから到達できない特別な IP であるためです。したがって、この変更は、オンプレミスの DNS フォワーダー設定に必要です。

パート **2: Citrix ADC** を構成する

トポロジーに示すように、Citrix ADC を Azure 仮想ネットワーク（この場合は VNet A）に展開し、Citrix ADC の GUI を介してアクセスします。

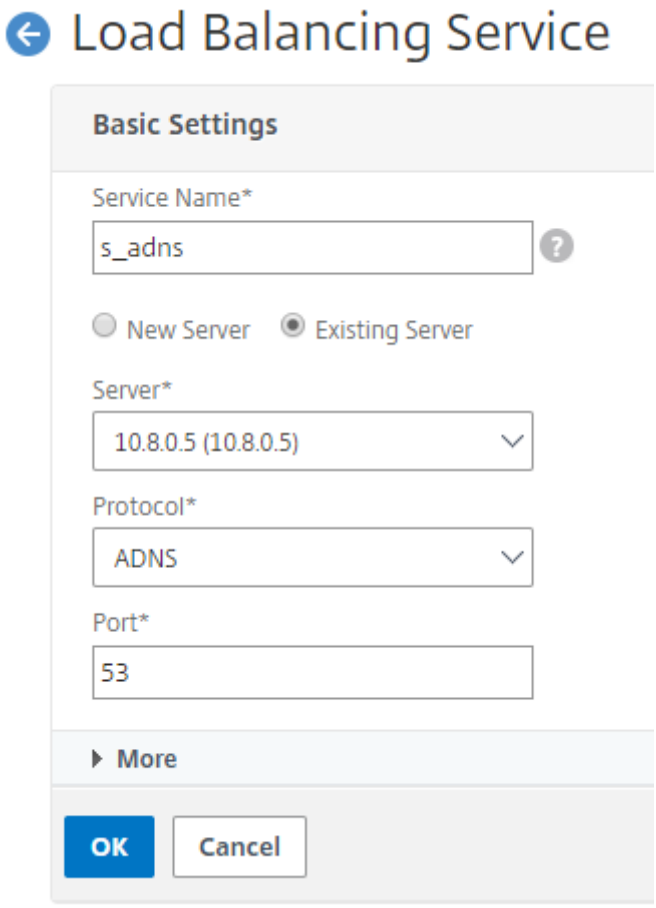
Citrix ADC GSLB の構成

手順 1: ADNS サービスの作成
手順 2: サイトを作成する — ローカルおよびリモート
手順 3: ローカル仮想サーバーのサービスを作成する
手順 4: GSLB サービスの仮想サーバーを作成する

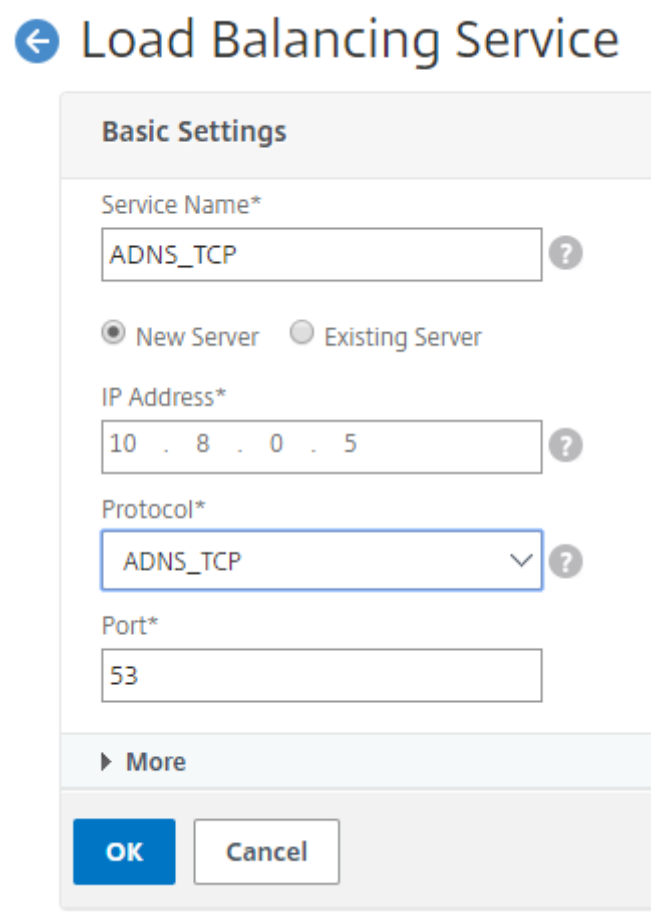
ADNS サービスの追加

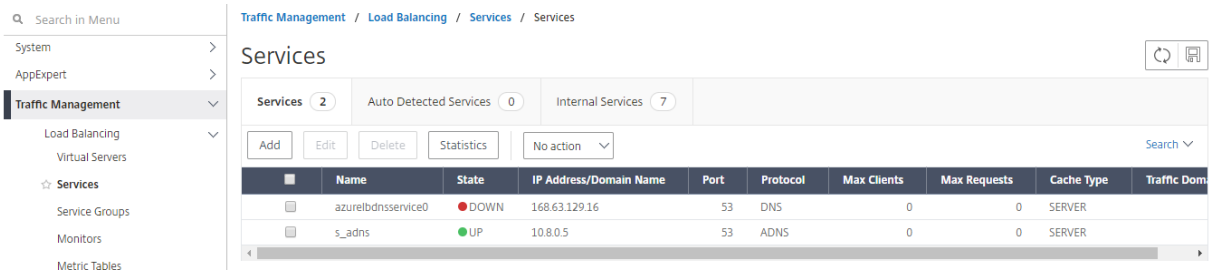
Citrix ADC の GUI にログインします。[設定] タブで、[トラフィック管理] **>** [負荷分散] **>** [サービス] に移動します。サービスを追加します。次に示すように、TCP と UDP の両方で ADNS サービスを構成することをお勧めします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



© 1999–2021 Citrix Systems, Inc. All rights reserved.

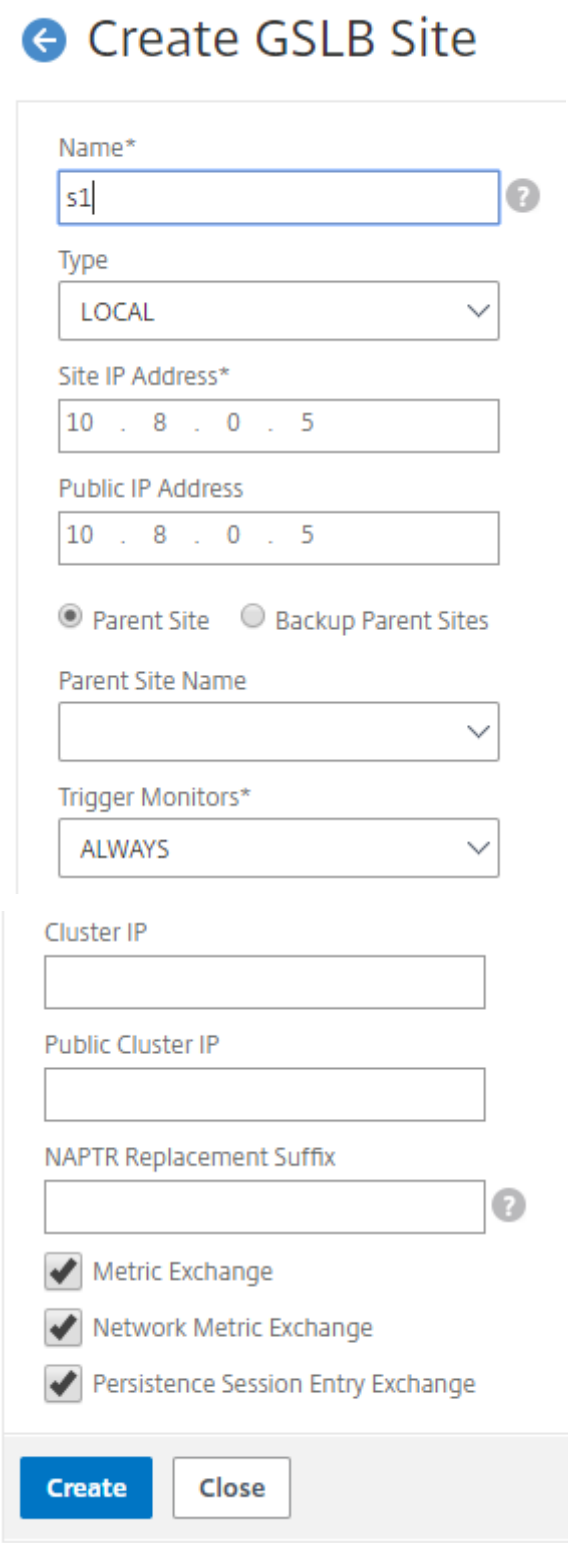




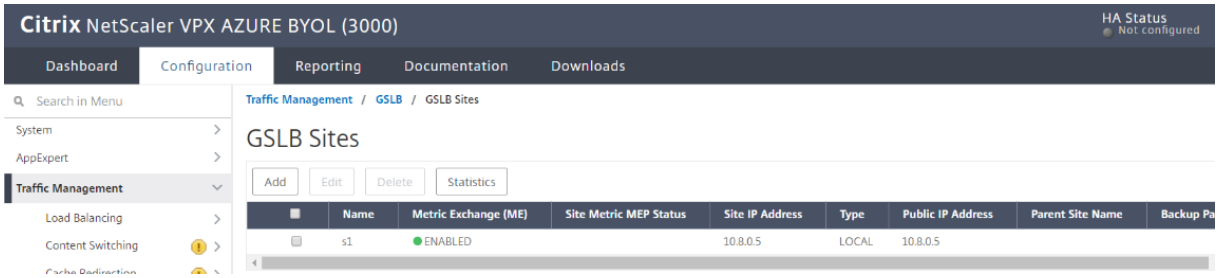
GSLB サイトの追加

GSLB が構成されるローカルサイトとリモートサイトを追加します。[設定] タブで、[トラフィック管理] **> [GSLB] > [GSLB** サイト] に移動します。ここに示すようにサイトを追加し、他のサイトについても同じ手順を繰り返します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

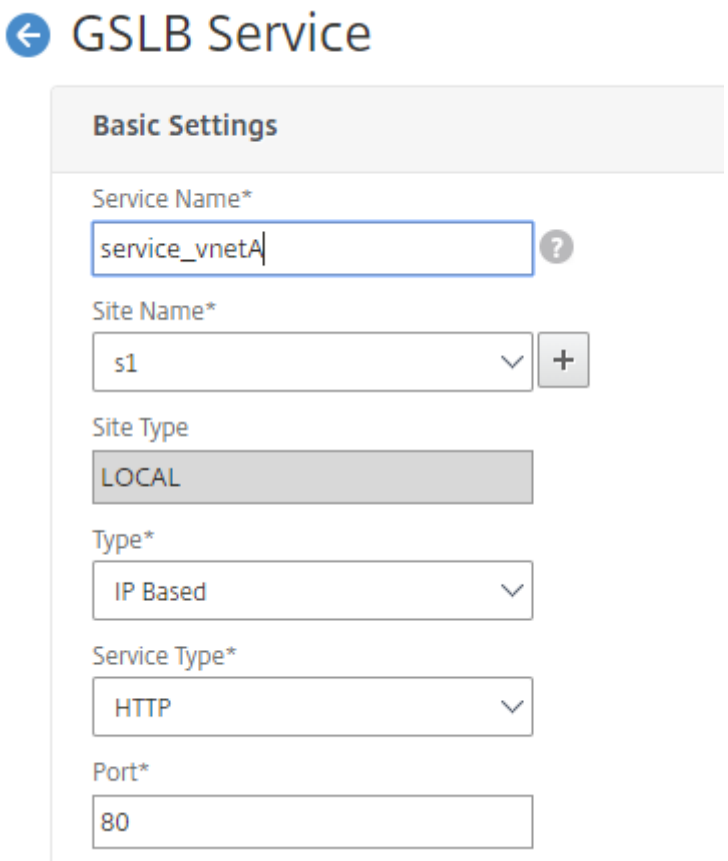


© 1999–2021 Citrix Systems, Inc. All rights reserved.

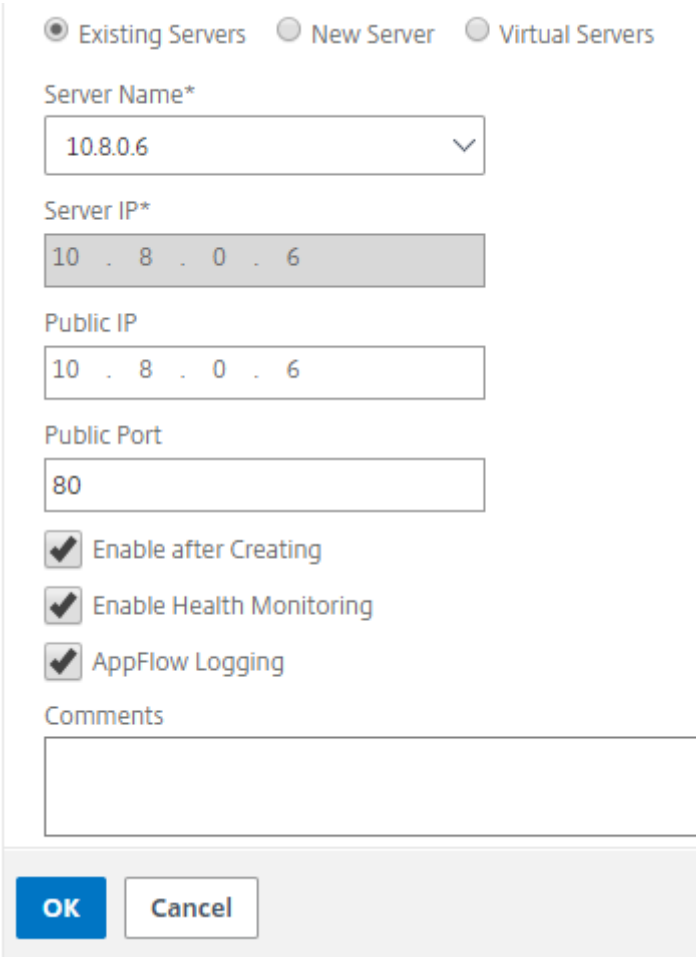


GSLB サービスの追加

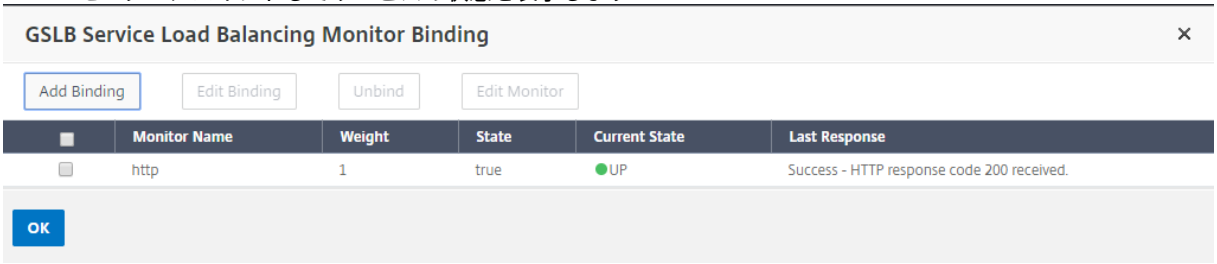
App サーバーの負荷分散を行うローカルおよびリモートの仮想サーバーに GSLB サービスを追加します。[設定] タブで、[トラフィック管理] **> [GSLB] > [GSLB** サービス] に移動します。次の例に示すように、サービスを追加します。HTTP モニターをバインドしてサーバーのステータスを確認します。



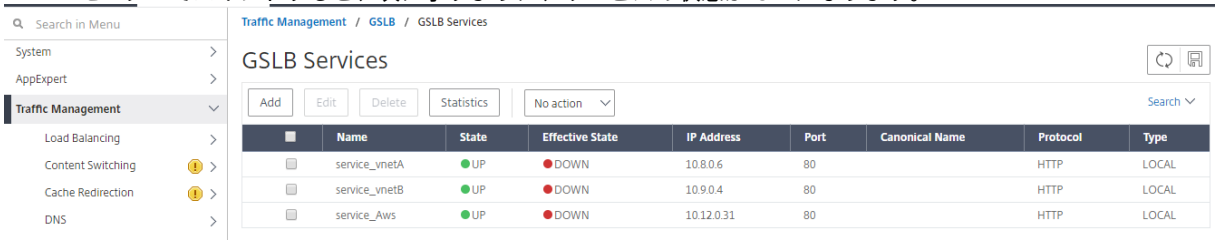
© 1999–2021 Citrix Systems, Inc. All rights reserved.



サービスを作成したら、GSLB サービス内の詳細設定タブに移動し、[モニター] タブを追加して、GSLB サービスを HTTP モニターにバインドしてサービスの状態を表示します



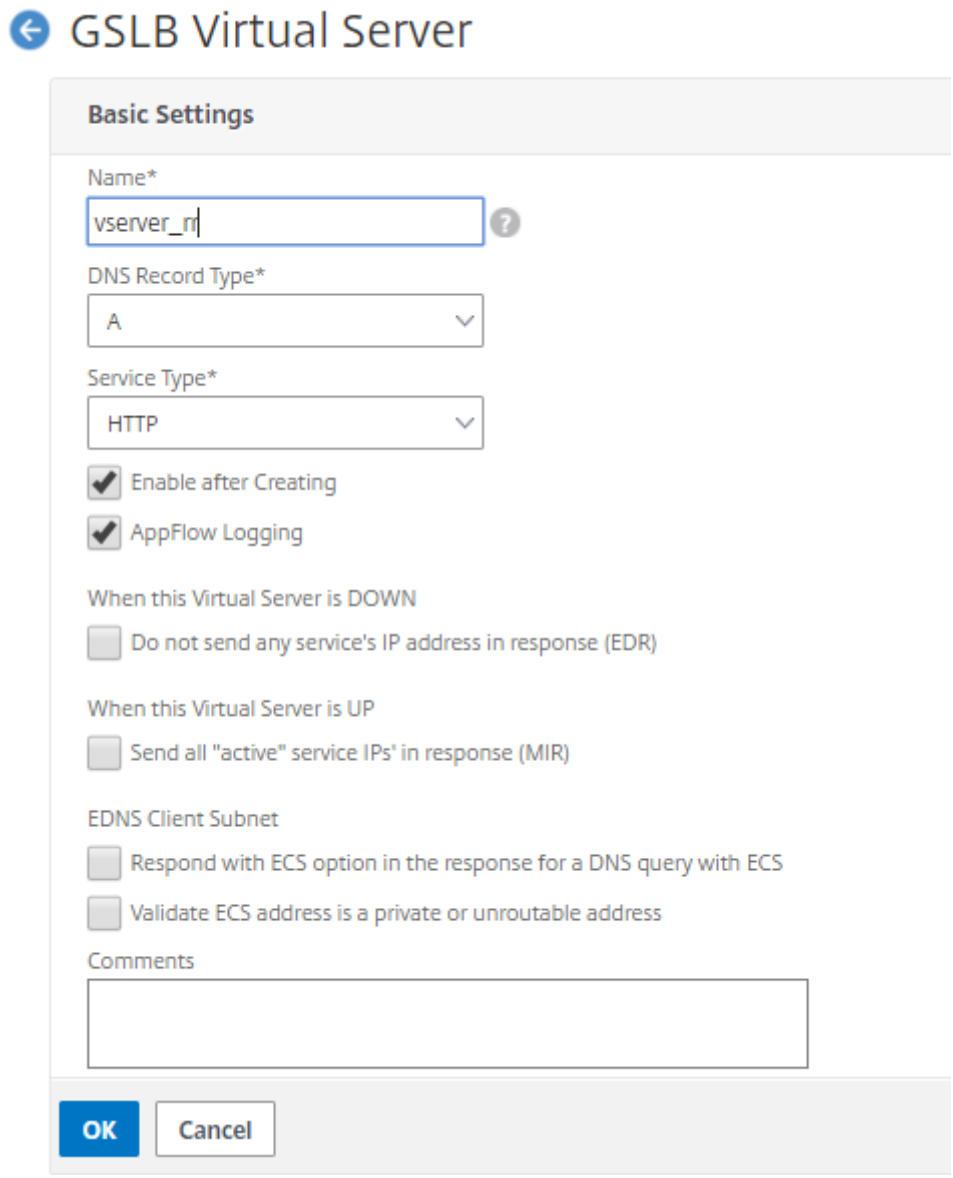
HTTP モニターでバインドすると、次に示すように、サービスの状態が UP になります。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

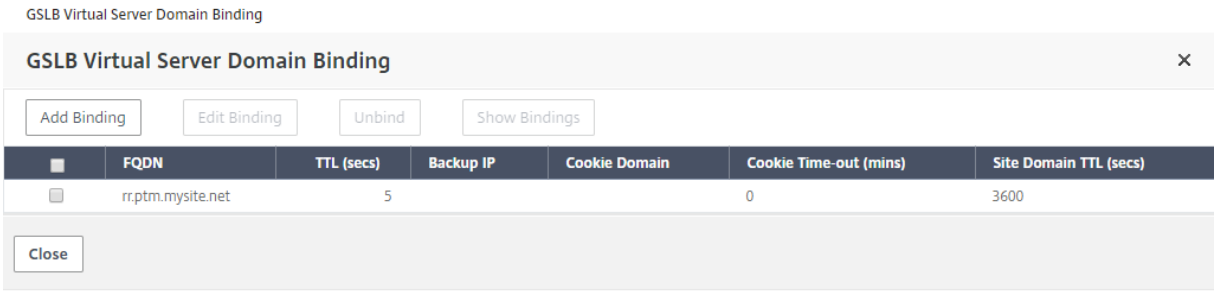
GSLB 仮想サーバーの追加

アプリケーションサーバーのエイリアス GSLB サービスにアクセス可能な GSLB 仮想サーバーを追加します。[設定] タブで、[トラフィック管理] **> [GSLB] > [GSLB** 仮想サーバー] に移動します。次の例に示すように、仮想サーバーを追加します。GSLB サービスとドメイン名をバインドします。



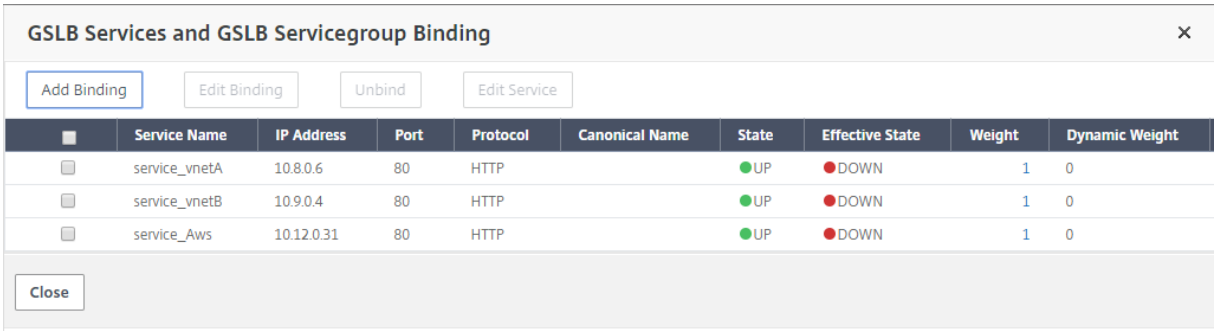
GSLB 仮想サーバーを作成し、適切な負荷分散方法（この場合はラウンドロビン）を選択した後、GSLB サービスとドメインをバインドしてステップを完了します

© 1999–2021 Citrix Systems, Inc. All rights reserved.

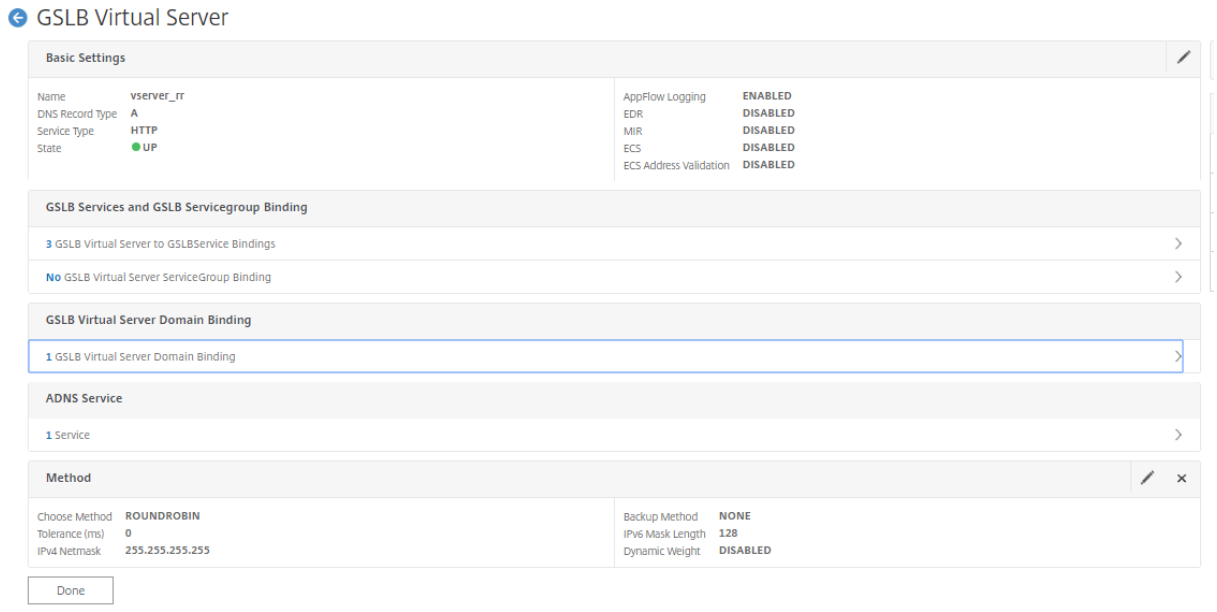


仮想サーバー内の [詳細設定] タブに移動し、[ドメイン] タブを追加してドメインをバインドする

[詳細設定] **>** [サービス] に移動し、矢印をクリックして GSLB サービスをバインドし、3 つのサービス (VNet A、VNet B、オンプレミス) すべてを仮想サーバーにバインドします。

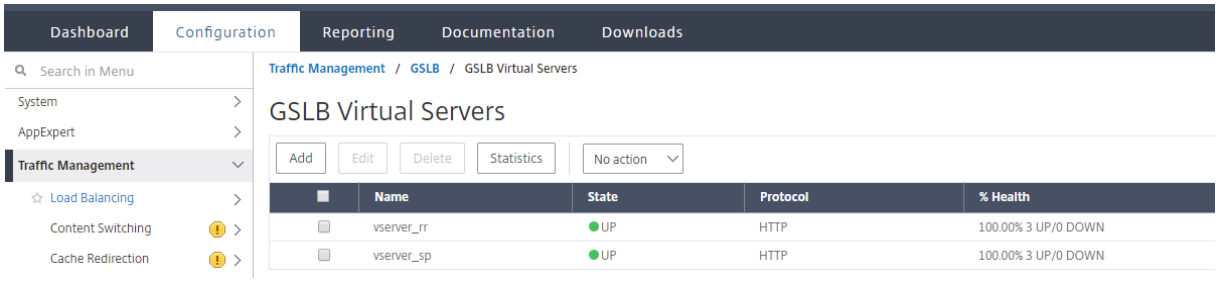


GSLB サービスとドメインを仮想サーバーにバインドすると、次のように表示されます。



GSLB 仮想サーバーが稼働していて、100%正常であるかどうかを確認します。モニターにサーバーが稼働しており、正常であることが示されると、サイトが同期しており、バックエンドサービスが使用可能であることを示します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



展開をテストするには、クラウドクライアントマシンまたはオンプレミスクライアントマシンからドメインURL`rr.ptm.mysite.net`にアクセスします。クラウド Windows クライアントマシンからアクセスすると仮定すると、オンプレミスのアプリケーションサーバーであっても、サードパーティまたはカスタム DNS ソリューションを必要とせずにプライベート DNS ゾーンでアクセスされることがわかります。

結論

主要なアプリケーション配信ソリューションである Citrix ADC は、Azure DNS プライベートゾーンの負荷分散機能と GSLB 機能を提供するのに最適です。Azure DNS プライベートゾーンをサブスクライブすることで、Citrix ADC Global Server Load Balancing（GSLB）のパワーとインテリジェンスを利用して、複数の地域にあるワークロードやデータセンター間でイントラネットトラフィックを分散し、セキュアな VPN トンネルを介して接続することができます。このコラボレーションにより、企業は Azure パブリッククラウドに移行したいワークロードの一部にシームレスにアクセスできます。

Citrix フェデレーション認証サービスのログオン証拠の概要

May 18, 2020

はじめに

Federated Authentication Service（FAS）は Active Directory 証明機関（CA）と統合して、Citrix 環境内でのシームレスなユーザー認証を実現する Citrix コンポーネントです。FAS のアーキテクチャと展開については、「フェデレーション認証サービスのドキュメント」を参照してください。

パスワードやスマートカードを必要とせずに、ユーザーが VDA（または公開アプリ）にシングルサインオンできるように FAS を展開できます。FAS ログオン証拠機能は、Citrix Gateway および StoreFront によって FAS に渡されるログオン証拠を提供します。FAS は証拠を検証して、信頼できる ID プロバイダ（IdP）によって発行されたことを確認できます。

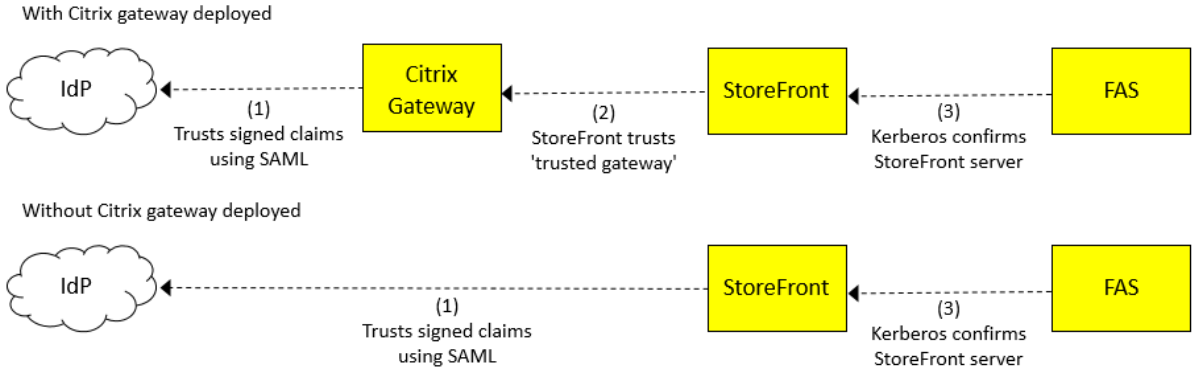
この資料では、FAS ログオン証拠機能を構成する方法について説明します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

概要

FAS トラスト

FAS インフラストラクチャには、Citrix Gateway（NSG)、StoreFront（SF)、FAS の間の「信頼チェーン」が含まれます。各矢印は、信頼するコンポーネントから * 信頼されるコンポーネントを指しています * 。



これらの各コンポーネント間で信頼される重要なデータは、システムにアクセスするユーザーのユーザープリンシパル名 (UPN) です。UPN は、(矢印の反対方向に) リンクを通って流れます。UPN は、システム内を流れるように別の UPN に変換することもできますが、このトピックとは直接関係ありません。

ID プロバイダー (IdP) は、ユーザーが認証する場所です。IdP は、多くの場合、Okta や Azure などのサードパーティ Web サイトです。ユーザーは、認証情報のセット (パスワードやより複雑なものなど) を提供することによって IdP で認証されます。チェーンに沿ったコンポーネントは、コンポーネント間の信頼チェーンのために UPN が本物であることを受け入れます。

信頼は次の方法で確立されます。上の図では、1、2、3 というラベルが付いています。

(1) Citrix Gateway または StoreFront は、署名された要求（ユーザーの UPN を示す要求）を含むプロトコルを使用して IdP を信頼します。信頼する側は、IdP によって行われた要求を検証できます。これは、署名の有効性を確認するために使用する証明書で構成されているためです。検証には、SAML (セキュリティーアサーションマークアップ言語) と OpenID Connect の 2 つの主要なプロトコルが使用されます。ログオン証拠機能は、現在 SAML のみをサポートしています。

(2) この信頼は、信頼される Citrix Gateway の詳細を使用して StoreFront を構成することによって確立されます。これらのコンポーネント間のプロトコル「CitrixAgBasic」を使用すると、StoreFront で、信頼された Citrix Gateway から呼び出されていることを確認できます。

(3) この信頼は Kerberos を使用して確立されます。FAS は、信頼される StoreFront サーバーのリストを使用して構成されます。Kerberos は、呼び出し元の StoreFront サーバーの ID がこのリストに含まれていることを確認するために使用されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

セキュリティ

セキュア認証は、正しく確立された信頼チェーンに依存します。信頼チェーンは、セキュアな認証の信頼のルートである IdP によって提供される証拠を検証することによって強化されます。信頼チェーンを介して FAS に提供されるユーザー資格証明にはユーザー名（UPN）が含まれますが、FAS 自体が検証できる秘密（パスワードなど）は含まれていないため、これは重要です。したがって、パスワードの公開は IdP に限定されます。ほとんどのフェデレーション認証システムは、FAS を含むこの方法で動作します。

ログオンの証拠

FAS ログオン証拠機能は、FAS 展開におけるセキュリティ保証を強化します。これにより、FAS へのアクセスを許可または拒否するルールを定義できます。

ログオン証拠（または単に「証拠」）は、ユーザーの認証時に IdP によって作成されるデータです。このデータは UPN と共に、システム全体に流れます。VDA の起動時に、FAS は証拠が有効であることを確認してから、起動を続行できます。

現在、SAML をサポートする IdP のみがサポートされています。証拠は SAML 応答であり、IdP によって署名された一連のクレームを含む XML ドキュメントです。(IdP は認証の信頼のルートです)。

FAS プラグイン

FAS には、ログオンの証拠が有効であることを確認する機能が組み込まれていません。代わりに、FAS アサーション SDK を使用して独自の FAS プラグインを作成する必要があります。プラグインは、提供された UPN と証拠 (SAML 応答) のチェックを担当します。

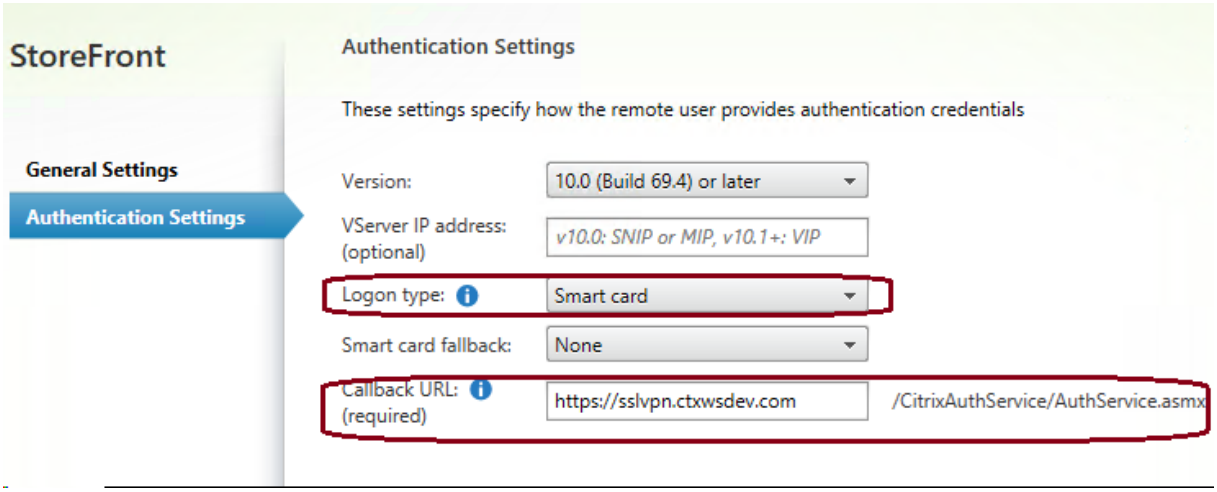
ログオン証拠収集を構成する

手順 **1-**配置を作成する

通常どおり、Citrix Gateway、StoreFront、および FAS を使用して展開を作成します。IdP に対して SAML 認証を使用するように、Citrix Gateway または StoreFront を構成します。

> 重要:
>
> Citrix Gateway を使用している場合は、Citrix Gateway の詳細を使用して StoreFront を構成するときに、コールバック *URL* を構成 する必要があります。これは、ログオン証拠がコールバックを介して送信されるためです。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



ログオンの種類を「スマートカード」に設定することをお勧めします。これにより、ネイティブクライアントが SAML 認証を実行しやすくなります。

配置が正しく機能していることを確認します。つまり、VDA で資格情報の入力を求められずに VDA セッションにログインして起動できることを確認します。

手順 **2-**サンプル **FAS** アサーションプラグインをインストールする

FAS Assertion SDK には、独自のプラグインのベースとして使用できるサンプルプラグインが含まれています。

> 注:
>
> 変更を加えずにサンプルプラグインをインストールすることを強くお勧めします。

プラグインのインストール手順については、FAS アサーション SDK に付属の *Readme.txt* ファイルを参照してください。

手順 **3-FAS** アサーションプラグインが動作していることを確認する

プラグインのインストール後、追加のイベントが FAS サーバーのイベントログの **Windows** ログ**/**アプリケーションセクションに書き込まれます。ログとトレースの説明については、FAS アサーション SDK を参照してください。

手順 **4-Citrix Gateway** で証拠収集を有効にする

認証に Citrix Gateway を使用している場合は、証拠が Citrix Gateway から StoreFront に送信されるように、証拠収集機能を有効にする必要があります。これを行うには、Citrix ADC 管理コンソールを使用して、Gateway サーバーの「SAML レスポンスの保存」オプションを有効にします。「SAML 認証」を参照してください。

手順 **5-StoreFront** で証拠収集を有効にする

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> ログオン証拠を有効にする場合は、FAS サーバー上に FAS アサーションプラグインモジュールを展開する必要があります。

デフォルトでは、StoreFront は FAS に証拠を送信しません（SAML 認証が構成されている場合でも）。StoreFront でログオン証拠の使用を有効にするには、Store という名前のストアに関連付けられた認証サービスで有効にします。

```
Get-Module "Citrix.StoreFront.*  -ListAvailable | Import-Module

$StoreName = "Store" $StoreVirtualPath = "/Citrix/" + $StoreName $store
    = Get-STFStoreService  -VirtualPath $StoreVirtualPath $auth = Get-
   STFAuthenticationService  -StoreService $store

$auth.AuthenticationOptions.CollectFasEvidence = $true

$auth.Save()
<!--NeedCopy-->
```

手順 **6-**サンプル **FAS** アサーションプラグインの変更

サンプルプラグインのスケルトンコードは、証拠を受け入れます。サンプルのコードを更新して、提供されたログオン証拠 (SAML 応答) が有効であることを確認します。

提供された証拠が確認されていることを確認することは、お客様の責任です。次の点を考慮してください。

- SAML クレームに暗号的に有効な署名があるかどうかの確認
- SAML クレームが IdP の証明書で署名されていることの確認
- SAML 要求内の UPN が、表示されている UPN に対応しているかどうかの確認
- 請求が許容可能な期間内に発行されたことを確認する（「許容可能」の判断はお客様次第です）

StoreFront 認証 SDK

StoreFront 認証 SDK を使用して、証拠データの高度なカスタマイズを実行できます。詳しくは、SDK で提供されている、またはhttps://developer-docs.citrix.com/で入手可能なドキュメント「Custom Federated Logon Service Sample 1811.pdf」を参照してください。

関連情報

- Citrix フェデレーション認証サービスのドキュメント
- StoreFront の PowerShell SDK のドキュメント
- https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/の Citrix Federated Authentication Service Assertion SDK

© 1999–2021 Citrix Systems, Inc. All rights reserved.

XenApp および XenDesktop 7.6 用の HDX ポリシーテンプレートを現在のバージョンにアップグレードする

May 18, 2020

XenApp および XenDesktop には、ユーザーへの展開を簡素化する HDX ポリシーテンプレートが含まれています。このドキュメントでは、これらのテンプレートを使用してポリシーを作成する際の設計上の考慮事項について説明します。また、特定のユースケースに適した設定を決定するのに役立つ計画ガイダンスも提供されています。

このドキュメントの対象読者は、HDX の概念、ポリシーテンプレート、製品の以前のバージョンに精通した上級 Citrix 管理者です。

このドキュメントは、XenApp および XenDesktop のポリシーに関する包括的な製品ドキュメントに代わるものではありません。

XenApp および XenDesktop では、製品に付属する組み込みテンプレートと、Citrix サポートサイトから入手できるカスタムテンプレートがサポートされています。このドキュメントでは、組み込みのテンプレートに焦点を当てています。

セキュリティと制御テンプレート

このテンプレートは、XenApp および XenDesktop ktop でデフォルトで有効になっている機能を最小限に抑えるために使用します。このテンプレートには、ユーザーデバイスの

- 印刷します
- クリップボード
- 周辺機器
- ドライブのマッピング
- ポートリダイレクション
- Flash アクセラレーション

セキュリティおよび制御テンプレートを適用すると、より多くの帯域幅が使用され、サーバーあたりのユーザー密度が低下する可能性があります。

高いサーバ拡張性テンプレート

サーバーリソースの浪費を避けるには、このテンプレートを適用します。このテンプレートはユーザーエクスペリエンスとサーバーのスケーラビリティの均衡をとります。単一のサーバー上でホストできるユーザー数を増大させながら、良質のユーザーエクスペリエンスを提供します。とりわけ、このテンプレートは Thinwire 互換モード（ビデオコーデックを使用しない）を有効にし、サーバー側のビデオレンダリングを防止します。

このテンプレートを使用して、サーバーごとに最大のユーザー密度を提供できます。この設計は、Windows 8、Windows 10、Windows Server 2012 R2 などの最新のオペレーティングシステムを実行する VDA を対象として

© 1999–2021 Citrix Systems, Inc. All rights reserved.

います。Citrix では、Windows 7 および Windows Server 2008 R2 用のサフィックス「-レガシー OS」が別個のテンプレートも提供されています。

このテンプレートの機能

グラフィックの圧縮にビデオコーデックを使用不可にします。この変更だけでは、サーバーごとのユーザー密度が向上し、サーバーレンダリンググラフィックスをトレードオフします。ほとんどのユーザーアプリケーションは、サーバーレンダリングのマルチメディア再生エクスペリエンスを低下させながら、この変更の影響を受けません。さらに密度を上げるために、このテンプレートの設定では、サーバーレンダリングのマルチメディア再生がデフォルトの Windows アプリケーションで防止され、Citrix リダイレクトテクノロジは可能な限り許可されます。

このテンプレートの使用方法

ベストプラクティスは、このテンプレートから作成されたポリシーをサーバー内のすべてのユーザーに適用することです。優先度の高いポリシーを目的のユーザーに適用することで、例外を設定できます（異なる印刷設定や Framehawk や DCR などの高度なグラフィックモードなど）。

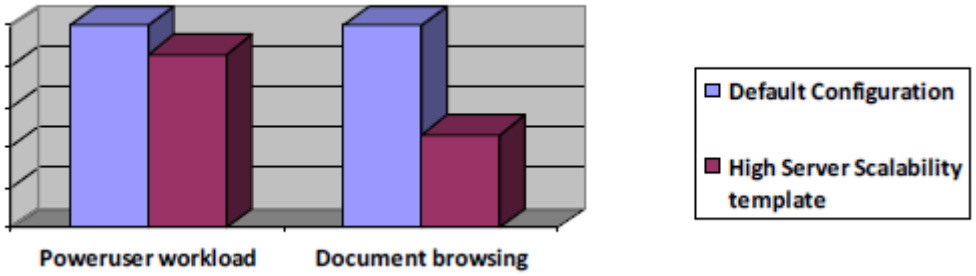
このテンプレートを使用する場合の考慮事項

- このテンプレートから作成されたポリシーを使用して、シンプルなグラフィックタスク作業（オフィススイートなど）を使用するためのクライアント側の前提条件はありません。
- ユーザーへの影響を最小限に抑えてマルチメディア再生リダイレクトに対応するには、最高のマルチメディアリダイレクトをサポートする最新のレシーバーを搭載した Windows または Linux クライアントデバイスを使用します。iOS と Mac では、マルチメディア再生オプションが制限されています。また、ユーザーがデフォルトのアプリケーションとして Internet Explorer と Windows Media Player を持っていることを確認してください。
- ユーザーへの影響を最小限に抑えてマルチメディア再生リダイレクトに対応するには、最高のマルチメディアリダイレクトサポートを提供する最新のレシーバーを搭載した Windows または Linux クライアントデバイスを使用します。iOS および Mac では、マルチメディア再生オプションが制限されています。また、ユーザーがデフォルトのアプリケーションとして Internet Explorer と Windows Media Player を持っていることを確認してください。
- すでに述べたように、サーバーでレンダリングされたマルチメディア再生は、使用するアプリケーションやメディアタイプによって最適でないか、まったく妨げられる可能性があります。
- テンプレートは、デスクトップの壁紙やメニューアニメーションなどのいくつかのパーソナライゼーションやグラフィック効果を無効にします。オペレーティングシステムではより多くの最適化が可能ですが、これは望ましくないスケーラビリティの影響を引き起こす可能性があるため、このテンプレートの設定をテストして比較した後にのみ適用してください。これらの中には、「ドラッグ中にコンテンツを表示する」があり、伝統的にリモートアクセスのシナリオでは無効になっていますが、テンプレートでは有効になっています。これを無効にしても、このテンプレートで使用される Thinwire 互換モードの動作のため、テンプレートの全体的なパフォーマンスは向上しません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- LyncOptimization Pack や Citrix ユニバーサルプリンターサーバーなどの製品の追加により、ユーザーエクスペリエンスが向上し、ユーザー密度が向上する可能性があります。
- サーバーあたりのユーザー密度の増加に加えて、このテンプレートを使用すると、Microsoft Office のような単純な GUI のセッションあたりの必要な帯域幅も減少する可能性があります。
- 印刷は、デフォルトのクライアントプリンターのみをマッピングするように構成され（セッションごとに複数のクライアントプリンターが自動的にマッピングされないようにします）、Citrix ユニバーサルプリンターのドライバーを使用します。両方の設定を実装すると、セッションの確立時および切断時の処理を減らすことができます。
- 場合によっては、デスクトップ構成リダイレクト (DCR) を使用すると、サーバーごとのユーザー密度を向上させることができます。このグラフィックモードは、Windows 7、8、および 8.1 VDA および Windows または Mac 向け Receiver のみと互換性があるため、このテンプレートでは推奨されません。

ハイサーバスケーラビリティテンプレートを使用した場合の **CPU** の節約



VDA：単一セッション 1920x1080、Windows 10 32 ビット、2GB の RAM、2vCPU@3.2GHz

免責事項：これはサンプル比較です。実際の削減額は、ユーザーのワークフローによって異なります。

各テンプレートの説明と考慮事項の後、テンプレートを使用してリソース消費の節約を視覚化するための指標比較が提供されます。これらは、LoginVSI 4.1「パワーユーザー」ワークロードの単一セッションを使用して実施された単純なテストに基づいているため、パフォーマンスのベンチマークとして意図されていません。組織で一般的なワークロードを使用してテストし、その環境に関連するシステムのスケーラビリティを確認してください。

高いサーバ拡張性 ― レガシー **OS**

この高サーバースケーラビリティテンプレートは、Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。

このテンプレートは、Windows 7 および Windows Server 2008 R2 オペレーティングシステムを使用する VDA 上のサーバーあたりのユーザー密度を最大化するために用意されています。これらのオペレーティングシステム用に最適化された従来の Thinwire グラフィックスモードを使用し、XenApp 6.5 および XenDesktop 5.6 と同様の結果を提供します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

このテンプレートの使用方法

レガシーグラフィックモードはマシンポリシーであり、サーバー上のすべてのセッションに適用する必要があります。グラフィック以外の設定（異なる印刷設定など）の例外は、優先度の高いポリシーを目的のユーザーに適用することで実現できます。

このテンプレートの機能

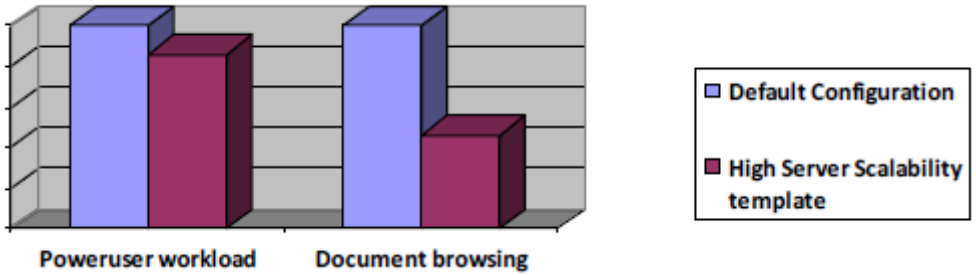
「レガシーグラフィックモード」と「ドラッグ中に内容を表示」を除く他のすべての設定は、ハイサーバースケーラビリティテンプレートと同じです。次の考慮事項から指定されていない限り、すべて同じ考慮事項が適用されます。

Thinwire レガシーモードについて詳しくは、シトリックス製品ドキュメントサイトを参照してください。

このテンプレートを使用する場合の考慮事項

- 管理者は、VDA ソフトウェアラスタライザー（7.x 機能）が無効になっている場合、XenApp 6.5 および XenDesktop 5.6 と同様のユーザーエクスペリエンスとスケーラビリティを期待できます。詳しくは、XenDesktop での 3D アプリケーションディスプレイの互換性を拡げる — ブラックリスト、暫定的な回避策を参照してください。
- 必要に応じて、DCR を使用すると、サーバごとのユーザ密度も向上する可能性があります。

サーバ拡張性が高い場合の **CPU** の節約 **—** レガシー **OS** テンプレート



VDA: 単一セッション 1920x1080、Windows 7 32 ビット、2GB の RAM、2vCPU@3.2GHz

免責事項**:** グラフはサンプル比較です。実際の削減額は、ユーザーのワークフローによって異なります。

WAN テンプレート用に最適化

このテンプレートは、共有 WAN 接続を使用するブランチオフィスのタスクワーカーや、低帯域幅接続のリモートロケーションで、ビデオコンテンツがほとんどない (Thinwire 互換モードに適した) グラフィカルにシンプルなユーザーインターフェイスを持つアプリケーションにアクセスするためのものです。このテンプレートでは、ビデオ再生エクスペリエンスと一部のサーバースケーラビリティが帯域幅の効率性を最適化するため犠牲にされます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

このテンプレートは、グラフィカルにシンプルなユーザーインターフェイスを使用してアプリケーションにアクセスする低帯域幅接続で接続する際のユーザーエクスペリエンスを向上させるために機能します。テンプレート設計は、Windows 10 や Windows Server 2012 R2 などの最新のオペレーティングシステムを実行する VDA 用です。Windows 7 および Windows Server 2008 R2 には、「-レガシー OS」というサフィックスが付いた別のテンプレートが用意されています。

このテンプレートの機能

このテンプレートは、グラフィックの圧縮のためのビデオコーデックの使用を無効にします。この変更は、Office アプリケーションの帯域幅要件を削減するのに非常に効果的ですが、サーバーレンダリングのビデオ品質が低下し、CAD アプリケーションなどのインターフェイスが高度にグラフィカルな場合は、対話性が低下する可能性があります。

このテンプレートでは、Windows Media Layer と Flash の Citrix マルチメディアリダイレクトのすべて（デフォルトで有効になっています）を許可し、使用中の WAN リンクに必要な場合は Windows メディアをオンザフライで最適化できます。

ユーザーがマルチメディアを連続的に表示する場合は、このテンプレートを使用しないでください。その場合は、既定の設定を使用するか、ビデオコーデックを使用して圧縮を有効にしてこのテンプレートをカスタマイズします。

このテンプレートの使用方法

このテンプレートから作成したポリシーは、記載されている WAN リンクを介してユーザーにサービスを提供するデリバリーグループに、またはユーザー単位（高いポリシー優先度）で適用できます。ユーザー接続によってポリシーが決定され、クライアント IP アドレス、NetScaler Gateway のアクセス条件など、使用可能なユーザー設定ポリシーフィルタが使用されます。

このテンプレートを使用する場合の考慮事項

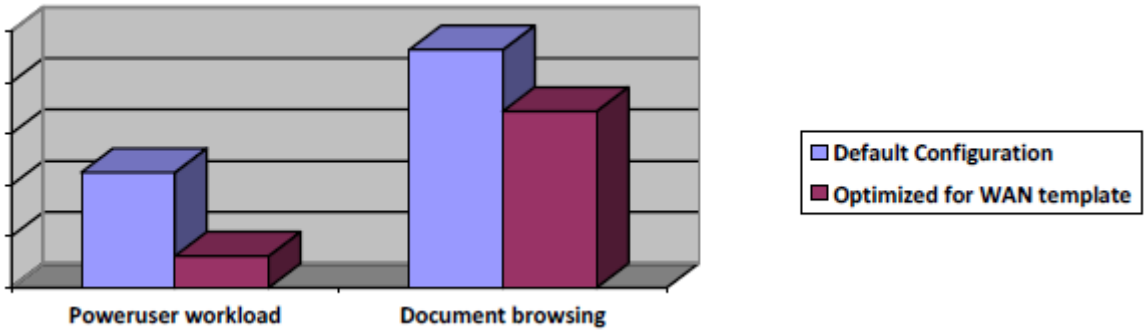
- このテンプレートから作成されたポリシーを使用して、シンプルなグラフィックタスク作業（オフィススイートなど）を使用するためのクライアント側の前提条件はありません。
- このテンプレートを使用すると、ユーザーがマルチメディアコンテンツを連続的に表示することを示している可能性があります。このユーザー行動が受け入れられる場合は、上記の推奨事項を参照してください。
- サーバーでレンダリングされたマルチメディア再生は、フレームレートがターゲット最大 16 に制限されているため、最適ではありません。
- グラデーションの色（スカイラインなど）を持つ複雑なグラフィック画像は、徐々に変化しませんが、テンプレートの「単純なグラフィックの色深度」設定では、ディスプレイの色をピクセルあたり 16 ビットにサブサンプリングして、帯域幅要件を軽減します。
- このテンプレートでは、デスクトップ壁紙やメニューアニメーションなどの個人用設定やグラフィック効果が無効になります。オペレーティングシステムではより多くの最適化が可能ですが、これは望ましくないスケーラビリティの影響を引き起こす可能性があるため、このテンプレートの設定をテストして比較した後にのみ適

© 1999–2021 Citrix Systems, Inc. All rights reserved.

用してください。これらの中には、「ドラッグ中にコンテンツを表示する」があり、伝統的にリモートアクセスのシナリオでは無効になっていますが、テンプレートでは有効になっています。これを無効にしても、このテンプレートで使用される Thinwire 互換モードの動作のため、テンプレートの全体的なパフォーマンスは向上しません。

- LyncOptimization Pack や Citrix ユニバーサルプリンタサーバーなどの製品の追加により、ユーザーエクスペリエンスが向上し、潜在的にユーザー密度が向上します。
- WAN の最適化に加えて、セッションが主に（Microsoft Office など）単純な GUI を持っている場合、このテンプレートを使用すると、サーバーごとのユーザー密度が向上します。
- 印刷は、デフォルトのクライアントプリンターのみをマッピングするように構成され（セッションごとに複数のクライアントプリンターが自動的にマッピングされないようにします）、Citrix ユニバーサルプリンターのドライバーを使用します。テンプレートは両方の設定を実装し、印刷に必要な帯域幅を減らします。
- ユニバーサルプリンタドライバは、すべてのプリンタで有効になっています。プリンターに関係なく、低帯域幅の要件を保証できます。一部のプリンタ固有のドライバおよびプリントサーバーを使用すると、汎用プリンタドライバよりも優れた結果が得られる可能性がありますが、追加の構成やテストが必要なため、一般的な使用には有効化できません。
- プリントサーバーへの直接接続が無効になり、クライアントデバイスに接続されたネットワークプリンターは Citrix 汎用プリンタードライバーを使用して WAN を横切り、クライアントから印刷ジョブをスプールします。これらのアクションは、印刷帯域幅を管理するために行われます（ICA セッション内で最適化されています）。これは、プリンタ固有のドライバが WAN リンク上でどのように動作するかを予測できないためです。
- 制限された帯域幅リンクでは、デスクトップ構成リダイレクト (DCR) は推奨されず、このテンプレートでは無効になっています。

WAN 向けに最適化テンプレートを使用した場合の帯域幅の節約



VDA：単一セッション 1920x1080、Windows 10 32 ビット、2GB の RAM、2vCPU@3.2GHz

免責事項：これはサンプル比較です。実際の削減額は、ユーザーのワークフローによって異なります。

WAN 向けに最適化 **—** レガシー **OS** テンプレート

この WAN の最適化テンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィッ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

クモードに依存します。

このテンプレートは、Windows 7 または Windows Server 2008 R2 などのレガシーオペレーティングシステムに接続する際のユーザーエクスペリエンスを向上させるために機能します。VDA は、低帯域幅接続で、グラフィカルにシンプルなユーザーインターフェイスを持つアプリケーションにアクセスします。従来の Thinwire グラフィックスモードを使用して、XenApp 6.5 および XenDesktop 5.6 と同様の結果が得られます。

このテンプレートの使用方法

レガシーグラフィックモードはマシンポリシーであり、サーバー上のすべてのセッションに適用されます。グラフィック以外の設定 (異なる印刷設定など) に例外を設定するには、優先度の高いポリシーを目的のユーザーにフィルター処理します。

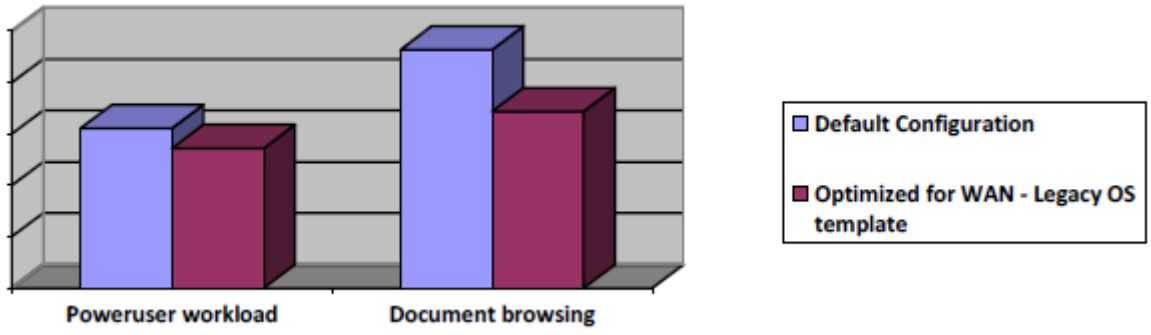
このテンプレートの機能

「従来のグラフィックモード」、「ドラッグ中に内容を表示」、「エクストラカラー圧縮」を除く他のすべての設定は、「WAN 用に最適化」テンプレートと同じです。以下に指定しない限り、そのテンプレートのすべての考慮事項が適用されます。

Thinwire レガシーモードについて詳しくは、Citrix 製品ドキュメントのサイトのグラフィックのポリシー設定を参照してください。

このテンプレートを使用する場合の考慮事項

- 管理者は、XenApp 6.5 および XenDesktop 5.6 と同様のユーザーエクスペリエンスと帯域幅効率を期待できます。



VDA: 単一セッション 1920x1080、Windows 7 32 ビット、2GB の RAM、2vCPU@3.2GHz

免責事項: これはサンプル比較です。実際の削減額は、ユーザーのワークフローによって異なります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

超高精細ユーザーエクスペリエンステンプレート

このテンプレートは、デフォルトの設定を適用してユーザーエクスペリエンスを最大化します。このテンプレートは、複数のポリシーが優先順に処理されるシナリオで使用します。

この製品は、高解像度のユーザーエクスペリエンスを提供するように構成された出荷です。このテンプレートをよく見ると、[高画質] と [最高品質] の印刷を除く既定値が適用され、これらの値が既定よりも大きく設定されます。

このテンプレートを使用するタイミング

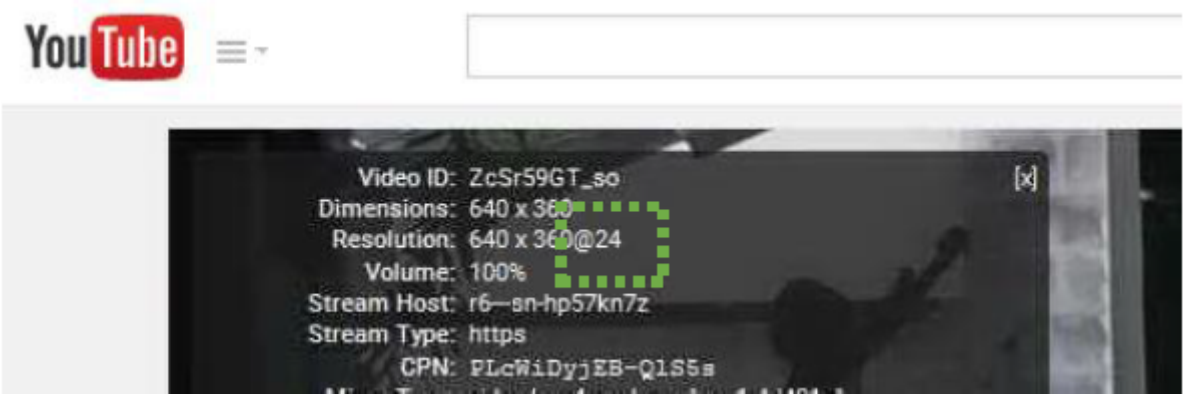
このテンプレートを使用して、作成したポリシーを使用して、ユーザーエクスペリエンスを最大限に高めることができます。このポリシーは、特定のフィルタを持つ他のポリシー（VIP ユーザなど）よりも優先されます。

このテンプレートの使用方法: フィルタを使用してポリシーを作成して適用し、テンプレートから作成された他のポリシーよりも優先度の高いユーザーまたはシナリオを選択します。このポリシーは、サーバースケーラビリティポリシーや WAN など、一般的なユーザーベースで使用できます。

このテンプレートを使用する場合の考慮事項

- クライアントハードウェアと Citrix Receiver の更新が必要です。たとえば、2.0GHz よりも高速な CPU と h.264 のサポート、Receiver for Window 4.x/Mac 11.8/Linux 13.0 が必要です。ユーザーデバイスが要件を満たしていない場合、このテンプレートで作成されたポリシーに悪影響を及ぼす可能性があります。
- 組み込みポリシーの説明で説明したように、このテンプレートを適用すると、より多くの帯域幅が消費され、サーバーあたりのユーザー密度が低下する可能性があります。
- VDA GPU ソリューションを考えてみましょう。グラフィックや過酷な処理ニーズを持つハイエンドユーザーアプリケーションは、GPU の処理能力を活用できるため、パフォーマンスが向上し、場合によってはサーバーのスケーラビリティが向上します。詳しくは、Citrix 製品ドキュメントの「HDX 3D Pro」を参照してください。
- デフォルト構成と同様に、このテンプレートでは、Receiver がサポートしていて有効になっている場合、スクリーングラフィックスの圧縮にビデオコーデック（h.264）を使用できます。画質は、必要に応じてビデオコーデックによって自動的に調整され、「画質設定」は必要ありません。
- 高画質設定は、圧縮からビデオコーデック (h.264) を使用せずにこのテンプレートを使用する場合にのみ適用されます (サーバーごとのユーザー密度を上げるため)。これにより、Thinwire 互換モードと呼ばれるグラフィックスモードになります。管理者は、[圧縮からビデオコーデック] で優先度の高いポリシーを設定するか、またはクライアントがビデオコーデックのサポートを持っていないか、無効にしている場合 (クライアント互換性マトリックスを参照)、これを実現できます。このような状況では、VDA とクライアントデバイスが無制限の広帯域 LAN ネットワークを介して接続する場合のみ、非常に高精細なユーザーエクスペリエンスを得ることができます。
- このテンプレートでは、HD エクスペリエンスを必要とするほとんどのユースケースに適した、Target フレームレート設定の 30 fps も使用しています。デフォルトの 30 fps は、エンドユーザーの HD 画質（デフォルトで 24 ～30 fps）に合わせて調整できる初期ベースラインと見なされます。ハイエンドのグラフィカルおよび GPU 対応アプリケーションを使用しているユーザーは、最大 60fps までの高い値を要求できます)。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



- このテンプレートでは、Windows Media Player および Flash のマルチメディアを Citrix Receiver for Windows/Linux にリダイレクトすることができます。IOS デバイスに対しては Windows Media Player のみリダイレクトできます。クライアントで最新の Citrix Receiver を使用して、最新の機能強化を活用します。
- このテンプレートは、最高の印刷出力品質や使用可能なすべての設定オプションなど、最高のユーザーエクスペリエンスのために印刷を構成します。ユーザーがデバイスに多数のプリンターをインストールし、メーカーのプリンタードライバーがリモート印刷用に最適化されていない場合、帯域幅の使用率が非常に高くなり、サーバーあたりのユーザー密度が低下し、VDA での相互運用性の問題が発生する可能性があります。

付録

テンプレートの詳細なポリシー設定は次のとおりです。

テンプレート	最高品位ユーザーエクスペリエンス	高サーバースケーラビリティ	高いサーバ拡張性 — レガシー OS	WAN の最適化	WAN 向けに最適化 — レガシー OS
帯域幅					
セッション全体の最大帯域幅				0 注：単に設定を公開する	
グラフィック					
従来のグラフィックモード	無効		有効		有効
デスクトップコンポジションリダイレクト				無効	無効
圧縮にビデオコーデックを使用する	使用可能な場合に使用	使用しない	-	使用しない	なし

© 1999–2021 Citrix Systems, Inc. All rights reserved.

テンプレート	最高品位ユーザーエクスペリエンス	高サーバースケーラビリティ	高いサーバ拡張性 — レガシー OS	WAN の最適化	WAN 向けに最適化 — レガシー OS
ターゲットフレーム数	30	16	12	16	16
保持する最低フレーム数	10	8	8	8	8
表示品質	高	中	なし	低	なし
簡素なグラフィックに対する優先的色の解像度	24bpp		なし	16bpp	なし
非可逆圧縮のレベル	なし	なし		なし	高速
許可される最大表示色数	なし	なし		なし	16bpp
エクストラ色圧縮	無効	無効	無効	無効	有効
デスクトップ UI					
デスクトップの壁紙	許可	禁止	禁止	禁止	禁止
ドラッグ中にウィンドウの内容を表示する	許可	許可	禁止	許可	禁止
動的ウィンドウプレビュー	有効			無効	
メニューのアニメーション	許可	禁止	禁止		
マルチメディア					
WAN 接続での Windows Media マルチメディアリダイレクトの最適化		禁止	許可		
ビデオ品質の制限			最大 480P		

© 1999–2021 Citrix Systems, Inc. All rights reserved.

テンプレート	最高品位ユーザーエクスペリエンス	高サーバースケーラビリティ	高いサーバ拡張性 — レガシー OS	WAN の最適化	WAN 向けに最適化 — レガシー OS
Windows メディアフォールバック防止	未構成	クライアントにあるすべてのコンテンツのみを再生			
Flash ビデオフォールバック防止	構成されていません	小さなコンテンツのみ			
Flash ビデオフォールバック防止エラー *.swf		デフォルトのサンプルを適用する（ポリシーを参照）			
マルチメディア会議	許可	禁止			
オーディオ					
オーディオ品質	高品位オーディオ	音声認識に中程度最適化	Low — 低速接続用		
印刷					
クライアントプリンターを自動作成する	すべてのクライアントプリンターを自動作成する	デフォルトのクライアントプリンターのみを自動作成する	デフォルトのクライアントプリンターのみを自動作成する		
ダイレクトコネクションプリントサーバー	有効		無効		
ユニバーサルプリンタードライバーの使用 (UPD)	要求されたドライバが使用できない場合にのみユニバーサル印刷を使用する	ユニバーサル印刷のみを使用する	ユニバーサル印刷のみを使用する		
ユニバーサル印刷品質制限	制限なし		中解像度 (600 DPI)		

© 1999–2021 Citrix Systems, Inc. All rights reserved.

テンプレート	最高品位ユーザーエクスペリエンス	高サーバースケーラビリティ	高いサーバ拡張性 — レガシー OS	WAN の最適化	WAN 向けに最適化 — レガシー OS
ユニバーサル印刷最適化デフォルト	[イメージ圧縮] = [最高品質]、[その他の設定] = 既定値	イメージ圧縮 = 標準品質、その他の設定 = 既定値	[イメージ圧縮] = [品質低下]、[その他の設定] = 既定値		
ファイルリダイレクト					
非同期書き込みを使用する	無効		有効		

> 注:
>
> - 太字の設定は、既定値と同じです。
> - デフォルト値に割り当てられる設定は、スタックポリシーを使用するときに望ましい結果が得られるようにするためです。
> - クロスアウトボックスは、各テンプレートのグラフィックモードに適用できない設定 (その行) を示します。
> - 空のボックスは、その列にテンプレートに特定の推奨がない設定を表します。
> - この表には、すべてのポリシー設定が一覧表示されるわけではなく、組み込みテンプレートで使用されているポリシー設定のみが一覧表示されます。ポリシー一覧については、シトリックス製品ドキュメントWeb サイトを参照してください。

グラフィックス配信に関する考慮事項

圧縮のためのビデオコーデックの薄線使用

XenApp/XenDesktop バージョン 7.6 FP3 では、基本的な Office アプリケーションのようなシンプルなグラフィックスを提供するためのサポートが強化されています。これにより、すでに展開されているネットワークリンク、クライアントデバイス、およびロックダウンされた受信機の寿命を延ばすことができます。宛先

これを実現するため、管理者は Thinwire グラフィックスをエンコードするためにビデオコーデックを使用するタイミングを制御できるようになりました。

デフォルトでは、製品にはビデオコーデックの使用が有効になっていて (利用可能な場合)、ほとんどの一般的な使用シナリオに適しています。

サーバーの高いスケーラビリティが最優先で、*WAN* 向けに最適化（帯域幅制限リンク）が使用されている場合は、ビデオコーデックの使用を無効にすることをお勧めします。ビデオコーデックを使用しない場合、セッションは、最小限の CPU と帯域幅要件で、テキストとシンプルなグラフィックス（ほとんどのビジネスアプリケーションの基盤）の配信を最適化することに集中できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

帯域幅が制限されている場合、サーバーでレンダリングされたビデオのパフォーマンスは最適ではありません。詳しくは、Citrix 製品ドキュメントの「Thinwire 互換モード」を参照してください。

GDI を使用できるレガシーオペレーティングシステム **(Windows 7** および **Windows** サーバー **2008 R2)**

従来のグラフィックモードを有効にすることをお勧めします。従来の Thinwire モードの設計は、従来の Windows オペレーティングシステムのアーキテクチャのためのものであり、多くのユースケースでは、これらのオペレーティングシステムのために最も最適化されたグラフィックスモードが残っています。

ドラッグ中にウィンドウの内容を表示する

以前のリリースでの推奨事項とは異なり、Thinwire 互換モードは、ドラッグ中にウィンドウの内容を表示できる場合に最も効果的です。

従来のグラフィックモードのポリシーを無効にし、圧縮のためのビデオコーデック（h.264）が必要ですが、最大ユーザー密度が望ましいシナリオでスケーラビリティを向上させます。

目標フレームレートと目標最小フレームレート

高サーバースケーラビリティと WAN 向けに最適化（帯域幅制限リンク）テンプレートでは、単純なグラフィックの使用を目的とした場合は、ターゲットのフレームレート設定を 16 または 12 に減らし、ターゲットの最小値を 8 に下げることをお勧めします。これらの設定は、これらのテンプレートの目的の目標を達成するのに役立ちます。

目標フレームレートは 16 を選択しました。これは、人間の目が動きを検出するための絶対最小値であるためです。

VDA とクライアントは、セッション中に配信する適切なフレームレートを継続的にネゴシエートします。一般に、フレームレートは、変更を画面に表示するために必要な最小値に保たれます。高モーションが検出されると、ビデオ再生からウィンドウのドラッグからスクロールまで何でも、セッションはターゲットフレームレートまでのすべての画面変化を配信しようとします。制限された帯域幅接続では、ターゲットのフレームレートを維持できない場合があります。VDA では、画面のグラフィックスの圧縮率を上げてフレームレートを下げてから、ターゲットの最小フレームレートに達するまで圧縮率を上げます（設定不可）。値に設定し、必要に応じてフレームレートをさらに下げます。これは、自動適応型ディスプレイ（以前の Citrix 製品で使用されていた技術）と考えてください。

> **注:** 表示品質を低に設定しても、高コントラストのテキスト (白黒など) には影響せず、高画質で配信されます。

色数

従来のモードとは異なり、XenDesktop および XenApp 7.x スーパーコーデックは色深度を制御できず、ピクセルあたり 24 ビットを受信します。FP3 では、圧縮にビデオコーデックを使用せずに Thinwire の機能強化の一環として、セッショングラフィックを 16 ビット/ピクセルで送信するオプションを追加しました（単純なグラフィックス設定では優先色深度で制御）。このオプションは、単純なグラフィックに必要な帯域幅を減らし、カラーグラデーションを使用する場合にのみ目立ちます。この場合、デバイスではサーバーの CPU 消費量がわずかに高くなる可能性があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

レガシーグラフィックモードの場合、スケーラビリティと WAN のレガシー OS テンプレートでは、「最大許容色深度」の設定も 16 または 12 に制限されています。従来のグラフィックモードを使用する場合、色深度を低く要求したり、他の条件に基づいて配信したりできることに注意してください。

DCR** に関する一言

デスクトップコンポジションリダイレクト（DCR）は、XenDesktop 5.5 で Citrix によって導入されたディスプレイ仮想チャネルです。このテクノロジーには多くの利点がありますが、現在 Windows 7、8、および 8.1 の VDA で利用可能であり、Citrix Receiver のサポートが減少し、主に顧客の採用が少なくなっています。また、DCR は低帯域幅の WAN リンクには推奨されません。このため、FP3 では、この仮想チャネルはデフォルトで無効になっており、Optimized for WAN テンプレートでは手動で無効にします。

HDX グラフィックスモードでの詳細

どのグラフィックスモードが使用されているかを確認する方法については、Citrix Support Knowledge Center の「HDX ディスプレイモードを確認する方法」を参照してください。

マルチメディアに関する考慮事項

すべてのテンプレートおよび製品では、デフォルトでマルチメディア再生のリダイレクトが許可されています。テンプレートで使用される追加設定は次のとおりです。

WAN 接続での **Windows Media** マルチメディアリダイレクトの最適化

デフォルトで許可されているのは、WAN での効率的な配信のためのメディアコンテンツのジャストインタイムトランスコーディングは処理負荷が高いため、High Server Scalability テンプレートでは禁止されています。NVIDIA GPU がサーバーで使用可能になり、「**WAN** 経由の **Windows Media** マルチメディアリダイレクトを最適化するために **GPU** を使用する」設定が有効になっている場合は、処理を GPU にオフロードできます。

ビデオ品質の制限

この設定は、Windows Media マルチメディアリダイレクトの最適化にのみ適用されます。小さな埋め込みビデオプレーヤーに相当する値が、それが使用される「WAN 用に最適化」テンプレートで初期推奨として選択されました。それ以外の場合、この設定は構成されません。

マルチメディア会議

VDA で実行されているユニファイドコミュニケーションまたは会議アプリケーションで使用されるクライアントから Web カメラをリダイレクトすると、必要なサーバーリソースが増加します。この機能は、ハイサーバスケーラビリティテンプレートでは無効です。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

マルチメディアおよび Flash リダイレクトポリシー設定について詳しくは、Citrix 製品マニュアルサイトの以下のトピックを参照してください。

- マルチメディアのポリシー設定
- Flash リダイレクトのポリシー設定

オーディオに関する考慮事項

この製品には、デフォルトの高品質オーディオ (約 128Kbps) が付属しています。この値は、このテンプレートから作成されたポリシーの優先順位が他のポリシーよりも高い場合に、超高精細テンプレートにも適用されます。

次の表に示す値は、オーディオ方向（出力と入力）の個別値です。

テンプレート	非常に高解像度のエクスペリエンスとデフォルト設定	高サーバースケーラビリティ	WAN の最適化
音質設定	高速	中	低
予想される帯域幅	128 キロビット/秒	60 キロビット/秒	44 キロビット/秒

印刷に関する考慮事項

XenApp および XenDesktop には、ほとんどのクライアント接続プリンターで動作できるユニバーサルプリンタードライバーが含まれています。デフォルトでは、VDA は VDA がプリンター固有のドライバーを見つけられない場合にのみこのドライバーを使用します。また、デフォルトでは、クライアント接続のすべてのプリンターがセッションにマッピングされます。

新しい組み込みテンプレートでは、デフォルトとは異なる次の印刷設定が使用されます。

デフォルトのクライアントプリンターのみを自動作成する

高いサーバスケーラビリティと WAN 向けに最適化 — 多くのプリンタではなく、1 つのプリンターを作成することで、両方のシナリオで節約できます。

ユーザーは、セッション中に既定のクライアントプリンターを変更できます。また、マップされたプリンターは、デュアルホップのシナリオでも更新されます。

ユニバーサルプリンター [ドライバー] のみを使用する

高いサーバー拡張性 — VDA が各接続でプリンタードライバーを検索する必要がなくなり、ディスク I/O 操作が節約され、プリンタープリモデルドライバーによるサーバー負荷が軽減されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

WAN 向けに最適化 — ユニバーサルプリンタドライバは、プリンターに関係なく低帯域幅の要件を保証できます。一部のプリンタ固有のドライバおよびプリントサーバーの使用 (追加セットアップが必要) は、汎用プリンタドライバよりも優れた結果が得られる可能性がありますが、追加の構成やテストが必要なため、一般的な使用にはお勧めできません。

プリントサーバーへの直接接続

この設定はデフォルトで有効になっています。クライアントで構成されたネットワークプリンターに、セッションから直接アクセスできます。この設定を有効にすると、ユーザーが使用できるオプション（プリンターによって異なります）が改善され、クライアントデバイスのトラフィックを節約できます。

WAN テンプレート用に最適化されている場合、ネットワークプリンターがユーザーと同じ場所に配置されている可能性が高いため、この設定は無効になります（印刷物を取得する必要があります)。したがって、Citrix ユニバーサルプリンタードライバーを使用して印刷するときに、印刷ジョブサイズが小さくなることを保証できます。さらに、印刷ジョブで使用される帯域幅は、セッション帯域幅の制限に準拠します。

SQL Server と Citrix データベース

May 18, 2020

Microsoft SQL Server は、Citrix Virtual Apps and Desktops の展開において重要なコンポーネントです。Citrix SQL の相互作用の計画と理解は、適切で優れたパフォーマンスを維持するうえで、お客様とお客様の組織にとって非常に有益です。SQL Server の高可用性と十分なコンピューティングリソースが不足していると、Citrix Infrastructure のユーザーエクスペリエンスとアップタイムに悪影響を及ぼします。

データベースの概要

Citrix Virtual Apps and Desktops の展開中に必要な、または作成される 3 つのデータベースがあります。

サイト:（サイト構成とも呼ばれます）は、実行中のサイト構成と、現在のセッション状態、接続、ロード、VDA ステータス情報などの仲介に関連する動的データを格納します。

構成ログ**:(**ログとも呼ばれます) には、サイト構成の変更と管理アクティビティに関する情報が格納されます。このデータベースは、構成ログ機能が有効化（デフォルトは有効）されているときに使用されます。

モニター：セッションや接続情報などのデータを格納するために、Director により使用されます。

以前のバージョンの Citrix Virtual Apps and Desktops（XenApp および XenDesktop 7.6 など）では、Citrix Virtual Apps and Desktops に必要なデータベースは、初期サイトの構成時に（Studio または SQL Server でスクリプトを実行することによって）1 つのデータベースとして作成されています。インストール後、管理者は、パフォーマンスを向上させるために、またはバックアップ/セキュリティのガイドラインに準拠するために、別のデータベースに分割することができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

新しいリリースの Citrix Virtual Apps and Desktops では、サイトの初期構成時、Studio を介して、または SQL Server でスクリプトを実行することによって、データベースを作成できます。データベースは自動的に 3 つの別々のデータベースに分割されます。

大規模な監視データベースがある環境では、監視データベースをサイト構成および構成ログデータベースとは異なるサーバーでホストすることが理想的です。これは、より多くのデータを記録し、変更がより頻繁に発生し、データは他のデータベースほど重要であるとはみなされません。詳しくは、「データベースのサイズ設定ガイダンス」または「VDI ハンドブック」の 97 ページを参照してください。

長期サービスリリース (LTSR) の各累積的な更新プログラム (CU) には、SQL データベーススキーマの修正プログラムが含まれています。たとえば、CTX230536を参照してください。予期しない問題から環境を保護するには、環境を最新の CU に定期的にアップグレードするプロセスがあることを確認してください。また、リソース使用率が高く、空き領域がある障害イベントや問題を検出するために、適切な SQL サーバーとデータベースの監視が行われていることを確認します。

Citrix と **SQL** の相互作用

Citrix Virtual Apps and Desktops ブローカーは、ブローカー通信、構成、監視、および監査データの格納のためのメッセージバスとしてデータベースを使用します。データベースは常時使用されており、SQL サーバー上で大量のコンピューティングリソースを消費する可能性があります。

たとえば、リソースの列挙（ユーザーに表示されるリソース）、リソースの起動、セッションの起動の各段階では、Citrix Delivery Controller が SQL サーバーと対話する必要があります。

列挙： Citrix ADC および StoreFront による認証が成功すると、Delivery Controller は Citrix サイトのデータベースにアクセスして、ユーザーが利用できるアプリケーションを AD 資格情報に基づいて確認します。リソースが識別されると、アプリケーション、デスクトップ、アイコンの名前などの追加情報がデータベースから取得されます。

起動：ユーザーが起動するアプリケーションまたはデスクトップを選択すると、StoreFront によって Delivery Controller への起動要求が開始されます。その後、Delivery Controller は SQL サーバー上のサイトデータベースにアクセスして、ユーザーの送信先となる適切な VDA を選択します。

セッションの初期化：セッションの起動後、VDA は Delivery Controller と通信し、セッション情報をサイトデータベースに書き込みます。

データベースの推奨事項

SQL Server の停止が Citrix Virtual Apps and Desktops のインフラストラクチャへの影響を最小限に抑えるため、Citrix がサポートする以下の高可用性オプションから選択できます。

- AlwaysOn 可用性グループ
- AlwaysOn フェイルオーバークラスタリング
- 基本可用性グループ
- Hypervisor の高可用性 *

© 1999–2021 Citrix Systems, Inc. All rights reserved.

> 注:
>
> Citrix は Hypervisor の高可用性をサポートしていますが、稼働時間が最も重要である EHR アプリケーションをホストする環境では使用することはお勧めしません。

Citrix と Epic では、エンドユーザーセッションの確立に構成ログとデータベースの可用性の監視は必要ありませんが、3 つのデータベースすべてで同じ高可用性アプローチを使用することをお勧めします。たとえば、SQL Always-On 可用性グループを HA 戦略として使用する場合は、これを 3 つのデータベースオブジェクトすべてに使用します。

また、Citrix データベース自体、特にサイトデータベースの完全バックアップを毎日実行することをお勧めします。保存期間は組織の要件によって異なりますが、通常、7 日間のフルバックアップと少なくとも 1 か月分の週単位のバックアップを維持します。トランザクションログのバックアップスケジュールは、組織の標準と、割り当てる必要がある使用可能なストレージの量に対するトランザクションログの増加率の組み合わせに基づいて作成する必要があります。SQL サーバーで利用可能なストレージを監視してください。

Citrix データベースのリカバリモデルを、使用している高可用性アプローチの要件に合わせます。

Microsoft の推奨事項では、インデックスを維持するために、お客様のセットアップメンテナンスプランを毎晩および毎週実行することをお勧めします。保守計画は、単に週に夜間にインデックスを再編成し、週末にインデックスを再構築することです。

この推奨事項により、特に大規模な監視データベースの場合、今日の操作中に大きなインデックスを再構築することによるパフォーマンスへの影響を回避できます。

Microsoft では、断片化が 30% を超える場合はインデックスを再構築し、30% 未満の場合は再編成することをお勧めしています。詳しくは、「データベースのメンテナンス」セクションを参照してください。

ローカルホストキャッシュ

データベースが使用できなくなるシナリオを考慮するため、Citrix はローカルホストキャッシュ（LHC）機能を Citrix Virtual Apps and Desktops 7.x プラットフォーム（7.12 以降、XenApp および XenDesktop 7.15 LTSR を含む）に追加しました。このオプションを有効にすると、Delivery Controller と Citrix サイト構成データベース間の通信が中断された場合に、公開アプリケーションのユーザーが接続できるようになります。SQL が、常時オン、ミラーリング、クラスタリングなどの高可用性アーキテクチャで構成されている場合、この機能により、SQL の完全停止が発生したり、ネットワーク接続が中断されたりしたときに、フォールトトレランスがさらに高くなります。

SQL の停止中はサイト管理機能を使用できず、フェイルオーバープロセスが瞬時に行われないため、これは SQL 高可用性の代替とは見なされません。SQL が停止した場合、仲介機能は LHC に移行し、VDA が再登録されるまで失われます。このシナリオは、SQL の接続性/可用性が復元されたときに、通常の操作モードに戻るときにも発生します。

ローカルホストキャッシュは、すべての Delivery Controller 上のローカル SQL Express LocalDB データベースに静的サイトデータのコピーを保持し、データベースの停止中もこのデータを利用して、VDA 登録とセッション仲介要求を継続的にサポートします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ローカルホストキャッシュの設計上の考慮事項

Epic Community Member の展開のサイズはさまざまであるため、Citrix と緊密に協力して、LHC を利用するために必要な追加のリソースを特定することをお勧めします。

- スケーラビリティに関する注意事項
  - XenApp および XenDesktop 7.15 の LHC に関する文書化された最大制限は、シングルゾーンでは 10,000 の VDA、マルチゾーン展開では 40,000 の VDA です。Citrix Virtual Apps 環境では、LHC とゾーンのスケーラビリティはログオン速度とユーザー数に依存します。したがって、環境で観察される実際のスケーラビリティは、公開された最大値よりも低くなる可能性があります。このアーキテクチャでは、予想されるセッション数が 10,000 を超えたり、ログオンレートが 1 秒あたり 10 ユーザーを超えたりする場合は、追加のゾーンを検討することをお勧めします。
- Delivery Controller のサイズ設定：LHC が有効な場合、ゾーンごとに選択されたプライマリ Delivery Controller（DC）がすべての VDA 登録、列挙、起動、および更新を処理します。
  - RAM: ローカルホストキャッシュサービスは、停止の期間と停止中のユーザーの起動回数に応じて、2 GB の RAM を消費する可能性があります。
  - CPU: 選出された DC の CPU 負荷が増えるため、補うために余分なコアを考慮する必要があります。

  Controller の CPU 構成、特に SQL Server Express LocalDB が利用できるコア数は、メモリ割り当て以上に、ローカルホストキャッシュのパフォーマンスに直接影響を及ぼします。この CPU オーバーヘッドが発生するのは、データベースとの接続が失われ、High Availability Service がアクティブである停止状態の間だけです。

  LocalDB は複数のコア（最大 4 個）を使用できますが、単一のソケットに制限されています。たとえば、ソケットをそれぞれ 1 コアを持つ 4 つのソケットを持つように追加しても、パフォーマンスは向上しません。それよりも複数のコアを持つ複数のソケットの使用をお勧めします。Citrix のテストでは、2x3（2 つのソケット、3 つのコア）の構成が、4x1 および 6x1 の構成より良好なパフォーマンスを示しました。
- ストレージ: ローカルホストキャッシュモードでは、ストレージ使用率は 2 ～3 分ごとに約 1 MB 増加します。1 秒あたりの平均ログオン数は 10 と仮定します。ストレージ消費量は、ログオン率に比例して増加します。詳しくは、「ローカルホストキャッシュ」の記事を参照してください。

データベース停止の影響

データベース全体の停止が発生した場合、Delivery Controller の重要な機能のほとんどが影響を受け、推奨される SQL HA 戦略の 1 つを設計および実装することの重要性が強調されます。次の表では、これらの効果について説明します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

コンポーネント	データベース停止の影響
サイト構成データベース	ユーザーは、仮想デスクトップに接続または再接続できません。注**:** ローカルホストキャッシュ (LHC) を使用すると、ホストされている共有デスクトップ、ホストされている Windows およびブラウザアプリケーション、および個人用デスクトップを持つユーザーは、サイトデータベースが使用できない場合でも、アプリケーションおよびデスクトップに再接続できます。LHC モードの場合、監視データは収集されず、サイトの設定変更はできません。
監視データベース	Director には履歴データが表示されず、Studio を起動できません。受信したユーザー要求と既存のユーザーセッションの仲介は影響を受けません。
構成ログデータベース	[Citrix Virtual Apps and Desktops] のログ設定で [データベースの切断時に変更を許可する] が有効になっている場合、構成ログデータベースの停止は影響を受けません（構成変更がログに記録されない場合を除く）。そうしないと、管理者は Citrix Virtual Apps and Desktops に変更を加えることができません。

SQL サイジングの推奨事項

環境のパフォーマンスと安定性を確保するために、SQL Server のサイズを正しく設定する必要があります。すべての Citrix 製品では異なる方法で SQL Server を使用し、お客様ごとに異なる使用パターンがあるため、一般的なサイズに関する推奨事項は提供できません。代わりに、製品ごとの SQL Server のサイジングに関する推奨事項を以下に示します。また、展開時にパフォーマンスを慎重に監視して、サイジングの前提を検証する必要があります。

Citrix 関連データベースのみをホストする SQL 環境の場合、最大 10,000 人のユーザーに対して最低 4vCPU と 8GB の RAM を SQL サーバーにプロビジョニングする必要があります。大規模な展開または高いログオンレートの展開では、最低 8 vCPU および 16 GB の RAM を使用することをお勧めします。Citrix Virtual Apps and Desktops 7.x の展開における SQL データベースのサイズ設定の概念について詳しくは、データベースのサイズ設定を参照してください。この資料には、予想されるトランザクションログの増加率など、ワークロードの特性に関する情報も含まれています。

監視データベースのサイズは、データ保持の設定によって異なることに注意してください。XenApp および XenDesktop 7.15 LTSR には、詳細な VDA パフォーマンスデータをキャプチャする機能を追加した後、7.6 LTSR よりも多くのオプションがあります。これらの設定の構成について詳しくは、「「監視のポリシー設定」」を参照してください。これをデータベースサイジング計算で考慮してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

CU の更新と修正

Citrix は年に数回、Citrix Virtual Apps and Desktops LTSR 用の CU をリリースします。これらの CU には、セキュリティ更新プログラムとバグ修正のみが含まれており、新機能は導入されていません。製品で特定された問題を解決するため、最新の CU を実行することをお勧めします。これらの修正の一部は SQL に関連しています。Citrix またはお客様によって特定されたロック、デッドロック、ストア手順などの問題に対処します。たとえば、XenApp 7.6 の CU5 まで、多くの SQL 関連の修正が行われています。推奨されるのは、各 CU の「解決済みの問題」セクションを確認し、ページ内の **SQL** を検索することです。

- The connection between the Delivery Controller and the SQL Server might be lost intermittently due to a deadlock in the SQL database. [#LC8477]

> 注:
>
> は、7.6 キュー 5 および 7.17 でリリースされました。

その他の参考ドキュメント

- XenApp および XenDesktop 7.15 LTSR
- VDI ハンドブック
- Citrix データベースのサイジング
- Citrix ローカルホストキャッシュ

Contributed by Henry Vernov, Principal System Engineer.

XenApp および XenDesktop のグループポリシー管理テンプレートの更新

May 18, 2020

テンプレートは、事前定義された開始ポイントからポリシーを作成するためのソースです。これらのファイルは、インポートまたはエクスポートできます。組み込み Citrix テンプレートは、特定の環境またはネットワーク状況に対して最適化され、次のように使用できます。

- サイト間で共有する独自のポリシーとテンプレートを作成するためのソース。
- 結果を引用できるため、展開環境間で結果をより簡単に比較するためのリファレンス。例: “…when using Citrix template x or y…”
- テンプレートをインポートまたはエクスポートすることにより、Citrix サポートまたは信頼するサードパーティとポリシーを通信するための手段。

この記事について

この文書には、XenApp および XenDesktop グループポリシー管理パッケージに組み込まれた Citrix テンプレートの追加テンプレートと更新をダウンロードするためのリンクが含まれています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix が提供するテンプレートは、Citrix Studio および GPO エディター（グループポリシー管理パッケージのインストール後）でも見つかりますが、インストーラパッケージに含まれないシナリオのアップデートとテンプレートをすばやく提供できるようにしたいと考えています。

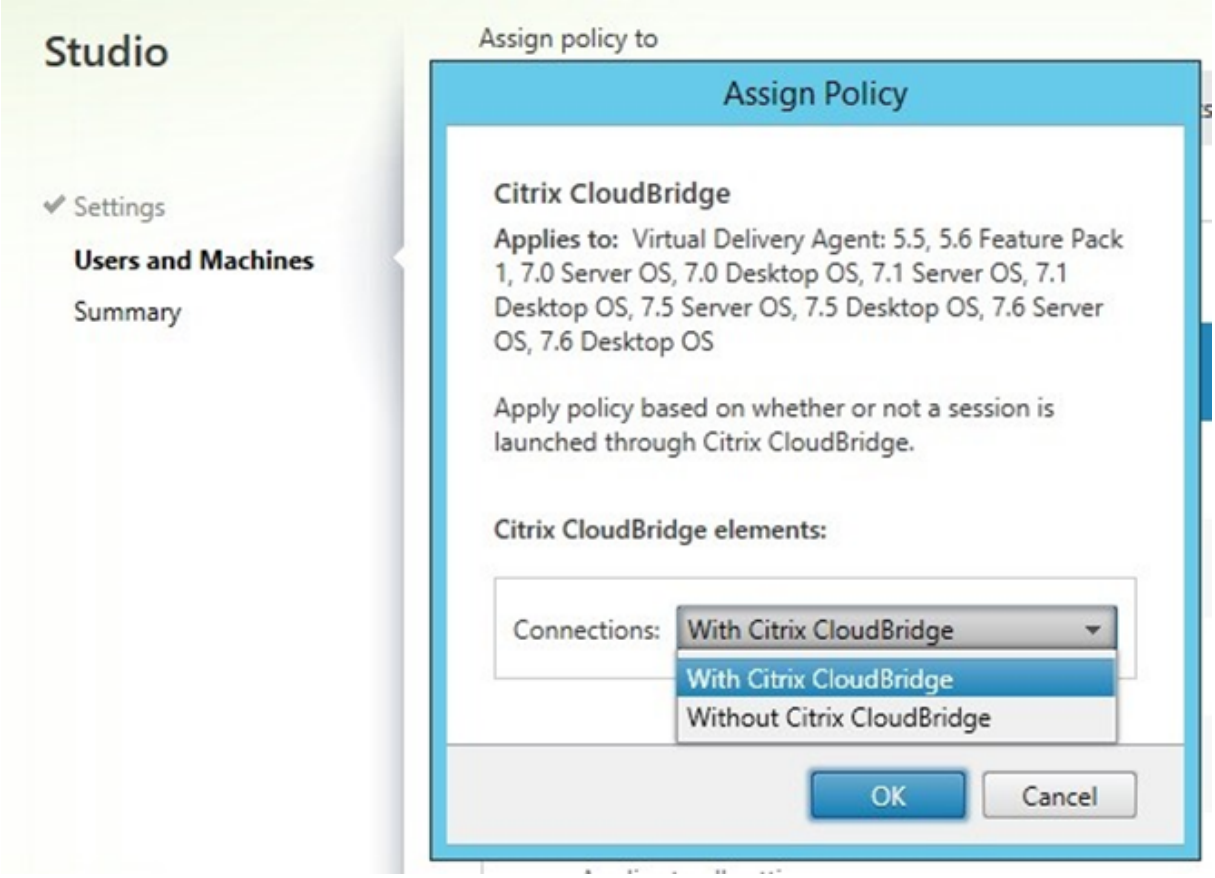
この記事のテンプレートは、特に指定がない限り、最新バージョンの XenApp および XenDesktop で使用してください。名前と説明は英語ですが、インポートして他の言語で使用できます。

テンプレート

クラウドブリッジ

このテンプレートは、CloudBridge WAN アクセラレーションの利点を最大限に活用するように設計された組み込み Citrix テンプレートのアップデートです。XenApp および XenDesktop ktop がクライアントと VDA 間のパスで CloudBridge WAN アクセラレーションデバイスの利点を最大限に活用できるようにする設定を構成します。

このテンプレートは、「Wwith Citrix CloudBridge」ポリシーフィルターを使用して存在する CloudBridge とのセッションに特化して割り当てることができます。これにより、CloudBridge やその他の接続で異なるポリシー設定を使用できます。



- テンプレートをダウンロードする
  注：インポート後、カスタムテンプレートとして表示されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Receiver for Chrome

このテンプレートは、Chromebook エンドポイントからのセッションに排他的または特別な影響を与えるいくつかのポリシー設定を公開します。

- テンプレートをダウンロードする

Citrix Receiver for HTML5

このテンプレートには、Citrix Receiver for HTML5 を使用するセッションに適用可能な設定が含まれています。このバージョンの Citrix Receiver では、XenApp および XenDesktop ktop のデフォルトインストールでは無効になっているため、WebSocket を有効にする必要があります。

- テンプレートをダウンロードする

信頼性の低いネットワークにおけるユーザーエクスペリエンスの向上

このテンプレートは、Framehawk UDP ベースのグラフィックスプロトコルを有効にし、これらのセッションに排他的または特別な影響を与える利用可能なポリシー設定の一部を公開します。

- テンプレートをダウンロードする

パススルー（デュアルホップ）アプリケーションセッション

管理対象/プール/RDS でホストされる仮想デスクトップ環境では、XenApp へのパススルーセッションを使用して、デスクトップイメージにないアプリケーションをユーザーに提供するのが一般的です。このテンプレートは、デスクトップにアプリケーションを提供する XenApp 展開用です。

これにより、アプリケーションセッションサーバーの CPU 使用率が低下すると同時に、デスクトップセッションがクライアントエンドポイントデバイスへの配信を最適化できるようになります。これを実現するには、グラフィックスの圧縮用にビデオコーデックを無効にし、圧縮されたグラフィックスをアプリケーションからデスクトップに配信します。

重要**:** このテンプレートを使用すると、アプリケーションとデスクトップ間のトラフィックが増加します。

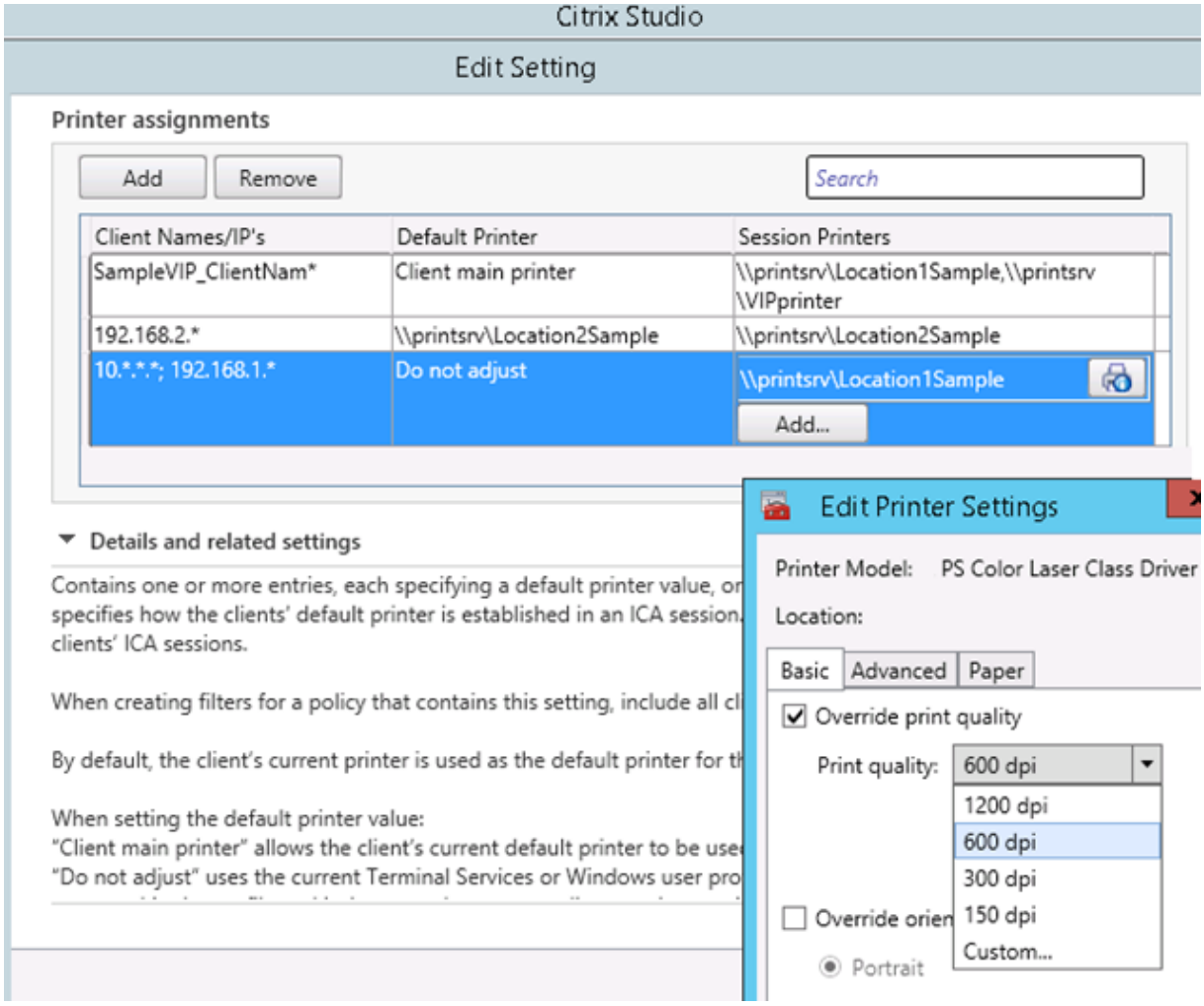
- テンプレートをダウンロードする

Citrix ユニバーサルプリントサーバー

これは、Citrix ユニバーサルプリントサーバーの展開を構成するための開始点として使用するように設計されたサンプルテンプレートです。このポリシーでは、VDA 管理者が以前にインストールした場合は、プリンター固有のドライバーを使用できます。インストールされていない場合は、Citrix ユニバーサルプリンタードライバーが使用されます。また、サンプルプリンタの割り当て (セッションプリンタと既定のプリンタ設定の新しい代替) も一覧表示されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

この割り当ては、展開に適したものに置き換える必要があります。このテンプレートは、適切な構成のためにプリンターへのドメインアクセスが必要です。



- テンプレートをダウンロードする

以前のバージョンのテンプレート

次のリンクには、7.6FP3 より前のバージョンのテンプレートが含まれています。これらのテンプレートは、インポート時にカスタムテンプレートとして表示されます。

- テンプレートをダウンロードする

免責

上記のサンプルおよびダウンロードしたポリシーテンプレート (サンプルコード) は、現状のまま提供されます。いかなる表明、保証、条件も一切ありません。利用者は、自己の責任において使用、変更、配布することができます。Citrix は、商品性、特定用途に対する適合性、資格、非侵害性に関するあらゆる保証を含む、明示、黙示、書面、口

© 1999–2021 Citrix Systems, Inc. All rights reserved.

頭、法定によるいかなる保証も一切付与しません。上記の一般性を制限することなく、お客様は、(a) サンプルコードにエラー、設計上の欠陥、その他の問題があり、結果としてデータの損失や財産の損傷、(b) サンプルコードを完全に機能させることができない場合があり、(c) Citrix は予告なしにまたはお客様への責任、現在のバージョンおよび/または将来のバージョンのサンプルコードの利用を停止します。いかなる場合でも、このコードは、生命維持関連または爆発物関連の作業を含む、ただしそれに限定されない、極度に危険な作業に使用すべきではありません。CITRIX 社およびその関連会社または代理人は、契約違反またはその他の責任理論に基づき、直接的、特別、付随的、懲罰的、結果的またはその他の損害を含むがこれに限定されないが、サンプルコードの使用に起因するいかなる損害（ただし、これらに限定されない）について、一切の責任を負いません。そのような損害の可能性。コードの著作権は Citrix に属しますが、コードの配布には Citrix の著作権属性ではなく、独自の標準の著作権属性のみを含める必要があります。ユーザーは、ユーザーによるこのコードの使用、変更、配布により生じたいかなる申し立てに対しても、Citrix を免責し、Citrix を弁護することに同意します。

* この記事は、Citrix サポートナレッジセンターに掲載されていました。

XenApp および XenDesktop 7.11 から現在のバージョンまで：遅延および SQL ブロッキングクエリの改善

May 18, 2020

遅延を伴う仲介のパフォーマンス情報は、この記事XenApp および XenDesktop 7.7：ゾーン、遅延、および仲介のパフォーマンスに記載されています。この記事では、XenApp および XenDesktop 7.11 からの遅延との仲介に関する改善点について説明します。また、VDA 登録時のデッドロックを防止するための機能強化についても説明します。

遅延の改善による仲介の改善

XenApp および XenDesktop 7.11 では、コア仲介 SQL コードを再確認しました。このコードでは、ロードが最も少ない VDA を特定し、その VDA に起動リクエストを送信します。「完璧な」負荷分散アルゴリズムから「十分に良い」負荷分散アルゴリズムに切り替えることにしました。

XenApp および XenDesktop 7.11 より前のバージョンでは、最小負荷の VDA が検索され、その VDA が使用可能になるまで他の起動要求がロックまたはブロックされました。これにより、他のすべての仲介要求がブロックされました。

XenApp および XenDesktop 7.11 では、現在ロックされていない最も負荷の低いワーカーが検索されます。つまり、最も負荷の少ないワーカー（おそらく 2 番目または 3 番目に負荷の少ないワーカー）を取得することはできませんが、他のすべての起動要求をロックすることなくこれを行うことができます。ロック解除された労働者が見つからない場合は、座ってロックを待ちます。十分な VDA があれば、すべての VDA を同時にロックすることはまれですが、その動作は以前のアルゴリズムと同じです。

一部のシナリオでは、管理者は負荷分散のわずかな違いに気づくかもしれませんが、最も負荷の低い VDA を使用しないことに注意する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

コア仲介コードには、SQL ブロッキングの問題が改善された他の場所があります。大規模なサイトでは、7.13 または 7.6 CU3 ブローカーを使用して、現在知られているすべての機能強化を行うことをお勧めします。

パフォーマンス結果

次の表は、前の記事内のデータに 2 つのデータポイントを追加し、遅延の改善による仲介を示します。

製品バージョン	**7.7**	**7.11** 以降	**7.7**	**7.7**	**7.11** 以降
待ち時間（ミリ秒）	90	90	250	250	250
コンカレント要求	48	48	36	48	48
平均応答時間	12.9	3.7	26.7	-	7.6
1 秒あたりのブローカー要求数	3.7	12.6	1.3	-	6.3
エラー (%)	0	0	4.6	42.8	0
10,000 人のユーザーを起動するまでの時間	4 時間 55 秒	所要時間 8 時間	2 時間 03 分	なし	所要時間 6 時間

250 ミリ秒の遅延でわかるように、XenApp および XenDesktop 7.11 は、90 ミリ秒の 7.7 コードよりも優れたパフォーマンスを発揮するようになりました。したがって、多くのデータポイントのテストに時間を費やすのではなく、以前に失敗したものをテストしました。7.11 以降では、ブローカーと SQL Server 間の遅延があっても、リソースの仲介が速くなることがわかります。

LTSR 7.6 CU3 コントローラをご利用のお客様は、同様の改善の恩恵を受けることができます。LTSR 7.6 CU3 がレイテンシーとともに展開されるとは思っていませんが、これらの変更により、レイテンシーがなくてもパフォーマンスが向上します。また、LTSR 7.6 CU3 がレイテンシーで導入されているお客様もいることがわかっています。

登録ストームのシリアル化

残念ながら、ロックがあることがわかっている領域は VDA 登録です。ロックの理由は、ワーカーを登録するときにデッドロックを避けるためです。これで、複数の登録スレッドにわたって一貫した順序でワーカーのセッションをロックしないため、デッドロックの原因をよりよく理解できるようになりました。セッション ID でセッションロックを行い、VDA 登録のデッドロックを停止します。

この動作の変更を内部でテストし、再登録スケールのテストでいくつかの問題を解決するのに役立つことがわかりました。ただし、非常に複雑な環境を使用しているお客様もいるため、このロックを完全に削除していないため、より多くのテストに時間をかけることができます。代わりに、我々は、XenApp と XenDesktop ktop を持つお客様

© 1999–2021 Citrix Systems, Inc. All rights reserved.

のために、このロックの使用に調整可能を提供してきました 7.12 以降. この調整可能な設定は、XenApp および XenDesktop 7.12 データベースの「chb_Config.Site」テーブルにあります。

```
    select SerializeMultiSessionAudits,
       SerializeMultiSessionDeregistrations from chb_config.Site

    SerializeMultiSessionAudits SerializeMultiSessionDeregistrations

    --------------------------- -----------------------------------

    1 1
<!--NeedCopy-->
```

これらのフラグを 0 に設定すると、ロックの使用が解除されます。

```
    update chb_config.Site set SerializeMultiSessionAudits=0,
       SerializeMultiSessionDeregistrations=0

    select SerializeMultiSessionAudits,
       SerializeMultiSessionDeregistrations from chb_config.Site

    (1 row(s) affected)

    SerializeMultiSessionAudits SerializeMultiSessionDeregistrations

    --------------------------- -----------------------------------

    0 0

<!--NeedCopy-->
```

XenApp および XenDesktop 7.15 以降、このロックはデフォルトで無効になっています。また、XenApp および XenDesktop 7.15 以降にアップグレードすると、ロックが無効になります。調整可能は、ロックを再度有効にする必要があるお客様向けに提供されます。

この記事は、Chris Gilbert によって書かれたブログ記事から変更されました。元のブログを読み、コメントを表示するには、*https://www.citrix.com/blogs/2017/03/06/latency-and-sql-blocking-query-improvements/*にアクセスしてください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

XenApp および XenDesktop ktop バージョン 7.6 のデータベースサイズ設定ガイダンス

May 18, 2020

免責

このドキュメントには、Citrix 以外の関係者が管理する Web サイトへのリンクが含まれています。Citrix は、これらの第三者のウェブサイトのコンテンツまたは使用について責任を負わず、いかなる責任も負いません。Citrix は、これらのリンクをお客様に提供することを目的としてのみ提供しており、リンクを含めることは、Citrix がリンク先のウェブサイトを推奨することを意味するものではありません。お客様の責任の下で、お客様が使用する Web サイトにコンピューターウィルスやそのほかの破壊的な問題がないことを確認してください。

概要

一般的な XenDesktop 7 の展開環境は、次の 3 つのデータベースで構成されます。

- サイト構成データベース XenDesktop 展開環境の現在の構成と状態を保存します。
- データベースの監視 Director 内に表示する履歴データを格納する
- 構成ログデータベース XenDesktop 展開環境に対する構成変更を追跡する

既定では、構成ログと監視データベース (セカンダリデータベース) は、サイト構成データベースと同じサーバーにあります。初期状態では、これらのデータベースに同じ名前が設定されます。サイトを作成した後で、セカンダリデータベースの場所を変更することをお勧めします。

一般的な展開では、SQL Server によって提供される一時データベース TempDB も使用します。

各データベースは、異なる目的を果たし、異なる速度で成長します。

このドキュメントでは、各データベースに関する情報と、XenDesktop 7 をサポートするようにデータベースのサイズを設定する際に考慮すべき主な考慮事項について説明します。

注：提供されるすべての数字は推定値です。展開間のバリエーションが予想されます。

このドキュメントでは、ホストされた共有デスクトップ (HSD) と仮想デスクトップインフラストラクチャ (VDI) のサイズ設定の違いについても説明します。混在環境では、2 つのデスクトップタイプの推定値を組み合わせて、データベース全体のサイズの見積もりを生成する必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ドキュメント **XenDesktop** 点

このドキュメントは、7.6 XenDesktop をカバーするように拡張されました。これは、7.6 で追加された機能のサイズ変更に関する更新を可能にするためです。データベースのサイジングに影響する 3 つの新機能は次のとおりです。

- 接続リース — 圧縮されたリースファイルは、サイトデータベースに格納されます。
- アプリケーション使用率の監視 — 環境内で使用されるすべてのアプリケーションの詳細が監視データベースに格納されます。
- 修正プログラムインベントリの監視 — 環境内のコントローラー、VDA、および VDA イメージに適用される Citrix 修正プログラムの詳細

テーブルサイズに関する情報が以下で更新されました。7.6 から 7.5 では、1 秒あたりのトランザクションとトランザクションログの増加が類似していることがわかりました。そのため、これらのセクションは更新されませんでした。

概要レベルの考慮事項

サイトデータベース

サイトデータベースには、システムを実行するための構成情報が含まれています。

その使用法は、次の特徴があります。

- ユーザーのログオン時に追跡するセッションおよび接続情報が生成されると、最大サイズに達します。
- アクティブなセッションがなく、VDA がすべてシャットダウンされ、登録解除されると、最小サイズに達します。
- データベースには永続情報がほとんど格納されていないため、48 時間後にピークサイズに達します。
  これは、サイトデータベース内で 48 時間維持されている接続のログが小さいためです。
- データベースのベースラインサイズは、サイトの構成情報が大きくなるにつれて大きくなります。
  つまり、より多くのワーカーとユーザーがより多くのデータベース領域を消費します。
- ログオン中に 1 秒あたりのトランザクション数が高くなります。各ユーザーのログオンでは、複数の個別のトランザクションが実行され、同時起動レートに基づいて拡張されるためです。
- VDA ハートビートトランザクションの低レベルのバックグラウンドノイズ。各 VDA は 5 分に 1 回ハートビートを提供し、この更新によってデータベース上のトランザクションがトリガーされます。

障害の影響

サイトデータベースが停止すると、システムの管理と監視ができなくなります。既存の接続は維持されます。XenDesktop 7.6 の接続リースでは、新しい接続と再接続を行うことができます。以前のバージョンでは、新しい接続と再接続はできません。

監視データベース

監視データベースには、サイトに関する履歴情報が含まれています。この情報は、Director が履歴情報を表示するために使用されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

その使用法は、次の特徴があります。

- 最大サイズは、次のように構成された保存期間によって制御されます。
  - プラチナ以外のお客様の場合、デフォルトは 7 日間で、最大期間は 7 日間です。
  - プラチナ会員の場合、デフォルトは 90 日間で、最大期間はありません。
- システムが構成された保持期間に達する必要があるため、ピークサイズに達するまでに時間がかかる場合があります。
- 監視サービスによる更新のバッチ処理の特性により、1 秒あたりのトランザクションのレベルが低くなります。1 秒あたりのトランザクションが 20 回のトランザクション/秒のマークを通過することはまれです。
- 監視サービスからの定期的な連結呼び出しが原因で発生するバックグラウンドトランザクション。
- 一晩処理が実行され、構成された保存期間外のデータが削除されます。

障害の影響

監視データベースが停止すると、サイトのデータが収集されなくなります。つまり、Director 内ではデータが表示されません。

構成ログデータベース

構成ログデータベースには、サイトに対するすべての構成変更の履歴ログが含まれます。この情報は、レポートの生成や Studio での表示に使用されます。

その使用法は、次の特徴があります。

- 最大サイズは、構成アクティビティの量に依存するため、予測するのが難しいです。
- Director からのすべてのアクション（セッションのリセットなど）はこのデータベースにログに記録されるため、管理者が Director を使用するにつれ、増加が遅くなる可能性があります。
- 構成の変更が行われていない場合に、データベースで発生する最小限のトランザクション。
- 更新は可能な限りバッチ処理されるため、更新中のトランザクションレートは低くなります。
- データを手動で削除する。構成ログデータベース内のデータは、保持ポリシーの対象ではなく、管理者が手動で行う場合を除き、削除されません。

障害の影響

構成ログデータベースが停止した場合の影響は、次のように、サイト構成によって異なります。

- 構成ログデータベースが使用できないときにサイトが変更を許可しない場合、XenDesktop 展開を再構成することはできません。
- 構成ログデータベースが使用できないときにサイトで変更が許可されている場合は、追跡されていない構成変更が XenDesktop 展開に加えられることがあります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

一時データベース

テンポラリデータベースは、SQL Server によって提供されるシステム全体のデータベースです。これは、読み取りコミットされたスナップショット分離用のバージョンストアとして使用されます。XenDesktop 7 では、この SQL Server 機能を使用して、XenDesktop データベース内のロック競合を軽減します。

バージョンストアのサイズは、アクティブなトランザクションの数によって異なります。しかし、一般的に、それは数 MB を超えていません。

TempDB のパフォーマンスは、XenDesktop ktop 仲介のパフォーマンスに影響します。これは、新しいデータを生成するトランザクションには TempDB 領域が必要となるためです。ただし、XenDesktop ではトランザクションが短くなる傾向があり、バージョンストアのサイズを小さく保つのに役立ちます。

テンポラリデータベースは、クエリが大きな中間結果セットを生成する場合にも使用されます。

TempDB のサイズ設定と構成に関するガイダンスは、MSDN にあります。

http://technet.microsoft.com/en-us/library/ms175527(v=sql.105).aspx

競合の主な領域は、使用するファイル数の中心です。SQL Server 2000 などの古いバージョンの SQL Server では、新しいバージョンよりも多くのファイルが必要です。使用するファイル数について詳しくは、以下を参照してください。

http://www.sqlskills.com/blogs/paul/a-sql-server-dba-myth-a-day-1230-tempdb-should-alwayshave-one-data-file-per-processor-core/

読み取りコミットされたスナップショットの分離

すべての XenDesktop 7 データベースでは、Read-Committed Snapshot Isolation を使用することをお勧めします。詳しくは、「How to Enable Read-Committed Snapshot in XenDesktop」を参照してください。

データベースのサイジング

データベースのサイズは、稼働日中に作成されたセッションや接続の数など、多くの重要な要素に依存します。

セッションとは、一定期間実行されているデスクトップまたはアプリケーションのことです。セッションは、切断され、に再接続される可能性があります。

接続は、ユーザーがセッションに接続するたびに行われます。切断すると、接続は閉じられますが、セッションは閉じられません。ユーザーが再接続すると、既存のセッションへの新しい接続が作成されます。

サイトデータベース

サイトデータベースの最大サイズは、次のように、VDA とアクティブセッションの数に基づきます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ユーザー	アプリケーション	種類	予想されるピークサイズ 7.5 (MB)	予想されるピークサイズ 7.6 (MB)
1,000	50	HSD	30	31
10,000	100	HSD	60	198
100,000	200	HSD	330	752
1,000	-	VDI	30	30
10,000	-	VDI	115	121
40,000	-	VDI	390	426

各公開アプリケーションは、一意のアイコンを格納するために 110 KB をデータベースに追加します。

> 注:
>
> 7.6 のサイズが大きくなるのは、Controller 間のレプリケーションの一部として接続リースがデータベースに格納されているためです。

監視データベース

3 つのデータベースのうち、監視データベースは時間の経過とともに最大に成長すると予想されます。

そのサイズは、以下を含む多くの要因に依存します。

- ユーザー数
- セッションの数
- 接続数
- VDI ワーカーまたは HSD ワーカー
- 保存期間の構成

以下は、いくつかのデータポイントでのデータベースのサイズの見積りです。このデータは、XenDesktop のスケールテスト時に表示されるデータに基づく推定値です。推定値は現実的であると考えられている。

しかし、データベースを維持しているお客様は、自分のデータベースが推定値よりも小さいことがわかります。

HSD ユーザーは、HSD サーバーあたり 100 ユーザーに基づいています。

最大保存期間

保持されるデータの最大量は、ライセンスによって次のように制御されます。

- プラチナ以外のお客様は、最大 1 週間（7 日）のデータを保持できます。
- プラチナのお客様は、無制限のデータを保持できます。デフォルトは 3 か月 (90 日) です。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

保持期間は、*Set-MonitorConfiguration* コマンドレットを使用して調整できます。

構成された保存期間より古いデータは、データベースから削除されます。

データベースのサイズ設定の監視

稼働週 5 日で、ユーザー 1 人あたり 1 回の接続と 1 回のセッションで見積もり

ユーザー	種類	1 週間（MB）	1 か月（MB）	3 か月（MB）	1 年（MB）
1,000	HSD	151	70	230	900
10,000	HSD	2,830	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500
40,000	VDI	464	1,700	5,400	21,500

稼働週 5 日で、ユーザーあたり 2 回の接続と 1 回のセッションによる見積もり

ユーザー	種類	1 週間（MB）	1 か月（MB）	3 か月（MB）	1 年（MB）
1,000	HSD	30	100	330	1,300
10,000	HSD	240	925	3,000	12,000
100,000	HSD	2,400	9,200	30,000	119,000
1,000	VDI	25	85	240	1,100
10,000	VDI	200	750	2,500	9,800
40,000	VDI	800	3,000	9,700	38,600

HSD は、負荷分散情報のログ記録により、時間の経過に伴ってより多くのデータを生成しますが、当初は VDI デスクトップと同じサイズであることに注意してください。

データベースのサイズ設定の監視

7.5 からの主な変更点は次のとおりです。

- Hotfix 情報
  以下のデータは、ワーカー (VDI または HSD) ごとに 3 つの修正プログラムに基づいています

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- アプリケーション使用履歴
  これは主に HSD システムに関係します。

稼働週 5 日で、ユーザー 1 人あたり 1 回の接続と 1 回のセッションで見積もり

ユーザー	種類	1 週間（MB）	1 か月（MB）	3 か月（MB）	1 年（MB）
1,000	HSD	151	605	1,966	7,865
10,000	HSD	2,830	11,301	36,712	146,834
100,000	HSD	7,194	28,585	92,758	370,841
1,000	VDI	13	49	157	622
10,000	VDI	117	409	1,287	5,090
40,000	VDI	460	1,610	5,058	19,999

稼働週 5 日で、ユーザーあたり 2 回の接続と 1 回のセッションによる見積もり

ユーザー	種類	1 週間（MB）	1 か月（MB）	3 か月（MB）	1 年（MB）
1,000	HSD	159	635	2,063	8,251
10,000	HSD	2,904	11,599	37,684	150,718
100,000	HSD	7,940	31,572	102,465	409,672
1,000	VDI	21	79	253	1,008
10,000	VDI	191	708	2,258	8,974
40,000	VDI	759	2,805	8,941	35,532

構成ログデータベース

構成ログデータベースのサイジングに関するガイダンスは、Director の毎日のアクティビティと構成されたサイトのサイズによって劇的に変化するため、非常に困難です。

セッションまたはユーザーに影響を与えるアクティビティはログに記録され、セッションのログオフやリセットなどが含まれます。ユーザーのセッションを一覧表示するなど、パッシブなアクティビティはそうではありません。

デスクトップの展開に使用されるメカニズムは、ログに記録されるデータのサイズにも影響します。

MCS を使用していない HSD 環境では、データベースのサイズは 30 MB から 40 MB の間になる傾向があります。

MCS 環境では、すべての VM ビルドデータがログに記録されるため、データベースサイズが 200 MB を超える可能性があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

7.6 では、構成ログデータベースに対する大幅な変更は行われませんでした。

100 k の HSD セッションのログオン時のデータベースアクティビティ

スケーラビリティテストで、100k の HSD セッションログオンをシミュレートする際、トランザクションログの増加は、次の 2 つのログオンレートで測定されました。

- 100,000 人のユーザーが 1 時間以上ログインしています
- 2 時間以上ログインしているユーザー数 100 万人

これらのレートは、サンプルデータポイントを提供するために選択されました。

環境は、次のもので構成されています。

- 2 台の Delivery Controller
- 43 人の HSD の VDA ワーカー
- データベースで構成された 3 つの SQL Server が 1 つの常時可用性グループ内に保持

サーバ設定の詳細については、このドキュメントの最後を参照してください。

トランザクションログの増加

すべてのデータベースのトランザクションログの増加は、パフォーマンスモニターカウンター SqlServer: データベース — ログファイル使用サイズ (KB) を使用して監視されました。

サイトデータベース

システムがアイドル状態になると、トランザクションログは 1 時間に 3.5 MB ずつ増加します。これは、VDA とブローカーサービスのハートビートの組み合わせです。

テスト	ログオンの総増加量 (MB)	ログオフの総増加量 (MB)
1 時間以上 100 万回	1,900	1,150
2 時間以上 100 万回	1,900	1,150

ログの増加は、測定される期間にわたって線形です。このデータは、ユーザーログオンごとに、トランザクションログが 20 KB 増加することを示唆しています。ユーザーのログオフごとにトランザクションログは 12 KB 増加します。

したがって、1 日あたりの増加は、ユーザーログオン/ログオフサイクルあたり 32 KB です。

監視データベース

システムがアイドル状態になると、トランザクションログは 1 時間あたり 30.5 MB 増加します。これは、統合ストアドプロシージャと HSD VDA ロードインデックスの更新を組み合わせたものです。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

テスト	ログオンの総増加量 (MB)	ログオフの総増加量 (MB)
1 時間以上で 100,000	670	190
2 時間以上で 100,000	650	220

ログの増加は、測定される期間にわたって線形です。このデータは、ユーザーのログオンごとにトランザクションログが 7 KB 増加することを示唆しています。ユーザーのログオフごとにトランザクションログは 2 KB 増加します。

したがって、1 日あたりの増加は、ユーザーログオン/ログオフサイクルあたり 9 KB です。

1 秒あたりのトランザクション数

すべてのデータベースのトランザクションログの増加は、次のパフォーマンスモニターカウンターを使用して監視されました。

- SQL サーバー: データベース — トランザクション/秒
- SQL Server: データベース — 書き込みトランザクション/秒

サイトデータベース

システムがアイドル状態の場合、5 トランザクション/秒で、1 回の書き込みトランザクションが VDA と Broker のハートビートを維持します。

> 注：これらの数字は、与えられた期間から取られた推定値です。正確な負荷は、1 秒あたりの同時起動回数によって異なります。

テスト	1 秒あたりのログオントランザクション	ログオン書き込みトランザクション/秒	ログオフトランザクション/秒	ログオフ書き込みトランザクション/秒
1 時間以上で 100,000	870	310	250	100
2 時間以上で 100,000	475	170	135	60

監視データベース

システムがアイドル状態の場合、統合ストアドプロシージャは 1 分に 1 回実行され、トランザクションが生成されます。しかし、トランザクションのレベルは小さいです。一般に、連結ストアドプロシージャごとに 2 ～3 のトランザクションと 1 つの書き込みトランザクションがあり、3 つの連結ストアドプロシージャが実行されます。アクティブ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

な期間中は、より多くの作業が実行されるにつれてオーバーヘッドが増加します。

> 注：これらの数字は、与えられた期間から取られた推定値です。

テスト	1 秒あたりのログオントランザクション	ログオン書き込みトランザクション/秒	ログオフトランザクション/秒	ログオフ書き込みトランザクション/秒
1 時間以上で 100,000	4	2	4	2
2 時間以上で 100,000	4	2	3.5	2

CPU 使用率

このテストに使用されたすべての SQL サーバーは、ハイパースレッディングが有効になっているデュアルヘキサコアサーバーでした。ハードウェアの正確な仕様については、このドキュメントの最後に記載されています。

サーバーは、実行中の負荷に対してサイズが大きすぎることがわかっていました。これにより、ハードウェアに適用される制限と最大値を特定することができました。SQL CPU の負荷は、デュアル 16 進コアシステムではなく、単一のクアッドコアを持つ SQL Server によって実際に処理されることが予想されます。

テスト中に、パフォーマンスモニタカウンタ
Processor – % Processor Time – _Total を使用してシステム CPU を監視しました。

プライマリレプリカ

アイドル状態の CPU は、使用可能な CPU の 0～2%で実行されました。統合ストアドプロシージャにより、システム CPU の 1 ～8 ～10% の間、毎分スパイクが発生しました。これは、処理されるデータの量に基づいて拡張されることが予想されます。

1 時間で 100,000 人のユーザーのログオン中、CPU は 7%に上昇し、環境内にセッションとユーザーが増えるにつれて、11%に直線的に増加しました。統合ストアドプロシージャのスパイクは、CPU の 18% に達するスパイクを引き起こす、合計 CPU に 7% を追加することに注意してください。

ログオフ中 CPU は 3.5% で稼働し、統合ストアドプロシージャの 7% 余分な CPU を使用しました。全体的に、ログオンおよびログオフ率を維持するために、デュアルヘキサコアの 20%未満が必要であることを示唆しています。

注**:** Windows Server 2012 スケジューラは、必要な場合にのみハイパースレッドを使用するバイアスです。つまり、システムが 50% の負荷に達するまで、可能な場合はコアごとに 1 つのスレッドしか実行されないため、24 のハイパースレッドで 20% の負荷が 4.8 コアで実行されます。

ワークロードを考慮すると、これは負荷の高いテストであり、XenDesktop の展開には単一のクアッドコア SQL サーバーが適切であると考えられます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

セカンダリレプリカ

セカンダリレプリカは、ログオン時に 2% の CPU、ログオフ時に 1.5% を構成していることが判明しました。これは、ほとんどの場合、レプリカがプライマリのデータをディスクに格納し、同期レプリカのみがトランザクションに関与するため、プリンシパルレプリカはセカンダリが確認するまでトランザクションをコミットしないためです。

プライマリレプリカに一致する HA ハードウェアの推奨事項に基づいて、この負荷は、同様に指定されたサーバーによって非常に簡単に処理されます。

一時データベースの使用

TempDB は、バージョンストア、大規模なクエリセット用の領域、その他のテンポラリテーブルの使用など、多くの目的で使用されます。

一時データベースのサイズ設定

この SQL 構成では、TempDB は 8 つのデータベースファイルで構成され、それぞれのサイズが 5 GB に固定されています。これにより、TempDB の同時使用が向上しますが、十分なスペースが提供され、自動拡張イベントは発生しません。キャプチャされたデータに基づいて、この展開ではサイズが大きすぎました。しかし、十分なディスク容量がありました。

また、TempDB データベースファイルの数が、利用可能な CPUS 数の 1/2 の間にあるが、実際の競合が存在することを知らずに 8 を超えないという一般的なガイダンスにも対応しています。

SQL Server では複数のログファイルの利点がないため、TempDB ログファイルは 1 つだけ使用されます。

バージョンストア

TempDB には、XenDesktop データベースで使用されるコミットされたスナップショットの読み取り分離に関連する行バージョンのバージョンストアが含まれています。

使用状況は、次のパフォーマンスカウンターで測定できます。

- SQL Server: トランザクション — バージョンストアサイズ (KB)
- SQLServer: トランザクション — バージョンクリーンアップレート (KB/秒)
- SQLServer: トランザクション — バージョン生成レート (KB/秒)

1 時間で 100,000 ログオン中に、バージョンストアのサイズは 10 MB から 30 MB の範囲にとどまりました。バージョンが作成され、クリーンアップされた際のこぎり歯の効果があります。ログオフ時の範囲は 10 MB から 21 MB でした。アイドル状態のとき、バージョンストアのサイズは 1 MB から 4 MB の範囲でした。

バージョン生成率は、ログオン時の 250 ～500 KB の範囲でした。ログオフ時は 150 ～400 KB/秒、アイドル時は 0 ～250 KB/秒でした。

バージョンクリーンアップは、1 分に 1 回実行され、ログオン時に 2,500 KB/s、ログオフ時に 1,750 KB/s、アイドル期間中に 400 KB/s に達しました。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ディスク I/O

ログオンテスト中に、ディスク I/O は、次のパフォーマンスカウンターで測定されました。

- 物理ディスク — ディスク読み取りバイト/秒
- 物理ディスク：ディスク書き込みバイト/秒
- 物理ディスク — ディスク読み取り/秒
- 物理ディスク：ディスク書き込み/秒

SQL サーバーはすべてのデータをメモリに保持でき、システムでの読み取りアクティビティはほとんど発生していないため、読み取り I/O は最小限であることが判明しました。

データベースとストレージシステムのレイアウトにより、ボリュームは分割され、1 つのボリュームはすべてのデータファイルを保持し、もう 1 つのボリュームはすべてのトランザクションログファイルを保持していました。

データには、テーブルに配置するのが難しいパターンが表示されます。一般に、トランザクションログの書き込みバイト/秒は、1 時間のテストでは 800 KB/秒、2 時間のテストでは 400 KB/秒でした。1 分に 1 回、統合ストアドプロシージャを実行すると、トランザクションログに 30 MB/秒のスパイクが表示されました。

統合ストアドプロシージャの分析は、統計がクエリプランを最適ではないし、一時テーブルが TempDB に流出することを示しています。これにより、TempDB のトランザクションログへの書き込みがトリガーされます。

このデータ転送は、1 時間のテストでは 300 回の書き込み入出力操作/秒 (IOPS)、2 時間のテストでは 200 回の書き込み IOPS という定常状態になります。統合ストアドプロシージャの急増により、実行中にさらに 2〜300 の書き込み IOPS が追加されます。大規模な環境では、統合ストアドプロシージャが 1 秒未満で実行されることに注意してください。

各データベースがチェックポイントされると、データはメモリ内のテーブルからデータボリューム上のデータファイルに同期されます。

SQL チェックポイントについて詳しくは、http://technet.microsoft.com/enus/を参照してください。

これらのチェックポイントは、アクティビティが非常に短く、通常は 1 秒未満です。

ログオン中、チェックポイントは 6〜7 MB/秒と 500 回の書き込み IOPS を消費しました。ログオフの間、チェックポイントは 7 MB/秒（200〜700 IOPS）を消費しました。サイトデータベースと監視データベースでは、チェックポイントまでのデータ量が異なるため、数値は異なります。

データベースのメンテナンス

大規模な展開でのデータベースのメンテナンスは重要です。データベースが適切に管理されていない場合、データベース領域が不足しているためにデータベースが停止することがあります。たとえば、トランザクションログが自動拡張に設定されてディスクがいっぱいになったり、トランザクションログが固定サイズでいっぱいになったりします。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

トランザクションログの保守

常時可用性グループやデータベースミラーリングなどの SQL Server の高可用性機能を使用する場合、XenDesktop データベースはフルトランザクションログモードで実行されます。

フルトランザクションログモードで実行すると、トランザクションログは、データベースまたはトランザクションログのバックアップが実行されるまで増加し続けます。

既定では、SQL Server はログファイルを自動拡張するように構成するため、トランザクションログファイルが監視されていない場合に問題が発生する可能性があります。これにより、次の 2 つの問題が発生します。

1. トランザクションログファイルは、多くのディスク領域を消費する可能性があります。
2. トランザクションログが大きくなるたびに、ログスペースがゼロになるまですべてのトランザクションが停止します。

ログファイルは定期的にバックアップすることをお勧めします。これは、スケジュールされたジョブまたは保守計画で行うことができます。

または、SQL Server エージェントを使用して、使用されるログのサイズがしきい値を超えたときを監視し、バックアップジョブを実行します。

スケールテストでは、4 GB の固定サイズのログが使用され、ログファイルの使用率が 80% に達したときにログを別のファイルにバックアップするようにアラートが設定されました。これにより、ログが増加し、すべてのディスク領域が消費されなくなり、ディスク領域がゼロになり、データベースが停止します。

サンプルジョブでは、次のようなスクリプトが実行されます。

```
1  バックアップログ [CitrixXenDesktopサイトデータベース] ディスクへ = N'D:
       ログバックアップCitrixXenDesktopSiteDB.bak' ノーフォーマット、ノイ
       イン、圧縮、名前 = N'サイトトランザクションログのバックアップ '、ス
       キップ、巻き戻し、NOUNLOAD
```

アラートに使用する SQL パフォーマンスカウンタは次のとおりです。

SQLServer: データベース-使用率のログ-CitrixXenDesktop サイトデータベース

3 つのデータベースそれぞれについて、この操作を繰り返します。

ログファイルのバックアップは、実行中の XenDesktop 環境への影響が最小限であることが判明しました。仲介時間はごくわずかですが、重要なものではありません。

ジョブの構成のついて詳しくは､次を参照してください｡http://msdn.microsoft.com/en-us/library/ms187880.aspx

アラートの構成について詳しくは、次を参照してください。http://msdn.microsoft.com/en-us/library/ms191508.aspx

© 1999–2021 Citrix Systems, Inc. All rights reserved.

インデックスメンテナンス

データベースに入力されるデータが増えるにつれて、インデックスの一部がいっぱいになり始めます。つまり、各 SQL ページに格納されるレコードが少なくなります。SQL ページは 8 KB です。これにより、データベースはメモリ内とディスク上のストレージ要件を増やします。インデックスを維持することで、ページの満杯性を高めることができ、データベースのメモリ要件が軽減されます。

インデックスを維持するために、お客様のセットアップメンテナンスプランを毎晩および毎週実行することをお勧めします。保守計画は、単に週に夜間にインデックスを再編成し、週末にインデックスを再構築することです。

この推奨事項により、特に大規模な監視データベースの場合、今日の操作中に大きなインデックスを再構築することによるパフォーマンスへの影響を回避できます。

Microsoft では、断片化が 30% を超える場合はインデックスを再構築し、30% 未満の場合は再編成することをお勧めしています。詳しくは、Microsoft TechNet のインデックスの再編成と再構築を参照してください。

インデックスを再編成した後、統計も更新する必要があります。これは、データベースが大きくなるにつれて特に重要です。そうしないと、統計が低くなり、SQL が最適ではない SQL クエリプランを生成する可能性があります。

省スペースの観点から、次の Microsoft スクリプトは 1.2 GB の監視データベースに対して実行されました。これは、ページの充填を改善し、300 MB のスペースを解放しました。

サードパーティ製スクリプト

Microsoft

Microsoft では、次のスクリプトを使用して、WSUS SQL データベースのインデックスを更新することをお勧めしています。

http://gallery.technet.microsoft.com/scriptcenter/6f8cde49-5c52-4abd-9820-f1d270ddea61

「USE SUSDB」を変更することで、このスクリプトを XenDesktop データベースに対して実行することもできます。このスクリプトは、断片化された 30% を超えるインデックスを再構築し、30% 未満のインデックスを再編成するという Microsoft のベストプラクティスに従います。次に、データベースの統計情報を更新します。

オーラ・ハレングレン

より高度なスクリプトは、次の場所から入手できます。

http://ola.hallengren.com/

これらのスクリプトは、SQL Server コミュニティでよく評価されています。具体的には、次のインデックススクリプトを使用できます。

http://ola.hallengren.com/sql-server-index-and-statistics-maintenance.html

これらのスクリプトは、インデックスを再編成または再構築するためのレベルをより細かく制御するために使用できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

サーバ構成のテスト

SQL サーバーの構成

SQL 可用性グループは、同じように指定された 3 台の Dell R720XD サーバーで構成されています。

システム仕様:

- ハイパースレッディングを有効にした 2.30GHz で動作する 2 ヘキサコアのインテル Xeon CPU E5-2630
- エチメチスラム
- PERC H710P ミニ（1 GB のバッテリバックアップ式キャッシュ搭載）
- 26 台の 300 GB の 10k RPM の SAS ドライブ

ディスクは次のボリュームに分割されました。

- システムボリューム
  - OS とページファイルを含む
  - RAID 1 ミラーとして 2 台のディスク
  - 合計容量 278 GB
- データベースボリューム
  - SQL Server インスタンスとデータベースデータファイルを格納する
  - RAID 10 ミラーストライプとして 16 台のディスク
  - 合計容量 2,231 GB
- ログボリューム
  - データベースログファイルを格納する
  - RAID 10 ミラーストライプとして 8 台のディスク
  - 合計容量：1,115 ギガバイト
- ソフトウェア:
  - Windows Server 2012 R2 の Standard エディション、テスト時の最新の Windows 更新プログラムを含む (2014 年 8 月)
  - 累積更新プログラム 1 を適用した SQL Server Enterprise 2012 SP2
- 設定の変更
  - 最大 61,440 MB を使用するように SQL Server が構成されました。
  - データベース包含がすべての SQL インスタンスで有効になっている
  - SQL Server エージェントサービスが自動的に開始するように構成されました。
- 可用性グループの設定:
  - すべてのサーバーが Windows フェイルオーバークラスター内に配置されている
  - 常時可用性グループがクラスター内で構成されました。
  - セカンダリレプリカは同期コミットするように構成されており、トランザクションが完了する前に両方のレプリカでトランザクションがコミットされている必要があります。
  - 可用性グループに対して読み取り専用レプリカルーティングが構成され、有効になっています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Delivery Controller と **HSD** テストサーバ

Delivery Controller と HSD テストサーバーは、HP BL460c G1 ブレードを使用して、同じ構成のハードウェアで実行されていました。デリバリーコントローラには 2 台のサーバーが使用され、43 台のサーバーで HSD ワークロードがシミュレートされました。

注：これらのサーバーは比較的古いですが、セッションシミュレーションは主に HSD サーバーではなくデリバリーコントローラに負荷をかけることに重点を置いているため、HSD サーバーのワークロードは低くなります。

システム仕様:

- 1.86 GHz で動作する 2 つのクアッドコア Intel Xeon L5320、ハイパースレッド対応ではない
- 16 GB ECC RAM
- HP スマートアレイ E200IRAID カード（バッテリバックアップキャッシュなし）
- 36 GB または 72 GB の SAS ハードディスク

ソフトウェア:

- Windows Server 2012 R2 の Standard エディション、テスト時の最新の Windows 更新プログラムを含む (2014 年 8 月)
- Citrix

オーバーフローによる **PVS RAM** キャッシュの分析

May 18, 2020

この資料では、ディスクへのオーバーフローを伴うフィーチャ *RAM* キャッシュを使用する場合に *RAM* キャッシュサイズを正確に決定する方法について説明します。

ディスクへのオーバーフローを伴う RAM キャッシュは、vDisk 書き込みが Windows の非ページプール RAM に最初に書き込まれる PVS 機能です。ユーザーが指定した RAM キャッシュサイズが指定したサイズに達すると、PVS は RAM キャッシュコンテンツをディスクにフラッシュして、新しいデータ用のスペースを作成します。RAM キャッシュのサイズは、ワークロードのパターンやその他のバリエーションに基づいて変動します。PoolMon は、pooltag *VhdR* を検索して、現在の RAM キャッシュ使用量のスナップショットを撮るツールです。

この PVS 機能について詳しくは、オーバーフローを伴う RAM キャッシュの使用に関するブログを参照してください。

> 重要
>
> この記事で説明するツールは、Provisioning Services に関する高度な知識を持つ管理者を対象としています。この情報を使用して、プロセスモニタ (ProcMon) など、一般的に使用されるツールやプロセスを使用する以外に、パフォーマンス関連の問題をデバッグできます。この情報により、PVS ドライバがどのように機能するかをよりよく理解できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

メモリプールモニタ

PoolMon (poolmon.exe) は、メモリプールモニターを参照します。これは、OS によって収集されたデータ（システムページングおよび非ページングカーネルプールからのメモリ割り当て、およびターミナルサービスセッションに使用されるメモリプール）を表示するために使用されます。このデータは、プール割り当てタグによってグループ化されます。

非ページプールメモリでは、プールモンツールを使用して *VhdR* で表される **pooltag** の存在を確認できます。VhdR は RAM キャッシュの割り当てに使用されます。このタグは pooltag *VhdL* とともに、非ページプールメモリ内の RAM キャッシュに関連付けられたデータを分析するスクリプトを作成する場合に役立ちます。

> ヒント
>
> 開発者およびテスターは通常、ドライバが作成されたとき、ドライバコードが変更されたとき、またはドライバのストレステスト時にメモリリークを検出するために、PoolMon を使用します。PoolMon は、テストプロセスの各段階で使用して、ドライバのメモリ割り当てと解放操作のパターンを検証することもできます。たとえば、ドライバが任意の時点で使用しているプールメモリの量を判断するために使用できます。メモリプールモニターの使用方法について詳しくは、Microsoft 開発者ネットワークサイトを参照してください。

Windows パフォーマンスアナライザの使用

Windows パフォーマンスアナライザー (WPA) は、Windows パフォーマンスレコーダー (WPR) によって記録されるイベント (特に Windows のイベントトレーシング) に関連するグラフとデータテーブルを作成できるツールです。WPA を使用すると、PVS ドライバ、ストレージスタック、および VHDX ディスクへの書き込み時に発生するパフォーマンス関連の問題をデバッグする際に、パフォーマンスのボトルネックを特定できます。これらのツールを使用すると、評価を実行し、分析用のイベントトレースログファイルを開くことができます。Windows パフォーマンスアナライザーについて詳しくは、Microsoft Developer Network サイトを参照してください。

> 注
>
> WPA および WPR は、Windows Assessment and Deployment Kit（Windows ADK）に含まれています。この導入キットについて詳しくは、Microsoft Web サイトを参照してください。Windows パフォーマンスアナライザーの最新バージョンについては、Microsoft の Web サイトを参照してください。

Windows パフォーマンスアナライザと **Provisioning Services** しくみ

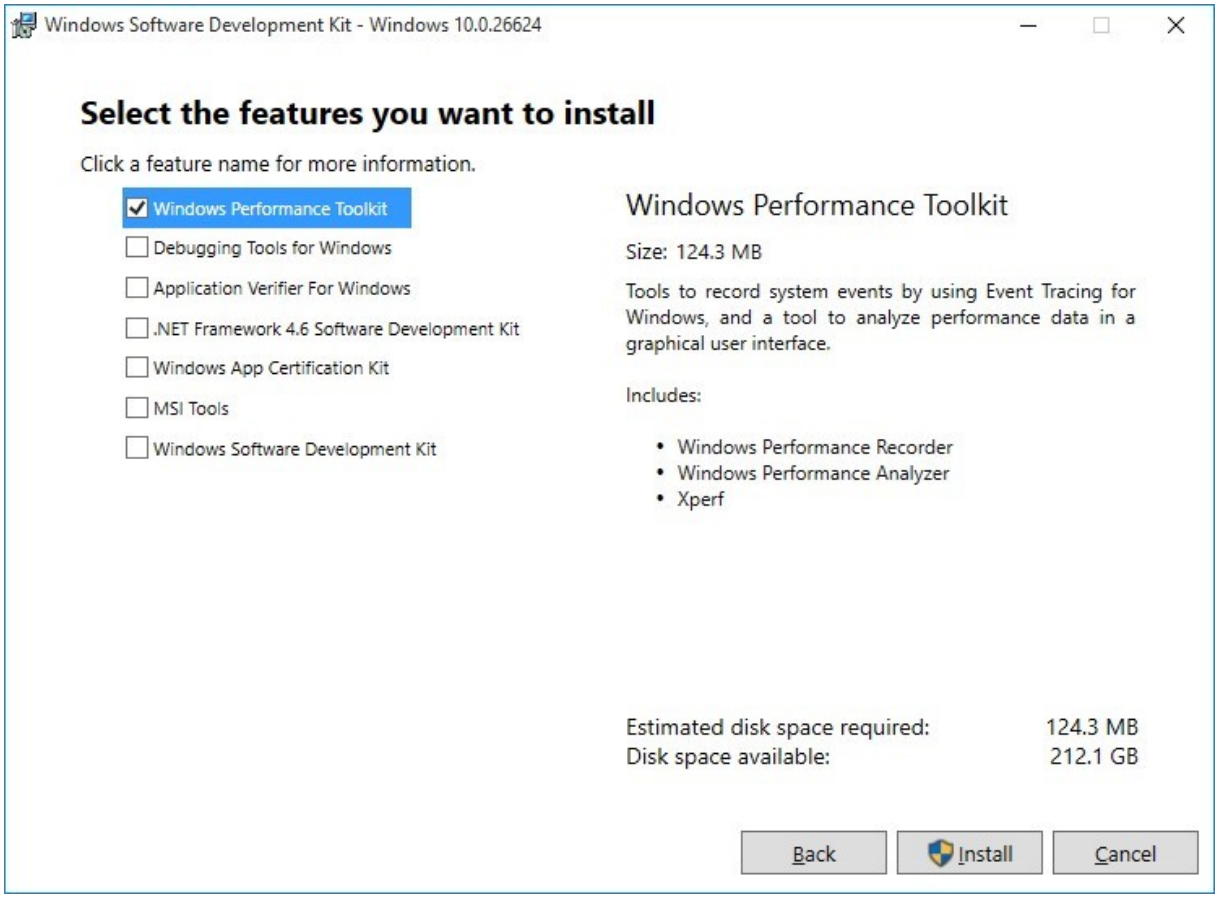
PVS は、Windows 用のイベントトレース（ETW）メカニズムによってキャプチャされたイベントを生成します。この機能は、ユーザーモードアプリケーションとカーネルモードドライバーによって発生したイベントをトレースおよびログに記録する方法を提供します。ETW は Windows OS に実装され、開発者が一連のイベントトレース機能を使用するための簡単な方法を提供します。詳しくは、Microsoft 開発者ネットワークを参照してください。

Windows パフォーマンスアナライザのインストール

WPA をマスターイメージにインストールする必要があります。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

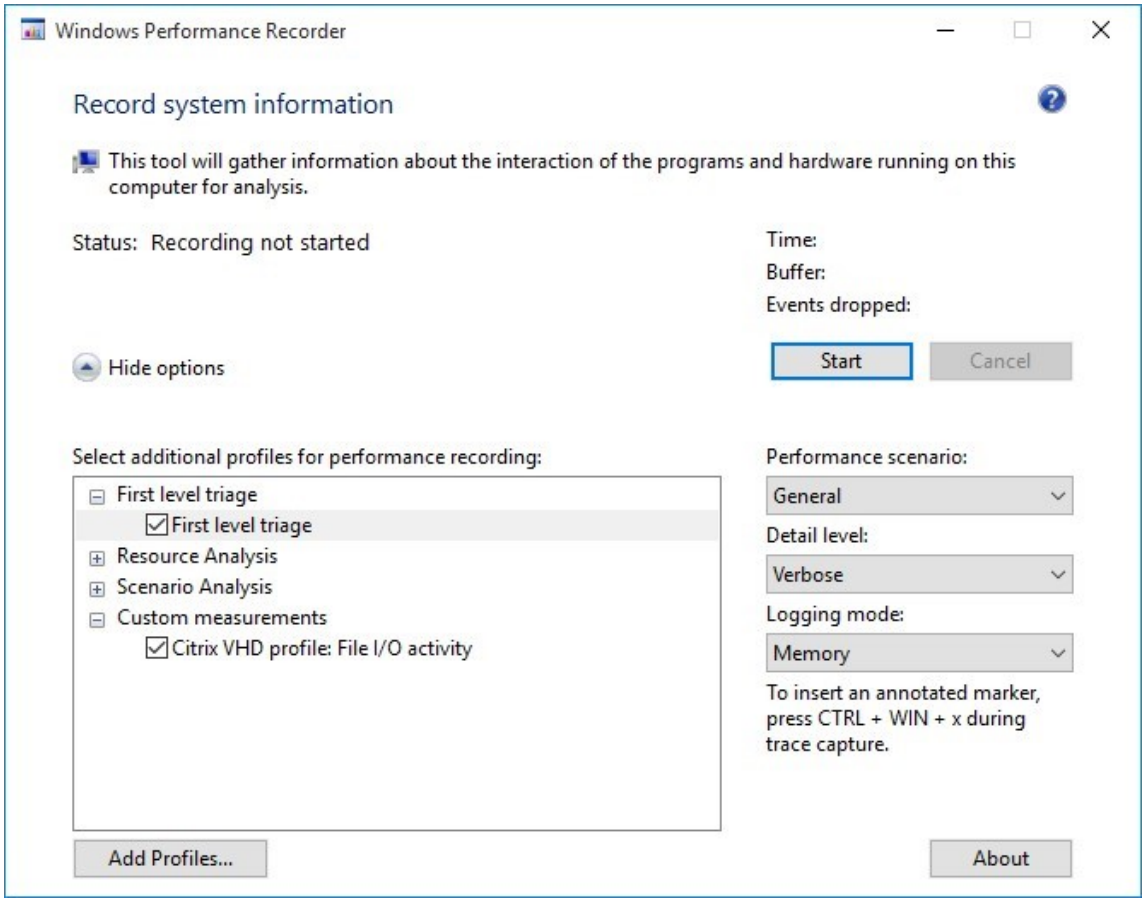
WPA は、Windows 10 オペレーティングシステムの最新の SDKの一部です。WPA と WPR の両方を含むパフォーマンスツールキットを選択的にインストールできます。



WPA と WPR をインストールした後、WPR を使用して PVS ディスクとファイル I/O アクティビティをシミュレートします。このトラフィックが作成されたら、WPA を使用してデータを分析します。次のアクションを実行するには、次の手順に従います。

1. ターゲットデバイスで WPR を起動し、[プロファイルの追加] をクリックします。
2. [プロファイルの追加] 画面で、PVS 固有のテンプレートまたはプロファイルを参照します。これにより、PVS イベントプロバイダーによって生成されたイベントを受け取ることができます。プロファイルをインポートした後、WPR 画面に戻り、分析する追加オプションを選択し、[スタート] ボタンをクリックします。

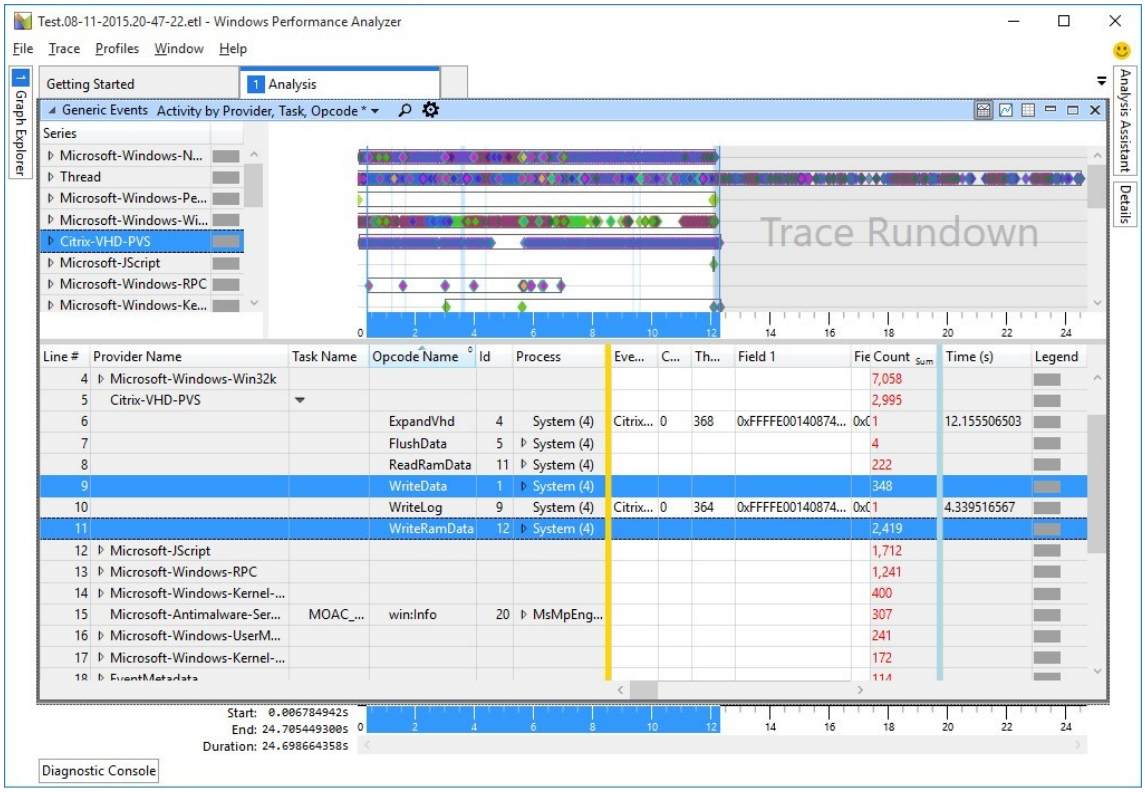
© 1999–2021 Citrix Systems, Inc. All rights reserved.



オプションを追加し、「開始」をクリックすると、PVS アクティビティをシミュレートできます。この例では、小さなメモリバッファ（128 MB）を持つ新しいライトキャッシュが作成されます。より大きなファイル (279 MB) が C: UsersUserDocumentstest.bin にコピーされ、PVS ドライバーが非ページプールにデータを書き込んで、フェイルオーバーが発生したときに何が起こるかを検証し、ローカルディスク (D: vdiskdif.vhdx など) への書き込みを開始します。ファイルをコピーし、バッファの容量を強制的に超えたら、WPR で取得プロセスを停止し、WPA を使用して結果を開くことができます。

3. WPA を使用して、グラフエクスプローラを開き、[システムアクティビティ] を展開し、[汎用イベント] を選択します。例として以下の画面を使用して、「データの書き込み」および「RAM データの書き込み」セクションの内容を表示します。この情報には、D: ドライブ上の VHDX ファイル（348 ファイル）を含め、C: vDisk（2419 ファイル）に書き込まれているファイルの正確な数が表示されます。

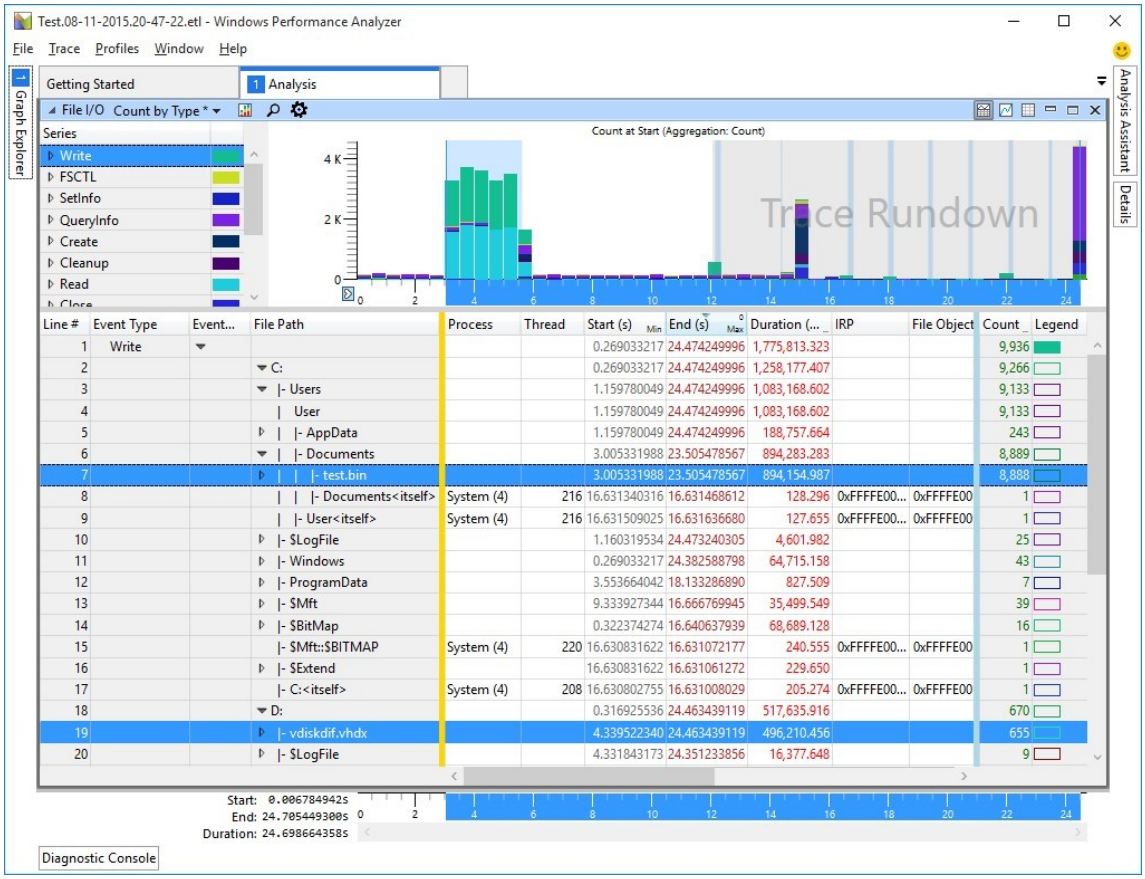
© 1999–2021 Citrix Systems, Inc. All rights reserved.



> ヒント
>
> WriteData は RAM にキャッシュされ、ディスクにフラッシュされていないため、表示されている値よりも小さくなります。

4. **[**グラフエクスプローラ] 画面に戻り、[ファイル **IO]** を展開し、[タイプ別にカウント] を展開します。以下の図は、IO（ファイル数）の削減と、C: UsersUserDocumentstest.bin への書き込みと、D: vdiskdif.vhdx にあるスピルオーバー書き込みキャッシュファイルの間の所要時間を示しています。このデータを使用して、潜在的なパフォーマンスのボトルネックを表示し、PVS フィルタドライバを問題として効果的に除外できます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



5. ファイルカウントと書き込み間隔 (ログファイルとスピルオーバーライトキャッシュの間の) を確認したら、デバッグプロセスをさらに進んで、ディスクオフセットを使用してデータが最初に書き込まれる場所 (および最後に書き込まれる場所) を把握できます。Windows パフォーマンスアナライザで、[グラフエクスプローラ] を開き、[システムアクティビティ] を展開し、[汎用イベント] を選択します。列ビューを変更して、WPA ツールがさまざまな記憶域レイヤーのデータ遷移を表示できるようにします。さらにデバッグするには、PVS 環境に戻り、RAM キャッシュバッファを 0 MB に設定してから、レコーダー（WPR）とアナライザー（WPA）ツールを再実行します。以下の図は、ディスクへのスピルオーバーの発生方法を示しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Citrix Secure Browser で保護されたブラウザーを使用してレガシー **Web** アプリケーションの寿命を延ばす

May 18, 2020

Web アプリケーションやフレームワークの世界では、多様性を採用する必要があります。さまざまな種類のユーザー、グループ、企業が Web 対応のビジネスアプリケーションに接続するには、適切なツール、アプリケーション、および権限にアクセスする必要があります。ほとんどの場合、これらのアプリケーションへのアクセス方法を決定するコンプライアンス要因があります。古いブラウザフレームワークを使用する古いサブシステムをサポートする必要がある企業は、適切なアクセスを提供し、ビジネスクリティカルなアプリケーションのコンプライアンス要件を満たすという困難な作業に直面しています。以下のドキュメントでは、Citrix Secure Browser を使用して、更新および移行戦略を作成しながら、レガシー Web アプリケーションおよびブラウザーのアクセスと使用期間を延ばす方法について説明します。

このソリューションでは、ユーザーの接続方法や内部サイトへの接続に使用するブラウザーに関係なく、外部または内部ユーザーがアクセスできる準拠のブラウザーを公開する必要があります。このソリューションは、XenDesktop サーバー OS の VDA、StoreFront、NetScaler Gateway、および XenApp セキュアブラウザーを使用します。ユーザーは、IT 管理者が設定したすべての要件を満たしている場合、準拠しているブラウザまたはエンドポイントをリダイレクトしてネイティブブラウザーを使用します。ポリシーが非準拠のブラウザまたはエンドポイントを検出すると、コンテナー化されたリモート公開ブラウザセッションにユーザーをリダイレクトします。ユーザーは、環境への接続方法に関係なく、リソースごとに 1 つの URL しか知る必要がありません（トレーニングとサポートのコストが削減されます）。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

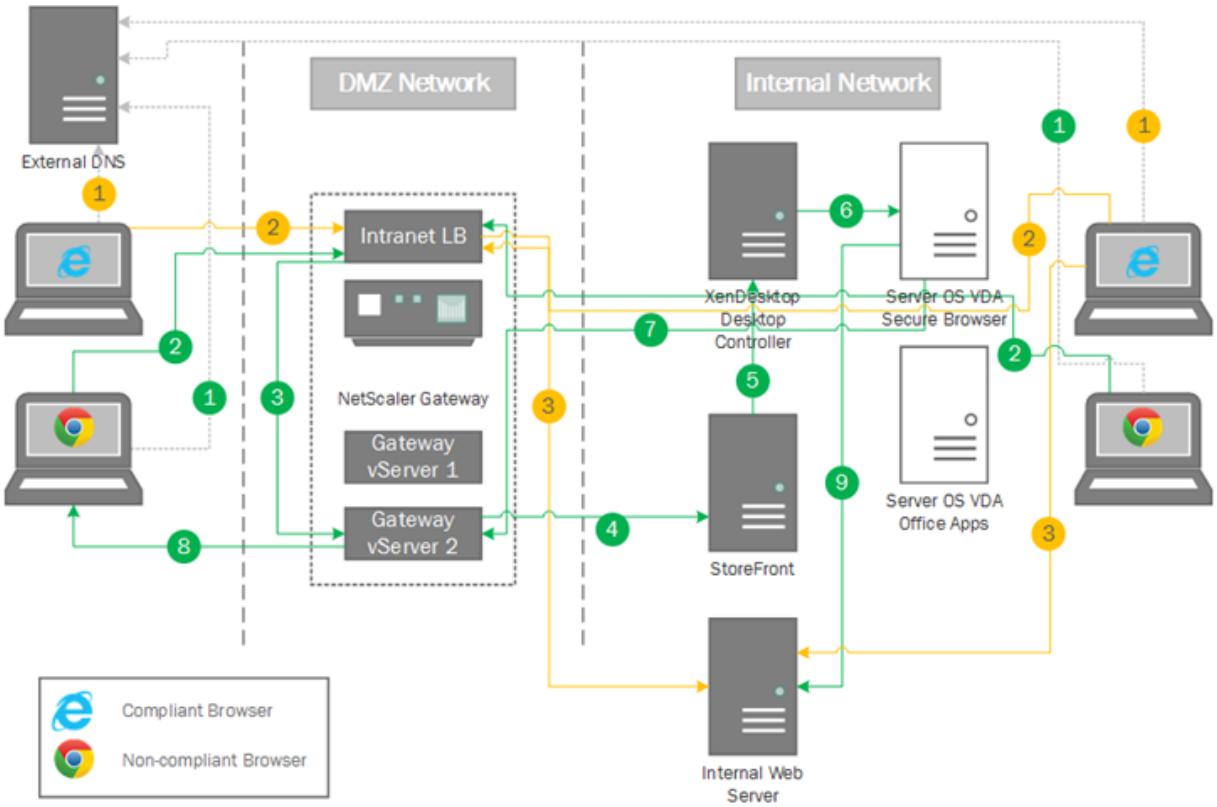
アーキテクチャ

次のセクションでは、ユーザが内部ネットワークと外部ネットワークのどちらから接続しているかに関係なく、ユーザが内部サイトにアクセスする方法について説明します。このシナリオでは、1 つのブラウザータイプ (Internet Explorer) が準拠のブラウザーで、もう 1 つのブラウザー (Google Chrome) が非準拠のブラウザーとなります。コンプライアンスポリシーにどのブラウザーをマッピングするかは、各社が決定します。

このソリューションでは、NetScaler Gateway が公開アプリケーションへの外部アクセス用に構成されていることを前提としています。これは、図 1 では Gateway vServer 1 として表されています。2 番目の仮想サーバー（Gateway vServer 2）は、セキュアブラウザー用の HTML5 Receiver セッションを起動するようにユーザーをリダイレクトします。

使用例

現在のブラウザーでサポートされなくなったレガシー Web アプリケーションを維持する必要があります。この場合、IT 部門は Internet Explorer 8 用に設計された Web サイトを維持する必要がありますが、ベンダーは新しいブラウザや他のブラウザーをサポートするための拡張機能をリリースしなくなりました。この問題を解決するために、IT 管理者はセキュリティで保護されたブラウザーを公開し、ブラウザーの要件を満たすユーザーがサイトにアクセスできるようにします。次の図は、内部ユーザーと外部ユーザーのワークフローにおける各接続について説明しています。



© 1999–2021 Citrix Systems, Inc. All rights reserved.

接続ワークフロー

1. すべてのユーザーは、外部 DNS サーバーから解決するサイト URL を入力します。この例では、https://train.qckr.net
2. ブラウザーは NetScaler Gateway ロードバランサーに接続し、コンプライアンス要件を決定します。
3. ブラウザーが非準拠の場合、内部ユーザーと外部ユーザーの両方が NetScaler Gateway 仮想サーバーにリダイレクトされます。ブラウザーが準拠している場合、NetScaler Gateway は外部ユーザーのロードバランサーを介して内部サイトへの接続をプロキシし、ローカルブラウザーを内部ユーザーのサイトにリダイレクトします。
4. 仮想サーバーは、StoreFront によって列挙されたセッションを自動的に開始します。
5. StoreFront が XenDesktop コントローラーに接続し、セッション情報とルーティングを確認します。
6. セッションは、Secure Browser デスクトップグループを介して開始されます。この場合、公開された準拠ブラウザーを備えたサーバー OS VDA です。
7. セッションは、NetScaler Gateway アプライアンス上の ICA プロキシを介して接続されます。
8. Citrix Receiver for HTML5 は、ネイティブブラウザー内でユーザーのセッションを確立します。
9. 内部サイトは、Citrix Receiver for HTML5 とのセキュアブラウザセッションを介して表示されます。

セットアップと構成

このセクションでは、NetScaler Gateway のリモート接続を使用する現在の XenDesktop 環境にソリューションを実装する方法について説明します。

ソリューションの要件

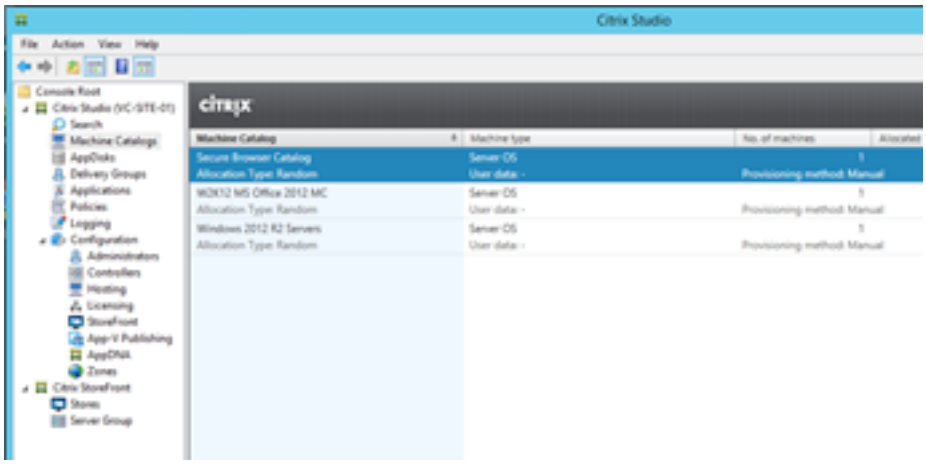
セットアップには、次のコンポーネントのインストールと構成が必要です。

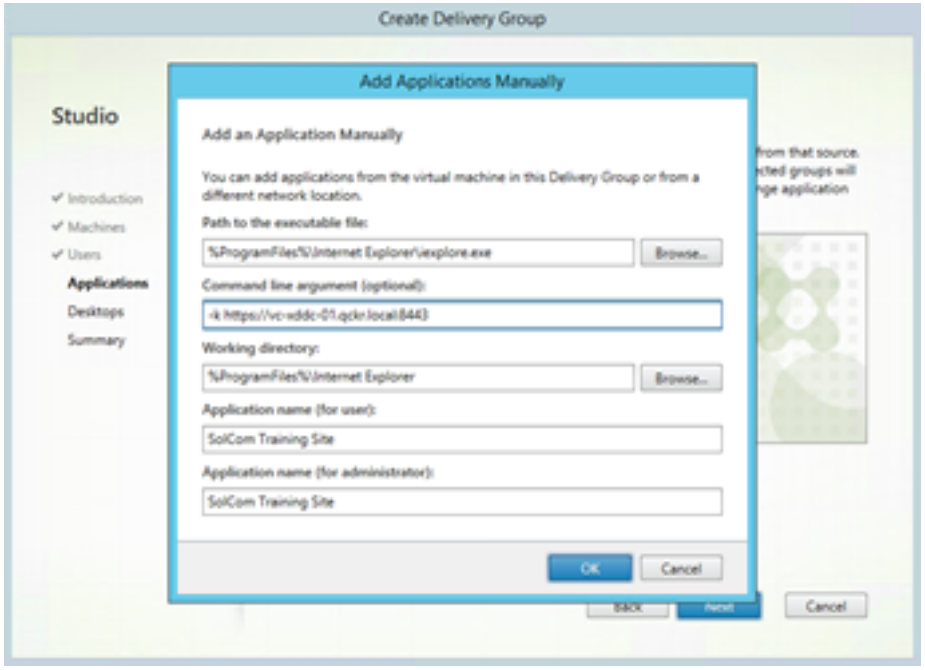
- XenDesktop コントローラーサーバー
- 外部アクセス用に構成されたストアを持つ Citrix StoreFront サーバー
- XenDesktop 仮想サーバーを使用した NetScaler Gateway
- インストールされているブラウザーをセキュアブラウザとして使用するサーバー OS VDA
- 新しい NetScaler ロードバランサーを指す外部 DNS アドレス
- 新しい NetScaler Gateway 仮想サーバーを指す外部 DNS アドレス

© 1999–2021 Citrix Systems, Inc. All rights reserved.

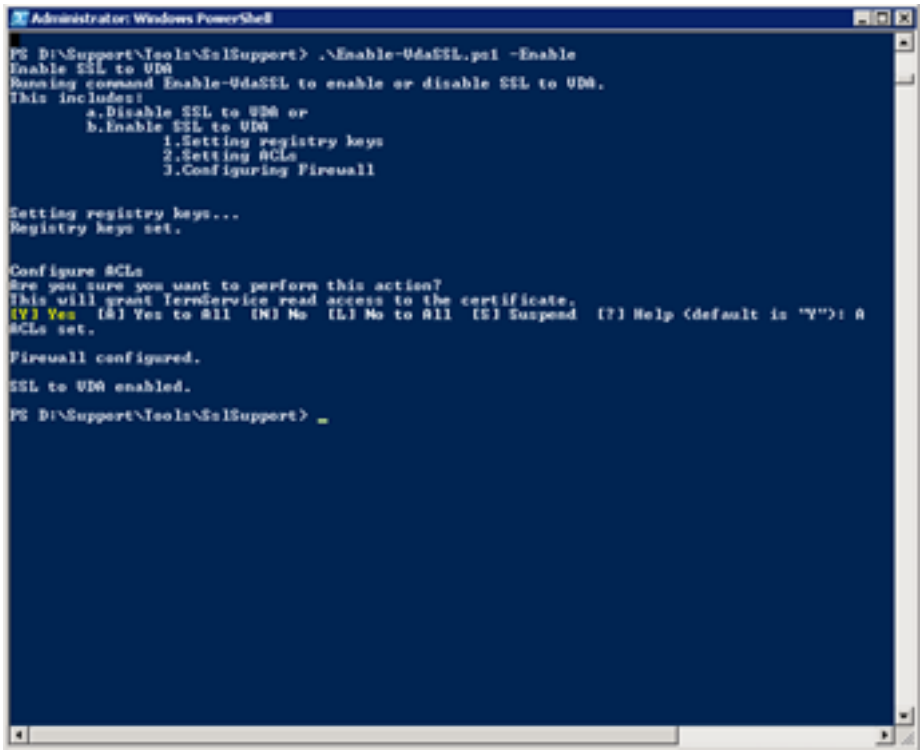
構成

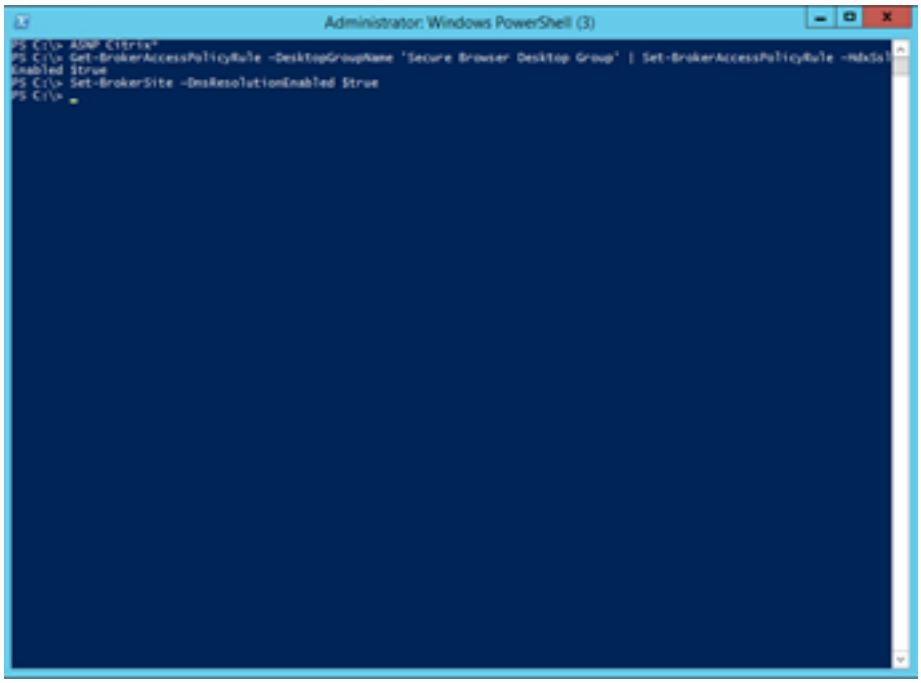
XenDesktop コントローラ





© 1999–2021 Citrix Systems, Inc. All rights reserved.





サーバー OS の VDA を、セキュアブラウザカタログという名前の新しいマシンカタログに追加します。

セキュアブラウザカタログ用のデリバリーグループを作成し、Internet Explorer を公開します。コマンドラインパラメータで、**-k と入力します <URL of Internal Site>。-k パラメータを使用すると、Internet Explorer をキオスクモードで開くことができます。この例では、Internet Explorer 8 を公開し、URL に内部サイトを使用しています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

デリバリーグループを特定のユーザーおよびグループに割り当てることができます。ユースケースで必要でない場合は、デスクトップアクセスを追加する必要はありません。

サーバー OS VDA で、サーバーまたはクライアント認証証明書をインストールします。これにより、Controller と VDA の通信で SSL が有効になります。

XenDesktop 7.6 以降のインストールメディアをマウントします。PowerShell コマンドウィンドウを開き、% メディアドライブ% を実行します。\ サポート\ ツール\ *SslSupport*\ 有効化 *VdaSSL.ps1* —有効化

サーバー OS の VDA インスタンスを再起動します。

XenDesktop コントローラーでは、PowerShell コマンドウィンドウを開き、コマンド *ASNPCitrix** を実行します。

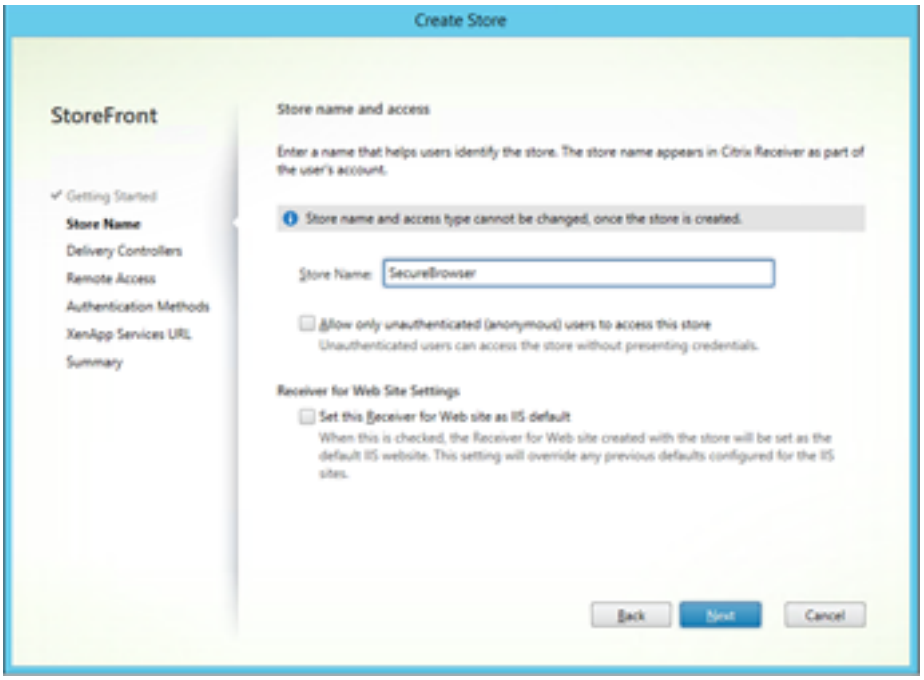
以下の 3 つのコマンドを実行して、ブローカと VDA のセキュアな通信を有効にします。

```
Get-BrokerAccessPolicyRule  -DesktopGroupName 'Secure Browser Desktop
    Group' | Set-BrokerAccessPolicyRule  -HdxSslEnabled $true*
<!--NeedCopy-->
```

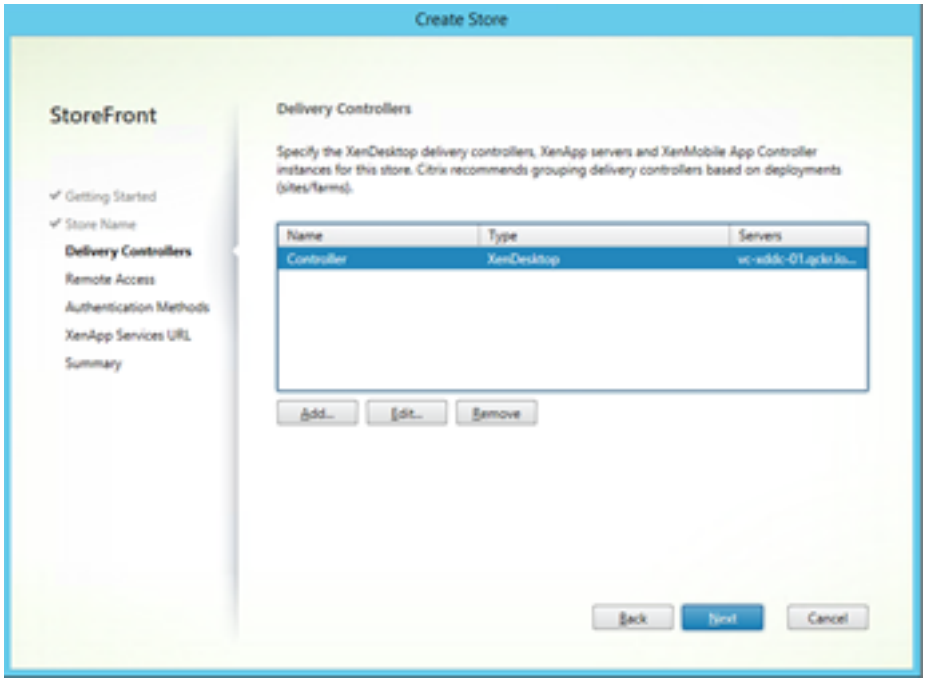
```
Set-BrokerSite  -DnsResolutionEnabled $true
<!--NeedCopy-->
```

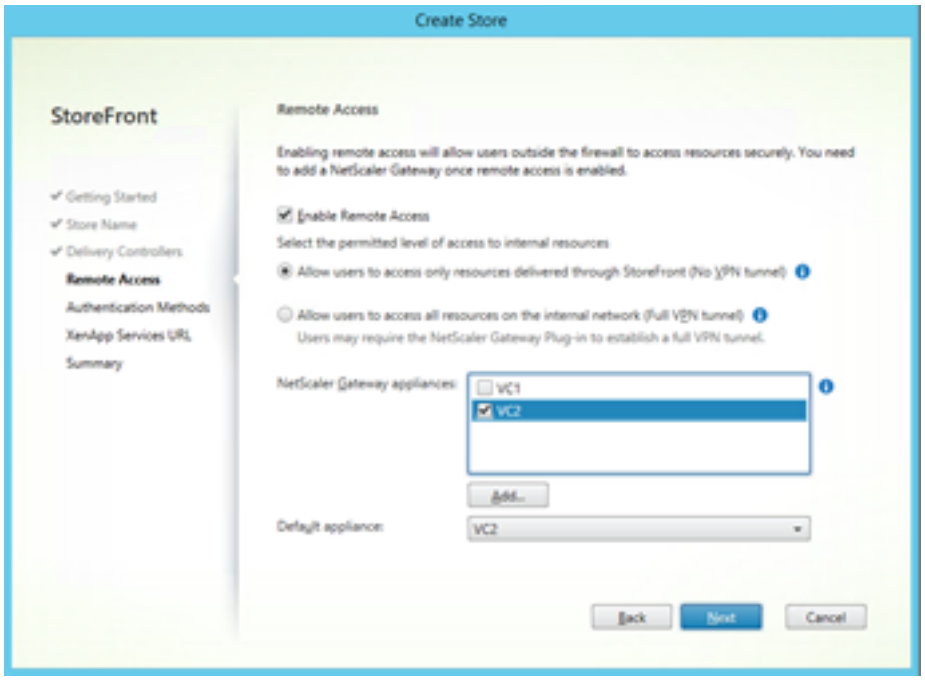
```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true*
<!--NeedCopy-->
```

StoreFront

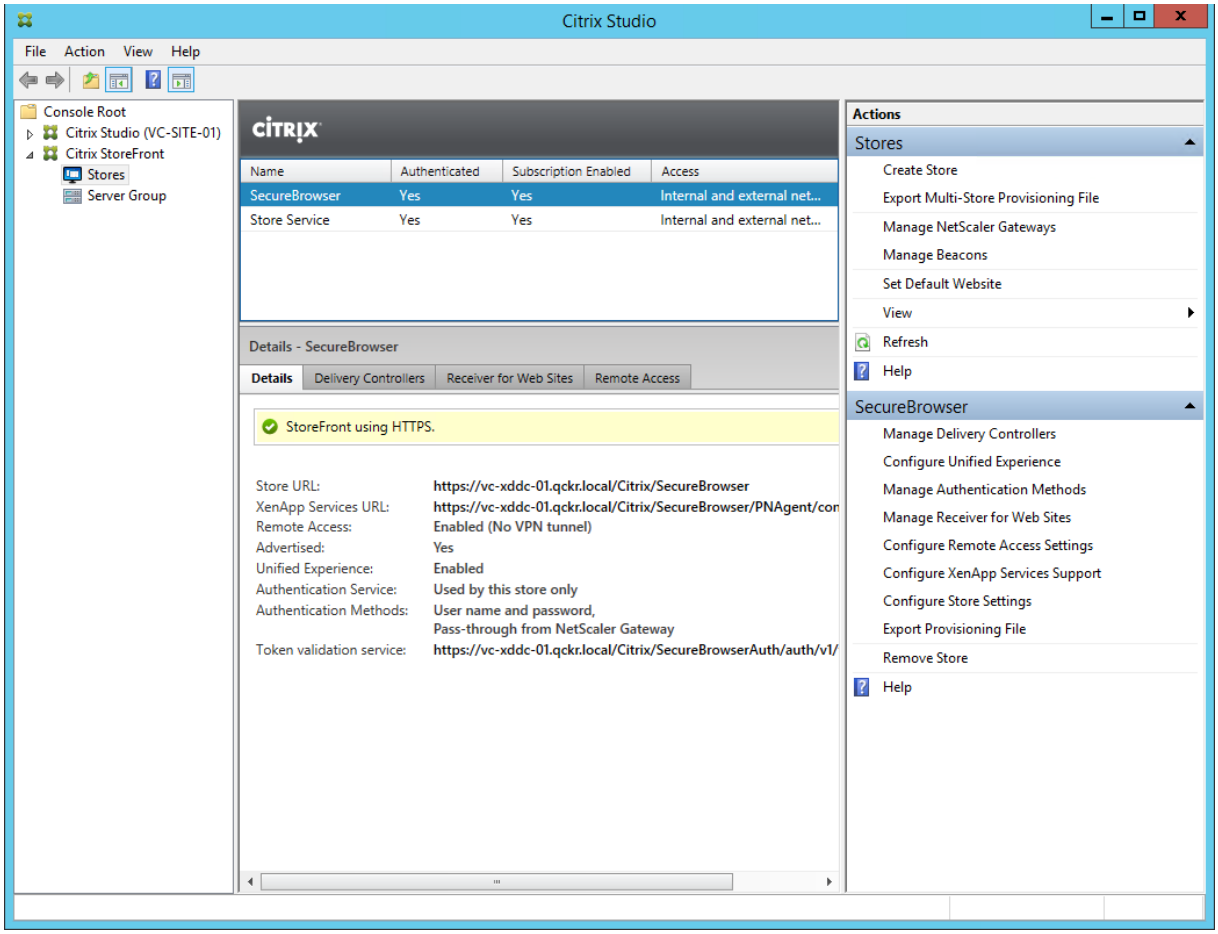


© 1999–2021 Citrix Systems, Inc. All rights reserved.

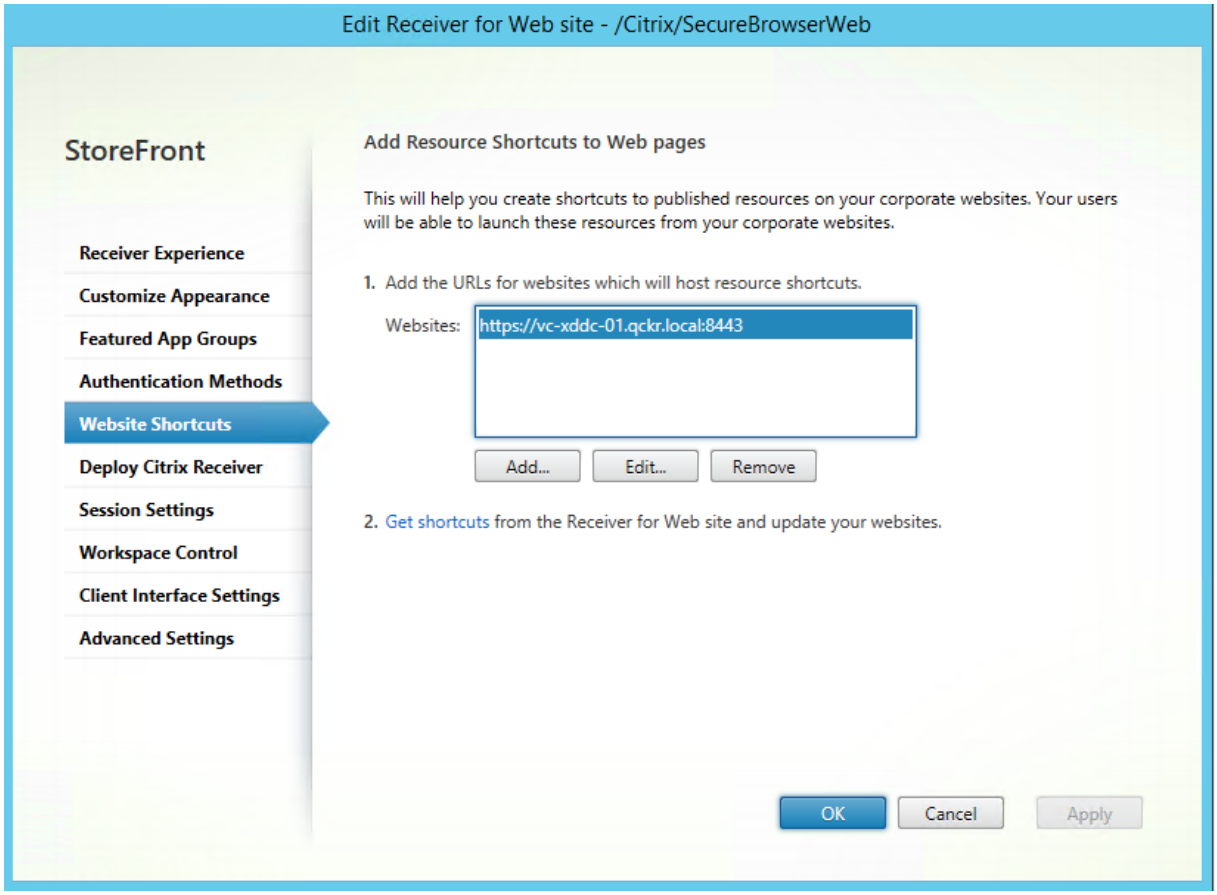




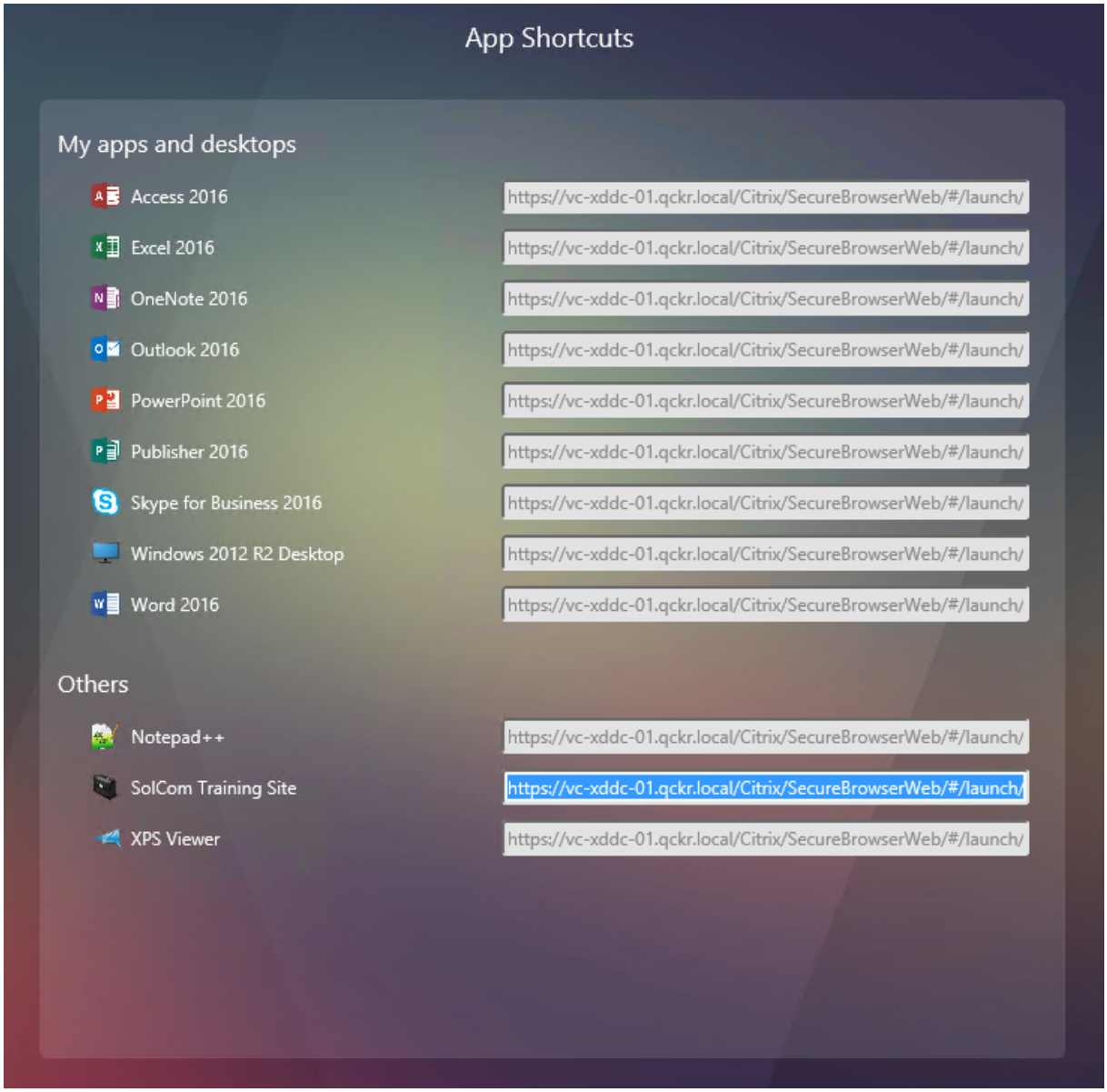
© 1999–2021 Citrix Systems, Inc. All rights reserved.



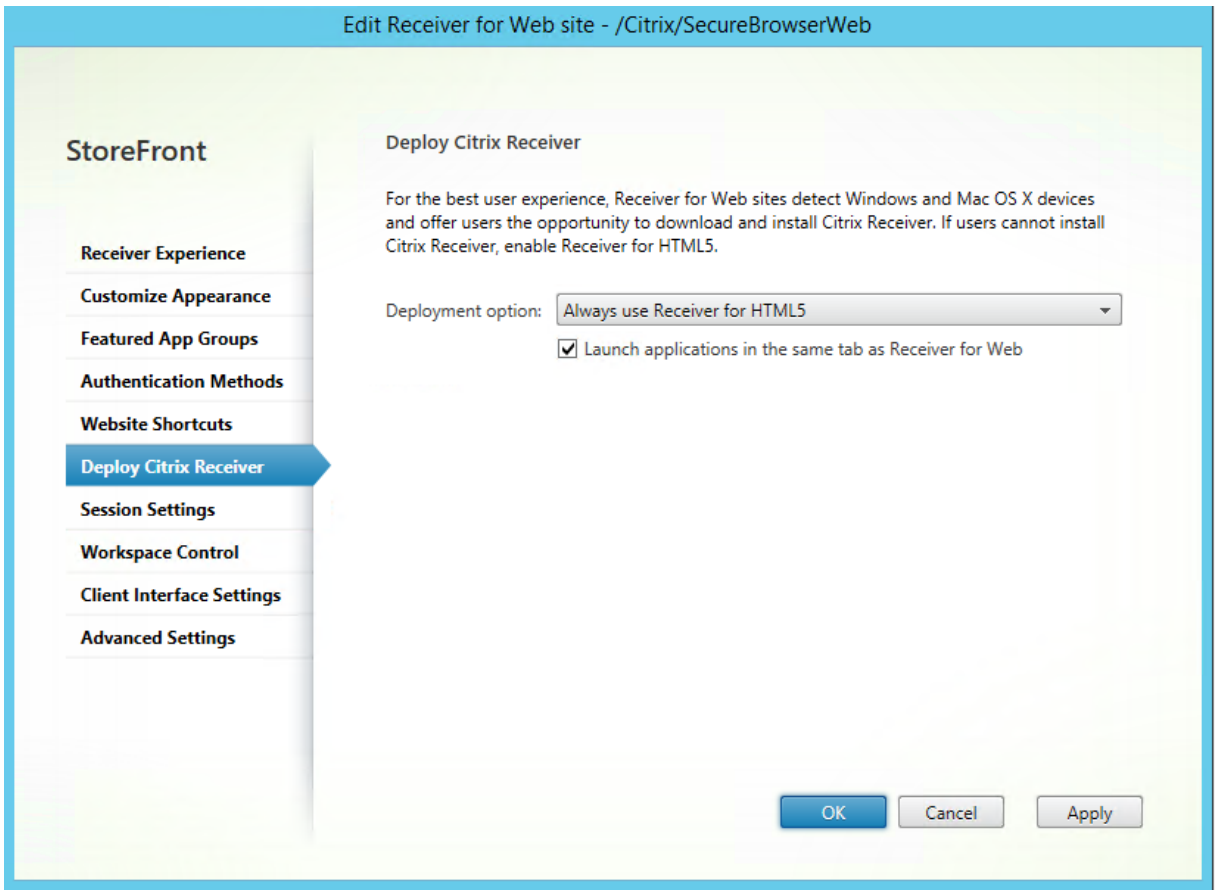
© 1999–2021 Citrix Systems, Inc. All rights reserved.



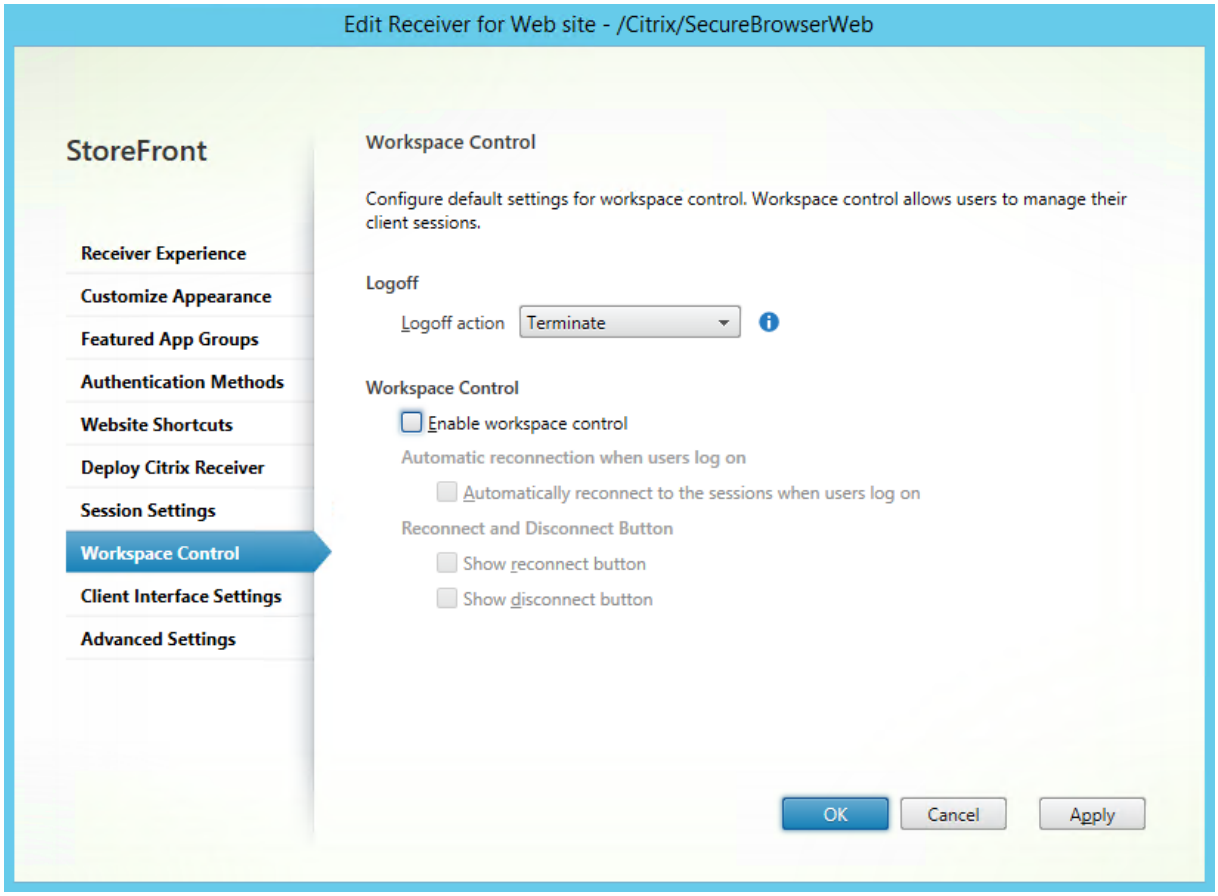
© 1999–2021 Citrix Systems, Inc. All rights reserved.



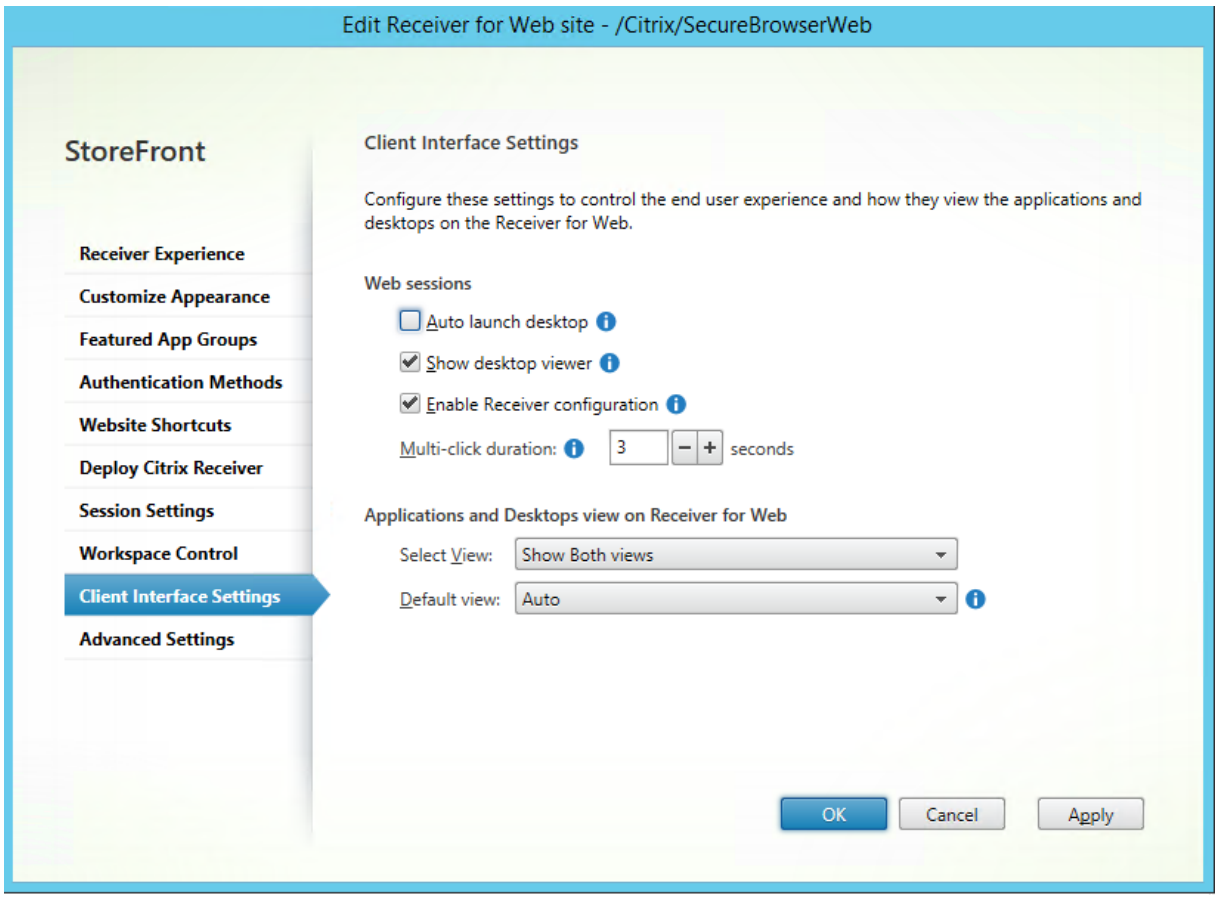
© 1999–2021 Citrix Systems, Inc. All rights reserved.



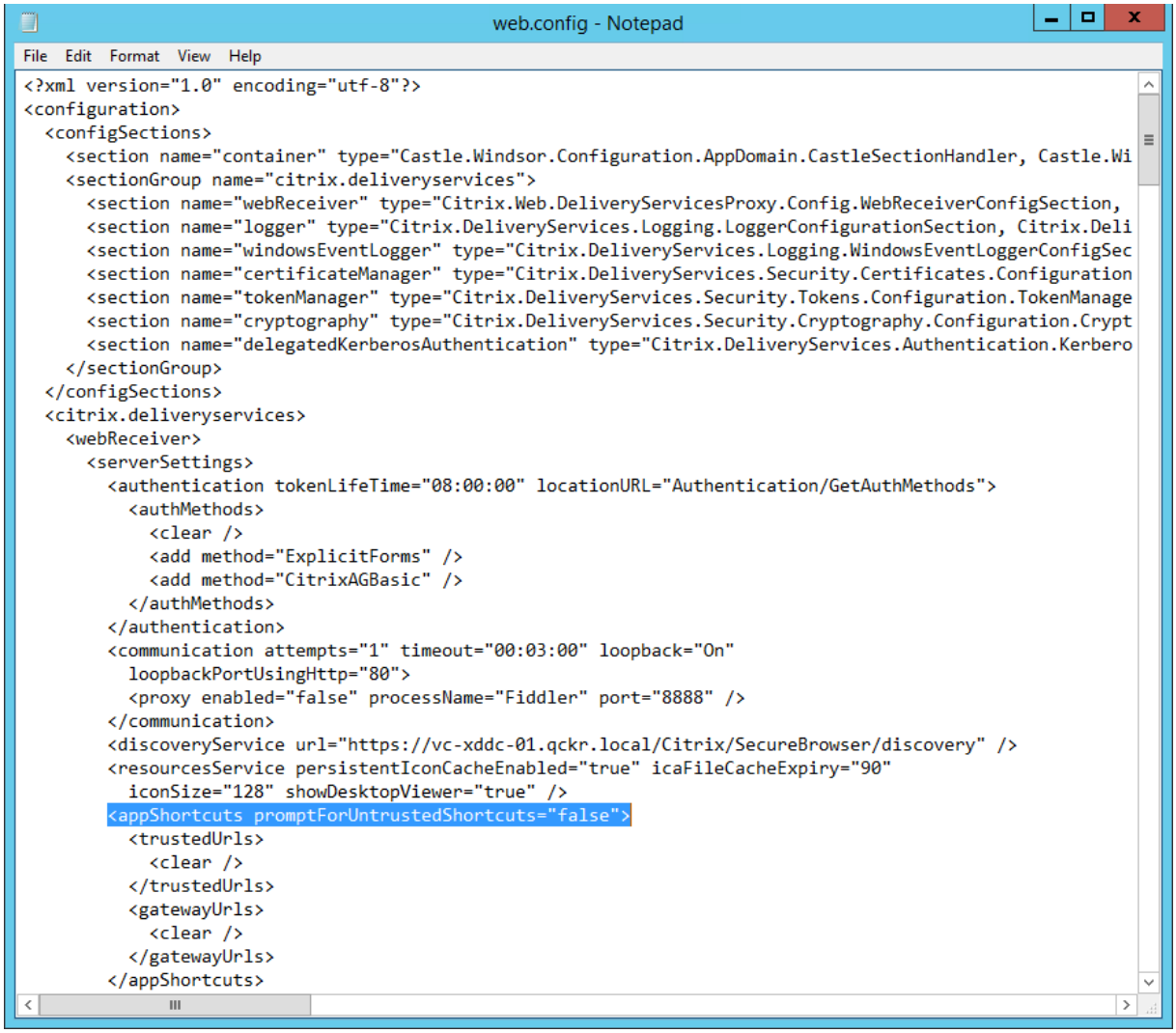
© 1999–2021 Citrix Systems, Inc. All rights reserved.



© 1999–2021 Citrix Systems, Inc. All rights reserved.



© 1999–2021 Citrix Systems, Inc. All rights reserved.



SecureBrowser という新しいストアを作成し、[認証されていないユーザーのみにこのストアへのアクセスを許可する] を選択します。すべてのユーザーが NetScaler Gateway から Controller にトークンを渡すため、トラフィックは認証されます。

XenDesktop コントローラーを追加します。

リモートアクセスを有効にし、次の手順で構成する 2 つ目の NetScaler Gateway を追加します。この構成では、StoreFront /NetScaler Gateway 構成で コールバックアドレスまたは **VIP** アドレスを使用する必要はありません。

ウィザードの既定値を使用して、ストアの作成を完了します。

ストアを作成したら、[**Receiver for Web** サイトの管理] をクリックします。

Receiver for Web サイトの管理ページで、「構成」をクリックし、「**Web** サイトへのショートカット」に移動し、内部 Web サイト URL を追加して、「ショートカットの取得」リンクをクリックします。

公開されている セキュアブラウザーアプリケーションへのアクセス権を持つ通常のユーザーとしてログオンします。

セキュアブラウザアプリケーションの URL をコピーし、テキストファイルに保存して、後で NetScaler Gateway

© 1999–2021 Citrix Systems, Inc. All rights reserved.

構成で使用できるようにします。

Citrix Receiver の **Web** サイトプロパティの編集］に戻り、［Citrix Receiver の展開］をクリックし、［常に **Receiver** を **HTML5** で使用する］を選択します。［**Receiver for Web** と同じタブでアプリケーションを起動する］オプションを選択します。

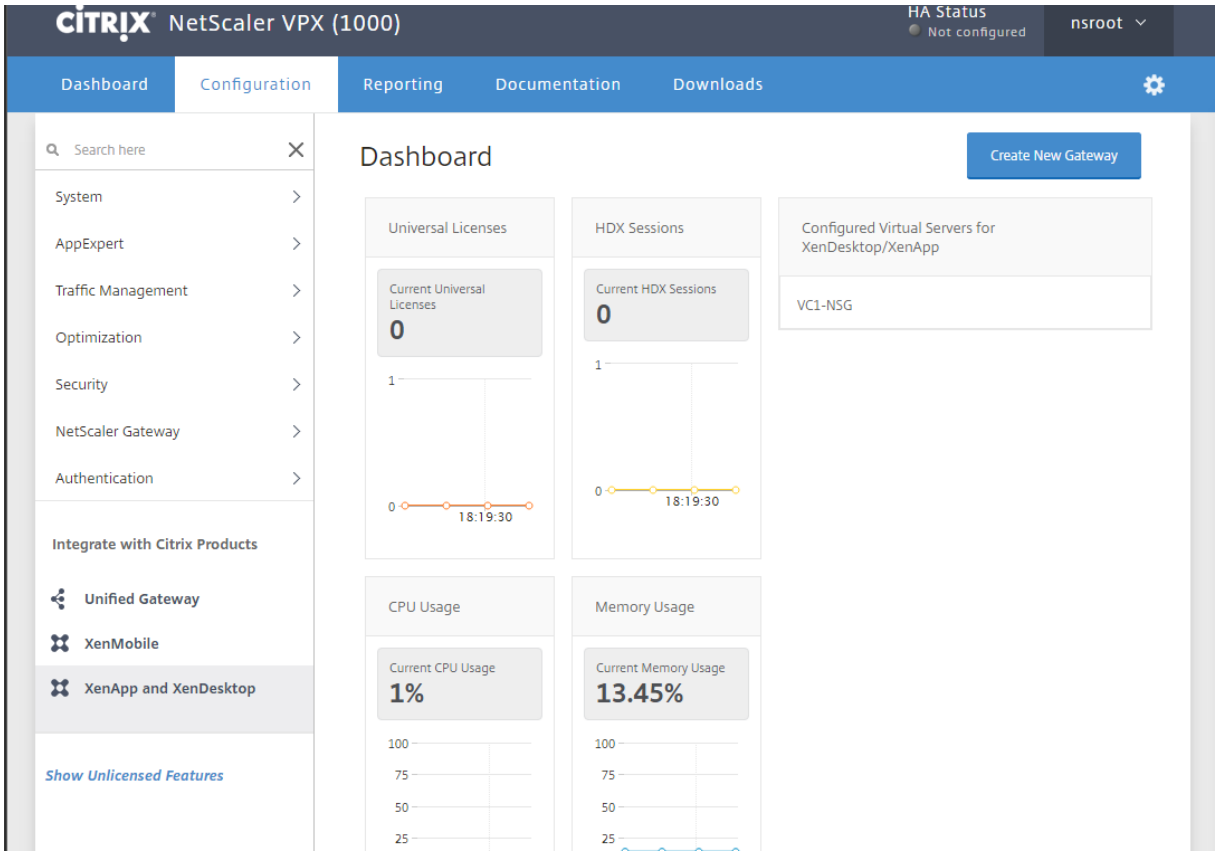
[ワークスペース制御] をクリックし、[ログオフ操作] で [終了] を選択します。[**Workspace** コントロールを有効にする] オプションをオフにします。

[クライアントインターフェイスの設定] をクリックし、[デスクトップを自動起動] オプションをオフにし、[**OK**] をクリックして設定を保存します。

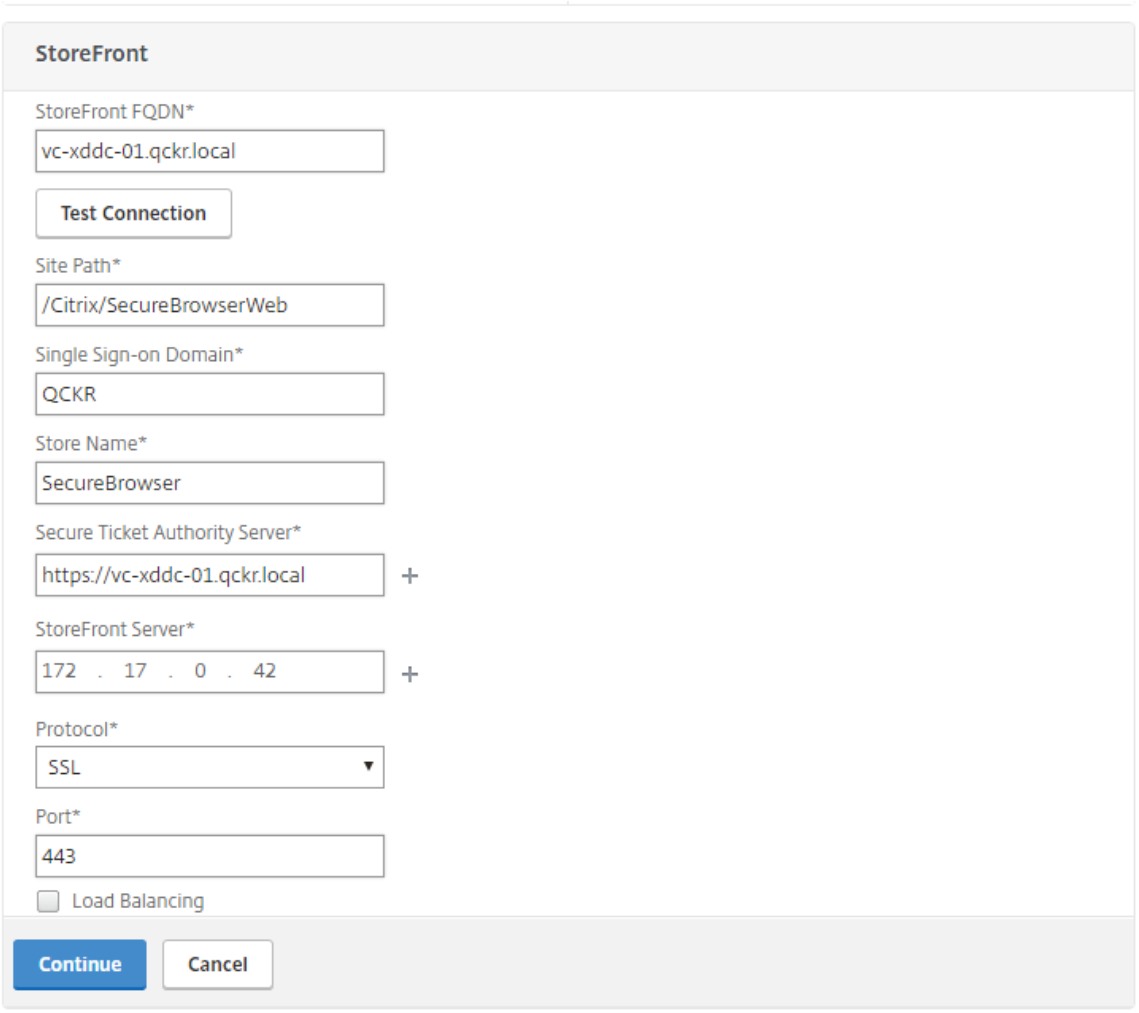
テキストエディタで、ファイル C:\inetpub\wwwroot\Citrix\SecureBrowserWeb\web.config. を開きます。

設定を見つけ *<appShortcuts promptForUntrustedShortcuts="true">*、**false** に設定して変更を保存します。この設定を無効にすると、StoreFront でユーザーにアプリケーションを起動するかどうかを確認するメッセージが表示されなくなります。

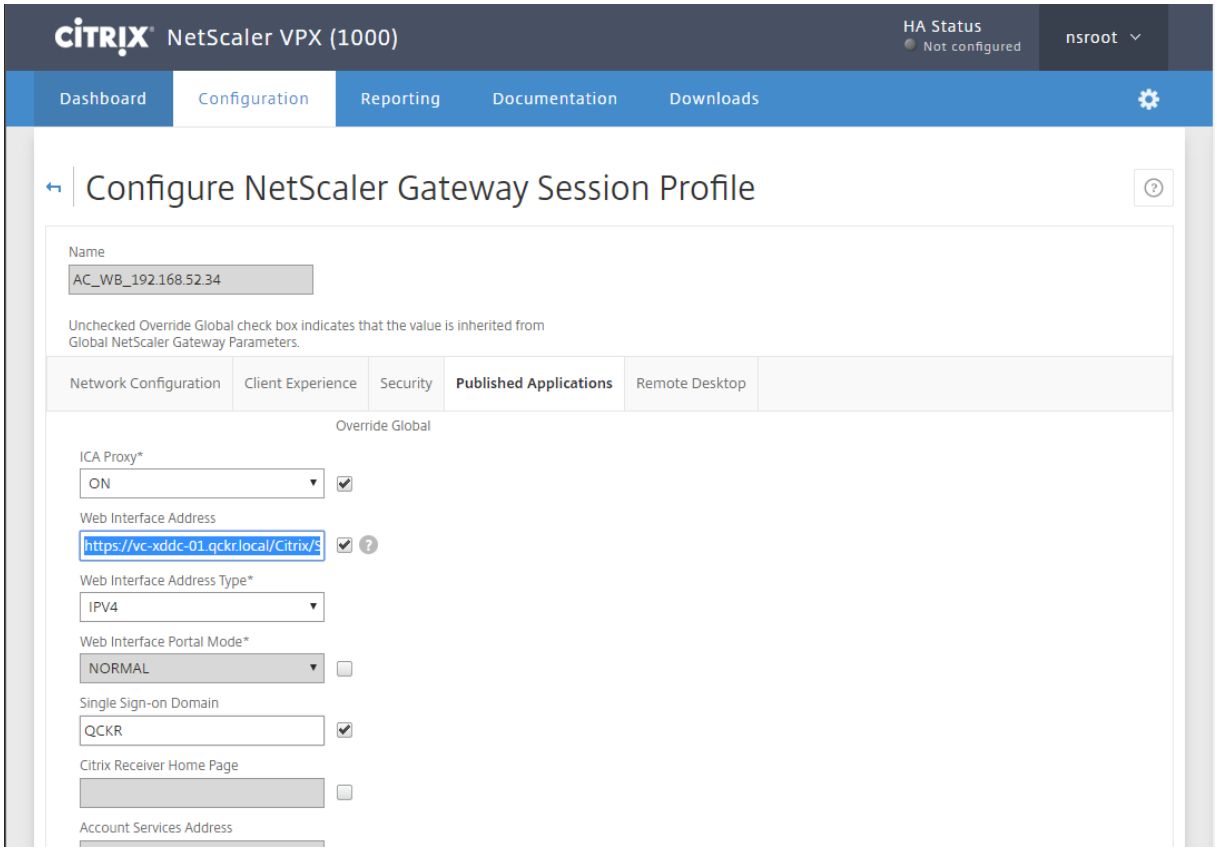
NetScaler Gateway

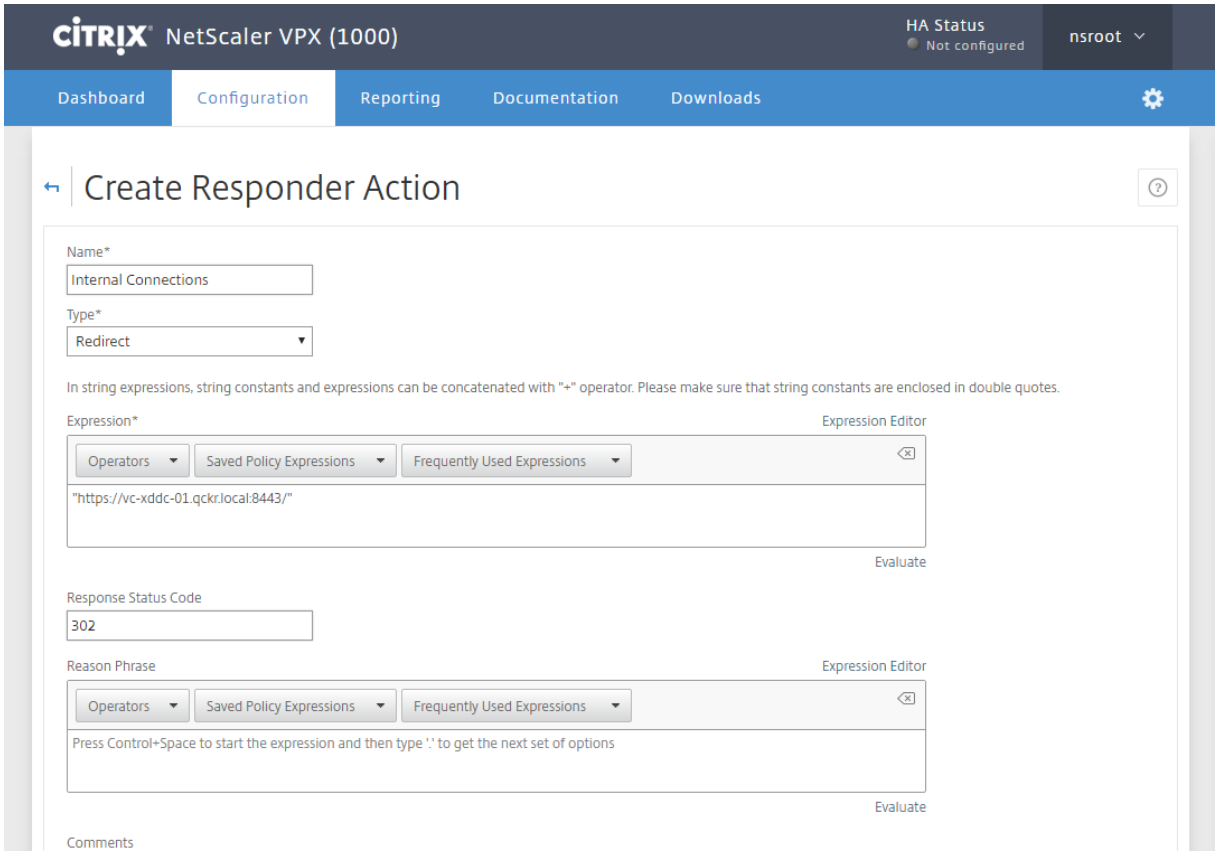


© 1999–2021 Citrix Systems, Inc. All rights reserved.

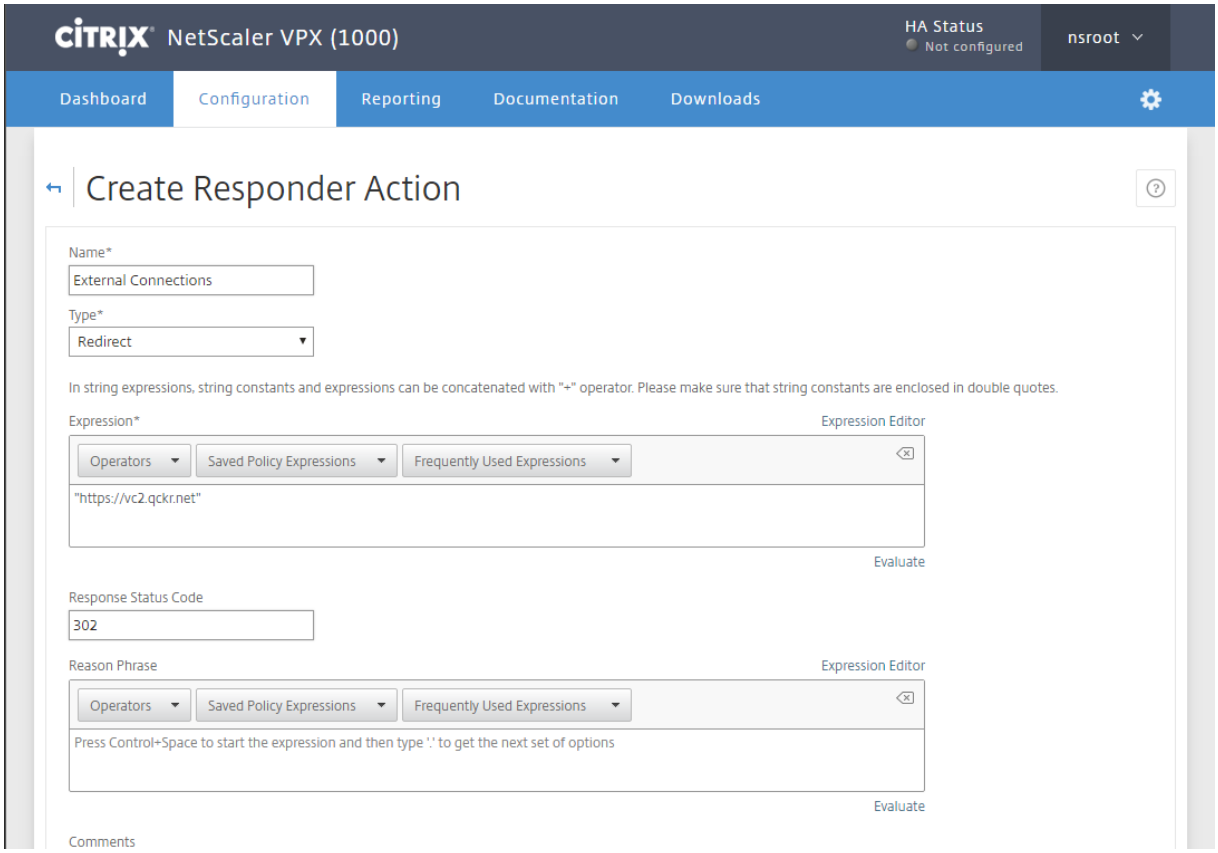


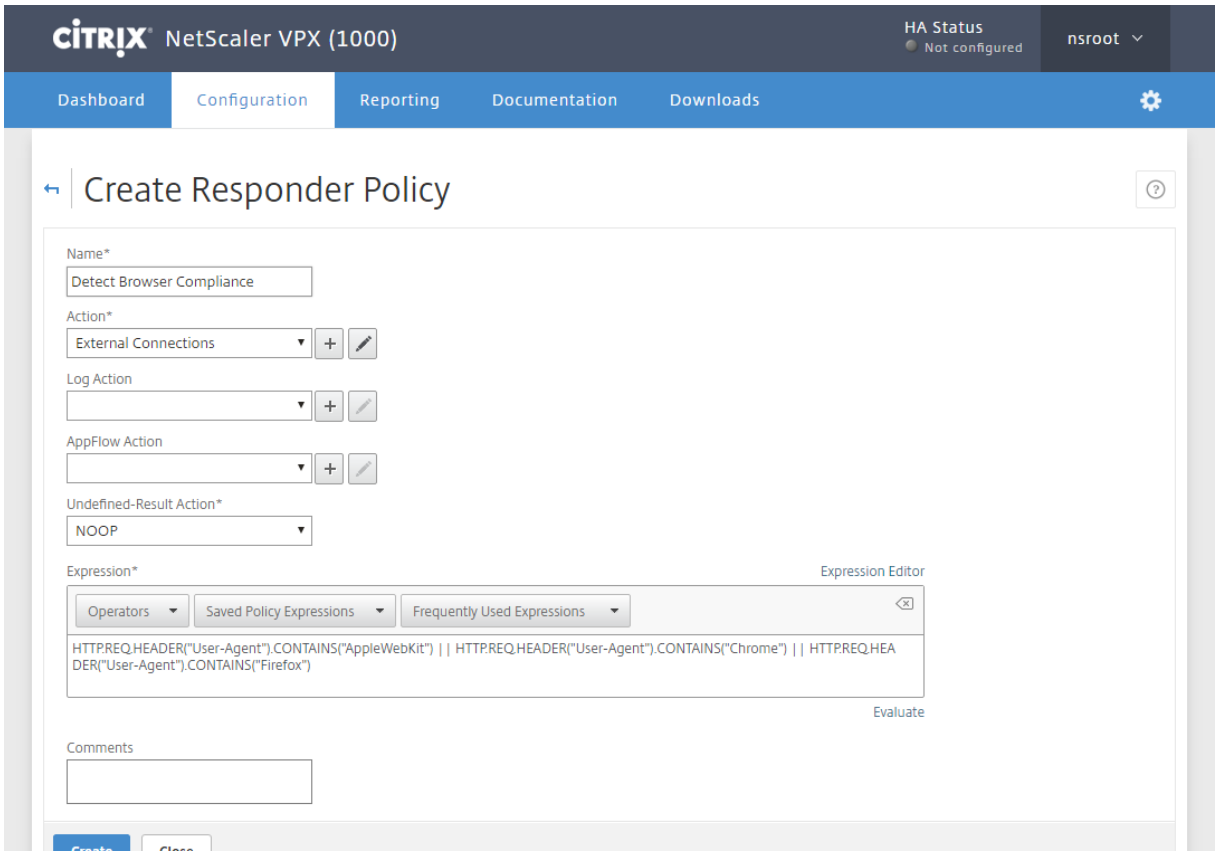
© 1999–2021 Citrix Systems, Inc. All rights reserved.



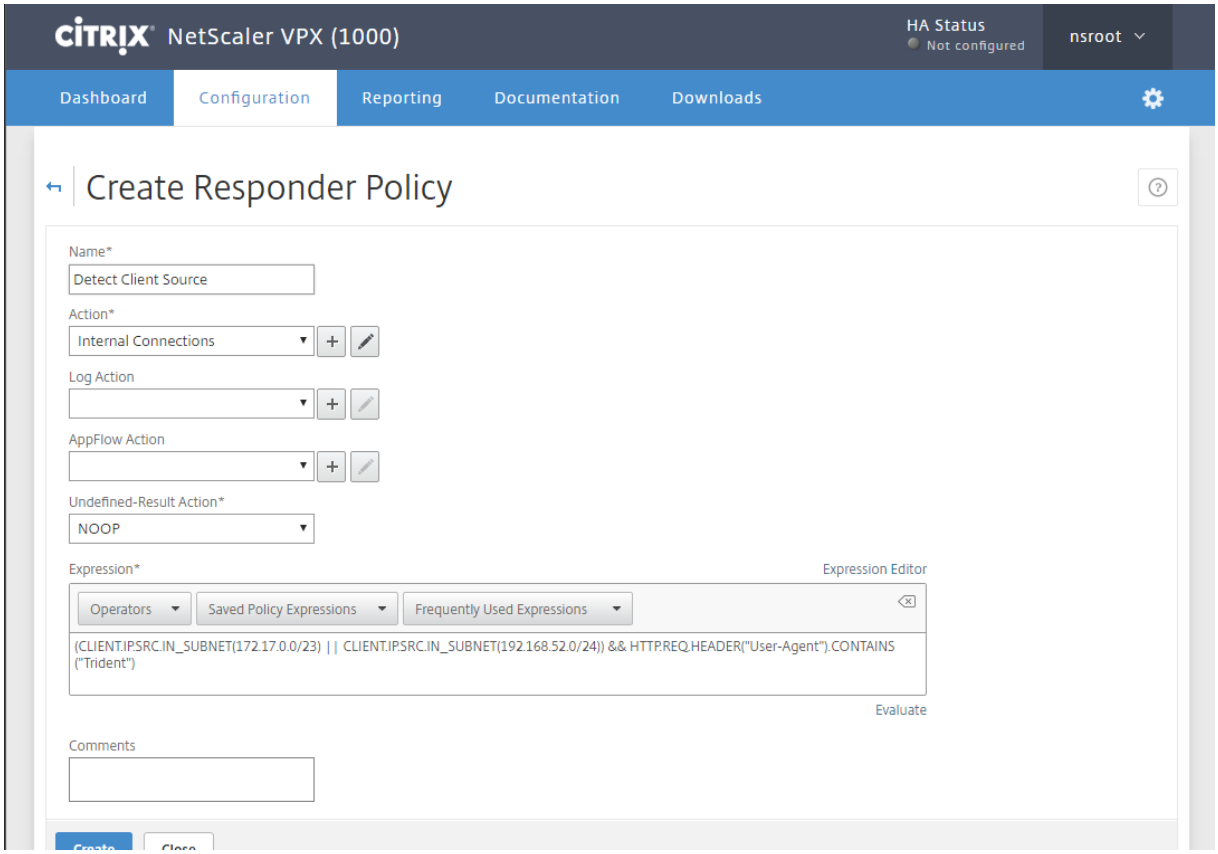


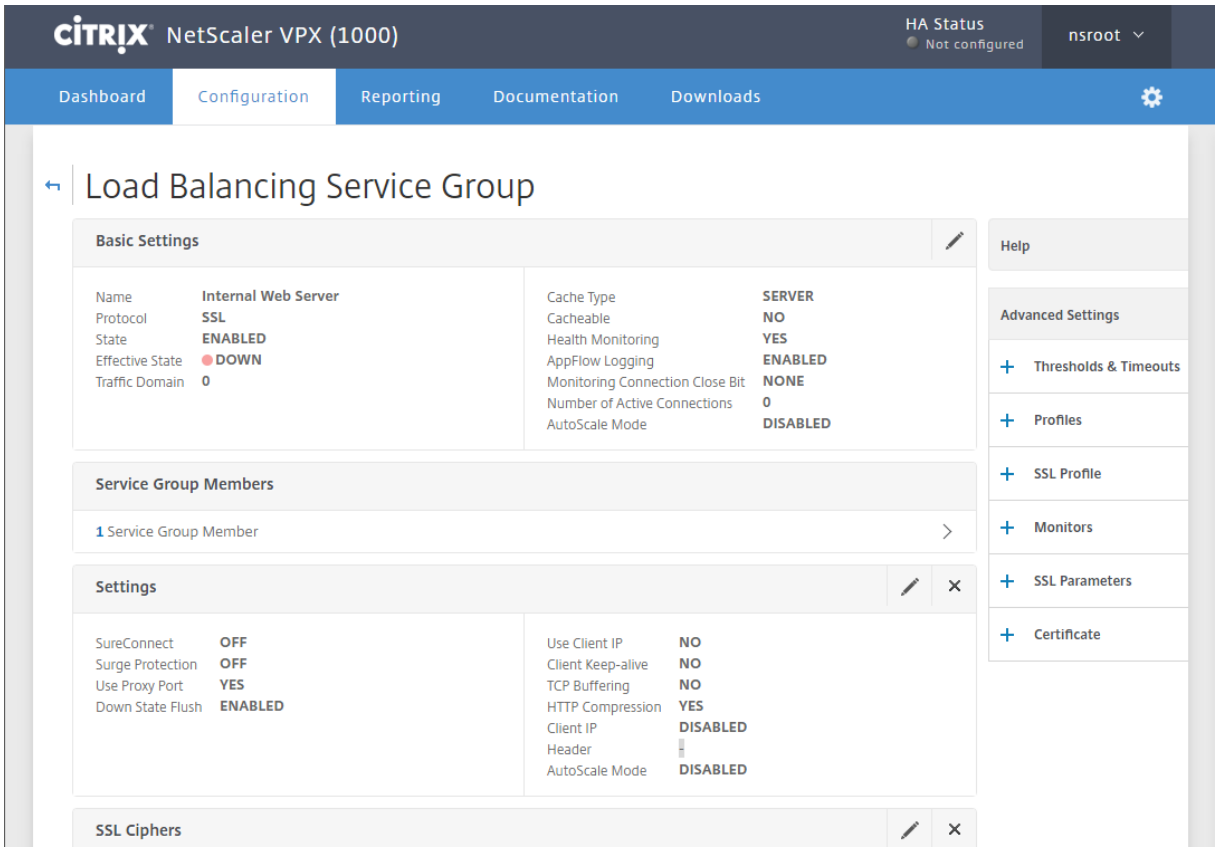
© 1999–2021 Citrix Systems, Inc. All rights reserved.



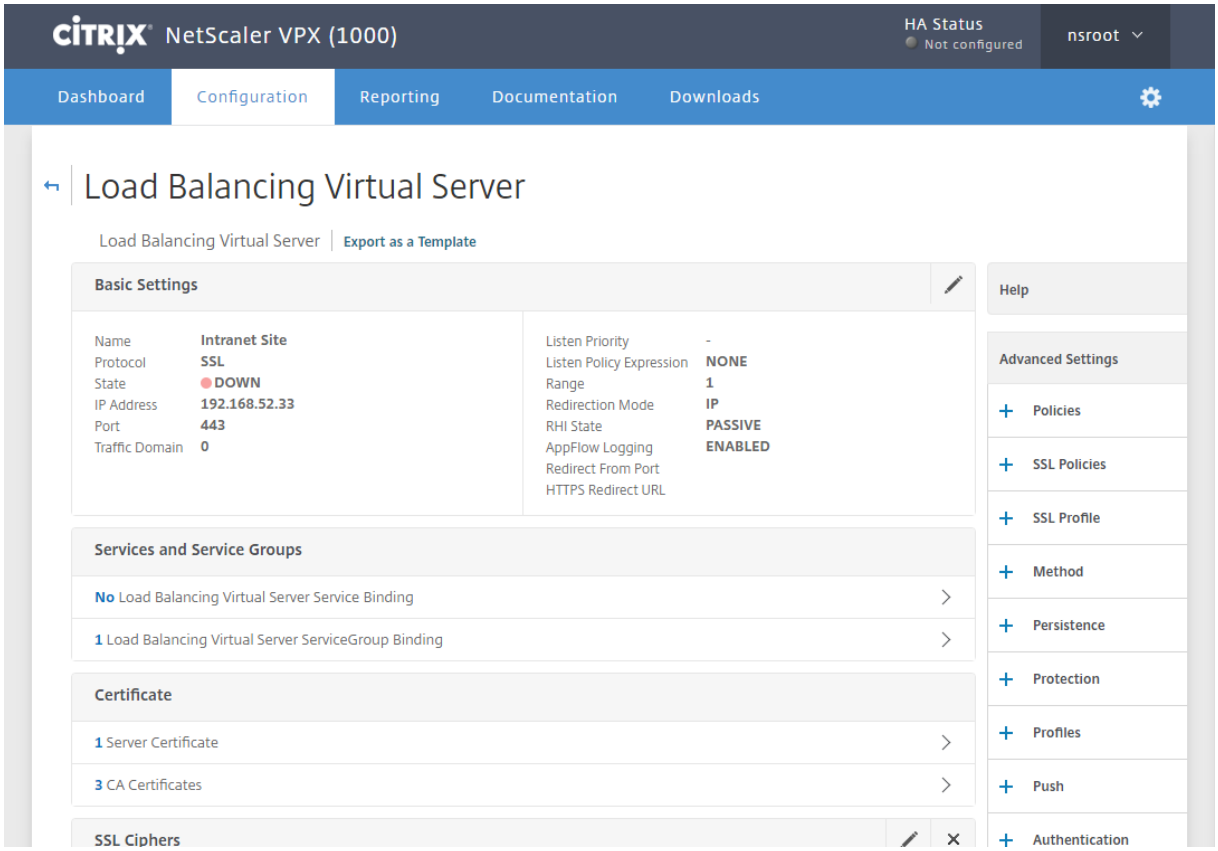


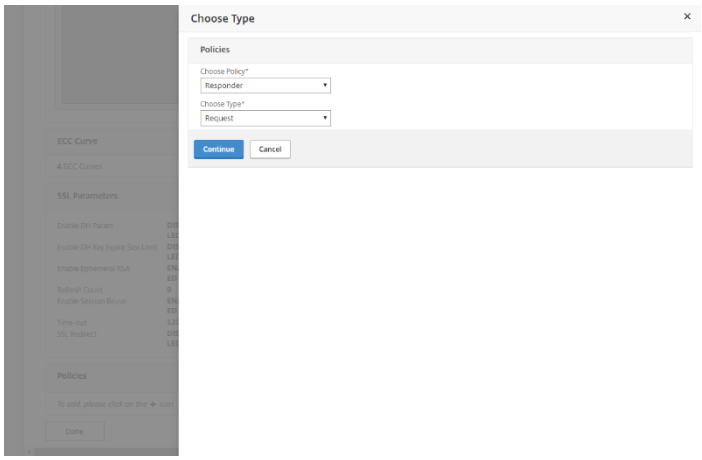
© 1999–2021 Citrix Systems, Inc. All rights reserved.



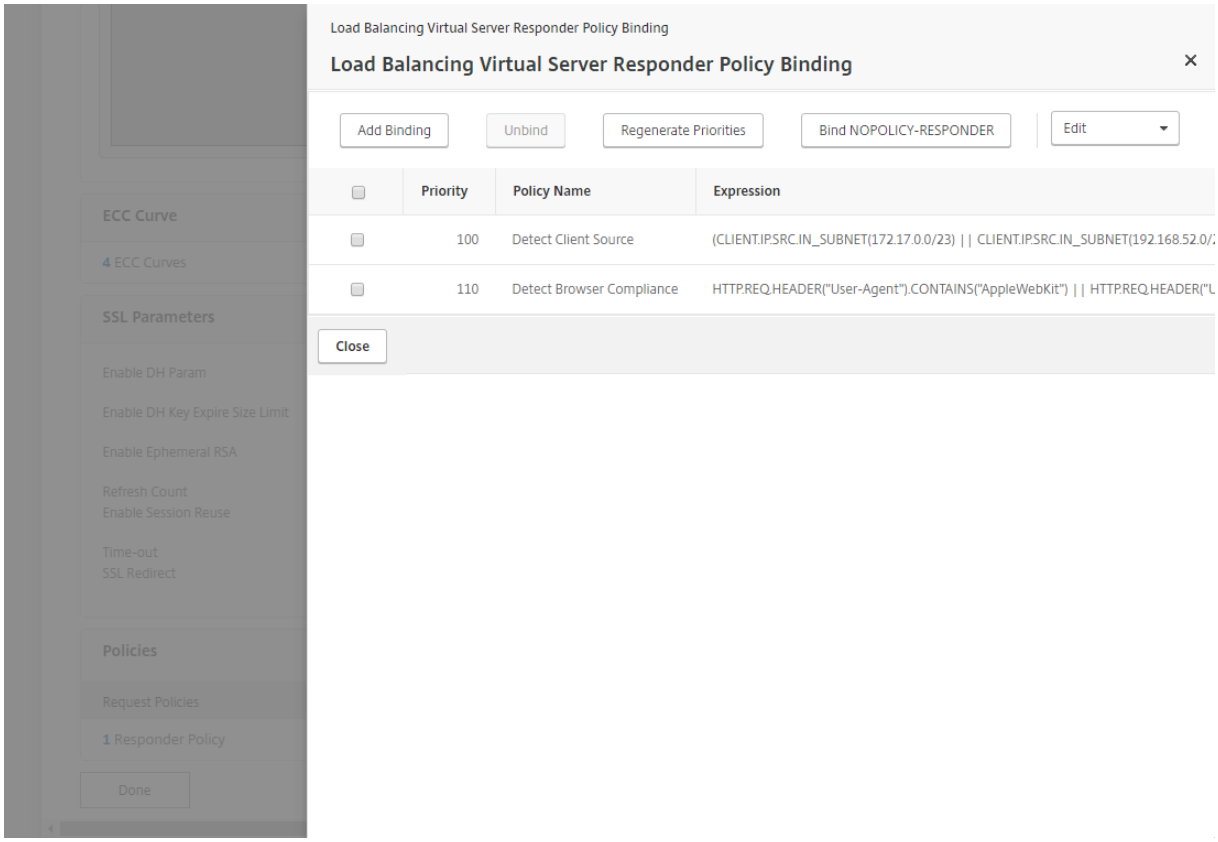


© 1999–2021 Citrix Systems, Inc. All rights reserved.





© 1999–2021 Citrix Systems, Inc. All rights reserved.



NetScaler Gateway の GUI で、ナビゲーションペインで「**XenApp** および **XenDeskto**p」をクリックし、ダッシュボードで「新しいゲートウェイの作成」をクリックします。

StoreFront プロパティで、[サイトパス] を [/Citrix/SecureBrowserWeb] に設定し、[ストア名] を StoreFront サーバーの新しいストアとして セキュアブラウザに設定します。

ウィザードを続行し、新しい仮想サーバーを保存します。

「**NetScaler Gateway** 」ノードで、「ポリシー」を展開し、「セッション」に移動します。

[**Actions**] タブを選択し、2 番目の仮想サーバー用に新しく作成したアクションを編集してから、**AC_WB_** ポリシーアクションを編集します。

[公開アプリケーション] タブで、[**Web** インターフェイスアドレス] フィールドに以前に保存した アプリのショートカット **URL** を貼り付け、[**OK**] をクリックします。

ナビゲーションウィンドウで、[**AppExpert**] ノードをクリックし、[レスポンダー] セクションを展開し、[アクション] をクリックします。

新しい アクションを追加し、「内部接続」という名前を付け、タイプを 「リダイレクト」に設定します。

[式] フィールドで、接続する内部サイトの URL を引用符で囲んで追加します。たとえば、`https://mysite.acme.com`

[作成] をクリックしてアクションを保存します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

新しいアクションを追加し、「外部接続」という名前を付け、タイプを 「リダイレクト」に設定します。

「式」フィールドで、2 番目の NetScaler Gateway 仮想サーバーの URL を引用符で囲んで追加します。たとえば、`https://gateway.acme.com`

[作成] をクリックしてアクションを保存します。

[レスポンダーポリシー] ノードに移動します。

新しいポリシーを追加し、「ブラウザコンプライアンスを検出」という名前で、「アクション」ドロップダウンで、以前に作成した「外部接続」アクションを選択します。

未定義の結果アクションを **NOOP** に設定します。

[式] フィールドに、次のテキストを追加します。

HTTP.REQ. ヘッダー (「ユーザーエージェント」) . 含まれています (「AppleWebKit」)	HTTP.REQ. ヘッダー（「ユーザーエージェント」）. 含む (「クローム」)	HTTP.REQ. ヘッダー（「ユーザーエージェント」）. 含まれています (「Firefox」)

上記の式は、非準拠のブラウザ、またはこのユースケースでは Internet Explorer ではないブラウザーを検出します。

[作成**]** をクリックして変更を保存します。

新しいポリシーを追加し、「クライアントソースの検出」という名前を付けて、「アクション」を「内部接続」アクションに設定します。

未定義の結果アクションを **NOOP** に設定します。

[式] フィールドに、次のテキストを追加します。

(CLIENT.IP.SRC.IN_SUBNET(172	クライアント.IP.SRC.IN_ サブネット (192.168.52.0/24)) &&&HTTP. 要求ヘッダー (「ユーザーエージェント」) . 含む (「トライデント」)

上記の各サブネットを内部ネットワーク環境に合わせて置き換えるか追加します。この場合、ユーザーエージェントは Internet Explorer の構成済みバージョンと一致し、クライアントが内部ネットワークから接続していることを確認します。

[作成**]** をクリックして変更を保存します。

ナビゲーションウィンドウで、[トラフィック管理] **>** [負荷分散] を展開し、[サーバー] を選択します。内部サイトの

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ホストに使用するサーバーを追加します。

ナビゲーションペインで、[**Load Balancin**] の下の [**Service Groups**] をクリックし、新しいサービスグループを追加し、プロトコルを **SSL** に設定し、前の手順で作成した サーバーを [**Service Group Members**] リストにバインドします。

[完了] をクリックします。

ナビゲーションウィンドウで、[負荷分散] ノードの [仮想サーバー] をクリックし、[追加] をクリックして、サーバーに [イントラネットサイト] という名前を付けます。

プロトコルを **SSL** に設定し、ロードバランサーの IP アドレスを入力します。

前の手順で作成した サービスグループ内部 **Web** サーバーをバインドし、外部アクセス用の証明書を構成します。ロードバランサーが SSL を内部 Web サーバーにオフロードできるように、内部ルート CA 証明書を CA 証明書にバインドします。

詳細ウィンドウの [詳細 設定] で、[**+** ポリシー] をクリックします。プラス（+）記号をクリックして、新しいポリシーをバインドします。

[ポリシーの選択**]** で **[**レスポンダー] を選択し、[続行] をクリックします。[クライアントソースの検出] を選択し、優先順位を 100 に設定します。

[バインド] をクリックします。

[レスポンダーポリシー] セクションをクリックし、[バインドの追加] をクリックし、[ブラウザーのコンプライアンスを検出**]** を選択して、優先度を **110** に設定します。[バインド] をクリックします。

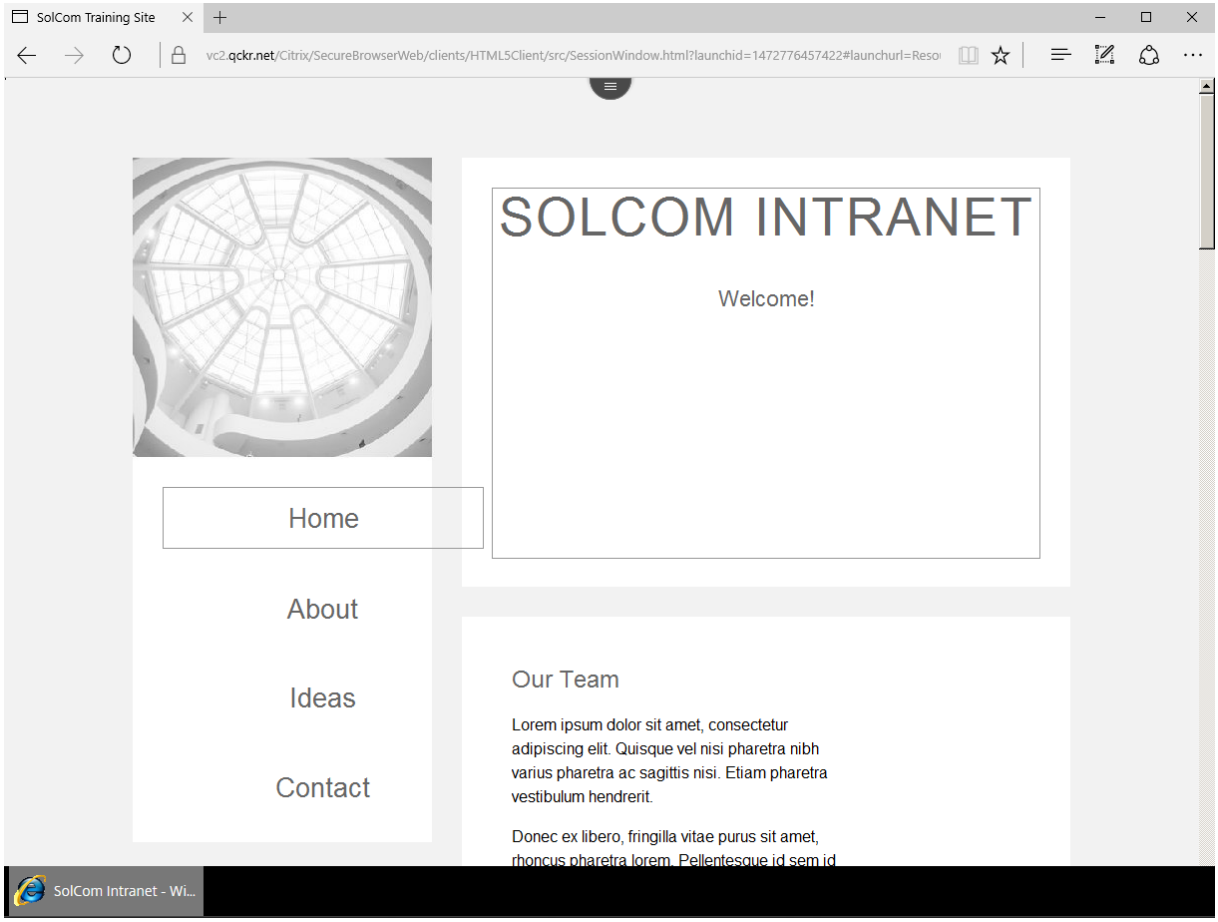
[閉じる] をクリックし、[完了] をクリックします。

NetScaler Gateway 構成を保存します。

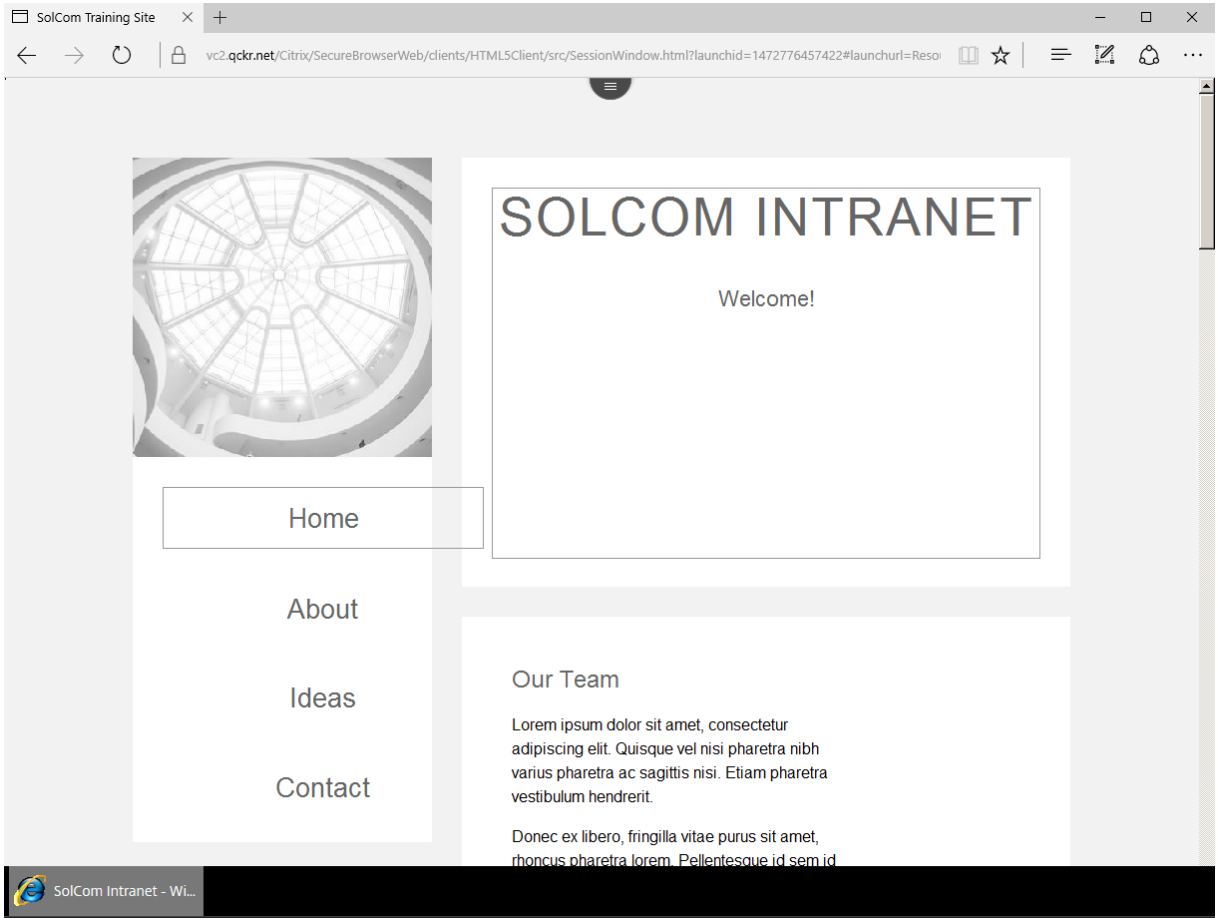
ユースケースの結果と期待

このセクションでは、各ユーザーが前述の設定でどのように接続するかについて、ユースケースと予想される結果を確認します。以下のすべてのユースケースでは、ユーザーがローカルにインストールされたブラウザーを開き、トレーニングサイトの外部 URL を入力します。

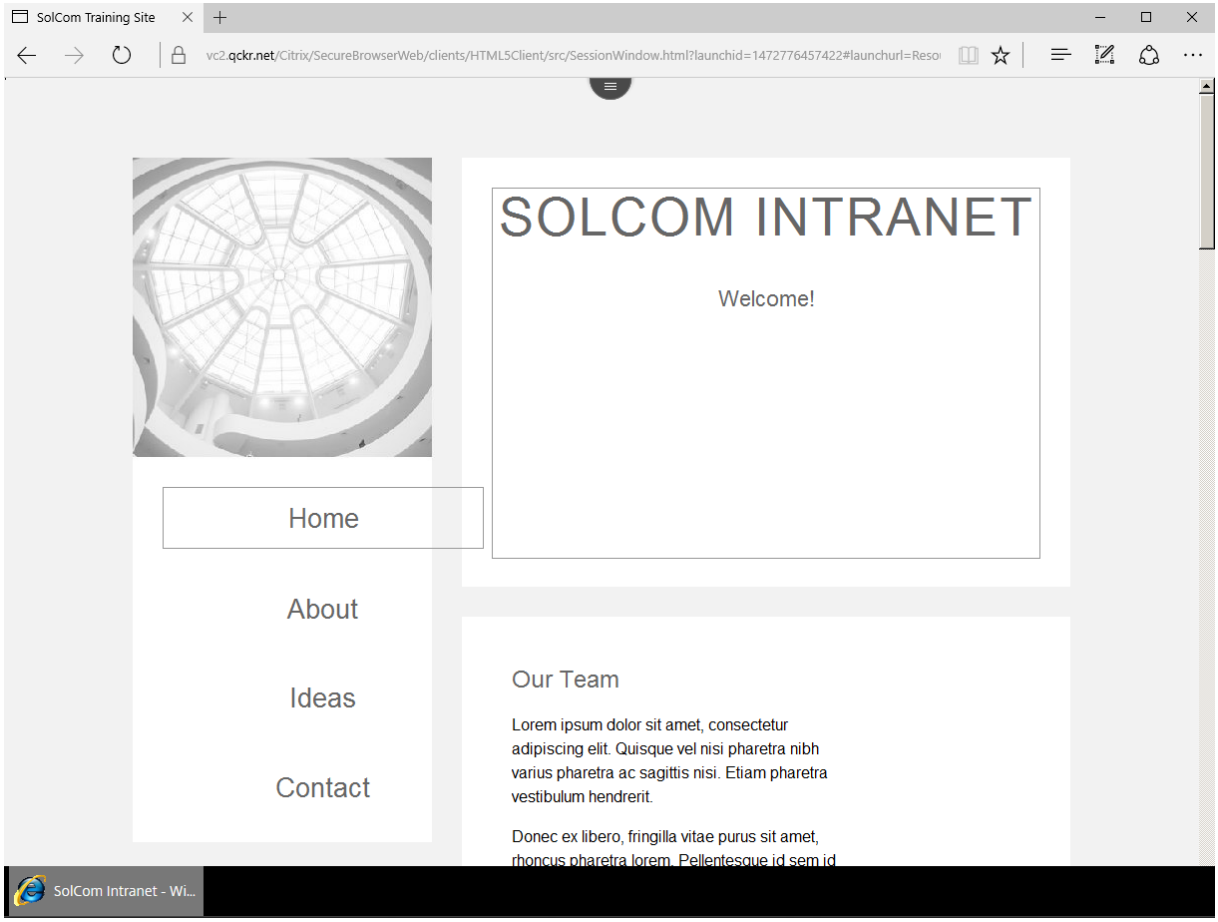
© 1999–2021 Citrix Systems, Inc. All rights reserved.



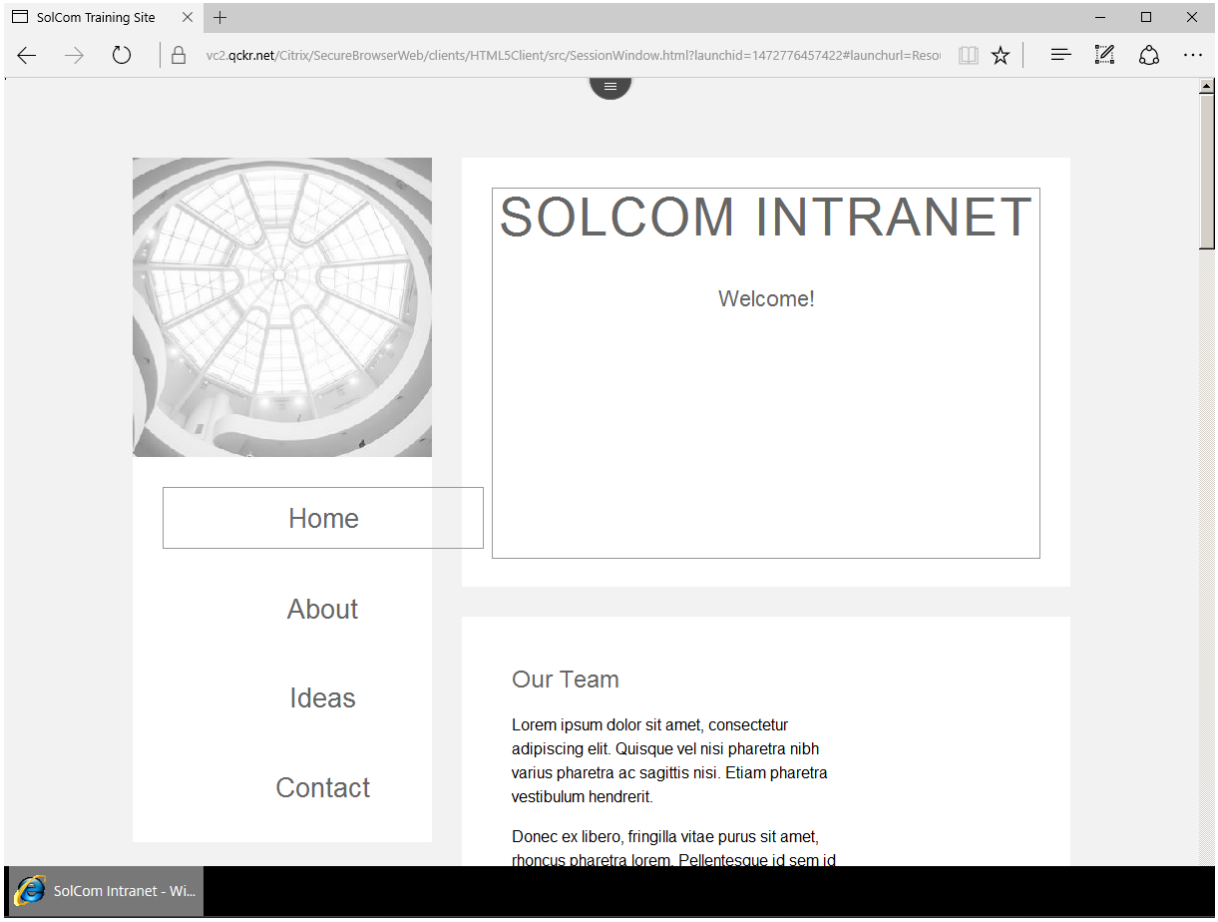
© 1999–2021 Citrix Systems, Inc. All rights reserved.



© 1999–2021 Citrix Systems, Inc. All rights reserved.



© 1999–2021 Citrix Systems, Inc. All rights reserved.



非準拠のブラウザーを持つ外部ユーザ

予想される結果：ユーザーがブラウザタブで Citrix Receiver セッションを起動し、公開されているセキュアブラウザーを使用してサイトをレンダリングします。

準拠ブラウザーを持つ外部ユーザ

予想される結果：NetScaler Gateway は、ローカルブラウザと内部 Web サイト間のトラフィックをプロキシします。

非準拠のブラウザーを持つ内部ユーザー

予想される結果：公開されているセキュアブラウザーを使用してサイトをレンダリングするブラウザタブで Citrix Receiver セッションを起動します。

準拠ブラウザーを持つ内部ユーザー

予想される結果：ユーザーセッションが内部サイトにリダイレクトされます。クライアントが内部ネットワークから接続しているため、NetScaler Gateway は接続をプロキシしません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

既知の制限事項

- NetScaler Gateway 仮想サーバーへの動的 URL の受け渡しは、セキュリティで保護されたブラウザーの Citrix Receiver for HTML5 の使用をサポートしていません。
  - 起動 URL を仮想サーバーに渡すには、セッションプロファイルで ICA プロキシを無効にします。ICA プロキシは、Citrix Receiver for HTML5 の要件です。
- Citrix Receiver for HTML5 では、コンテンツのリダイレクトはサポートされていません。
  - 管理者は、Web サイト用に StoreFront で Citrix Receiver を構成できます。
- 複数のサイトを持つ環境では、サイトごとに異なる NetScaler Gateway セッションポリシーを作成し、それらを仮想サーバーにバインドするか、内部サイトの URL をホストできる内部起動ポータルを作成します。

参照ドキュメント

- SSL を使用して XenApp および XenDesktop 7.6 で ICA 接続をセキュリティで保護する方法

ローカルホストキャッシュのサイズ設定とスケーリング

May 18, 2020

ローカルホストキャッシュは、XenDesktop 7.6 で提供される接続リース機能を置き換えるために、XenApp および XenDesktop 7.12 で導入されました。ローカルホストキャッシュは、接続リースよりも多くのシナリオをカバーしますが、設計上の考慮事項は異なります。

接続リース機能の設計上の考慮事項の詳細については、https://www.citrix.com/blogs/2014/11/11/xendesktop-7-6-connection-leasing-design-considerations/を参照してください。

- ローカルホストキャッシュは、接続リースよりも多くのユースケースをサポートします。
- ローカルホストキャッシュは、接続リースよりも多くのリソース（CPU とメモリ）を必要とします。
- 停止モードでは、ゾーンごとに 1 つのブローカのみが VDA 登録とブローカセッションを処理します。
- 選挙プロセスは、停止時にどのブローカーがアクティブになるかを決定しますが、ブローカーリソースは考慮しません。
- ゾーン内の 1 つのブローカが通常の操作中にすべてのログオンを処理できない場合、停止モードでは正常に機能しません。
- 停止モード中はサイト管理を使用できません。
- 高可用性 SQL Server が引き続き推奨される設計です。
- 断続的なデータベース接続のシナリオでは、SQL Server を分離し、すべての根本的な問題が修正されるまで、サイトを停止モードのままにすることをお勧めします。
- ゾーンあたり 5,000 の VDA に制限があります（強制されません）。
- 14 日間の制限はありません。
- プールされたデスクトップは、デフォルトの構成では停止モードではサポートされません。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

アーキテクチャ

XenDesktop 7.6 で接続リースが導入され、サイトデータベースが停止している間もリソースに引き続きアクセスできるようになりました。VDI プールされたデスクトップはサポートされていませんでした。デフォルトでは、ユーザーは過去 14 日以内にリソースに接続している必要があります。さらに制限事項として、通常の操作中に最後に接続したデスクトップまたはアプリケーションホストにユーザーを接続しようとすることがありました。これが利用できない場合、接続は仲介されません。

2 つのテクノロジー（接続リースとローカルホストキャッシュ）のアーキテクチャは非常に異なっており、動作するには異なるリソースが必要です。接続リースでは、個々の XML リースファイルが作成されます。これには、サイト内のリソース数によっては、数 GB のディスク容量が必要になる場合があります。ローカルホストキャッシュは、ローカル SQL Server データベースを使用し、ディスク領域の使用効率が向上しますが、接続リースよりもメモリと CPU がかなり多くなります。両方とも、メインサイトデータベースからの詳細がブローカー（コントローラ）に同期される同期のフェーズがあります。接続リースの初期同期では、ファイルシステム上に作成される個々のファイルの数が多いため、かなりの IOPS が発生する可能性があります。ローカルホストキャッシュは、IOPS を必要とする SQL データベースを使用しますが、これらの書き込みを最適化する SQL という利点があります。

複数のブローカーを使用した接続リース設定では、各ブローカーは XML リースのコピーを持ち、停止時に接続を仲介できるため、負荷の分散に役立ちます。ただし、ローカルホストキャッシュでは、すべての接続を仲介し、VDA 登録を処理する単一のブローカーが選択されます。サイト内のすべての VDA は、この単一のブローカに再登録されます。そのため、ブローカーは、通常の操作ではマルチブローカサイトと比較して、特に多数の VDA を持つサイトではリソースの需要が高くなります。

ローカルホストキャッシュは、sqlserver.exe プロセスとしてタスクマネージャに表示される Microsoft LocalDB を使用します。データベースバッファプールキャッシュに最大 1 GB のメモリを使用するように構成されています。しかし、SQL エンジンがそれ自身や他の小さなキャッシュのためにメモリを必要とするため、プロセスはこれを超えて成長します。一般に、停止時間が長くなり、停止モード中にアクセスされるリソースが増えるほど、LocalDB メモリの使用量が増加します。ただし、サイトデータベースの接続が復元されると、sqlserver.exe はこのメモリを保持し、すぐにメインプールに返されません。

停止モード時の **CPU** ソケットとコアの影響

以前のリリースの XenApp および XenDesktop では、管理者はブローカー（コントローラー）マシンの CPU 構成（物理マシンまたは仮想マシンのソケット数とコアの数のレイアウト）に必ずしも関心を寄せていませんでした。

ローカルホストキャッシュは、LocalDB と呼ばれるランタイムバージョンの SQL Server を使用します。LocalDB には、4 つのコアまたは 1 つのソケットのうち小さい方に制限する特定のライセンスがあります。これは、物理マシンまたは仮想マシンがシングルコアまたはデュアルコアのみを持つ複数のソケットで構成されている場合、パフォーマンスに大きな影響を与える可能性があります。4 つのソケットとソケットごとに 1 つのコアを持つブローカーマシンは、LocalDB を単一のコアを使用するように制限しますが、1 ソケット 4 コアマシンとして設定されている同じ VM は、LocalDB が 4 つのコアすべてにアクセスできるようにします（他のプロセスと共有しますが）。停止モードでは、LocalDB は、通常の動作時と同じブローカと SQL コードを実行します。SQL クエリの多くは CPU を大量に消費し、停止モード中の仲介のパフォーマンスに直接影響を与えます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

その他の要因には、サイト構成自体が含まれます。

- 公開アプリケーションの数
- 仲介されるユーザーの数
- ユーザーがセッションを起動しようとする頻度
- Active Directory パフォーマンス

ブローカの CPU 使用率の合計が 100% に近づくと、仲介応答時間が長くなり、ログオンの処理に時間がかかり、一部のログオンが失敗することがあります。

複数のブローカーがあるサイト

サイト停止モードでは、1 つのブローカーだけが登録要求とログオン要求を処理します。マルチブローカーのサイトでは、停止中にアクティブになるブローカーを指名するために選挙プロセスが行われます。しかし、この選挙プロセスは、ブローカーが利用可能な物理的なリソースを考慮しません。つまり、ブローカーが異なる量のリソースを持つサイトでは、選出されたブローカーが必ずしも CPU や RAM に関して最も強力であるとは限らず、停止モード中にパフォーマンスが低下する可能性があります。各ブローカが選出された場合に備えて、ローカルホストキャッシュの追加要件を満たしていることが重要です。

サイトデータベースとの同期

CitrixConfigSync サービスは、サイトデータベースからブローカーのローカルコピーへのデータのインポートを処理します。これは、サイト構成の変更についてサイトデータベースを監視し、変更が発生したときに新しいインポートをトリガーします。現在のローカルデータベースのコピーは、インポートの開始前に作成されます。サイト内のリソース（VDA など）の数が多いほど、インポートにかかる時間は長くなりますが、5000 の VDA を持つサイトの場合は 10 分未満になります。

データベースの場所

ローカルデータベースは、次の場所に格納されます。

C: Windows サービスプロファイルネットワークサービスデータベース名.mdf

信頼性を確保するために、CitrixConfigSync サービスは、新しいサイトデータベースの同期を開始する前に、以前に同期されたデータベースのインポートのバックアップを作成します。何らかの理由で同期が成功しない場合は、同期が正常に完了するまでバックアップが使用されます。データベースは手動でコピーしないでください。

ローカルホストキャッシュとコネクションリースの比較

© 1999–2021 Citrix Systems, Inc. All rights reserved.

	接続リース	ローカルホストキャッシュ
ディスク領域	2 GB を推奨	サイトの構成によって異なります。125 K ユーザを持つ 50 台の RDS ホストでは、300 MB が使用されます。
RAM	100 MB	3 GB、最大 1 GB、高可用性サービスおよび CitrixConfigSync サービスの場合は 2 GB です。
構成を同期する時間	IOPS に依存、40,000 の VDA：約 26 分	5,000 台の VDA：約 7 分
停止中のアクティブ化に要する時間	150 秒、30 秒のデフォルト SQL タイムアウト + 120 秒の待機期間（設定可能）	VDA の数とブローカとの最後の登録同期によって異なります。停止モード中に VDA 登録に使用できるブローカは 1 つのみであるため、多数の VDA では、すべての VDA が登録されるまでに数分かかることがあります。
通常のオペレーションのリストアに要する時間	リースを無効にするのに 120 秒かかります。その後、VDA をブローカーに再登録する必要があります。	上記のように、VDA はセカンダリブローカからの登録を解除し、プライマリブローカに再登録する必要があります。
サポートされる VDA の数	50,000	5,000. サイトにはこれ以上のものがありますが、サイトデータベースの同期に必要な時間は VDA の数に応じて増加します。多数の VDA を持つ単一のブローカーのパフォーマンスにより、停止中に一部の接続が仲介されないことがあります。
停止中のサイト管理	いいえ	いいえ

ローカル **DB** のメモリ制限の設定

LocalDB プロセスは、キャッシュ用に 1 GB の RAM に制限されていますが、通常は変更する必要はありません。この値は、必要に応じて変更できます。変更を有効にするには、サイトが通常の操作 (停止モードではなく) で、サイトデータベースの同期を強制する必要があります。

メモリを 768 MB に減らすには、次の手順に従います。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

手順 **1.** C:\Program ファイル\ Citrix\ ブローカー\ サービス\ 高可用性サービス.exe.config ファイルを編集します。

<appSettings>“ セクションを探し、エントリを追加します。

```
<add key="MaxServerMemoryInMB"value="768"/>
```

手順 **2.** データベースの同期を強制するには、高可用性サービスを停止します。sqlserver.exe が実行されている場合は、タスクマネージャーまたは PowerShell を使用して停止します。

手順 **3.** 次に、サイトに簡単な変更を加えます。たとえば、デリバリーグループの説明を「.」を追加して変更し、再度削除します。次に、高可用性サービスを起動します。これは sqlserver.exe を起動し、同期が発生します。

メモリを減らしすぎるとパフォーマンスに影響するため、推奨されません。ただし、2 GB に増やすとパフォーマンスが大幅に向上せず、CPU リソースは RAM よりもボトルネックになります。

ローカルホストキャッシュの有効化または無効化

接続リースとローカルホストキャッシュの両方を無効にできますが、一度にアクティブにできるのはそのうちの 1 つだけです。

ブローカーサイトの設定 — コネクションリースの有効化 $False

Set-BrokerSite –LocalHostCacheEnabled $True

制限事項

デスクトップは、停止モードで使用する前に、割り当てられている必要があります。割り当てられていないデスクトップは仲介に使用できません。これにより、ユーザーが実際にデスクトップを割り当てているにもかかわらず、すべての割り当てが同期される前に停止が発生した場合、デスクトップが使用不能になり、「メンテナンスモード」と報告される可能性があります。

プールされたデスクトップは、デフォルトの構成では停止モードではサポートされません。回避策はありますが、セキュリティとパフォーマンスに潜在的な影響があります。プールされたデスクトップを含むデリバリーグループを、ログオフ時に再起動しないように構成すると、そのグループ内のパワーオンされたプールされたデスクトップは停止モードで使用できるようになります。ただし、ユーザーがログオフした後、デスクトップが再起動されないため、デスクトップはクリーンな状態になりません。これは、どのようなシナリオでもセキュリティ上の問題になる可能性があります。そのデスクトップの次のユーザーがそのデスクトップのローカル管理者である場合、以前のユーザーのデータにアクセスできる可能性があります。また、このリスクは標準（管理者以外）ユーザーにとってはそれほど懸念されませんが、アプリケーションが不適切に動作し、時間の経過とともにパフォーマンスの問題が発生する可能性があることに注意してください。重要**:** 管理者は、再起動されていないプールされたデスクトップを停止モードで使用する場合、この回避策を使用する場合の潜在的な影響を慎重に検討する必要があります。

接続リースと同様に、停止中にサイトを変更することはできません。データベースは実質的にメインサイトデータベースのスナップショットであり、新しい同期が発生するたびに破棄されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

ストレス条件下での **6** および **8** の **vCPU** ブローカの性能比較

サイトは、50 の RDS ワーカーと 5075 の VDI VDA で構成されていました。各 RDS ワーカーは、2500 人のシミュレートされたユーザーをサポートできます。1 秒あたり 20 ユーザーという起動レートが設定されました。異なる数の公開アプリケーションがサイトに追加されました。

RDS ワーカーの場合、VDI 5075 では 100,000 人のユーザーが起動されました。

テストは、通常およびローカルホストキャッシュの動作（停止）モードで実施されました。

6 vCPU システムでは、CPU のヘッドルームはほとんどなく、少数の例外があります <10) occurred when the published app count was >。

Windows 更新プログラムは、多くの実行中にグループポリシーによって無効にされ、tiworker.exe プロセス (Windows インストーラーモジュール) が長期間にわたってコア全体を使用することがわかりました。これにより、多数の起動失敗が発生し、テストが再実行されました。ブローカープロセッサはかなり古いですが、tiworker プロセスは新しいものの単一のコアを消費し、テストに影響を与えます。

ハイパーバイザー構成

- XenServer 7.0
- AMD オプテロン 8431 2.4 GHz — 4 x 6 コア
- 128 GB RAM
- 読み取りキャッシュが有効
- SSD ベースのストレージを搭載した Windows Storage Server 2012R2

ブローカー構成

- 3 つのコアを備えた 2 つのソケット、4 つのコアを備えた 2 つのソケット
- 10 GB RAM
- Windows Server 2016
- VDA タイプごとに 1 つのデリバリーグループ
- ユーザーに表示されるすべてのアプリケーション
- XenDesktop 7.12

StoreFront の構成

- StoreFront サーバー ×6
- Windows Server 2016
- 仮想 CPU×4
- 10 GB RAM

© 1999–2021 Citrix Systems, Inc. All rights reserved.

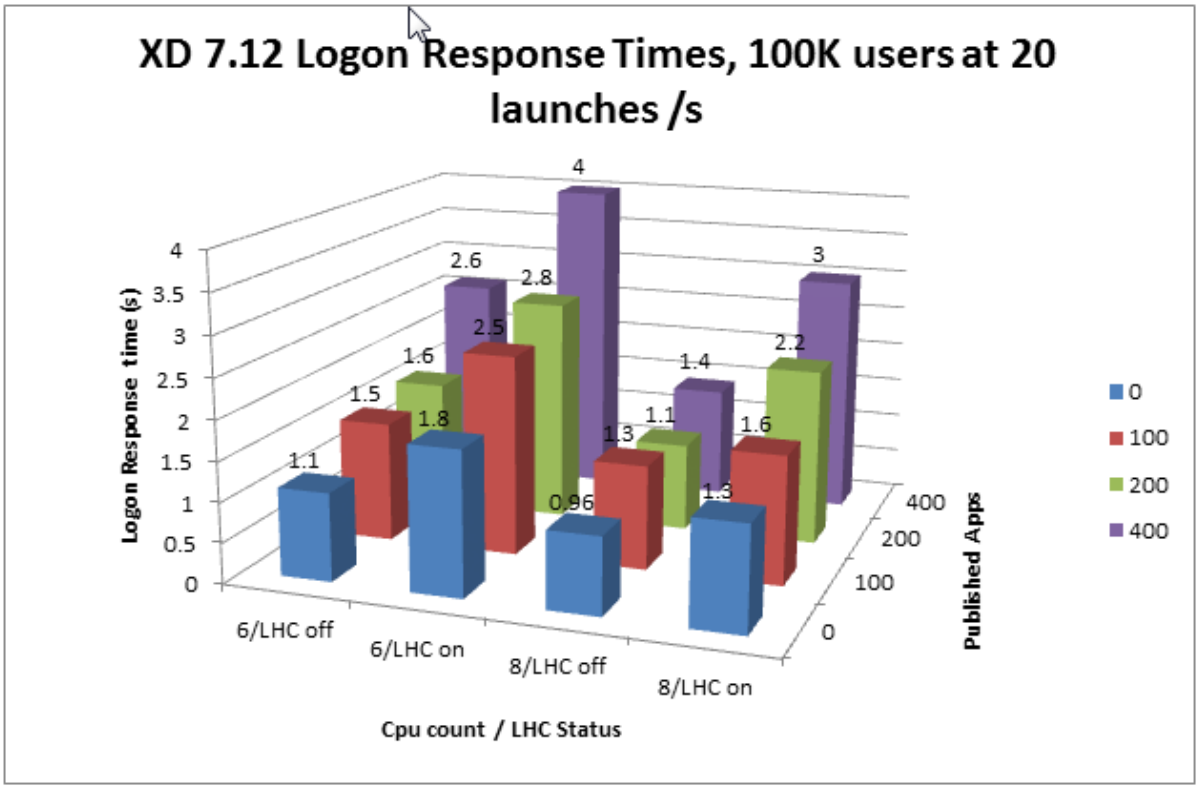
NetScaler の構成

- VPX 8000 version 11.063.16

SQL サーバーの構成

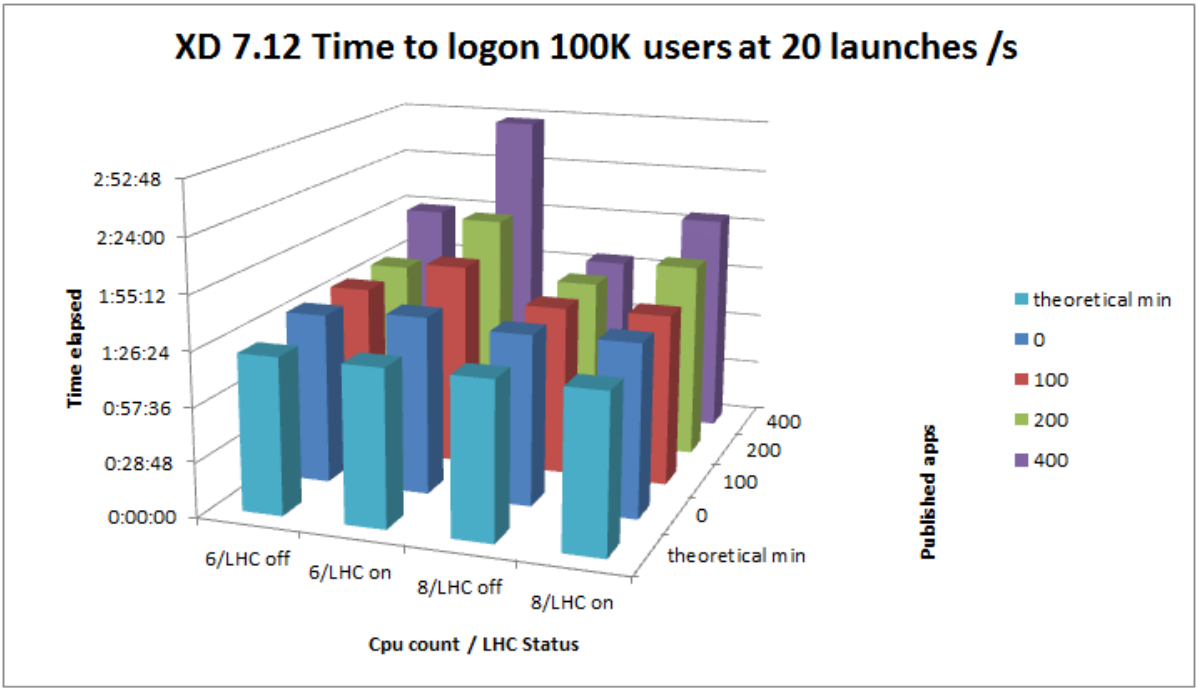
- インテル E5-2630 2.3GHz 2x12 コア
- SQL Server 2012
- RAM (メモリ)

注**:** サイトデータベースのみがオフラインになりました。監視データベースと構成データベースは、テスト中もアクセス可能でした。これは、モニタサービスがテスト中に一部の CPU を消費していたことを意味します。

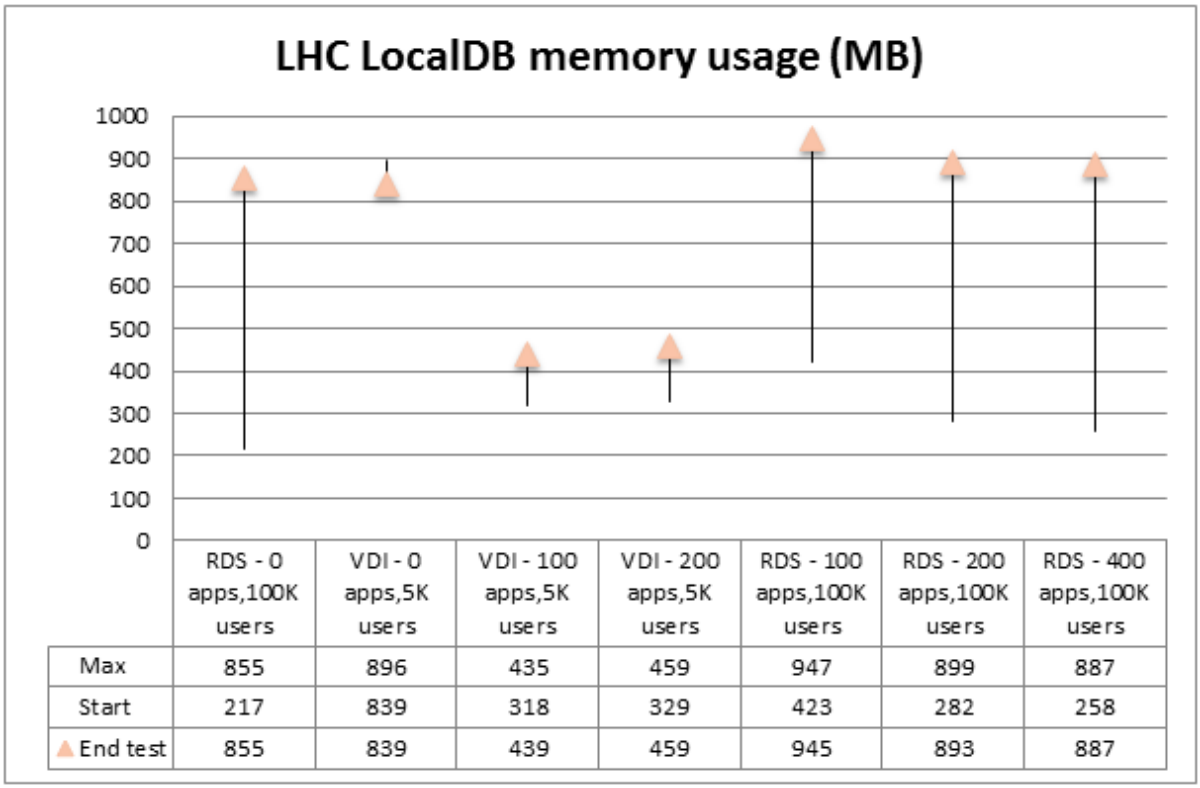


通常、アプリケーションの数が増えると、ログオンの応答時間が長くなり、停止の応答時間は通常の操作よりも悪くなります。vCPU 数を増やすと、応答時間が短縮されます。テストで使用される CPU はかなり古く、より現代的な CPU は一般的により良いパフォーマンスを与えることに注意してください。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



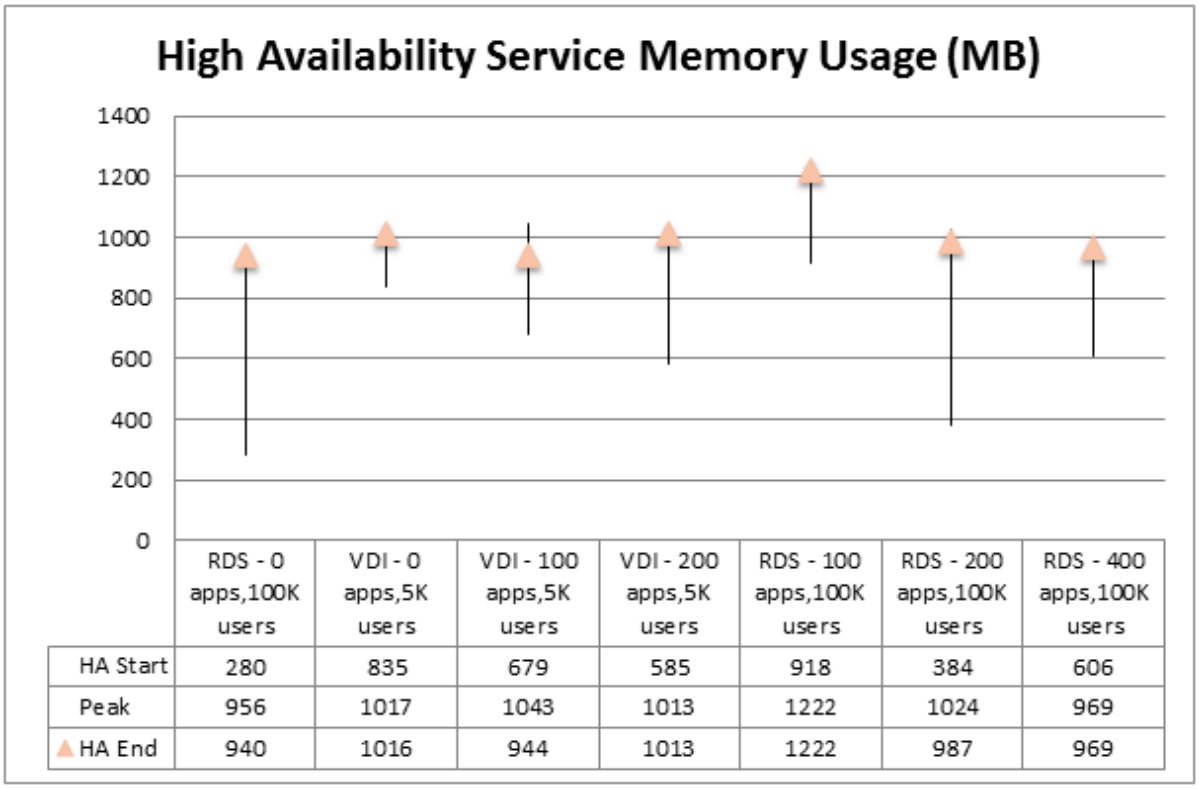
「理論上の最小」行は、環境が 1 秒あたり 20 回の起動を処理できた場合に、100,000 人のユーザーがログオンに要する絶対最小時間であり、1 時間 23 分 20 秒になります。これらのテストでは、0 のアプリケーション行が 6 vCPU の場合は 1:30:57、8 vCPU の場合は 1:30:48 を管理していました。Active Directory ドメインのパフォーマンスは、ユーザーが認証される速度に多少影響します。



	RDS - 0 apps,100K users	VDI - 0 apps,5K users	VDI - 100 apps,5K users	VDI - 200 apps,5K users	RDS - 100 apps,100K users	RDS - 200 apps,100K users	RDS - 400 apps,100K users
Max	855	896	435	459	947	899	887
Start	217	839	318	329	423	282	258
End test	855	839	439	459	945	893	887

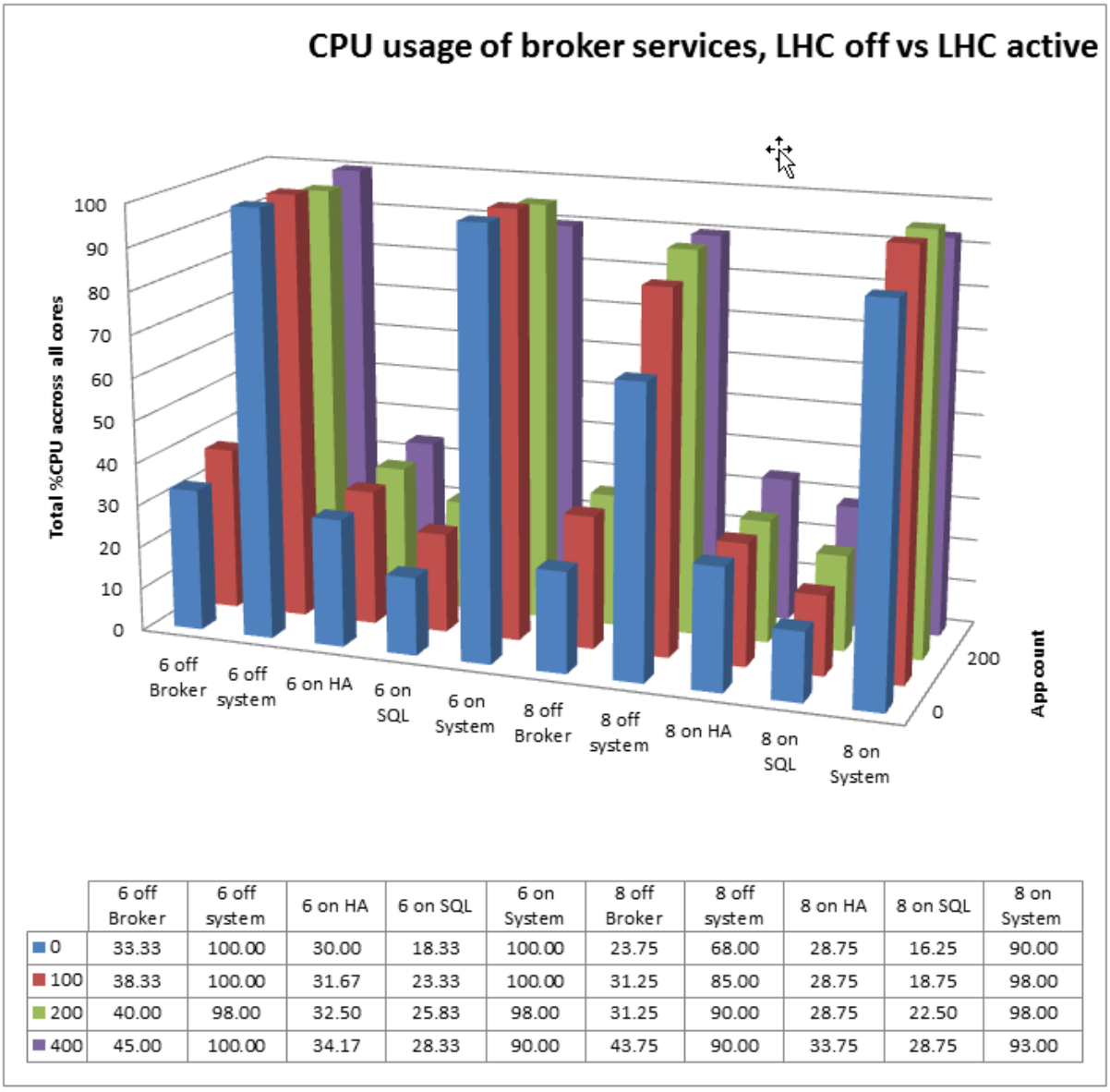
© 1999–2021 Citrix Systems, Inc. All rights reserved.

通常の条件下では、LocalDB メモリの使用は動作中に増加し、システムに負荷がない限り、そのメモリにハングアップします。処理されるユーザーが多いほど、使用されるメモリは最大で 1 GB まで大きくなります。最初の VDI テストでは、LocalDB は以前の RDS 実行からメモリを解放していませんでした。後続の VDI テストでは、テストの前にブローカが再起動され、使用メモリが少なくなりました。



	RDS - 0 apps,100K users	VDI - 0 apps,5K users	VDI - 100 apps,5K users	VDI - 200 apps,5K users	RDS - 100 apps,100K users	RDS - 200 apps,100K users	RDS - 400 apps,100K users
HA Start	280	835	679	585	918	384	606
Peak	956	1017	1043	1013	1222	1024	969
HA End	940	1016	944	1013	1222	987	969

© 1999–2021 Citrix Systems, Inc. All rights reserved.



	6 off Broker	6 off system	6 on HA	6 on SQL	6 on System	8 off Broker	8 off system	8 on HA	8 on SQL	8 on System
0	33.33	100.00	30.00	18.33	100.00	23.75	68.00	28.75	16.25	90.00
100	38.33	100.00	31.67	23.33	100.00	31.25	85.00	28.75	18.75	98.00
200	40.00	98.00	32.50	25.83	98.00	31.25	90.00	28.75	22.50	98.00
400	45.00	100.00	34.17	28.33	90.00	43.75	90.00	33.75	28.75	93.00

注：値は合計システム CPU に正規化されているため、33.33% は 6 つのコアのうち 2 つであり、30% は 8 vCPU セットアップでは 2-1/2 コアです。

「オフ」という用語は通常のサイト動作を指し、「オン」はローカルホストキャッシュがアクティブであることを意味します。

毎秒 20 人のユーザーのリクエスト起動率は、通常の操作でもブローカーにとって非常に厳しいものです。通常の動作では、6 vCPU システムにはヘッドルームがありません。公開アプリケーションの数が増えるにつれてブローカの CPU が増加し、応答時間が遅くなります。ローカルホストキャッシュがアクティブな場合、セカンダリブローカー（HA）サービスは、CPU リソースのための LocalDB（SQL）と競合し、通常の動作よりも悪い応答時間を与える必要があります。

8 vCPU システムでは、いくつかのヘッドルームがあり、LocalDB はスケールアップしますが、この環境では、CPU が少量であるにもかかわらず、2-1/2 コアでピークに達しました。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

通常の操作では、同期が発生しない限り、LocalDB は CPU を消費しません。

停止中、プライマリブローカーは事実上 CPU を使用しません。

データベースのサイズ

5075 VDI 構成の場合、LocalDB は約 40 MB でした。これは、アプリケーションおよびログオンの数に応じて、100,000 RDS で 100 ～300 MB の間で変化しました。新しいインポートが開始される前にデータベースのコピーが作成されるので、LocalDB 用に 1 GB の領域を許可します。

概要

サイトデータベースが停止している間、ローカルホストキャッシュは接続リースよりも幅広いリソースと条件をサポートしますが、運用時には多くの CPU とメモリが必要になります。

複数のブローカーサイトでは、どのブローカーも停止ブローカーとして選出される可能性があるため、すべてのブローカーが停止モードで対処するのに十分なリソースを持っている必要があります。ブローカーリソースの評価は行われないため、より強力で強力なブローカーがあるサイトでは、停止中に最も強力なブローカーが選出される可能性があります。

コアとソケットのレイアウトは、ブローカーの設計の一部として考慮する必要があります。

公開アプリケーションの数は、ログオンの応答時間と最大ログオンスループットに影響します。

CPU リソースが不足しているブローカは、起動に失敗する可能性があります。

接続リースと比較して、ローカルホストキャッシュの停止モードでのパフォーマンスをテストするには、2 つのコアと 2 GB の RAM を追加することをお勧めします。

LocalDB データベースには、1 GB のディスク容量で十分です。

オーバーロードされたブローカは、接続に失敗します。

This article was written by Joe Deller.

XenApp および **XenDesktop 7.9** での **Citrix** ユニバーサルプリントサーバーの負荷分散

May 18, 2020

テスト方法

すべてのテストシナリオは現実の方法で行われ、最終エンドでの印刷は唯一のシミュレーションコンポーネントでした。テストシステムは、XenServer 仮想マシン、インフラストラクチャ（DDC、StoreFront、ユニバーサル

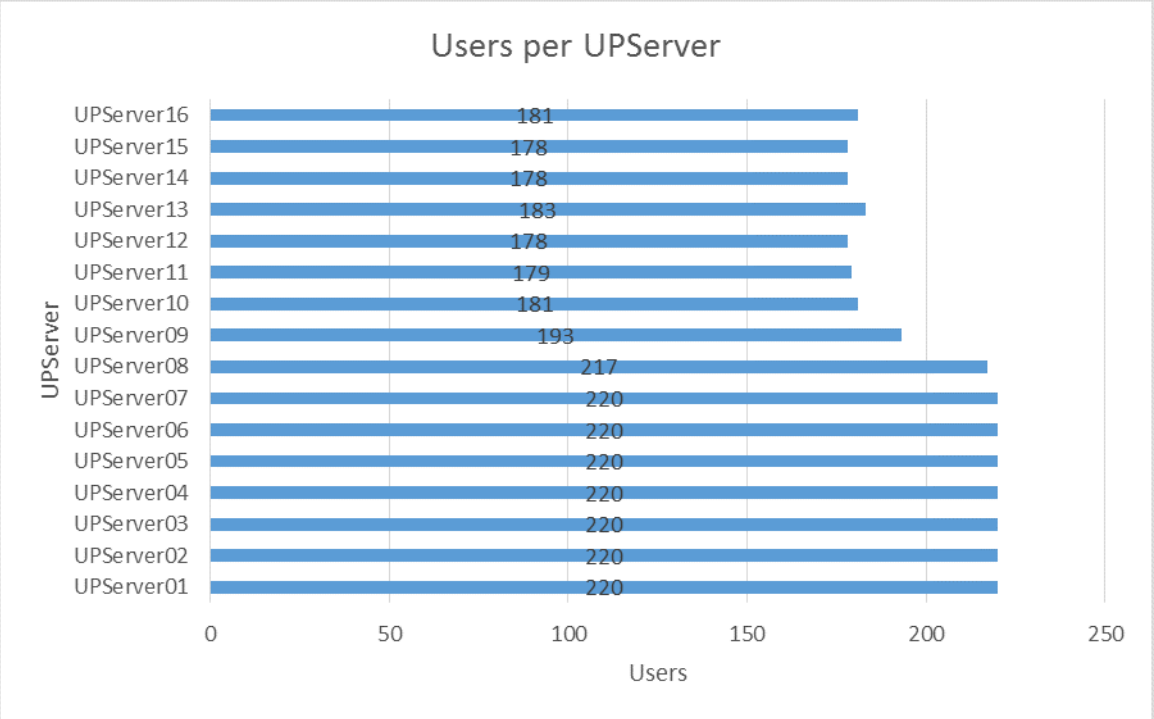
© 1999–2021 Citrix Systems, Inc. All rights reserved.

プリントサーバー）用の Windows 2012R2、XenApp の VDA システム、XenDesXenDesktop の VDA システム用の Windows 10、Citrix Receiver を介した ICA 起動用の Windows 8.1 で構成されています。各 ICA ランチャーは 10 台のプリンターに接続され、ICA ランチャー間でプリンターが重複せず、カスタムスクリプトが使用され、XenApp VDA セッションごとにランダムプリンターが提供されます。また、カスタムスクリプトは、AutoIt を使用して同一の印刷アクションを実行する各セッション内の印刷を制御しました。最後に、内部で開発されたツールを使用して、ICA セッションの起動を調整し、テスト用の perfmon データを収集しました。

ユニバーサルプリントサーバーの負荷分散サイジング

環境内の他のすべてのコンポーネントと同様に、ユニバーサルプリントサーバーの負荷分散を最適に実行するには、サイジングが非常に重要です。大きな文書の印刷はニーズに応じて主観的であるため、この記事では主に印刷速度に焦点を当て、平均的な仕事とみなすものを使用します。

内部テストにより、負荷分散で Universal Print Server インスタンスを設定する必要がないことがわかりました。また、必ずしもそうではないプリンタの配布について話しているときに、追加のユニバーサルプリントサーバーインスタンスで印刷を増やすことができます。特に、構成されているユニバーサルプリントサーバーインスタンスが多すぎる場合です。この場合、最初に利用可能なユニバーサルプリントサーバーインスタンスへのユーザーのスキューがあります。



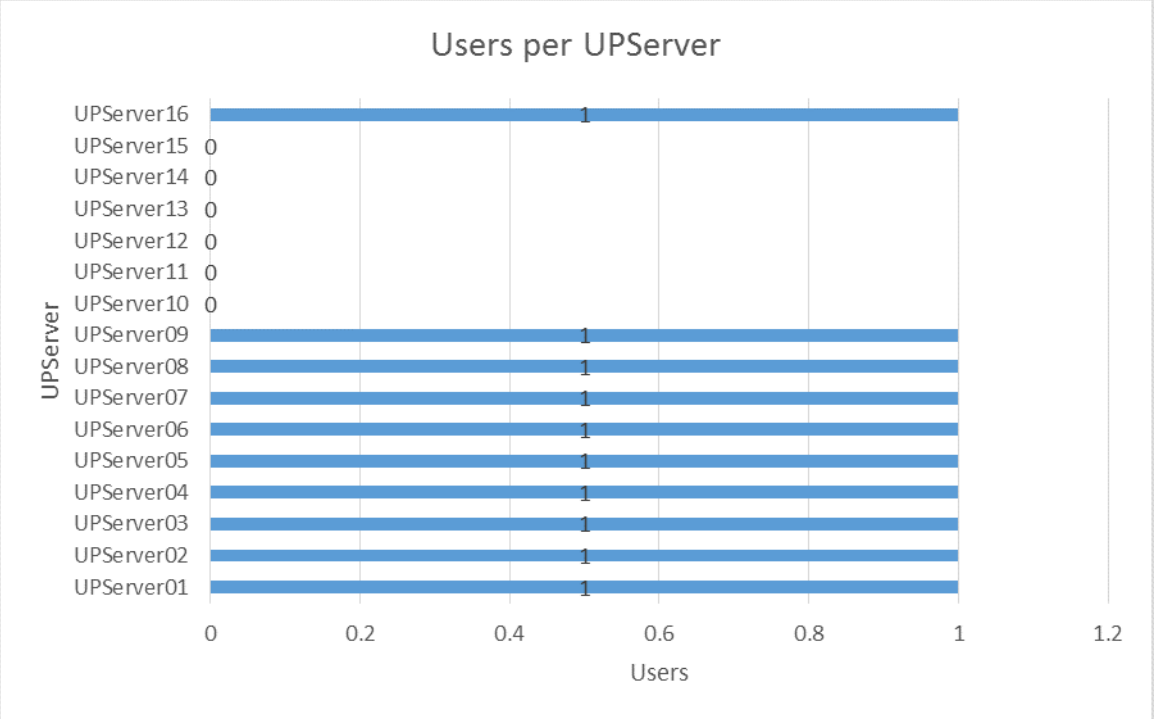
このグラフは、16 台のユニバーサルプリントサーバーインスタンスを利用する 48 台の XenApp サーバーで 3,500 台のユーザーテストシナリオを示しています。上記のように、最初の 8 つの Universal Print Server インスタンスは接続の大部分を占め、接続の均等な分布はありませんでした。このシナリオでは、印刷レートが低くなることも想定しています。これについては後ほど説明します。

この問題が発生する理由を理解するには、負荷分散メカニズムがユニバーサルプリントサーバーインスタンスをどの

© 1999–2021 Citrix Systems, Inc. All rights reserved.

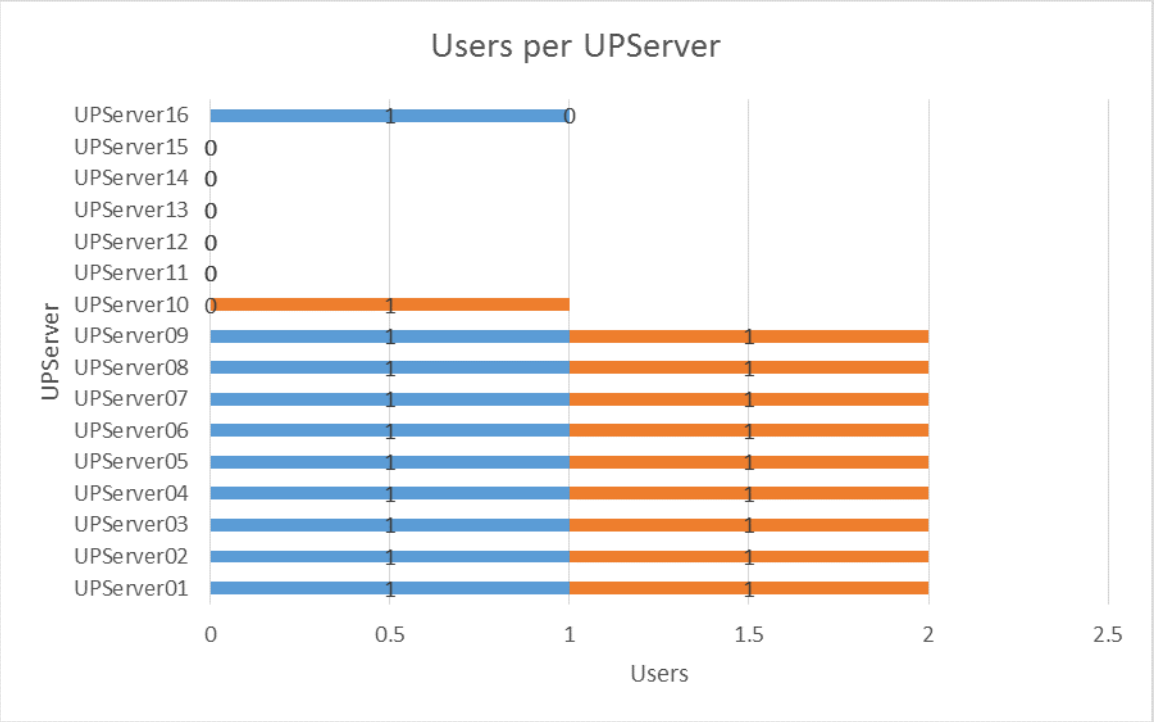
ように選択するかを検討する必要があります。16 ユニバーサルプリントサーバーのインスタンス (番号 1-16) の負荷分散と単一の XenApp サーバーで 10 最大ユーザー（便宜上誇張されています）があるとします。また、負荷分散されたユニバーサルプリントサーバーのインスタンスが、負荷分散ポリシーのユニバーサルプリントサーバーの番号順になっているとします。

XenApp でユーザーがログオンしてセッションを作成すると、そのユーザーが受信するユニバーサルプリントサーバーのインスタンスはランダムになります。これは、使用可能なユニバーサルプリントサーバーの任意のインスタンスである可能性があり、どのサーバーにも優先権が与えられていません。この例では接続のためにサーバー 16 を受信したとします。最初のユーザーがログオンし、セッションの作成が完了したら、別のユーザーがログインします。このユーザーは、ポリシーのリスト内の最初のユニバーサルプリントサーバーインスタンス（この場合はサーバー 1）を使用します。別のユーザーがログインし、サーバ 2 を利用しています。この傾向を続けると、以下に示すサーバーのロードが提供されます。10 人のユーザーがすべてログインすると、ユニバーサルプリントサーバーのインスタンス 1～9 と 16 は接続されますが、残りのサーバーは接続されません。



これで、XenApp サーバーをミックスに追加し、最大ユーザー数は 10 人です。このサーバーは、最初のユーザーがサーバー 16 ではなくサーバー 4 をランダムに受信することを除いて、前の例と同じ手順に従います。この場合、後続のログインごとに同じプロセスが実行されますが、現在接続が行われているサーバ 4 をスキップする点が異なります。この場合、サーバ 1～10 が接続されます。下のグラフでオレンジ色の追加のユーザーのバランスが取れていることを観察することができます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



引き続きサーバー数を増やすと、発生するスキューがわかりにくくなります。実際には、ユニバーサルプリントサーバーのインスタンスと同等またはそれ以上の数の XenApp ホストが必要です。また、より最適なロードに使用する予定のユニバーサルプリントサーバーインスタンスの倍数として、ユーザーセッション数を保持することをお勧めします。この観点から上記のシナリオを見ると, 2 つの XenApp サーバーと 16 のユニバーサルプリントサーバーインスタンスの場合、XenApp サーバーあたり最小 16 ユーザーのユーザーロードにする必要があることがわかります。同じ問題を調べるもう 1 つの方法は、XenApp サーバーあたり 10 人のユーザーのみをサポートしている場合、ユニバーサルプリントサーバーインスタンスは 10 個以下です。これにより、よりバランスのとれた負荷が得られ、利用可能なリソースがより効果的に利用されます。

上記は、厳密にユーザー接続バランシングを扱うセットアップを過度に単純化したものです。サーバあたりのユーザー数が増えたより複雑なセットアップは、想定される構成です。ユーザーの増加に伴い、前述の印刷速度は、ユニバーサルプリントサーバーのサイジングにおいて大きな役割を果たします。以下の式を使用して、環境に必要なユニバーサルプリントサーバーインスタンスを決定することをお勧めします。これにより、必要な印刷レートに基づいて、負荷分散に必要なユニバーサルプリントサーバーインスタンスの数を決定できます。サイジングを簡素化するために、この式を使用して、必要な印刷レートを提供するためのより理想的なセットアップのガイダンスを提供することができます。一般に、N を解決して、独自のプリントサーバー数を決定することに最も関心があります。

```
V\*P/N \< J
```

各項目の意味は次の通りです:

V = LB を使用する VDA の数

P = VDA あたりのアクティブなネットワーク印刷ジョブの 1 分あたりの平均数

N = 負荷分散されたプリントサーバーの数

© 1999–2021 Citrix Systems, Inc. All rights reserved.

J = ユニバーサルプリントサーバーでの 1 分あたりの最大ジョブ数

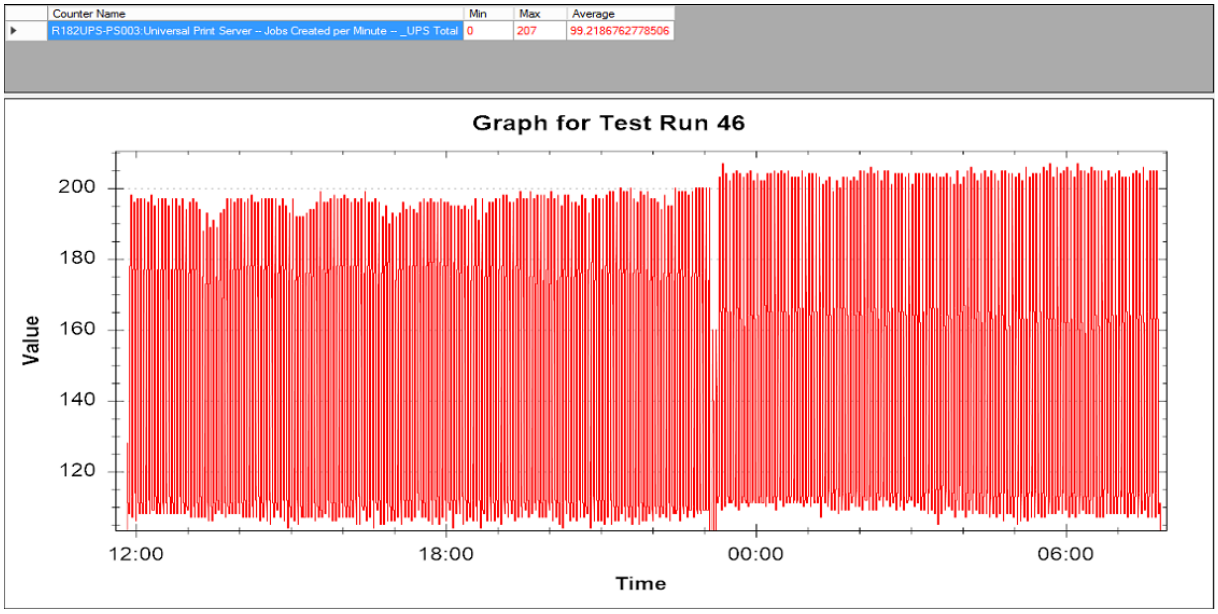
7.8 以降の VDA で P を観察するには、VDA 上の既存の Universal Print Client のパフォーマンスモニターカウンターを調べます。具体的には、ユニバーサルプリントサーバーポリシーが有効でネットワークが設定されている VDA で、通常の稼働日中にネットワークプリンターの 1 分間に作成されるジョブの平均を監視します。セッションにマッピングされたプリンタ。

J には、プリントサーバーのハードウェアパフォーマンスおよび印刷するドキュメントのサイズに応じて、50 ～100 の数値を指定します。

上記の式は一般化されており、お客様の環境の要件に大きく依存します。ユニバーサルプリントサーバーの負荷分散を実装する前に、ご使用の環境の印刷要件を完全に理解することが重要です。

毎分 **100** ジョブ（**JPM**）テスト

新しいユニバーサルプリントサーバーの負荷分散で最大の改善点の 1 つは、1 分あたりの同時印刷ジョブの増加です。毎分 100 ジョブという倍増の印刷レートのしきい値により、個々のユニバーサルプリントサーバーインスタンスでさらに高い密度を実現できるようになりました。負荷分散された複数のユニバーサルプリントサーバーインスタンスに分散すると、この増加倍数の影響が大きくなります。以下は毎分作成されたジョブカウンタ（式で参照されるもの）の perfmon 出力で、18 時間以上のテストサイクルで毎分～100 ジョブに平均しています。

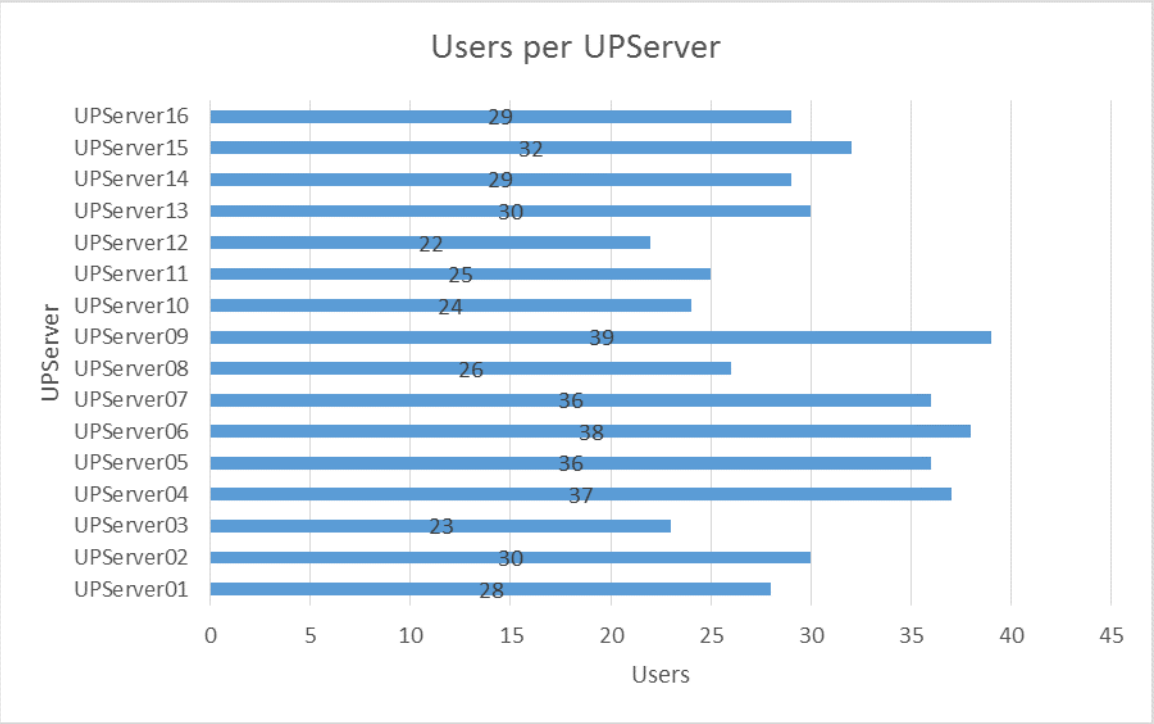


VDI ランダム化

VDI 環境で使用される負荷分散方法は、ランダム化機能の実装のみです。前述のように、負荷分散プロセスは VDA でのみ実行され、最初の接続がランダム化され、その後ログインはユニバーサルプリントサーバーインスタンスのリスト全体で負荷分散されます。VDI 実装には VDA ごとに 1 人のユーザーがいるため、ランダム化機能のみが適用されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

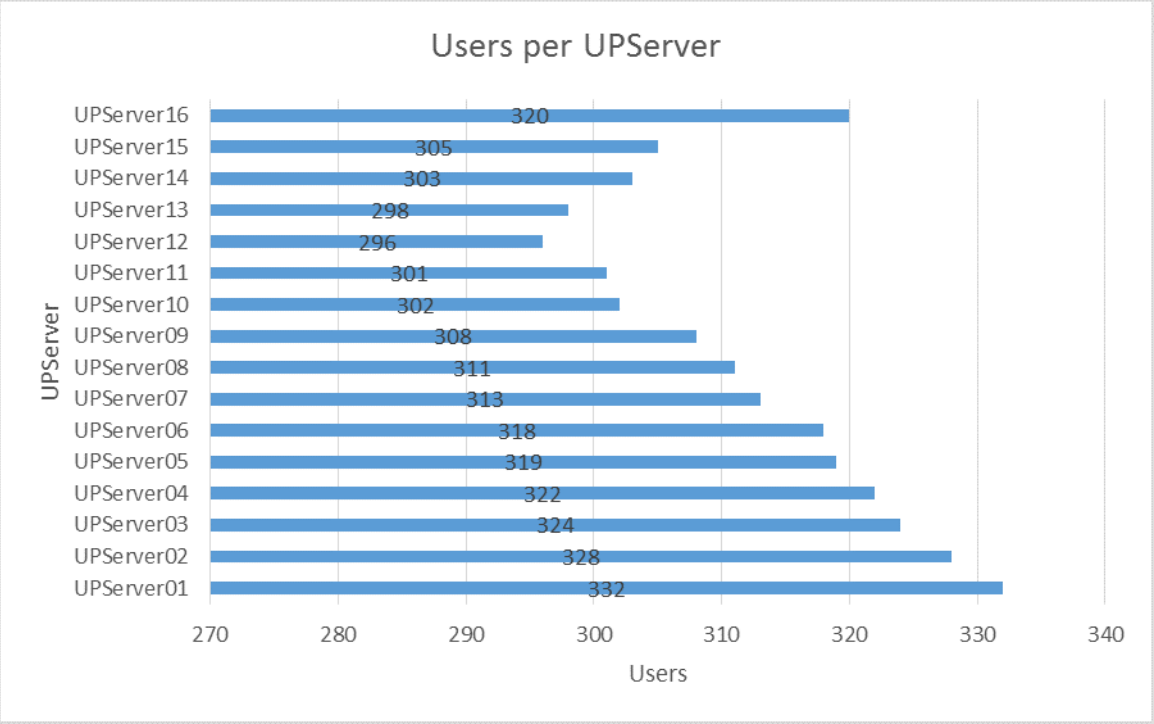
ランダム化が確実に機能するように、16 個のユニバーサルプリントサーバーインスタンスを使用して 500 人の XenDesktop テストを実行しました。これは、（完全に負荷分散された世界で）ユニバーサルプリントサーバーインスタンスあたり約 31 セッションに作用し、ランダム化の有効性を明確に判断します。以下は、このテストの結果として作成されたプリンタ接続です。接続がユニバーサルプリントサーバーのインスタンスにランダムに割り当てられていることは簡単に確認できます。



5000 ユーザーテスト

XenApp サーバー自体の密度により、ユニバーサルプリントサーバーの負荷分散の最大のメリットが実現されます。ユニバーサルプリントサーバーの負荷分散の規模が大きいユーザー数環境でどれだけ大きくなるかを判断するために、5,000 のユーザーテストの実行が、負荷分散を検証するのに十分な大きさであることが決定されました。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



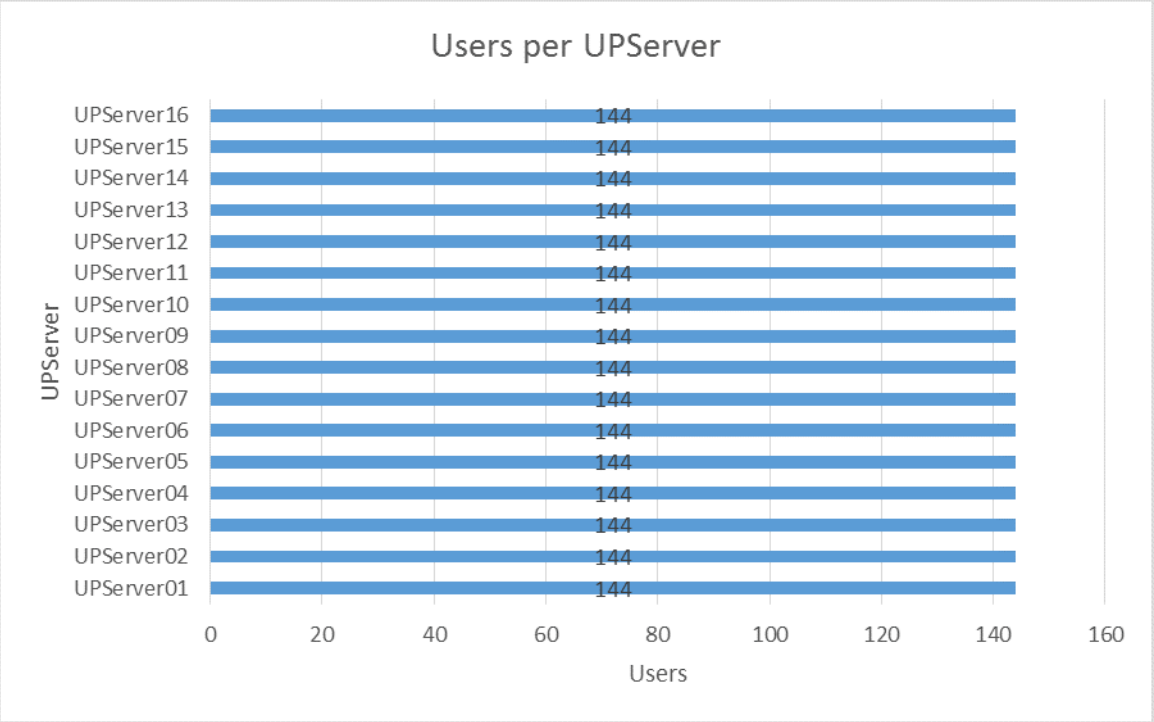
上記は、48 台の XenApp サーバーと 16 台のユニバーサルプリントサーバーインスタンスを備えた 5,000 台のユーザーテストの結果です。このユーザー数は、XenApp サーバーあたり約 100 ユーザー、または XenApp サーバーあたりユニバーサルプリントサーバーインスタンスごとに約 6.5 ユーザーです。この結果は、先に特定された歪みを示しています。これは、最適に設計されたテストではないためです。最終的には、これはロードバランシング機能のデモンストレーションを目的としています。

ユニバーサルプリントサーバーの負荷分散フェイルオーバー

デフォルトでは、ユニバーサルプリントサーバーのインスタンスは 180 秒 MINIMUM の失敗として報告されず、360 秒の失敗と見なされます。このタイムアウトは、ユニバーサルプリントサーバーインスタンスの障害が発生した瞬間にフェイルオーバーが発生しないため、理解しておくことが重要です。フェイルオーバーが発生する前に、ユニバーサルプリントサーバーインスタンスがリカバリを試行する時間があります。より迅速なフェイルオーバーが必要な場合は、環境のニーズに基づいて変更を行う必要があります。これらの変更は、Citrix ポリシーと、2 つのレジストリキーを使用して行うことができます。

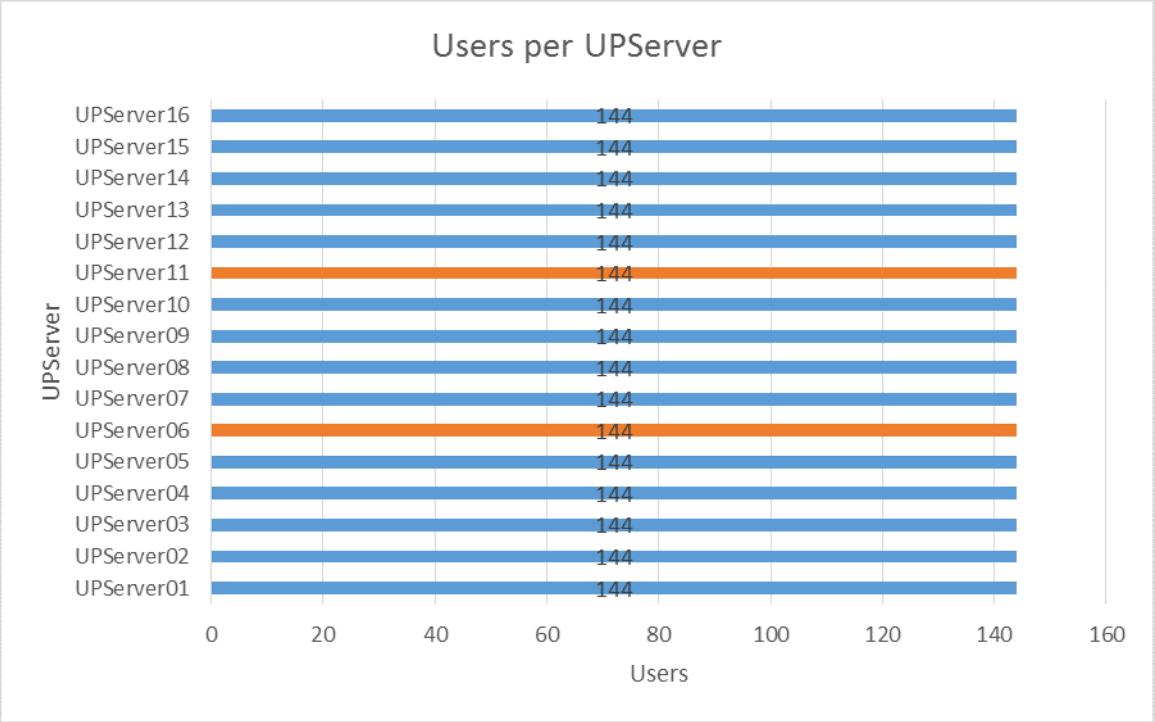
以下は、フェイルオーバーの実際のデモです。16 台のユニバーサルプリントサーバーインスタンスで 48 台の XenApp サーバー間で 2,304 人のユーザーが使用され、初期負荷分散とその後のフェイルオーバーが示されています。上記の値は、XenApp サーバーごとにユニバーサルプリントサーバーインスタンスあたり 3 ユーザーになるように、理想的には選択されています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

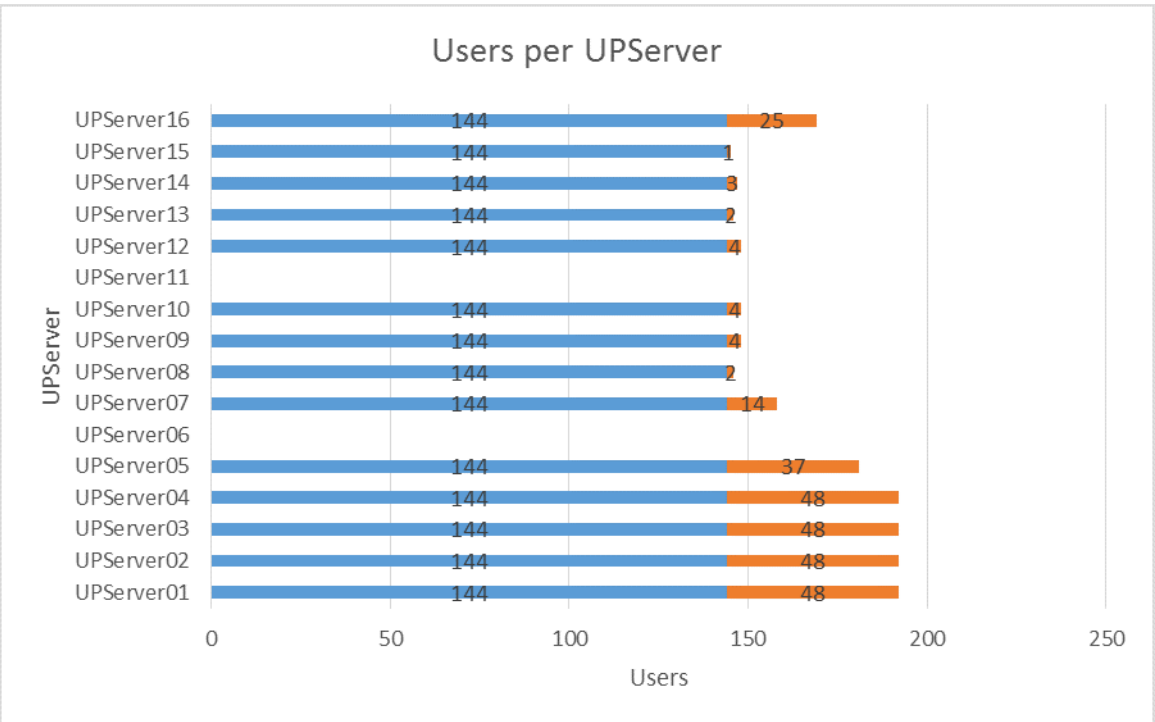


すべてのユニバーサルプリントサーバーインスタンスが均等にロードされ、すべてのユーザーがログインします。ユニバーサルプリントサーバーインスタンス UPServer06 および UPServer11 は、Hypervisor レベルで (ユニバーサルプリントサーバーインスタンスの可用性状態を判断するために PING が使用されているため) 強制シャットダウンの対象となり、完全に障害が発生したと見なされます。以下では、影響を受けるサーバー接続がオレンジ色で強調表示されています。次に、オレンジ色の失敗したサーバー接続が、残りのユニバーサルプリントサーバーインスタンスに再配布されます。

© 1999–2021 Citrix Systems, Inc. All rights reserved.



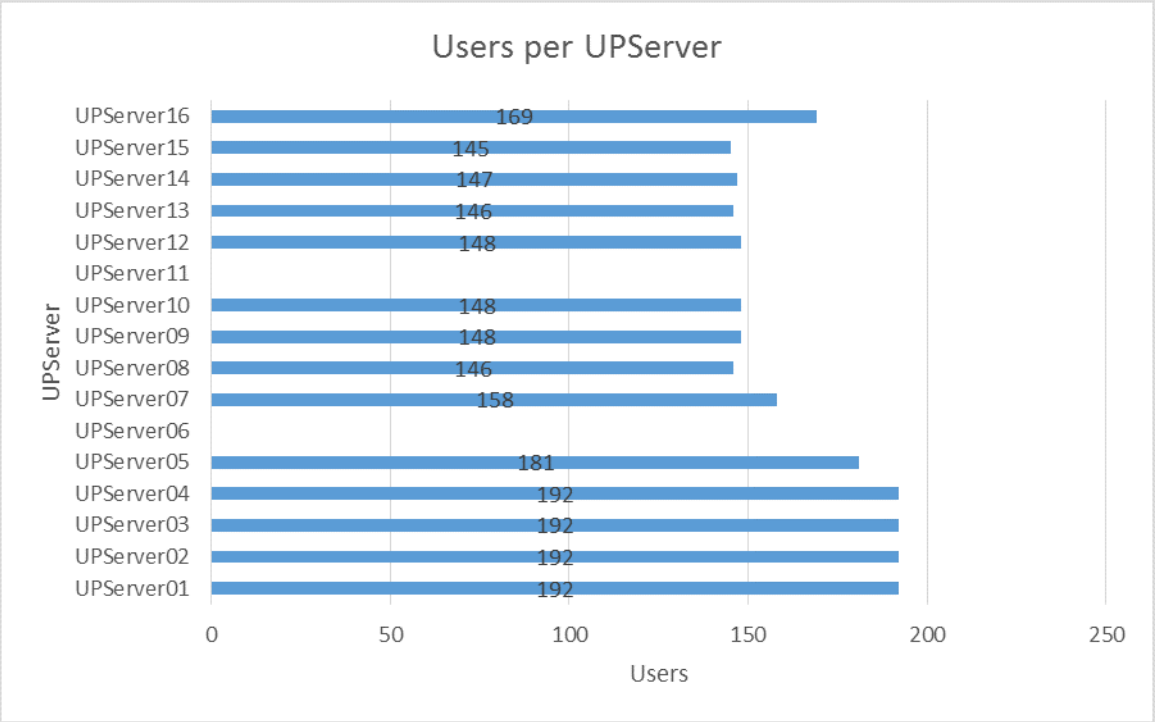
その後、使用可能な既存のサーバーへの新しい接続が確立されます。以下に、以前に失敗した接続が既存のサーバーにどのように再配布されるかを示します。



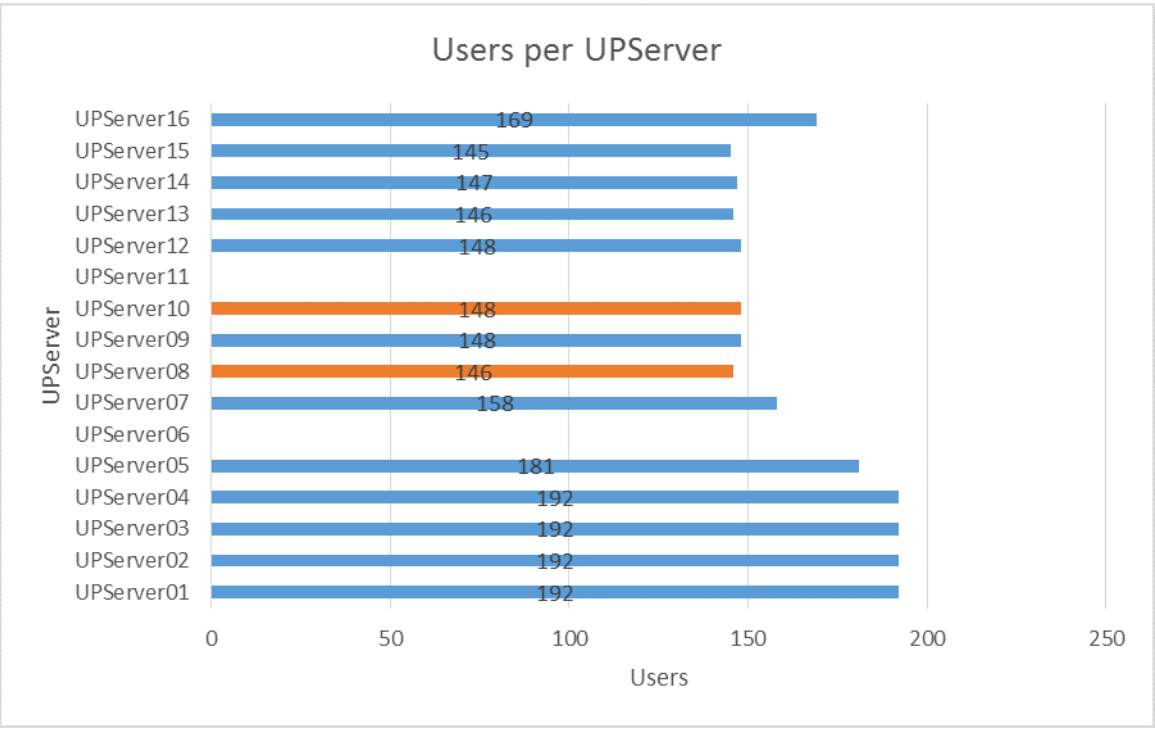
既に説明したように、既存の接続では動的に負荷分散されません。負荷分散は、ユーザーセッションのログオン時にのみ行われます。そのため、障害が発生したユニバーサルプリントサーバーインスタンスが再び使用可能になると、再調整やフェールバックは発生しません。障害が発生したユニバーサルプリントサーバーインスタンスがオンライン

© 1999–2021 Citrix Systems, Inc. All rights reserved.

に戻りますが、既存の接続は行われません。



これらのユニバーサルプリントサーバーインスタンスが再び利用可能になり、接続を受け入れることを示すには、追加のユーザーにログオンするか、それ以上のユニバーサルプリントサーバーインスタンスの障害を強制する必要があります。以下では、ユニバーサルプリントサーバーインスタンス UPServer08 および UPServer10 に強制的な障害が発生し、それぞれの接続がオレンジ色で強調表示されています。



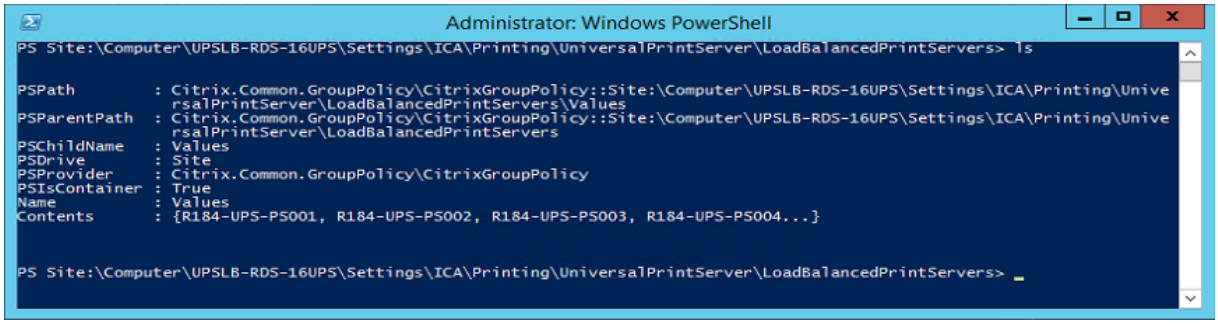
© 1999–2021 Citrix Systems, Inc. All rights reserved.

失敗すると、接続が他のサーバーに移行されることが分かります。この場合、以前に障害が発生した 2 台のサーバーに戻され、再度接続できるようになります。これらのサーバーは最も負荷が少ない（負荷がない）ため、接続の大部分を使用します。

複数のプリントサーバーの追加

複数のユニバーサルプリントサーバーインスタンスを負荷分散ポリシーに追加するには、Citrix ポリシー GUI または PowerShell コマンドレットを使用します。Citrix ポリシー GUI は、その使用において自明です。以下に、PowerShell を利用して、複数のユニバーサルプリントサーバーインスタンスを負荷分散ポリシーに追加する方法を示します。

1. `Add-PSSnapin Citrix.Common.GroupPolicy`
2. `New-PSDrive -PSProvider CitrixGroupPolicy -Name Site -Root \ -Controller localhost`
3. CD サイト: コンピュータ
4. 編集するポリシーを CD に追加 (UPSLB ポリシーを含むポリシー名)
5. CD 設定 ICAPRing ユニバーサルプリントサーバー負荷分散プリントサーバー
6. New-Item を使用して新しいプリンターを一覧に追加する



しかし、この方法の使用にはいくつかの注意点があります。まず、情報を正しく入力していることを確認してください。いくつかのプリンターをポリシーに手動で追加し、PowerShell ディスプレイでどのように表示されるかを確認して、正しく追加することができます。第 2 に、ポリシー UI をサイドステッピングしているため、実行されるプリントサーバーの検証はありません。

ユニバーサルプリントサーバーカウンタ

サイジングセクションで述べたように、現在の印刷状況に関する情報を決定するために使用できる新しい perfmon カウンタがあります。ユニバーサルプリントサーバーインスタンスと XenApp/XenDesktop システムの両方に一意のカウンタが存在します。

ユニバーサルプリントサーバーインスタンス全体に関連するカウンターは、前述の 1 分間に作成されたジョブカウンターなど、対応するユニバーサルプリントサーバーインスタンスに配置されます (これらのカウンターは、そのユニバーサルプリントサーバーインスタンスのみ、複数のインスタンス)。ユニバーサルプリントサーバーの負荷分散に関

© 1999–2021 Citrix Systems, Inc. All rights reserved.

連するカウンターは、現在の接続カウンターなど、各 XenApp/XenDesktop システム上に存在します（負荷分散は個々の VDA レベルで行われます）。

UPClient（VDA コンポーネント）固有のカウンタは、特定のユニバーサルプリントサーバーインスタンス、すべてのユニバーサルプリントサーバーインスタンス、または VDA 上のすべてのユニバーサルプリントサーバーインスタンスの合計としてデータをキャプチャするように構成できます。これらのカウンタは、perfmon から直接確認することも、PowerShell を使用してスクリプトを作成することもできます。次のカウンタは、perfmon の Citrix Printing Load Balancing セクションで使用できます。これらのカウンタは、VDA の合計（_loadbalancers_total）を選択するか、特定の VDA で使用可能なユニバーサルプリントサーバーインスタンス（ユニバーサルプリントサーバーインスタンス名）を選択することによってさらに選択できます。

アクティブなプリンタ接続カウンタ: **Performance\\Citrix Printing Load Balancer (SELECTION)\\Active Printer Connections**

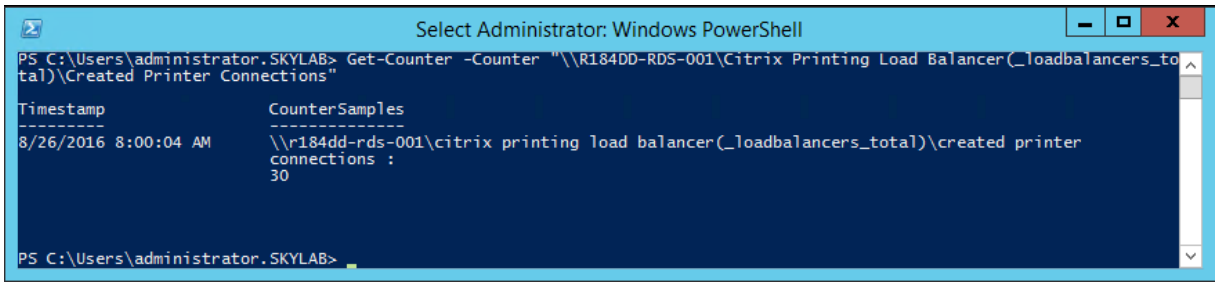
作成されたプリンタ接続カウンタ: **Performance\\Citrix Printing Load Balancer (SELECTION)\\Created Printer Connections**

削除されたプリンタ接続カウンタ: **Performance\\Citrix Printing Load Balancer (SELECTION)\\Deleted Printer Connections**

これらは標準のパフォーマンスモニターカウンターであるため、PowerShell の組み込み Get-Counter コマンドレットを使用して、特定の VDA から情報を取得できます。

```
Get-Counter -Counter \\\\\VDAName\\Citrix Printing Load Balancer(SELECTION)
\\COUNTER
```

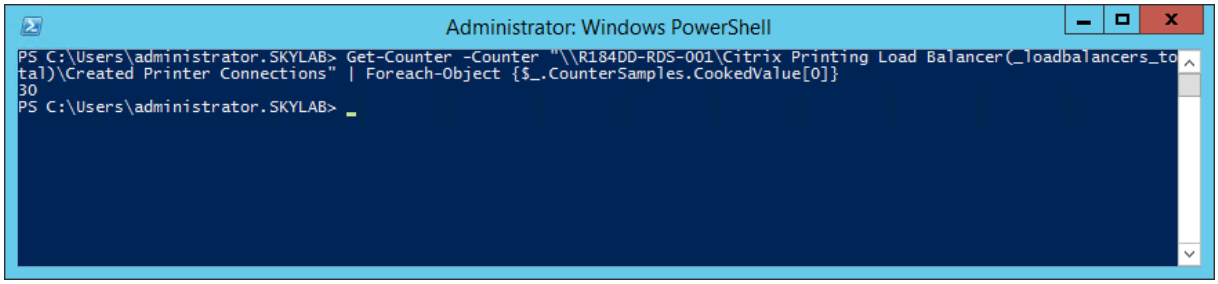
上記のコマンドは、SELECTION（ユニバーサルプリントサーバーインスタンス名または _loadbalancers_total）の目的の VDAName（名前、FQDN、または IP アドレス）から目的のカウンター（アクティブ/作成/削除されたプリンター接続）情報を取得します。これにより、カウンタオブジェクトの完全なリストが提供されます。



実際の値だけに関心がある場合は、このコマンドを他のコマンドにパイプして、調理された値（または接続値だけ）を取得する必要があります。これを実現するために、このコマンドを前のコマンドの最後に追加します。

```
| Foreach-Object { $_.CounterSamples.CookedValue[0] }
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.



テスト環境

テスト環境は、XenServer 6.2 および 6.5 を実行する 3 つの別々のプールされたハードウェアセットで構成されていました。Citrix インフラストラクチャコンポーネント（DDC、StoreFront、ICA ランチャー、メトリック収集）を含む単一の XenServer 6.2 プールと、ユニバーサルプリントサーバーインスタンスとテスト RDS VDA を含む 2 つの 6.5 プールが存在していました。テストには 2 つの独立した集中型ストレージリポジトリが使用され (プールバージョンごとに 1 つ)、すべてのテスト用仮想マシンがそこに配置されました。使用されるすべてのソフトウェアは、実施されたテストの時点で最も最新のものでした。すべてのテストは、結果の一貫性を保証するために、同じドライバとドライバのバージョンで実施されました。追加のドライバがテストされました。個々の結果は、使用するドライバによって異なります。

XenServer 6.2 物理サーバー **(x10)**

- インテル Xeon E5620 x 2.40 GHz (4 — コアハイパースレッディング) — 16 CPU
- 64 GB のメモリ
- NFS ストレージ

XenServer 6.5 物理サーバ（**x25**）

- インテル Xeon E5-2640 x 2.50 GHz (6 — コアハイパースレッディング) — 24 CPU
- 256 GB のメモリ
- NFS ストレージ

ユニバーサルプリントサーバ **VM**

- 16 vCPU（16 ソケット x 1 コア）
- 16 GB vRAM
- 75 GB のストレージ
- Windows Server 2012 R2

RDS 仮想仮想仮想機

- 16 vCPU（16 ソケット x 1 コア）

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- 16 GB vRAM
- 75 GB のストレージ
- Windows Server 2012 R2

ICA ランチャー仮想マシン

- 2 vCPU（2 ソケット x 1 コア）
- メモリメモリ
- 60 GB のストレージ
- Windows 8.1 x64 Enterprise

Citrix ユニバーサルプリントサーバーポリシー

ICA\印刷

- ユニバーサルドライバープリファレンス-XPS、EMF、PCL5c、PCL4、PS
- ユニバーサルプリンタードライバーの使用 — ユニバーサル印刷のみを使用
- ユニバーサルプリントサーバーの有効化 — Windows のネイティブリモート印刷へのフォールバックなしで有効
- プリンターが作成されるのを待つ — 有効
- 負荷分散のためのユニバーサルプリントサーバー — プリントサーバーのリスト

ユニバーサルプリントサーバーと RDS/VDA VM は、同じハードウェアプール物理サーバー内に保持され、一貫したハードウェア構成でテストが実行されることを確認しました。DDC および StoreFront サーバーは、DDC からのポリシーの伝播を除き、ユニバーサルプリントサーバーの負荷分散に影響を与えないため、上記に含まれていません。ドメインでは最小限のポリシーが使用され、XenDesktop/XenApp サイトはデフォルトのインストールであり、上記のユニバーサルプリントサーバーおよび負荷分散ポリシーを除きます。

SQL Server 高可用性ソリューションを使用するときにデータベース接続文字列を更新する

May 18, 2020

Citrix では、常にオンやミラーリングなどの SQL Server の高可用性データベースソリューションを使用している場合に、XenApp および XenDesktop データベース接続文字列を更新する PowerShell スクリプトがいくつか用意されています。

これらのスクリプトは、XenApp および XenDesktop ktop の PowerShell の API を使用するものです。

- **DB** 接続文字列関数**.ps1**: 実際の作業を行うコアスクリプト。このスクリプトには、他のスクリプトが使用する共通関数が含まれています。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- **Change_XD_Failover_Partner_v1.ps1**: フェイルオーバーパートナーを更新 (追加、変更、削除) します。このスクリプトは、各データベースのフェイルオーバーパートナーの場所 (FQDN) を要求します。(空のフェイルオーバーパートナーを指定すると、フェイルオーバーパートナーは削除されます。また、ClearPartner オプションを使用してパートナーを削除することもできます)。フェイルオーバーパートナーは、プリンシパルデータベースサーバーと同じ場所に設定しないでください。
- **Change_XD_To_ConnectionString.ps1**: 指定された接続文字列を使用して、データベースへの接続文字列を更新します。このスクリプトにより、特定の Citrix サービスが稼働していることを確認し、サイト内のすべての Controller でこれらのサービスを正しい順序で更新します。各データベースの接続文字列情報を引用符で囲みます。
- **Change_XD_To_MultiSubnetFailover.ps1**: マルチサブネットフェイルオーバー =trueの追加と削除を切り替えます。常に可用性グループを使用する場合は、接続文字列に MultiSubnetFailover=True を含めることをお勧めします。このオプションは、高可用性イベントが発生したときのリカバリを高速化します。単一サブネット環境と複数サブネット環境の両方に推奨されます。このスクリプトを 1 回実行して、オプションを追加します。オプションを削除する必要がある場合は、`Change_XD_To_ConnectionString.ps1` を使用してスクリプトを再度実行し、設定なしで文字列を指定します。
- **`Change_XD_To_Null.ps1`**: 何かが間違っているため、localhost 上のすべての接続文字列をリセットします。接続文字列を null にリセットすることにより、このスクリプトはコントローラを「初期」状態にします。このスクリプトを実行した後に Studio を実行すると、サイトを作成するか、既存のサイトに参加するかを尋ねられます。これは、何かが間違ってリセットが必要な場合に便利です。リセット後、Change_XD_To_ConnectionString.ps1 を使用して接続文字列の設定を再試行できます。

データベース接続文字列を手動で更新することもできます。「文字列を手動で更新する」を参照してください。PowerShell スクリプトをダウンロードするには、「手順」を参照してください。

要件および考慮事項

- スクリプトを実行するには、完全なサイト管理者である必要があります。
- 1 つのコントローラの **PowerShell** ウィンドウでスクリプトを実行します。PowerShell の v3 が必要です。
- XenApp および XenDesktop のコアコンポーネントをインストールし、サイトを起動して実行する必要があります。
- スクリプトを実行する前に、必須の構成ログを無効にします。
- マルチサブネットフェイルオーバーオプションは、.NET 4.5 以降でサポートされています。ただし、Studio が Windows 7 または 2008 R2 マシンで使用している MMC には以前の.NET バージョンが含まれているため、**Studio** のナビゲーションペインで ［構成］を選択すると、「キーワードがサポートされていません: `multisubnetfailover`」というエラーが表示されることがあります。そのような場合は、次のようにパッチを適用または更新します。
- .NET 3.5 SP1 の場合は、http://support.microsoft.com/kb/2654347を使用してパッチを適用します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

- .NET 4.0 の場合は、最低限 4.0.2 に更新することをお勧めします: http://support.microsoft.com/kb/2600211。

次に、Change_XD_To_MultiSubnetFailover.ps1 スクリプトを使用して、このオプションを使用してデータベース接続文字列を更新します。

手順

1. Citrix ShareFileからスクリプトを含む zip ファイルをダウンロードします。
2. ファイルを解凍します。
3. DB 接続文字列関数.ps1 内の関数を使用するため、実行するスクリプトと同じフォルダーに DBConnection-StringFuncs.ps1 があることを確認してください。
4. コントローラ上でスクリプトを実行します。

サイトをマルチサブネットフェイルオーバーに設定する場合は、Change_XD_To_MultiSubnetFailover.ps1 スクリプトを実行するだけで済みます。(注意:DBConnectionStringFuncs.ps1 スクリプトが同じフォルダーにあることを確認してください)。

> ヒント:
>
> - 接続文字列が更新されると、「Server=SQLxxx\\CITRIX\\...」が「Data Source=SQLxxx\\CITRIX\\...」に変更されたことを示すメッセージが表示されるのが普通です。「サーバー」と「データソース」という用語は同義語です。
> - 接続文字列を操作する場合は、Change_XD_スクリプトでDBConnectionStringFuncs.ps1の関数がどのように使用されるかを調べます。

文字列を手動で更新する

文字列を手動で更新するには、XenApp コマンドレットおよび XenDesktop PowerShell コマンドレットを実行します。

手順 **1.** SQL データベースを別の SQL サーバーに移動し、適切なアクセス許可を割り当てる

1. 元の SQL サーバ上のデータベースをバックアップし、新しい SQL サーバーにリストアします。
2. [**SQL Management Studio] > [**セキュリティ**] > [**ログイン**]** で、Delivery Controller コンピュータアカウントを追加します。たとえば、次のように入力します。
3. SQL ログインを追加するときは、[ユーザーマッピング] ページで、[サイトデータベース]、[監視データベース]、[ログデータベース] の 3 つの Citrix データベースをクリックします。
4. 3 つの Citrix データベースごとに、Delivery Controller コンピュータアカウントをさまざまなデータベースの役割に追加します。サイトデータベースには、ログデータベースと監視データベースよりも多くの役割があります。

```
Site database - ADIdentitySchema_ROLE

```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
Site database - Analytics_ROLE                # for 7.8 and newer
Site database - AppLibrarySchema_ROLE         # for 7.8 and newer
Site database - chr_Broker
Site database - chr_Controller
Site database - ConfigLoggingSiteSchema_ROLE
Site database - ConfigurationSchema_ROLE
Site database - DAS_ROLE
Site database - DesktopUpdateManagerSchema_ROLE
Site database - EnvTestServiceSchema_ROLE
Site database - HostingUnitServiceSchema_ROLE
Site database - Monitor_ROLE
Site database - OrchestrationSchema_ROLE       # for 7.11 and newer
Site database - public
Site database - StorefrontSchema_ROLE          # for 7.8 and newer
Site database - TrustSchema_ROLE               # for 7.11 and newer
Monitoring database - Monitor_ROLE
Monitoring database - public
Logging database - ConfigLoggingSchema_ROLE
Logging database - public
<!--NeedCopy-->
```

手順 **2.** 既存のデータベース接続を取得する (オプション)

次のコマンドを実行して、既存のデータベース接続文字列を確認します。

```
## Load the Citrix snap-ins
asnp Citrix.*

## Get the current Delivery Controller database connections
Get-ConfigDBConnection
Get-AcctDBConnection
Get-AnalyticsDBConnection              #  for 7.6 and newer
Get-AppLibDBConnection                 #  for 7.8 and newer
Get-OrchDBConnection                   #  for 7.11 and newer
Get-TrustDBConnection                  #  for 7.11 and newer
Get-HypDBConnection
Get-ProvDBConnection
Get-BrokerDBConnection
Get-EnvTestDBConnection
Get-SfDBConnection
Get-MonitorDBConnection
Get-MonitorDBConnection -DataStore Monitor
Get-LogDBConnection
Get-LogDBConnection -DataStore Logging
Get-AdminDBConnection
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
<!--NeedCopy-->
```

手順 **3.** 既存のデータベース接続の削除

Delivery Controller で、管理者として PowerShell を開き、次のコマンドを実行します。このプロセスは、既存のデータベース接続を消去します。

```
## Note the state of the log site
Get-LogSite

## Load the Citrix snap-ins
asnp Citrix.*

## Disable configuration logging for the XD site:
Set-LogSite -State Disabled

## Clear the current Delivery Controller database connections

## Note: AdminDBConnection must be the last command

Set-ConfigDBConnection -DBConnection $null -Force
Set-AcctDBConnection -DBConnection $null -Force
Set-AnalyticsDBConnection -DBConnection $null -Force             # for 7.6 and newer
Set-AppLibDBConnection -DBConnection $null -Force                # for 7.8 and newer
Set-OrchDBConnection -DBConnection $null -Force                  # for 7.11 and newer
Set-TrustDBConnection -DBConnection $null -Force                 # for 7.11 and newer
Set-HypDBConnection -DBConnection $null -Force
Set-ProvDBConnection -DBConnection $null -Force
Set-BrokerDBConnection -DBConnection $null
Set-EnvTestDBConnection -DBConnection $null -Force
Set-SfDBConnection -DBConnection $null -Force
Set-MonitorDBConnection -DataStore Monitor -DBConnection $null -Force
Set-MonitorDBConnection -DBConnection $null -Force
Set-LogDBConnection -DataStore Logging -DBConnection $null -Force
Set-LogDBConnection -DBConnection $null -Force
Set-AdminDBConnection -DBConnection $null -Force
<!--NeedCopy-->
```

エラーメッセージが表示された場合は、すべての Citrix サービスを再起動する必要があります。

```
Get-Service Citrix* | Stop-Service -Force
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
Get-Service Citrix* | Start-Service
<!--NeedCopy-->
```

Citrix サービスを再起動した後、引き続きエラーが表示される場合は、サーバーを再起動する必要があります。元のコマンドセットを再実行して、既存の接続が正しく削除されていることを確認します。

次のコマンドレットは、空の出力を返す必要があります。

```
## Load the Citrix snap-ins
asnp Citrix.*

## Get the current Delivery Controller database connections
Get-ConfigDBConnection
Get-AcctDBConnection
Get-AnalyticsDBConnection               #  for 7.6 and newer
Get-AppLibDBConnection                  #  for 7.8 and newer
Get-OrchDBConnection                    #  for 7.11 and newer
Get-TrustDBConnection                   #  for 7.11 and newer
Get-HypDBConnection
Get-ProvDBConnection
Get-BrokerDBConnection
Get-EnvTestDBConnection
Get-SfDBConnection
Get-MonitorDBConnection
Get-LogDBConnection
Get-AdminDBConnection
<!--NeedCopy-->
```

手順 **4.** 新しいデータベース接続文字列の指定

目的の接続文字列に合わせて変数を調整します。

- スタンドアロンの SQL Server 接続文字列の場合: `Server=SQLServerName; Initial Catalog=DBName; Integrated Security=True`
- データベースのミラーリング接続文字列の場合: `Server=PrimarySQLServerName; Initial Catalog=DBName; Integrated Security=True; Failover Partner=SecondSQLServer`
- Always On 機能による高可用性の場合: `Server=ListenerName; Initial Catalog=XDdb; Integrated Security=True; MultiSubnetFailover=True`

次のコマンドを実行して、新しい接続文字列を設定します。

```
$ServerName = "<dbserver>"
$SiteDBName = "<SiteDbName>"
$LogDBName = "<LoggingDbName>"
$MonitorDBName = "<MonitorDbName>"
```

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
$csSite = "Server=$ServerName;Initial Catalog=$SiteDBName;Integrated
    Security=True"
$csLogging = "Server=$ServerName;Initial Catalog=$LogDBName;Integrated
    Security=True"
$csMonitoring = "Server=$ServerName;Initial Catalog=$MonitorDBName;
    Integrated Security=True"

Set-AdminDBConnection -DBConnection $csSite
Set-ConfigDBConnection -DBConnection $csSite
Set-AcctDBConnection -DBConnection $csSite
Set-AnalyticsDBConnection -DBConnection $csSite              # for 7.6
    and newer
Set-HypDBConnection -DBConnection $csSite
Set-ProvDBConnection -DBConnection $csSite
Set-AppLibDBConnection  -DBConnection $csSite                # for 7.8
     and newer
Set-OrchDBConnection  -DBConnection $csSite                  # for
    7.11 and newer
Set-TrustDBConnection  -DBConnection $csSite                 # for
    7.11 and newer
Set-BrokerDBConnection -DBConnection $csSite
Set-EnvTestDBConnection -DBConnection $csSite
Set-SfDBConnection -DBConnection $csSite
Set-LogDBConnection -DBConnection $csSite
Set-LogDBConnection -DataStore Logging $null -force
Set-LogDBConnection -DataStore Logging -DBConnection $csLogging
Set-MonitorDBConnection -DBConnection $csSite
Set-MonitorDBConnection -DataStore Monitor -DBConnection $null -force
Set-MonitorDBConnection -DataStore Monitor -DBConnection $csMonitoring

## If necessary, enable configuration logging for the XD site:
Set-LogSite -State Enabled
<!--NeedCopy-->
```

> 注:
>
> 上記のすべてのSet-<service>DBConnectionコマンドが **[OK]** の結果を返したことを確認します。これらのコマンドの結果が **[OK]** 以外の場合は、ロギングまたはトレースを有効にして、接続エラーの原因を特定する必要があります。
>
> Set-LogDBConnection -DBConnection $nullとSet-MonitorDBConnection -DBConnection $nullが **OK** ではなく **DBUnconfigured** を返します。

手順 **5.** 新しいデータベース接続文字列のテスト

1. 次のコマンドを実行して、データベースへの接続を確認します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

```
## Load the Citrix snap-ins
asnp citrix.*

$ServerName = "<dbserver>"
$SiteDBName = "<SiteDbName>"
$LogDBName = "<LoggingDbName>"
$MonitorDBName = "<MonitorDbName>"
$csSite = "Server=$ServerName;Initial Catalog=$SiteDBName;
    Integrated Security=True"
$csLogging = "Server=$ServerName;Initial Catalog=$LogDBName;
    Integrated Security=True"
$csMonitoring = "Server=$ServerName;Initial Catalog=$MonitorDBName
    ;Integrated Security=True"

Test-AcctDBConnection -DBConnection $csSite
Test-AdminDBConnection -DBConnection $csSite
Test-AnalyticsDBConnection -DBConnection $csSite    # for 7.6 and
    newer
Test-AppLibDBConnection -DBConnection $csSite       # for 7.8 and
    newer
Test-BrokerDBConnection -DBConnection $csSite
Test-ConfigDBConnection -DBConnection $csSite
Test-EnvTestDBConnection -DBConnection $csSite
Test-HypDBConnection -DBConnection $csSite
Test-LogDBConnection -DBConnection $csSite
Test-LogDBConnection -DataStore Logging -DBConnection $csLogging
Test-MonitorDBConnection -DBConnection $csSite
Test-MonitorDBConnection -Datastore Monitor -DBConnection
    $csMonitoring
Test-OrchDBConnection -DBConnection $csSite       # for 7.11 and
    newer
Test-ProvDBConnection -DBConnection $csSite
Test-SfDBConnection -DBConnection $csSite
Test-TrustDBConnection -DBConnection $csSite      # for 7.11 and
    newer
<!--NeedCopy-->
```

2. Citrix Studio を再起動します。

詳細情報の表示

- スタンドアロン SQL Server、データベースミラーリング、および常時高可用性を構成する方法

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Active Directory OU ベースの Controller 検出

May 18, 2020

この Delivery Controller 検出方法は主に後方互換性のためにサポートされており、VDA for Windows Desktop OS でのみ有効です（VDA for Windows Server OS では使用できません）。

VDA を Controller に登録できるように構成できるその他の方法（推奨される方法を含む）については、「Controller への VDA 登録」を参照してください。

この検出方法では、サイト内のすべてのコンピューターが同じ Active Directory ドメインに属しており、Controller とデスクトップで使用されるドメイン間に相互信頼関係が設定されている必要があります。この検出方法を使用する場合、各デスクトップのレジストリで組織単位（OU）の GUID を構成する必要があります。

OU ベースのコントローラの検出を実行するには、コントローラ上で **Set-ADControllerDiscovery.ps1** PowerShell スクリプトを実行します（各コントローラには、$env: ProgramFiles\ Citrix\ Broker\ Service\ Setup Scripts フォルダーにこのスクリプトが含まれています）。スクリプトを実行するには、すべての管理タスクを実行できる権限に加えて、親 OU での CreateChild 権限が必要です。

Active Directory を使用して Controller が検出されるように構成する場合は、サイトを作成するときに、対応する組織単位（OU）を Active Directory 内に作成する必要があります。この OU は、環境内のコンピューターが属しているフォレスト内のどのドメインにも作成できます。ベストプラクティスとしては、サイト内の Controller もこの OU に含まれている方が望ましいですが、これは必須ではありません。適切な権限を持つドメイン管理者は OU を空のコンテナとして作成して、その OU の管理権限をほかの Citrix 管理者に委任できます。

スクリプトを実行すると、以下の重要なオブジェクトが作成されます。これらのオブジェクトは、標準的な Active Directory オブジェクトです。スキーマを拡張する必要はありません。

- Controller のセキュリティグループ。サイト内のすべての Controller のコンピューターアカウントは、このセキュリティグループに属している必要があります。サイト内のデスクトップは、このセキュリティグループに属している Controller からのみデータを受け入れます。

  すべての Controller で、VDA を実行するすべての仮想デスクトップに対する「ネットワーク経由でコンピューターへアクセス」権限が必要です。このため、Controller のセキュリティグループにこの権限を追加します。Controller にこの権限がない場合、VDA は登録されません。

- サイトの名前など、サイトに関する情報を含むサービス接続ポイント（SCP）オブジェクト。［Active Directory ユーザーとコンピューター］管理ツールでサイト OU を確認する場合、SCP オブジェクトを表示するには［表示］メニューの［拡張機能］を有効にする必要があります。

- サイトの OU 内に作成される RegistrationServices という名前のコンテナ。このコンテナには、サイトの各 Controller について 1 つの SCP オブジェクトが含まれます。Controller が起動すると、その SCP の内容が検証され、必要な場合は更新されます。

初回インストール後に複数の管理者が Controller を追加および削除する可能性がある場合は、RegistrationServices コンテナで子を作成および削除する権限と、Controller セキュリティグループのプロパティを書き込む権限が

© 1999–2021 Citrix Systems, Inc. All rights reserved.

必要です。これらのアクセス許可は、Set-ADControllerDiscovery.ps1 スクリプトを実行する管理者に自動的に付与されます。これらの権限はドメイン管理者または初回インストール時の管理者が付与できます。また、これを行うためのセキュリティグループを設定することをお勧めします。

サイト OU を使用する場合、以下の項目が適用されます。

- Active Directory に情報が書き込まれるのは、この製品をインストールまたはアンインストールするときや、起動した Controller の SCP の情報を更新するとき（Controller の名前や通信ポートを変更した後など）のみです。デフォルトでは、Set-ADControllerDiscovery.ps1 スクリプトによってサイト OU 内のオブジェクトに関する権限が適切にセットアップされ、各 Controller に SCP への書き込み権限が付与されます。サイト OU 内のオブジェクトの内容は、デスクトップと Controller の間の信頼を確立するために使用されます。以下の点を確認してください。
  - 許可された管理者のみが、セキュリティグループのアクセス制御リスト（ACL）を使用して Controller のセキュリティグループにコンピューターを追加したり削除したりできること。
  - 許可された管理者と各 Controller のみが、Controller の SCP 内の情報を変更できること。
- 展開でレプリケーションを使用する場合は、潜在的な遅延に注意してください。詳しくは、Microsoft 社のドキュメントを参照してください。複数の Active Directory サイトにドメインコントローラーがあるドメイン内でサイト OU を作成する場合は、特に重要になります。デスクトップや Controller、ドメインコントローラーの場所によっては、サイト OU を最初に作成したり、Controller をインストールまたはアンインストールしたり、Controller 名や通信ポートを変更したりしたときの Active Directory の変更内容が、適切なドメインコントローラーに複製されるまでデスクトップ側に反映されない場合があります。このような遅延が発生するときは、デスクトップが Controller との接続を確立できないためにユーザーが仮想デスクトップに接続できないなどの問題が発生します。
- この製品では、Active Directory の標準のコンピューターオブジェクトの属性を複数使用して、デスクトップを管理します。環境によっては、デスクトップの Active Directory レコードに格納されるコンピューターオブジェクトの完全修飾ドメイン名（FQDN）が、接続を行うユーザーに返される接続設定の一部として含まれている場合があります。この情報が DNS 環境の情報と一致していることを確認してください。

OU ベースの Controller 検出を使用して Controller をほかのサイトに移動するには、前述の Controller の移動に関する指示に従って操作します。古いサイトから Controller を削除した後（手順.2）、PowerShell スクリプト **Set-ADControllerDiscovery –sync** を実行します。このスクリプトにより、OU が現在の Controller の一覧と同期されます。移動先のサイトに参加した後（手順 3.）、そのサイトの任意の Controller 上で同じスクリプトを実行します。

OU ベースの検出に必要な権限

サイトを作成するには、スクリプトを実行する Citrix サイト管理者が、サイト OU にオブジェクト（SCP、コンテナ、セキュリティグループ）を作成する権限を持っている必要があります。

サイト OU が存在しない場合は、管理者にも作成権限が必要です。AD ドメイン管理者は、事前にサイト OU を作成して、Citrix サイト管理者 ID に権限を割り当てることをお勧めします。必要な場合、このスクリプトはサイト OU も作成できます。これを許可するには、管理者は新しい OU の親 OU に対して「OU の作成」権限が必要です。ただ

© 1999–2021 Citrix Systems, Inc. All rights reserved.

し、前述のように、Citrix はこれを推奨しません。

後で、サイトに Controller を追加したり、サイトから Controller を削除したりするには、Citrix 管理者にセキュリティグループのマシンを追加/削除する権限、および SCP を作成/削除する権限が必要です。

通常の操作では、Controller および VDA は、OU およびその下部で、すべてのオブジェクトに対する読み取り権限が必要です。VDA は、そのマシン ID として OU にアクセスします。このマシン ID には、Controller を検出できるように少なくとも OU の読み取り権限が必要です。Controller には、コンテナで現在の SCP オブジェクトにプロパティを設定する権限が必要です。

Citrix 管理者の完全な権限を子 OU に付与すると、これらのすべてのアクションが可能になります。ただし、セキュリティ要件が厳格な環境（スクリプトを実行できるユーザーやアクションの種類を制限しているなど）では、制御の委任ウィザードを使用して特定の権限を設定することができます。次に例を示す手順では、サイトを作成する権限を付与します。

1. 子オブジェクト（サービス接続ポイント（SCP）、コンテナ、セキュリティグループ）を含む OU を作成します。
2. OU を選択して右クリックし、［制御の委任］を選択します。
3. 制御の委任ウィザードで、OU の制御を委任するドメインユーザーを指定します。
4. ［委任するタスク］ページで、［委任するカスタムタスクを作成する］を選択します。
5. ［**Active Directory** オブジェクトの種類］ページで、デフォルトの［このフォルダ、このフォルダ内の既存のオブジェクト、およびこのフォルダ内の新しいオブジェクトの作成］を受け入れます。
6. [アクセス許可] ページで、[すべての子オブジェクトの 作成**]** チェックボックスと **[**すべての子オブジェクトの作成**]** チェックボックスをオンにします。
7. ウィザードを終了して、権限を確認します。

© 1999–2021 Citrix Systems, Inc. All rights reserved.

© 1999–2021 Citrix Systems, Inc. All rights reserved.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).