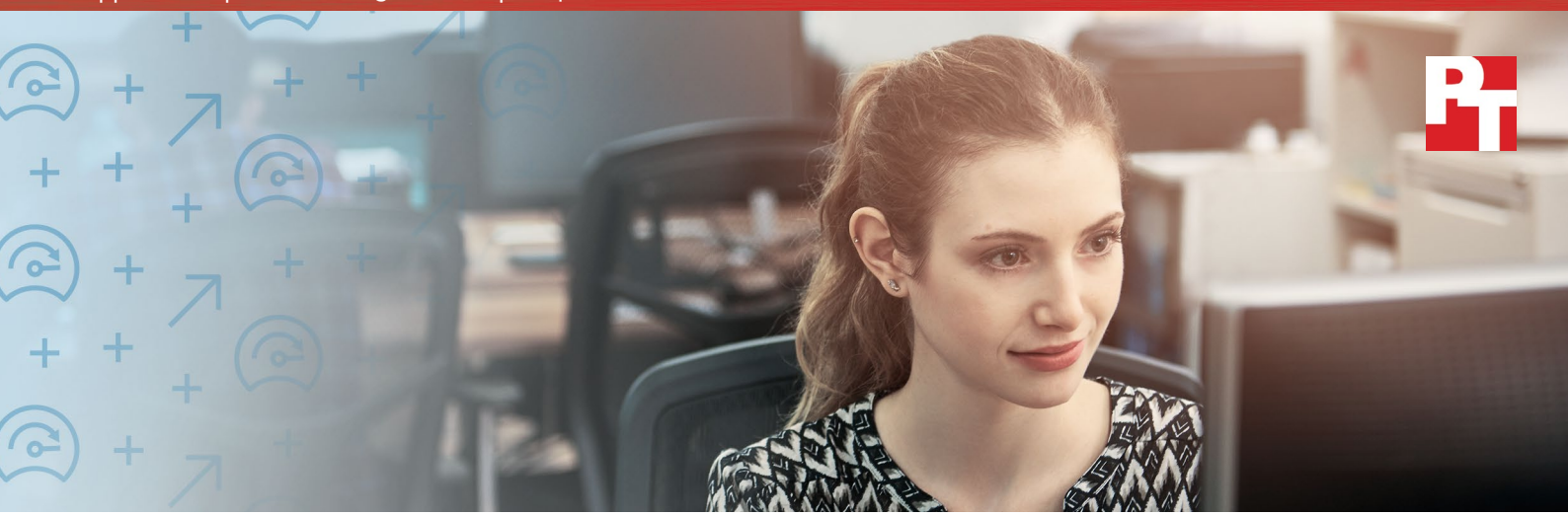


Bénéficiez des avantages d'un Cloud sur site et utilisez des outils habituels

Si vous utilisez des serveurs Dell EMC PowerEdge FC640 et des logiciels VMware, il peut être intéressant d'opter pour la gestion d'un Cloud privé au lieu de passer à un Cloud public

Le type de Cloud que vous choisissez maintenant affectera la gestion de votre datacenter pour les années à venir. Examinons donc quelques-unes des raisons pour lesquelles le choix d'un Cloud sur site peut constituer une bonne pratique commerciale par rapport au choix d'un Cloud public. Tout d'abord, la création et la mise en œuvre de votre propre Cloud privé peuvent faciliter le traitement des problèmes de sécurité, de conformité et de performances des applications critiques. Deuxièmement, même si certaines personnes estiment que les Clouds publics sont plus faciles à gérer que les Clouds sur site et qu'ils offrent un moyen sûr de réduire les coûts d'administration, si vous utilisez une architecture Dell EMC™ PowerEdge™ FX2 et des outils que vous connaissez bien, cela n'est pas forcément toujours vrai. En fait, dans certains cas, les déploiements sur site peuvent également générer des économies en termes de coût total de possession (TCO).

Nous avons constaté que la gestion d'une solution de Cloud privé sur site, exécutée sur des serveurs Dell EMC PowerEdge FC640 optimisés par les processeurs évolutifs Intel® Xeon®, nécessitait autant de temps, mais avec une moyenne de 34 % d'étapes en moins par rapport à la gestion d'un Cloud public Amazon Web Services™ (AWS). En outre, vous bénéficiez dans ce cas de l'avantage inhérent à l'utilisation du logiciel VMware® que vous connaissez déjà.

Les serveurs Dell EMC PowerEdge FC640 apportent la technologie la plus récente à votre Cloud privé

**par rapport à un Cloud public AWS*

Bénéficiez des avantages d'un Cloud sur site

Terminez les tâches rapidement

Temps de la gestion de Cloud similaire mais avec une moyenne de **34 % d'étapes en moins***

Bénéficiez des avantages d'un Cloud sur site

Dans l'environnement concurrentiel d'aujourd'hui, il est inévitable de se tourner vers le Cloud. Concernant le choix entre un Cloud public et un Cloud privé, c'est un peu comme choisir d'acheter ou de louer une voiture. Lorsque vous choisissez un Cloud public, comme par exemple l'option AWS que nous avons examinée, vous serez dépendant d'un contrat mensuel ou annuel et vous miserez sur la quantité de stockage des données et l'accès aux données nécessaires maintenant et dans un avenir proche. Tout comme lorsque vous louez une voiture, le dépassement des allocations de souscription peut entraîner des coûts supplémentaires. Avec un Cloud privé sur site, comme la solution Dell EMC PowerEdge FX2 que nous avons examinée, vous payez à l'avance et bénéficiez d'une plate-forme de serveur flexible et modulaire que vous pouvez diviser et allouer intégralement en fonction de vos besoins actuels, et reconfigurer à mesure que ces besoins évoluent au fil du temps. La création et la mise en œuvre de votre propre Cloud privé offrent également une multitude d'autres avantages :

Sécurité et conformité

Le maintien de la sécurité des données sensibles est un combat permanent. Le choix d'une solution de Cloud sur site signifie que vous savez toujours exactement où se trouvent vos données et que vous conservez la surveillance des stratégies de sécurité mises en œuvre pour protéger votre entreprise et ses clients. Ceci est particulièrement important si votre entreprise gère des informations médicales ou financières ou si elle doit répondre à des exigences réglementaires. Le stockage de ce type d'informations sur un Cloud public peut devenir de plus en plus complexe au fur et à mesure que votre organisation se développe.

Performances et continuité d'activité

Le passage aux nouvelles technologies peut perturber le personnel IT, qui aura peut-être besoin d'accéder à de nouvelles formations. Choisir une solution de Cloud sur site signifie que vous pouvez continuer à utiliser votre environnement VMware vSphere® existant et que vous pouvez créer et contrôler votre Cloud au moyen des plates-formes de gestion de Cloud VMware vRealize® Suite, ce qui facilite la mise à jour, la sécurisation et l'optimisation des applications critiques par les équipes IT, déjà familiarisées avec ces outils. Vous pouvez également maintenir les règles et politiques IT déjà en place dans l'entreprise lorsque vous choisissez une solution de Cloud privé Dell EMC PowerEdge FX2 sur site.

Personnalisation et compréhension

Vous savez mieux que quiconque quels clients, utilisateurs et applications doivent être traités en priorité. Il n'est pas réaliste de s'appuyer sur un service de Cloud public pour bénéficier de la granularité garantissant la disponibilité nécessaire à vos tâches prioritaires. Le choix d'une solution de Cloud sur site signifie que vous pouvez adapter la gestion des ressources en fonction de vos besoins spécifiques : vous n'avez pas besoin de vous conformer à une option de Cloud public de taille unique.

À propos de la solution Dell EMC PowerEdge FX2

Le Dell EMC PowerEdge FX2 est une plate-forme de serveurs modulaire qui combine serveurs, stockage et mise en réseau dans un châssis 2U unique.

Les nouveaux serveurs Dell EMC PowerEdge FC640 demi-hauteur à deux sockets sont équipés des processeurs évolutifs Intel Xeon, avec jusqu'à 2 To de mémoire, et un éventail de supports de stockage, notamment des disques SSD atteignant 240 Go.

Les serveurs Dell EMC PowerEdge FC640 sont également conçus pour fournir des mesures de sécurité intégrées de bout en bout, telles que la racine de base inviolable en silicium pour les mises à jour du micrologiciel, la protection supplémentaire contre les intrusions envers le matériel, le contrôle USB basé sur les règles et le lecteur crypté sécurisé.

Pour en savoir plus sur l'architecture Dell EMC PowerEdge FX, consultez la page www.dell.com/en-us/work/shop/cty/pdp/spd/poweredge-fx.

Terminez rapidement les tâches de gestion du Cloud

Que vous optiez pour un Cloud public ou un Cloud privé, quelqu'un doit toujours se charger de sa gestion. Si vous vous en tenez à un Cloud privé Dell EMC sur site, le personnel IT qui gère votre infrastructure PowerEdge et VMware existante s'en charge.

Nous avons enregistré la durée et les étapes nécessaires pour exécuter huit tâches courantes de la gestion de Cloud pour les deux options de Cloud. Nous avons choisi un large éventail de tâches qui donnent une image complète du cycle de vie de la gestion de Cloud. Ces tâches couvrent la configuration de la surveillance, que les administrateurs modifient fréquemment, et incluent la maintenance des comptes utilisateurs, à laquelle les administrateurs sont confrontés presque quotidiennement.

FX2 et réduction du TCO

Principled Technologies a mené une étude comparant les coûts de TCO d'une charge applicative d'analyse de Big Data basée sur Apache Spark sur un Cloud public AWS et sur une solution Dell EMC PowerEdge FX2 sur site. On constate que l'utilisation d'une solution Dell EMC FX2 sur site peut **économiser jusqu'à 42 % du TCO**. Cette étude utilisait un système d'exploitation et un environnement de test différents de ceux du rapport que vous lisez, mais elle pointe toutefois des économies réalisables liées aux performances. Cliquez ici pour lire l'intégralité du rapport « Run big data analytics on a powerful on-premises Dell EMC PowerEdge FX2 solution and save money over three years » (Exécutez des analyses de Big Data sur Dell EMC PowerEdge FX2, une puissante solution sur site, et réalisez des économies sur trois ans).[1]

Scénarios	Dell EMC et VMware		AWS	
	Durée (min:sec)	Étapes	Durée (min:sec)	Étapes
Création d'un nouvel utilisateur	01:01	20	00:59	22
Déploiement d'une VM personnalisée	00:14	7	00:34	14
Configuration de la surveillance des opérations	00:10	3	00:12	6
Configuration de la surveillance des fichiers log	00:07	3	00:10	7
Configuration de rapports de refacturation personnalisés	00:23	6	00:18	9
Configuration de la gestion des capacités	00:08	3	00:08	4
Déploiement d'une pile LAMP	00:17	6	00:47	15
Création d'un snapshot	00:15	9	00:12	8

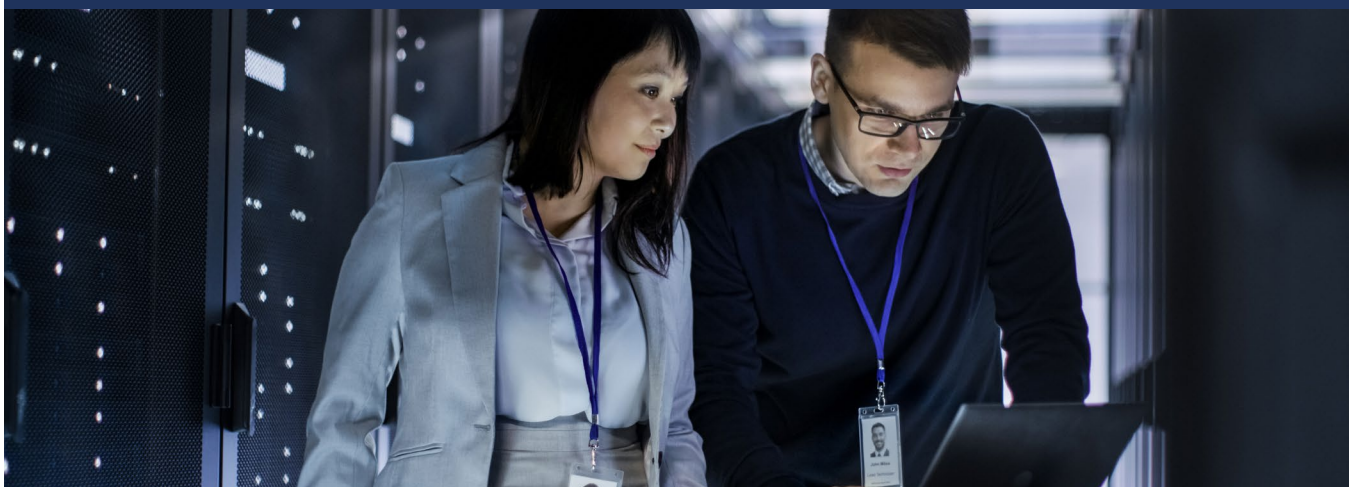
Voir l'Annexe D pour tous les résultats

Au cours des huit tâches de gestion courantes que nous avons testées, la solution de Cloud privé Dell EMC a nécessité une durée similaire, mais avec une moyenne de 34 % d'étapes en moins par rapport au Cloud public AWS. Ces résultats montrent également que le choix d'un Cloud public au lieu d'un Cloud sur site ne constitue pas un moyen infaillible pour réduire les coûts d'administration car le temps de gestion de l'administrateur est pratiquement identique.

À propos des processeurs évolutifs Intel Xeon

Les processeurs évolutifs Intel Xeon représentent la dernière génération de processeurs Intel pour serveurs. Ils sont disponibles en quatre configurations : Platinum, Gold, Silver et Bronze.

Au cours des tests que nous avons réalisés portant sur le Cloud privé sur site, le serveur Dell EMC PowerEdge FC640 utilisait des processeurs Intel Xeon Gold 5120. Ce processeur contient 14 cœurs fonctionnant à une fréquence de 2,20 GHz, avec une fréquence Max Turbo de 3,20 GHz. Pour en savoir plus sur les processeurs évolutifs Intel Xeon, visitez www.intel.com/content/www/us/en/processors/xeon/scalable/xeon-scalable-platform.html.



Conclusion

Nos administrateurs ont constaté que le choix d'une solution de Cloud privé sur site, exécutée sur une architecture Dell EMC PowerEdge FX2 et des serveurs FC640 optimisés par des processeurs évolutifs Intel Xeon, offre une bonne stratégie d'affaires dans certaines situations, par rapport à une solution de Cloud public AWS. En effet, l'utilisation de logiciels VMware pour effectuer diverses tâches courantes de la gestion de Cloud sur un Cloud privé sur site nécessitait un temps de gestion similaire, mais avec une moyenne de 34 % d'étapes en moins par rapport à l'option de Cloud public AWS. Un autre avantage principal est que les administrateurs de datacenters conservent un contrôle précis sur la façon dont ils implémentent leurs stratégies de sécurité et ajustent les ressources du Cloud privé pour des raisons de performances, sans se soucier de dépasser les allocations de souscription et en aidant votre datacenter à s'adapter aux besoins des entreprises en constante évolution.

1 Principled Technologies : Run big data analytics on a powerful on-premises Dell EMC PowerEdge FX2 solution and save money over three years (Exécutez des analyses de Big Data sur Dell EMC PowerEdge FX2, une puissante solution sur site, et réalisez des économies sur trois ans)

Le 5 novembre 2017, nous avons finalisé les configurations matérielles et logicielles testées. Les mises à jour des configurations matérielles et logicielles récentes et actuelles sont fréquentes. Il est donc possible que ces configurations ne correspondent pas aux toutes dernières versions disponibles au moment de la parution du présent rapport. Nous avons terminé les tests pratiques le 30 novembre 2017.

Annexe A : Informations de configuration du système

Informations de configuration du serveur	4 serveurs Dell EMC PowerEdge FC640
Nom et version du BIOS	Dell 1.0.1
Nom et numéro de version/build du système d'exploitation	VMware ESXi, 6.5.0, 5969303
Date d'application des dernières mises à jour/derniers correctifs du système d'exploitation	30/10/2017
Règle de gestion de l'alimentation	Performances
Processeur	
Nombre de processeurs	2
Fournisseur et modèle	Intel Xeon Gold 5120
Nombre de cœurs (par processeur)	14
Fréquence des cœurs (GHz)	2.20
Révision	1
Module(s) mémoire	
Mémoire totale du système (Go)	192
Nombre de modules mémoire	12
Fournisseur et modèle	Hynix HMA82GR7AFR8N-VK
Taille (Go)	16
Type	PC4-21300R
Vitesse (MHz)	2666
Vitesse du serveur (MHz)	2444
Contrôleur de stockage	
Fournisseur et modèle	Dell PERC H330 Mini
Version du microprogramme	25.3.0004
Version du pilote	4.27

Informations de configuration du serveur	4 serveurs Dell EMC PowerEdge FC640
Disques durs locaux	
Nombre de disques	2
Fournisseur et modèle des disques	Seagate® ST600MM0238
Taille de disque (Go)	600
Informations sur les disques (vitesse, interface, type)	Disques durs SAS 10 000 tr/min, 12 Gbit/s
Carte réseau	
Fournisseur et modèle	Intel Ethernet 10G 2P X710-k bND
Nombre et type de ports	2 x 10 GbE
Version du pilote	18.016

Informations de configuration du stockage	1 contrôleur de baie Dell Storage SC9000
Révision du microprogramme du contrôleur	6.7.5
Nombre de contrôleurs de stockage	2
Nombre de tiroirs de stockage	1
Nombre de disques par tiroir	24
Disques n° 1	
Nombre de disques	12
Fournisseur et numéro de modèle des disques	Dell LB806M
Taille de disque (Go)	800
Informations sur les disques (vitesse, interface, type)	SSD, SAS, 6 Gbit/s
Disques n° 2	
Nombre de disques	6
Fournisseur et numéro de modèle des disques	Dell HUSMH8040BSS200
Taille de disque (Go)	400
Informations sur les disques (vitesse, interface, type)	SSD, SAS, 12 Gbit/s
Disques n° 3	
Nombre de disques	6
Fournisseur et numéro de modèle des disques	Dell HUSMM1680ASS200
Taille de disque (Go)	800
Informations sur les disques (vitesse, interface, type)	SSD, SAS, 12 Gbit/s

Informations de configuration du boîtier pour serveur	Dell EMC PowerEdge FX2s
Nombre de modules de gestion	2
Révision du microprogramme de module de gestion	2.0
Micrologiciel du module CMC	2.00
Version du fond de panier central	1.0
Premier type de module d'E/S	
Numéro de modèle et fournisseur	Module passthrough Dell 1GBE
Révision du microprogramme de module d'E/S	X03
Nombre de modules	1
Emplacements occupés	A2
Blocs d'alimentation	
Numéro de modèle et fournisseur	Dell 0W1R7VA00
Nombre de blocs d'alimentation	2
Puissance en watts (W) de chaque bloc	2000
Ventilateurs	
Nombre de ventilateurs	8

Annexe B : Mise en place de l'environnement de test

Cette annexe détaille notre processus initial d'installation des environnements de Cloud privé Dell EMC et de Cloud public AWS. Les cas d'utilisation de nos tests supposent l'utilisation d'environnements préexistants ; ces étapes n'entrent pas dans le cadre de notre comparaison.

Déploiement d'un Cloud Dell EMC et VMware sur site

Nous avons configuré chaque serveur Dell EMC PowerEdge FC640 avec un lecteur virtuel utilisant deux disques physiques dans la configuration RAID 10 pour le stockage local et l'installation de l'hyperviseur. Nous avons créé quatre volumes (un pour chaque serveur) sur la baie Dell Storage SC9000 Array pour obtenir un stockage non local.

Installation de VMware ESXi 6.5

1. Rattachez le kit d'installation au serveur.
2. Démarrez le serveur.
3. Dans l'écran du programme d'installation VMware, appuyez sur Entrée.
4. Dans l'écran EULA, appuyez sur F11 pour accepter et continuer (Accept and Continue).
5. Sous Storage Devices, sélectionnez le disque approprié, puis appuyez sur Entrée.
6. Sélectionnez US en tant que configuration du clavier, puis appuyez sur Entrée.
7. Saisissez le mot de passe root à deux reprises, puis appuyez sur Entrée.
8. Appuyez sur F11 pour démarrer l'installation.
9. Pour redémarrer le serveur, retirez le kit d'installation, puis appuyez sur Entrée.
10. Une fois le serveur redémarré, appuyez sur F2, puis saisissez les credentials root.
11. Sélectionnez Configure Management Network, puis appuyez sur Entrée.
12. Sélectionnez IPv4 Configuration, puis entrez les détails de configuration souhaités. Appuyez sur Entrée.
13. Sélectionnez DNS Configuration, puis indiquez le serveur DNS primaire (Primary DNS Server). Appuyez sur Entrée.
14. Appuyez sur Échap, puis appuyez sur Y pour accepter les modifications.

Déploiement de l'appliance VMware vCenter Server 6.5

1. Ouvrez le dossier du kit d'installation.
2. Sélectionnez vcsa-ui-installer et cliquez avec le bouton droit de la souris sur l'application d'installation.
3. Cliquez sur Run as Administrator.
4. Cliquez sur Yes.
5. Dans la fenêtre installation de l'appliance 6,5, cliquez sur Install.
6. Sur la page Introduction, cliquez sur Next.
7. Acceptez les termes du contrat de licence et cliquez sur Next.
8. Cliquez sur l'option vCenter Server with an Embedded Platform Services Controller, puis cliquez sur Next.
9. Entrez l'adresse IP du serveur cible ESXi, le nom d'utilisateur et le mot de passe, puis cliquez sur Next.
10. Pour accepter le certificat, cliquez sur Yes.
11. Saisissez un mot de passe root pour l'appliance, confirmez-le, puis cliquez sur Next.
12. Sélectionnez la taille du déploiement (nous avons sélectionné Tiny et la taille de stockage par défaut), puis cliquez sur Next.
13. Cochez la case pour activer le mode Disque Thin, puis cliquez sur Next.
14. Entrez les informations réseau souhaitées (adresse IP de l'application, sous-réseau, passerelle et DNS), puis cliquez sur Next.
15. Vérifiez les informations de l'étape 1 et cliquez sur le bouton Finish.
16. Cliquez sur Continue pour passer à l'étape 2 du déploiement.
17. Sur la page Introduction, cliquez sur Next.
18. Entrez les serveurs NTP pour la synchronisation, activez SSH, puis cliquez sur Next.
19. Saisissez un nom de domaine, un mot de passe, un nom de site, puis cliquez sur Next.
20. Cliquez sur Next pour CEIP.
21. Vérifiez les paramètres de l'étape 2 et cliquez sur Finish.
22. Une fois l'installation terminée, cliquez sur Close.

Installation du plug-in d'authentification améliorée VMware

1. Ouvrez un navigateur Web et entrez l'adresse IP de l'appliance vCenter Server.
2. Cliquez pour ouvrir vSphere Web Client (Flash).
3. Cliquez sur Download Enhanced Authentication Plugin.
4. Cliquez sur Save File.
5. Accédez à Downloads et double-cliquez pour lancer l'application d'installation.
6. Cliquez sur OK.
7. Cliquez sur OK.
8. Dans l'écran de bienvenue de l'installation, cliquez sur Next.
9. Acceptez les termes du contrat de licence et cliquez sur Next.
10. Cliquez sur Install.
11. Cliquez sur Finish.
12. Dans la fenêtre Plug in Service Installation, cliquez sur Next.
13. Acceptez les termes du contrat de licence et cliquez sur Next.
14. Cliquez sur Install.
15. Cliquez sur Finish.

Déploiement et configuration de vRealize Operations Manager (vROM)

1. À partir du client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster.
2. Sélectionnez Deploy OVF template…
3. Cliquez sur Browse…
4. Accédez au fichier OVF, puis cliquez sur Open.
5. Cliquez sur Next.
6. Saisissez un nom pour OVF, puis cliquez sur Next.
7. Sélectionnez une ressource pour OVF, puis cliquez sur Next.
8. Passez en revue les détails du modèle et cliquez sur Next.
9. Acceptez les termes du contrat de licence et cliquez sur Next.
10. Choisissez la taille de la configuration (nous avons choisi Extra Small), puis cliquez sur Next.
11. Sélectionnez le format de disque virtuel et le datastore, puis cliquez sur Next.
12. Sélectionnez le réseau, puis cliquez sur Next.
13. Entrez les adresses IP DNS et de la passerelle par défaut.
14. Entrez l'adresse IP OVF et le masque de réseau.
15. Développez les paramètres supplémentaires et sélectionnez le fuseau horaire approprié.
16. Cliquez sur Next.
17. Vérifiez la configuration et cliquez sur Finish.
18. Mettez la machine virtuelle sous tension.
19. Accédez à l'adresse IP vROM dans le navigateur Web.
20. Cliquez sur New Installation.
21. Cliquez sur Next.
22. Saisissez un mot de passe pour le compte administrateur, confirmez-le, puis cliquez sur Next.
23. Choisissez une méthode de certificat, puis cliquez sur Next.
24. Renseignez le Cluster Master Node Name et entrez une adresse de serveur NTP.
25. Cliquez sur Next.
26. Cliquez sur Finish.
27. Une fois l'initialisation terminée, cliquez sur START vREALIZE OPERATIONS MANAGER.
28. Cliquez sur Yes.
29. Une fois vROM en ligne, connectez-vous à vROM en utilisant le compte admin et le mot de passe précédemment définis.
30. Dans l'écran de configuration, cliquez sur Next.
31. Acceptez les conditions générales d'utilisation, puis cliquez sur Next.
32. Entrez une clé de produit ou sélectionnez Product Evaluation, puis cliquez sur Next.
33. Cliquez sur Next.
34. Cliquez sur Finish.
35. Sélectionnez VMware vSphere.
36. Cliquez sur l'icône en forme d'engrenage pour lancer la configuration.
37. Entrez un nom d'affichage et l'adresse IP du vCenter.
38. Cliquez sur le signe plus vert, entrez le nom, le nom d'utilisateur et le mot de passe correspondant aux credentials de l'administrateur vCenter.

39. Cliquez sur OK.
40. Cliquez sur Test Connection.
41. Pour accepter le certificat, cliquez sur ACCEPT.
42. Une fois la connexion réussie, cliquez sur OK.
43. Cliquez sur SAVE SETTINGS.
44. Cliquez sur OK.
45. Cliquez sur CLOSE.

Déploiement et configuration de vRealize log Insight (vRLI)

1. À partir du client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster.
2. Sélectionnez Deploy OVF template…
3. Cliquez sur Browse…
4. Accédez au fichier OVF, puis cliquez sur Open.
5. Cliquez sur Next.
6. Saisissez un nom pour OVF, puis cliquez sur Next.
7. Sélectionnez une ressource pour OVF, puis cliquez sur Next.
8. Passez en revue les détails du modèle et cliquez sur Next.
9. Acceptez les termes du contrat de licence et cliquez sur Next.
10. Sélectionnez la taille de la configuration (nous avons choisi Extra Small), puis cliquez sur Next.
11. Sélectionnez le format de disque virtuel et le datastore, puis cliquez sur Next.
12. Sélectionnez le réseau de destination, puis cliquez sur Next.
13. Entrez les adresses IP du DNS, le domaine DNS et le chemin de recherche searchpath.
14. Entrez les adresses IP de la passerelle par défaut et de la VM.
15. Entrez le masque de réseau et développez la liste des options.
16. Saisissez un mot de passe root et confirmez-le, puis cliquez sur Next.
17. Vérifiez les données de configuration et cliquez sur Finish.
18. Mettez la machine virtuelle sous tension.
19. Accédez à l'adresse IP vRLI dans le navigateur Web.
20. Cliquez sur Next.
21. Cliquez sur Start New Deployment.
22. Entrez une adresse e-mail, puis entrez un nouveau mot de passe et confirmez-le.
23. Cliquez sur Save and Continue.
24. Entrez une clé de licence, ou cliquez sur Skip pour utiliser le mode d'évaluation.
25. Entrez une adresse e-mail et des URL pour les notifications système à fournir, puis cliquez sur Save and Continue.
26. Entrez les éventuels serveurs NTP supplémentaires, puis cliquez sur Test.
27. Une fois les tests réussis, cliquez sur Save and Continue.
28. Entrez d'autres paramètres de configuration SMTP ou cliquez sur Skip.
29. Cliquez sur Finish.
30. Cliquez sur Configure vSphere integration.
31. Saisissez l'adresse IP, le nom d'utilisateur et le mot de passe pour vCenter Server.
32. Cliquez sur Test Connection.
33. Une fois le test réussi, cliquez sur Save.
34. Cliquez sur OK.
35. Dans le menu latéral, cliquez sur vRealize Operations.
36. Saisissez le nom d'hôte, le nom d'utilisateur et le mot de passe pour vROM.
37. Cliquez sur Test Connection.
38. Une fois le test réussi, cliquez sur Next.
39. Cliquez sur OK.

Création et configuration du serveur Windows IaaS

1. À partir de la console Web vCenter, cliquez avec le bouton droit de la souris sur le cluster ou le serveur, sélectionnez New Virtual Machine, puis cliquez sur New Virtual Machine.
2. Sélectionnez Create a new virtual machine, puis cliquez sur Next.
3. Saisissez un nom pour la machine virtuelle, sélectionnez un datacenter, puis cliquez sur Next.
4. Sélectionnez une ressource de calcul, puis cliquez sur OK.
5. Sélectionnez un datastore, puis cliquez sur Next.
6. Sélectionnez la compatibilité/version souhaitée, puis cliquez sur Next.

7. Sélectionnez la gamme Guest OS (Windows) et la version Guest OS (Windows Server 2016), puis cliquez sur Next.
8. Personnalisez le matériel selon vos besoins (nous avons choisi 2 vCPU et 8 192 Mo de mémoire), puis cliquez sur Next.
9. Vérifiez la configuration et cliquez sur Finish.
10. Connectez-vous à la console virtuelle en utilisant la console Web ou VRMC.
11. Rattachez le kit d'installation Windows Server 2016.
12. Mettez la machine virtuelle sous tension.
13. Dans l'écran de sélection de la langue, cliquez sur Next.
14. Cliquez sur Install Now.
15. Saisissez la clé du produit, puis cliquez sur Next.
16. Sélectionnez Desktop Experience, puis cliquez sur Next.
17. Acceptez les termes du contrat de licence et cliquez sur Next.
18. Sélectionnez Custom install.
19. Cliquez sur Next.
20. Saisissez le mot de passe de votre choix pour l'administrateur, puis cliquez sur Finish.
21. Revenez à la console Web vCenter.
22. Cliquez avec le bouton droit de la souris sur la VM, sélectionnez Guest OS, puis sélectionnez Install VMware Tools…
23. Revenez à la VM, double-cliquez sur l'exécutable de configuration des outils VMware et suivez les instructions pour installer les outils VMware.
24. Exécutez Windows Update et redémarrez la VM si nécessaire.
25. Ajoutez le serveur au domaine.
26. Après avoir ajouté le serveur au domaine, dans la fenêtre du gestionnaire de serveur, cliquez sur Add Roles and Features.
27. Ajoutez les fonctionnalités suivantes : .NET 3.5 (HTTP and non-HTTP authentication), .NET 4.6 (HTTP and non-HTTP authentication), et IIS. Redémarrez si nécessaire.
28. Ouvrez un navigateur Web et accédez à `http://java.com/en/download/`
29. Cliquez sur Free Java Download.
30. Ouvrez le kit d'installation et suivez les instructions pour installer Java.
31. Une fois l'installation terminée, localisez l'installation Java à l'aide de la ligne de commande ou de l'Explorateur de fichiers (exemple d'emplacement : C:\Program Files\Java\jre1.8.version).
32. Dans le panneau de configuration, accédez à Advanced system settings.
33. Cliquez sur Environment Variables.
34. Cliquez sur New.
35. Entrez JAVA_HOME pour le nom de la variable et le chemin d'accès au dossier Java en tant que valeur.
36. Cliquez sur OK.
37. Rattachez le kit d'installation Microsoft SQL Server 2016 à la VM.
38. Lancez l'exécutable d'installation de Microsoft SQL Server.
39. Cliquez sur Installation, puis sélectionnez New installation ou ajoutez des fonctions à une installation existante.
40. Saisissez la clé du produit, puis cliquez sur Next.
41. Cochez Use Microsoft Update, puis cliquez sur Next.
42. Pour installer les fichiers de support de configuration, cliquez sur Install.
43. Sélectionnez SQL Server Feature Installation, puis cliquez sur Next.
44. Sélectionnez Database Engine Services, Full-Text Search, Client Tools Connectivity, Client Tools Backwards Compatibility et Management Tools Basic, puis Complete. Cliquez sur Next.
45. Acceptez les paramètres de configuration par défaut de l'instance, puis cliquez sur Next.
46. Acceptez les paramètres de configuration par défaut du serveur, puis cliquez sur Next.
47. Sélectionnez Mixed Mode, puis saisissez un mot de passe pour le compte SA. Cliquez sur Add Current User, puis sur Next.
48. Passez en revue les règles de configuration de l'installation, puis cliquez sur Install.
49. Dans l'écran de fin de l'opération, cliquez sur Close.
50. Ouvrez un navigateur Web et accédez à `http://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms`
51. Téléchargez Microsoft SQL Server Management Studio et suivez les instructions d'installation pour installer SSMS.

Déploiement et configuration de vRealize Automation (vRA)

1. À partir du client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster.
2. Sélectionnez Deploy OVF template…
3. Cliquez sur Browse…
4. Accédez au fichier OVF, puis cliquez sur Open.
5. Cliquez sur Next.
6. Saisissez un nom pour OVF, puis cliquez sur Next.
7. Sélectionnez une ressource pour OVF, puis cliquez sur Next.

8. Passez en revue les détails du modèle et cliquez sur Next.
9. Acceptez les termes du contrat de licence et cliquez sur Next.
10. Sélectionnez le format de disque virtuel et le datastore, puis cliquez sur Next.
11. Sélectionnez le réseau de destination, puis cliquez sur Next.
12. Cochez la case permettant d'activer SSH.
13. Entrez un hostname et un mot de passe, puis cliquez pour développer Networking Properties.
14. Entrez l'adresse IP de la passerelle et du DNS par défaut, puis entrez l'adresse IP de la VM.
15. Entrez le masque de réseau, puis cliquez sur Next.
16. Cliquez sur Finish.
17. Mettez la machine virtuelle sous tension.
18. Accédez à l'adresse IP vRA dans le navigateur Web.
19. Connectez-vous en saisissant `root` et le mot de passe entré à la phase de configuration.
20. Dans Installation Wizard, cliquez sur Next.
21. Acceptez les termes du contrat de licence et cliquez sur Next.
22. Sélectionnez la taille du déploiement (nous avons choisi le déploiement Minimal), conservez l'installation par défaut d'IaaS, puis cliquez sur Next.
23. Sélectionnez Use Time Server.
24. Cliquez sur le signe plus vert pour ajouter un serveur NTP.
25. Ouvrez une session de console distante sur le serveur Iaas Windows.

Installation de l'agent de gestion sur le serveur Windows IaaS

1. À partir du serveur Iaas Windows, ouvrez un navigateur Web et accédez à l'adresse IP vRA.
2. Connectez-vous en saisissant `root` et le mot de passe entré à la phase de configuration.
3. Dans Installation Wizard, cliquez sur Next.
4. Cliquez pour télécharger IaaS Management Agent.
5. Cliquez sur Save.
6. Cliquez sur Open.
7. Dans la fenêtre vRealize Automation Management Agent Setup, cliquez sur Next.
8. Acceptez les conditions générales d'utilisation, puis cliquez sur Next.
9. Acceptez le dossier de destination par défaut, puis cliquez sur Next.
10. Entrez les informations IP de l'appliance vRA, le nom d'utilisateur root et le mot de passe.
11. Pour charger le certificat de service du site de gestion, cliquez sur Load.
12. Cochez la case pour confirmer les correspondances d'empreintes digitales.
13. Cliquez sur Next.
14. Entrez le mot de passe du compte IaaS Windows VM Administrator, puis cliquez sur Next.
15. Cliquez sur Install.
16. Cliquez sur Finish.
17. Revenez au navigateur Web pour terminer la configuration vRA.

Fin de la configuration de vRA

1. Dans l'assistant d'installation de vRA, assurez-vous que l'hôte IaaS apparaît dans la liste, puis cliquez sur Next.
2. Cliquez sur Run pour exécuter l'outil de vérification des conditions préalables.
3. Cliquez sur Fix si des conditions préalables sont incorrectes.
4. Une fois la vérification terminée avec l'état OK, cliquez sur Next.
5. Entrez l'alias DNS ou le FQDN de l'appliance vRA, puis cliquez sur Next.
6. Saisissez un mot de passe pour le compte administrateur, confirmez-le, puis cliquez sur Next.
7. Entrez l'alias DNS ou le FQDN pour le serveur Web IaaS.
8. Saisissez le nom d'utilisateur et le mot de passe du serveur Web IaaS.
9. Entrez une phrase de passe de sécurité de la base de données, confirmez-la, puis cliquez sur Validate.
10. Une fois la validation réussie, cliquez sur Next.
11. Entrez le nom du serveur d'une instance SQL existante, puis sélectionnez Use existing empty database.
12. Cliquez sur Next.
13. Vérifiez les informations DEM, puis cliquez sur Next.
14. Vérifiez les informations des agents, puis cliquez sur Next.
15. Sélectionnez Generate Certificate, puis renseignez les valeurs Organization, Organizational Unit et Country Code.
16. Cliquez sur Save Generated Certificate.
17. Cliquez sur Next.

18. Sélectionnez Generate Certificate, puis renseignez les valeurs Organization, Organizational Unit et Country Code.
19. Cliquez sur Save Generated Certificate.
20. Cliquez sur Next.
21. Cliquez sur Validate.
22. Une fois la validation terminée, cliquez sur Next.
23. Créez les instantanés des VM ou des appliances que vous souhaitez, puis cliquez sur Next.
24. Cliquez sur Install.
25. Une fois l'installation terminée, cliquez sur Next.
26. Saisissez la clé de licence, puis cliquez sur Next.
27. Décochez la case de renoncement au programme Customer Experience Improvement Program, puis cliquez sur suivant.
28. Sélectionnez Configure Initial Content et cliquez sur Next.
29. Entrez un mot de passe pour le compte configurationadmin, puis cliquez sur Create Initial Content.
30. Une fois la configuration initiale du contenu terminée, cliquez sur Next.
31. Cliquez sur Finish.

Déploiement et configuration de vRealize Business for Cloud (vRBC)

1. À partir du client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster.
2. Sélectionnez Deploy OVF template…
3. Cliquez sur Browse…
4. Accédez au fichier OVF, puis cliquez sur Open.
5. Cliquez sur Next.
6. Saisissez un nom pour OVF, puis cliquez sur Next.
7. Sélectionnez une ressource pour OVF, puis cliquez sur Next.
8. Passez en revue les détails du modèle et cliquez sur Next.
9. Acceptez les termes du contrat de licence et cliquez sur Next.
10. Sélectionnez le format de disque virtuel et le datastore, puis cliquez sur Next.
11. Sélectionnez le réseau de destination, puis cliquez sur Next.
12. Conservez la devise par défaut (USD) et cochez la case d'activation de SSH.
13. Saisissez un mot de passe d'utilisateur root et confirmez-le.
14. Cliquez pour développer Networking Properties.
15. Entrez une passerelle, un domaine et un DNS par défaut.
16. Entrez l'adresse IP de la VM, le masque de réseau, puis cliquez sur Next.
17. Vérifiez les données de configuration et cliquez sur Finish.
18. Mettez la machine virtuelle sous tension.
19. Ouvrez un navigateur Web et accédez à `https://vRBC-IP:5480`
20. Entrez `root` et le mot de passe créé pendant le déploiement, puis cliquez sur Log in.
21. Entrez le nom d'hôte de vRA, le tenant par défaut, l'utilisateur admin et le mot de passe.
22. Cochez la case d'acceptation du certificat, puis cliquez sur Register.

Début de la configuration du tenant par défaut avec l'entrée de catalogue de la configuration initiale

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/`
2. Connectez-vous en tant que `configurationadmin` à l'aide du mot de passe précédemment créé.
3. Sélectionnez Administration.
4. Sélectionnez Users and Groups.
5. Sélectionnez Directory Users and Groups.
6. Recherchez `configurationadmin`.
7. Sélectionnez `configurationadmin`.
8. Cochez toutes les cases pour ajouter tous les rôles à l'utilisateur.
9. Cliquez sur Finish.
10. Cliquez sur Logout.
11. Cliquez sur Go back to login page.
12. Connectez-vous à vRA en tant que `configurationadmin`.
13. Sélectionnez Catalog.
14. Cliquez sur vSphere Initial Setup.
15. Cliquez sur Request.
16. Sélectionnez Yes pour configurer le tenant actuel, puis cliquez sur Next.

17. Entrez le nom, le FQDN et la ressource de calcul pour le terminal vSphere.
18. Entrez le nom d'utilisateur et le mot de passe du terminal vSphere, puis cliquez sur Submit.
19. Cliquez sur OK.
20. Sélectionnez Inbox.
21. Cliquez sur Manual User Action.
22. Sélectionnez l'action à effectuer.
23. Cliquez sur View Details.
24. Sélectionnez les modèles de VM à publier en tant qu'éléments de catalogue.
25. Dans le menu déroulant, sélectionnez le stockage de réservation.
26. Dans le menu déroulant, sélectionnez le pool de ressources de réservation.
27. Dans le menu déroulant, sélectionnez le réseau de réservation.
28. Cliquez sur Submit.
29. Une fois que la demande a abouti, déconnectez-vous de vRA.

Suite de la configuration du tenant par défaut

1. Connectez-vous à vRA en tant que `configurationadmin`.
2. Sélectionnez Business Management.
3. Entrez un numéro de série pour le produit, puis cliquez sur Save.
4. Sélectionnez l'onglet Infrastructure.
5. Cliquez sur Endpoints.
6. Cliquez sur Endpoints.
7. Cliquez sur New.
8. Sélectionnez Management, puis cliquez sur vRealize Operations Manager.
9. Entrez un nom pour le terminal, l'adresse de la VM, le nom d'utilisateur et le mot de passe.
10. Cliquez sur Test Connection.
11. Cliquez sur OK pour approuver le terminal.
12. Cliquez sur OK.
13. Sélectionnez l'onglet Administration.
14. Cliquez sur Directories Management.
15. Cliquez sur Directories.
16. Cliquez sur Add Directory.
17. Sélectionnez Add Directory over LDAP/IWA.
18. Entrez un nom de répertoire.
19. Renseignez les champs Base DN, Bind DN et Bind DN Password en suivant le format fourni en exemple.
20. Cliquez sur Test Connection.
21. Une fois le test de connexion réussi, cliquez sur Save & Next.
22. Cliquez sur Next.
23. Cliquez sur Next.
24. Sélectionnez les utilisateurs que vous souhaitez inclure, puis cliquez sur Next.
25. Sélectionnez les utilisateurs que vous souhaitez exclure, puis cliquez sur Next.
26. Cliquez sur Sync Directory.
27. Cliquez sur l'onglet Administration.
28. Cliquez sur vRO Configuration.
29. Cliquez sur Endpoints.
30. Cliquez sur New.
31. Sélectionnez Active Directory, puis cliquez sur Next.
32. Saisissez un nom pour le terminal, puis cliquez sur Next.
33. Entrez l'adresse IP du serveur, le nom unique de base (DC=domain,DC=com), le nom d'utilisateur (DOMAIN\Administrator) et le mot de passe.
34. Cliquez sur Finish.
35. Sélectionnez l'onglet Administration.
36. Cliquez sur Reclamation.
37. Cliquez sur Metrics Provider.
38. Sélectionnez le terminal vRealize Operations Manager.
39. Saisissez l'URL, le nom d'utilisateur et le mot de passe.
40. Cliquez sur Test Connection.

41. Cliquez sur Save.
42. Cliquez sur OK pour approuver le terminal.
43. Sélectionnez Infrastructure.
44. Cliquez sur Reservations.
45. Cliquez sur Reservations.
46. Sélectionnez la réservation créée par le blueprint Initial Setup.
47. Cliquez sur Resources.
48. Modifiez la réservation si nécessaire, puis cliquez sur OK.
49. Cliquez sur Placement Policy.
50. Cochez la case permettent d'utiliser vROM.
51. Cliquez sur Apply.
52. Cliquez sur Yes pour confirmer.

Configuration des packs de gestion vROM

1. Ouvrez un navigateur Web et accédez à `https://[IP-address-of-vROM].`
2. Connectez-vous en tant qu'`admin`.
3. Sélectionnez Administration.
4. Sélectionnez l'adaptateur VMware vRealize Log Insight.
5. Cliquez sur les engrenages pour configurer l'adaptateur.
6. Entrez un nom d'affichage et l'adresse IP du serveur vRLI.
7. Cliquez sur Test Connection.
8. Une fois la connexion réussie, cliquez sur Save settings.
9. Fermez la fenêtre.
10. Sélectionnez l'adaptateur VMware vRealize Business for Cloud.
11. Cliquez sur les engrenages pour configurer l'adaptateur.
12. Entrez un nom d'affichage et l'adresse IP du serveur vRBC.
13. Cliquez sur Test Connection.
14. Une fois la connexion réussie, cliquez sur Save settings.
15. Fermez la fenêtre.
16. Sélectionnez l'adaptateur VMware vRealize Automation.
17. Cliquez sur les engrenages pour configurer l'adaptateur.
18. Entrez un nom d'affichage et l'adresse IP du serveur vRA.
19. Cliquez sur le signe plus vert en regard de Credential.
20. Saisissez un nom pour le credential.
21. Entrez `administrator@vsphere.local` pour le nom d'utilisateur SysAdmin et le mot de passe associé.
22. Entrez `configurationadmin@vsphere.local` pour le nom d'utilisateur SuperUser et le mot de passe associé.
23. Cliquez sur OK.
24. Cliquez sur Test Connection.
25. Une fois la connexion réussie, cliquez sur Save settings.
26. Fermez la fenêtre.

Déploiement d'un Cloud public AWS

Nous avons testé l'utilisation d'un compte AWS gratuit et l'accès au mot de passe et aux paramètres du compte principal/root.

Ajout de règles supplémentaires pour le catalogue de services

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Dans le tableau de bord principal, sélectionnez IAM.
4. Cliquez sur Create policy pour créer une règle supplémentaire pour les administrateurs du catalogue.
5. Indiquez un nom de règle et une description.

6. Copiez le texte suivant dans Policy Document :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
             "Action": [
                 "ec2:CreateKeyPair",
                 "iam:AddRoleToInstanceProfile",
                 "iam:AddUserToGroup",
                 "iam:AttachGroupPolicy",
                 "iam:CreateAccessKey",
                 "iam:CreateGroup",
                 "iam:CreateInstanceProfile",
                 "iam:CreateLoginProfile",
                 "iam:CreateRole",
                 "iam:CreateUser",
                 "iam:Get*",
                 "iam:List*",
                 "iam:PutRolePolicy",
                 "iam:UpdateAssumeRolePolicy"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

7. Cliquez sur Create Policy.
8. Cliquez sur Refresh.
9. Dans le champ de recherche, saisissez `ServiceCatalog`.
10. Cochez la case en regard de `ServiceCatalogAdminFullAccess` et la règle nouvellement créée.
11. Cliquez sur Next: Review.
12. Passez en revue les détails, puis cliquez sur Create user.
13. Cliquez sur Policies pour créer une règle supplémentaire pour les utilisateurs du catalogue.
14. Cliquez sur Create policy.
15. Cliquez sur Select next to Create Your Own Policy.
16. Saisissez un nom et une description.
17. Copiez le texte suivant dans Policy Document :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ProvisionProduct"
            ],
            "Resource": "*"
        }
    ]
}
```

18. Cliquez sur Create Policy.
19. Revenez à la page AWS Dashboard.
20. Sélectionnez EC2.
21. Cliquez sur Key Pairs.
22. Cliquez sur Create Key Pair.
23. Entrez un nom pour la paire de clés.
24. Cliquez sur Create.
25. Lorsque vous y êtes invité, cliquez pour enregistrer le fichier.

26. Revenez à la page AWS Dashboard.
27. Sélectionnez Service Catalog.
28. Cliquez sur Create portfolio.
29. Saisissez un nom, une description et un propriétaire.
30. Cliquez sur Create.
31. Cliquez sur Upload new product.
32. Entrez un nom de produit, une description et un nom pour Provided by.
33. Cliquez sur Next.
34. Entrez les détails de support souhaités, puis cliquez sur Next.
35. Recherchez le modèle désiré ou entrez une URL S3 pour le modèle.
36. Entrez un titre et une description pour la version.
37. Cliquez sur Next.
38. Passez en revue les détails, puis cliquez sur Create.

Configuration de la CLI du connecteur AWS et téléchargement d'une AMI

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`.
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Sélectionnez S3.
4. Cliquez sur Create Bucket.
5. Saisissez le nom de bucket.
6. Sélectionner une région.
7. Cliquez sur Next.
8. Définissez les propriétés de la gestion des versions, la journalisation ou les balises si vous le souhaitez.
9. Cliquez sur Next.
10. Conservez les autorisations par défaut, puis cliquez sur Next.
11. Passez en revue les paramètres, puis cliquez sur Create Bucket.
12. Sélectionnez le bucket nouvellement créé.
13. Cliquez sur Upload.
14. Cliquez sur Add files.
15. Accédez aux fichiers de l'image ou du modèle de la VM.
16. Sélectionnez les fichiers.
17. Cliquez sur Open.
18. Examinez les autorisations, puis cliquez sur Next.
19. Examinez les propriétés, puis cliquez sur Next.
20. Examinez le téléchargement, puis cliquez sur Upload.
21. Cliquez sur la flèche déroulante en regard du nom d'utilisateur.
22. Cliquez sur My Security Credentials.
23. Cliquez sur Access Keys.
24. Cliquez sur Download Key File.
25. Si vous y êtes invité, cliquez Save.
26. Ouvrez une fenêtre de terminal ou de commande.
27. Installez awscli en exécutant la commande suivante : `pip3 install awscli --upgrade --user`
28. Vérifiez que awscli est correctement installé en exécutant la commande suivante : `aws --version`
29. Créez un fichier nommé `trust-policy.json` et saisissez les éléments suivants :

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
            }
         }
      }
   ]
}
```

30. Créez un fichier nommé `role-policy.json` et saisissez les éléments suivants :

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource": [
            "arn:aws:s3:::disk-image-file-bucket"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetObject"
         ],
         "Resource": [
            "arn:aws:s3:::disk-image-file-bucket/*"
         ]
      },
      {
         "Effect": "Allow",
         "Action":[
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
         ],
         "Resource": "*"
      }
   ]
}
```

31. Configurez l'interface de ligne de commande d'AWS en exécutant la commande suivante : `aws configure`
32. Entrez la clé d'accès AWS à partir du fichier de clés d'accès téléchargé.
33. Appuyez sur Entrée.
34. Entrez la clé secrète AWS à partir du fichier de clés d'accès téléchargé.
35. Appuyez sur Entrée.
36. Entrez le nom de région par défaut (nous avons utilisé `us-east-1`).
37. Appuyez sur Entrée.
38. Entrez le format de sortie (nous avons utilisé `json`).
39. Appuyez sur Entrée.
40. Créez un rôle pour importer les VM en exécutant la commande suivante : `aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json`
41. Appliquez une règle pour le rôle créé en exécutant la commande suivante : `aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json`
42. Créez un fichier nommé `containers.json` et entrez le texte suivant :

```
[
  {
    "Description": "UploadDescription",
    "Format": "VMDK",
    "UserBucket": {
        "S3Bucket": "name_of_bucket",
        "S3Key": "name_of_file.vmdk"
    }
}]
```

43. Importez la VM en exécutant la commande suivante : `aws ec2 import-image --description "UploadDescription" --license-type BYOL --disk-containers file://containers.json`
44. Vérifiez la progression du téléchargement en exécutant la commande suivante : `aws ec2 describe-import-image-tasks --import-task-ids import-ami-ID_goes_here`
45. Revenez à la console Web AWS.
46. Cliquez sur le bouton d'accueil.

Création d'une VM Windows 2012 R2 et d'un modèle

Création de la VM Windows 2012 R2

1. Accédez au client Web vSphere.
2. Connectez-vous en tant que `administrator@vsphere.local`
3. Sélectionnez Create a new virtual machine.
4. Choisissez Custom, puis cliquez sur Next.
5. Saisissez un nom pour la VM, puis cliquez sur Next.
6. Sélectionnez l'hôte, puis cliquez sur Next.
7. Sélectionnez le stockage approprié, puis cliquez sur Next.
8. Sélectionnez Windows, choisissez Microsoft Windows Server 2012 (64-bit), puis cliquez sur Next.
9. Pour le champ CPUs, sélectionnez deux sockets de processeur virtuels, et un cœur par socket virtuel, puis cliquez sur Next.
10. Choisissez 8 GB RAM, puis cliquez sur Next.
11. Pour le nombre de NIC, cliquez sur 1. Sélectionnez VMXNET 3, connectez-vous au réseau de la VM, puis cliquez sur Next.
12. Laissez le contrôleur de stockage virtuel par défaut, puis cliquez sur Next.
13. Choisissez de créer un nouveau disque virtuel, puis cliquez sur Next.
14. Définissez la taille du disque virtuel du système d'exploitation à 50 Go, choisissez thin-provisioned, spécifiez le stockage, puis cliquez sur Next.
15. Conservez le nœud du périphérique virtuel par défaut (0:0), puis cliquez sur Next.
16. Cliquez sur Finish.
17. Connectez le CD-ROM virtuel de la VM au disque d'installation Microsoft Windows Server 2012 R2.
18. Démarrez la machine virtuelle.
19. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez Open Console.
20. Dans l'écran Windows Language Selection, cliquez sur Next.
21. Cliquez sur Install Now.
22. Saisissez la clé du produit, puis cliquez sur Next.
23. Sélectionnez Windows Server 2012 R2 Datacenter (Server with a GUI), puis cliquez sur Next.
24. Cochez la case I accept the license terms, puis cliquez sur Next.
25. Cliquez sur Custom.
26. Cliquez sur Next.
27. Saisissez le mot de passe de votre choix pour l'administrateur dans les deux champs, puis cliquez sur Finish.
28. Connectez-vous à la VM, puis installez VMware Tools.
29. Définissez une adresse IP statique pour la VM.
30. Connectez-vous à Internet et installez toutes les mises à jour Windows disponibles. Redémarrez si nécessaire.
31. Activez l'accès au bureau à distance, désactivez les pare-feu, et désactivez également la sécurité IE si nécessaire.
32. Modifiez le nom d'hôte, associez le domaine approprié, puis redémarrez le système lorsque vous y êtes invité.
33. Dans la nouvelle VM, accédez à `https://IP-of-vra/software/index.html`, puis cliquez pour télécharger la version appropriée de l'agent invité Windows.
34. Cliquez sur Save, puis enregistrez l'agent invité sur le lecteur C:.
35. Accédez au fichier de l'agent invité, cliquez avec le bouton droit de la souris sur le fichier, puis sélectionnez Properties.
36. Cliquez sur Unblock.
37. Cliquez sur Apply, puis sur OK.
38. Pour extraire le fichier, double-cliquez dessus.
39. Cliquez sur le menu Start et entrez RUN.
40. Saisissez `sysprep` et appuyez sur Entrée.
41. Cliquez avec le bouton droit de la souris sur sysprep et sélectionnez Run as Administrator.
42. Cochez la case Generalize. Dans Shutdown Options, sélectionnez Reboot.
43. Une fois la VM arrêtée, revenez à la console Web vCenter et sélectionnez la VM.
44. Cliquez avec le bouton droit de la souris sur la VM, sélectionnez Clone, puis cliquez sur Clone to Template.
45. Dans le client vSphere, accédez à l'accueil, puis cliquez sur Customization Specifications Manager.
46. Cliquez sur New pour créer un nouveau modèle de personnalisation.
47. Choisissez Windows, nommez la personnalisation de l'invité, puis cliquez sur Next.
48. Saisissez un nom de propriétaire et une organisation, puis cliquez sur Next.
49. Sélectionnez Use the virtual machine name, puis cliquez sur Next.
50. Entrez une clé de produit si nécessaire, ou laissez le champ vide. Cliquez sur Next.
51. Saisissez un mot de passe pour le compte administrateur, confirmez-le, puis cliquez sur Next.
52. Choisissez le fuseau horaire correct, puis cliquez sur Next.

53. Si nécessaire, entrez une commande à exécuter lors de la première connexion. Cliquez sur Next.
54. Sélectionnez les paramètres du réseau standard, puis cliquez sur Next.
55. Sélectionnez Windows Server Domain et entrez les informations de domaine. Saisissez le nom d'utilisateur et le mot de passe AD, puis cliquez sur Next.
56. Cochez Generate New Security ID, puis cliquez sur Next.
57. Vérifiez l'écran récapitulatif et cliquez sur Finish.

Exportation de la VM en tant qu'OVF

1. Dans la console Web vCenter, cliquez avec le bouton droit de la souris sur la VM.
2. Sélectionnez Template, puis cliquez sur Export OVF Template…
3. Saisissez un nom pour OVF, puis cliquez sur OK.
4. Pour les tests AWS, téléchargez OVF en suivant la procédure de la section **Configuration de la CLI du connecteur AWS et téléchargement d'une AMI**.

VMware : création d'un blueprint dans vRA

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/`
2. Connectez-vous en tant que `configurationadmin`.
3. Sélectionnez Design, Blueprint, puis cliquez sur New.
4. Entrez un nom pour le blueprint. Cliquez sur OK.
5. Dans le modèle de conception, sélectionnez Machine Types, puis cliquez sur une machine vSphere et faites-la glisser vers le modèle.
6. Dans l'onglet Build Information, choisissez l'action Clone.
7. Choisissez le modèle créé précédemment dans Clone from.
8. Dans Customization, entrez le nom de la personnalisation invitée dans vSphere (notez que ce nom doit être saisi exactement).
9. Cliquez sur Machine Resources, puis définissez les valeurs minimale et maximale de vos préférences.
10. Cliquez sur Storage, puis sur New. Ajoutez le stockage désiré et cochez la case Allow user to see and change storage reservation policies.
11. Sélectionnez Networks & Security dans le modèle de conception, puis cliquez sur Existing Network et faites glisser le réseau existant vers le modèle.
12. Choisissez le réseau externe dans Existing Network, puis cliquez sur OK.
13. Revenez à la configuration de la machine vSphere, puis cliquez sur Network.
14. Cliquez sur New, puis choisissez le réseau externe. Entrez la configuration IP souhaitée.
15. Cliquez sur Finish.
16. Dans Blueprints, sélectionnez le blueprint créé, puis cliquez sur Publish.
17. Sélectionnez successivement Administration, Catalog Management, puis Services.
18. Sélectionnez le service souhaité, puis cliquez sur Manage Catalog Items.
19. Cliquez sur le signe plus vert.
20. Ajoutez l'élément de catalogue au service, puis cliquez sur OK.

AWS : création d'un modèle CloudFormation

1. Connectez-vous à la console Web AWS en tant qu'utilisateur root.
2. Accédez à `https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-sample-templates.html`
3. Sélectionnez la région appropriée (nous avons choisi la région Est des États-Unis (Virginie du Nord)).
4. Sélectionnez Services.
5. Sélectionnez EC2.
6. Pour l'instance Amazon EC2 dans un groupe de sécurité, cliquez sur View in Designer.
7. Modifiez le modèle afin que AWSInstanceType2Arch fasse référence à l'AMI téléchargée et convertie en suivant la procédure de la section **Configuration de la CLI du connecteur AWS et téléchargement d'une AMI**.
8. Après la modification, cliquez sur l'icône en forme de coche pour valider le modèle.
9. Après la validation, cliquez sur l'icône de page, puis cliquez sur Save.
10. Effectuez l'enregistrement en tant que fichier local ou dans un bucket Amazon S3.
11. Nommez le fichier et cliquez sur Save.
12. Revenez à la console AWS.
13. Sélectionnez Service Catalog.
14. Sélectionnez le portefeuille par défaut.
15. Cliquez sur Upload new product.
16. Entrez un nom pour le produit, une description, un constructeur, un fournisseur, puis cliquez sur Next.
17. Entrez les détails de support souhaités, puis cliquez sur Next.
18. Recherchez le fichier modèle à télécharger (s'il est stocké localement) ou spécifiez l'URL du modèle s'il stocké dans le bucket S3.
19. Entrez les détails de la version, puis cliquez sur Next.
20. Vérifiez les informations, puis cliquez sur Create.

Création des VM et du modèle de la pile LAMP

Création des VM de la pile LAMP

1. Dans la console Web vSphere HTML5, cliquez avec le bouton droit de la souris sur l'hôte d'infrastructure, puis sélectionnez New Virtual Machine.
2. Dans l'assistant Create New Virtual Machine, cliquez sur Next.
3. Entrez un nom correspondant au rôle de la VM (LAMP1, LAMP2 ou loadbalancer), assurez-vous que l'emplacement d'inventaire correct est sélectionné, puis cliquez sur Next.
4. Sélectionnez la ressource d'ordinateur correcte et cliquez sur Next.
5. Sélectionnez le stockage de destination pour les fichiers de la VM et cliquez sur Next.
6. Définissez la compatibilité avec ESXi 6.5 ou une version ultérieure, puis cliquez sur Next.
7. Remplacez le système d'exploitation invité par Linux, sélectionnez CentOS 7 (64-bit) dans le menu déroulant Version, puis cliquez sur Next.
8. Sélectionnez les valeurs correctes pour Network et Adapter, puis cliquez sur Next.
9. Examinez le récapitulatif des paramètres de la nouvelle VM, puis cliquez sur Finish.
10. Cliquez avec le bouton droit de la souris sur la VM nouvellement créée, puis sélectionnez Open Console. Pour alimenter la VM, cliquez sur l'icône de lecture verte.
11. Répétez les étapes 1 à 10 deux fois de plus pour créer un total de trois VM, avec les noms de VM suivants : LAMP1, LAMP2, loadbalancer.
12. Dans l'émulateur de la console vSphere, pour la première VM, cliquez sur l'icône représentant une clé, sélectionnez le lecteur de CD/DVD 1 et sélectionnez Connect to ISO image on local disk. Accédez au kit d'installation de CentOS 7, puis cliquez sur Open.
13. Lorsque l'invite CentOS 7 apparaît, utilisez les touches fléchées pour sélectionner Installer CentOS 7, puis appuyez sur Entrée.
14. Lorsque l'assistant d'installation de CentOS 7 apparaît, conservez les paramètres de langue et de clavier par défaut, puis cliquez sur Continue.
15. Sélectionnez Software Selection dans la page Installation Summary.
16. Remplacez la valeur de Base Environment par Infrastructure Server, puis cliquez sur Done.
17. Sélectionnez Installation Destination.
18. Pour nos tests, nous avons conservé le périphérique sélectionné par défaut et la méthode de division par défaut (Automatically configure partitioning). Cliquez sur Done.
19. Sélectionnez Network & Hostname.
20. Mettez la carte NIC sous tension, assurez-vous qu'une adresse DHCP est affectée et entrez un nom d'hôte correspondant à la VM (LAMP1, LAMP2 ou loadbalancer). Cliquez sur Done.
21. Commencez l'installation.
22. Pendant l'installation, cliquez sur Root Password, puis entrez un mot de passe root et confirmez-le.
23. Cliquez sur Reboot lorsque l'installation est terminée.
24. Répétez les étapes 12 à 23 deux fois de plus pour créer un total de trois installations CentOS 7 avec les noms d'hôte suivants : LAMP1, LAMP2, loadbalancer.
25. Effectuez une connexion à distance de la console à la première VM et connectez-vous avec les credentials root.
26. Exécutez la commande `vim /etc/sysconfig/selinux` pour ouvrir le fichier de configuration SELinux.
27. Modifiez `SELINX=enforcing to SELINUX=disabled`, enregistrez les modifications et quittez VIM.
28. Exécutez la commande `yum –y` update pour mettre à jour tous les modules.
29. Redémarrez le serveur lorsque les mises à jour des modules sont terminées.
30. Répétez les étapes 25 à 29 deux fois de plus pour désactiver SELinux et mettre à jour les packages modules défaut pour les trois VM.
31. À partir de la connexion à distance de la console à la VM LAMP1, exécutez la commande `yum –y install httpd php mariadb-server mariadb` pour installer le service Apache HTTP, PHP5 et MariaDB.
32. Exécutez la commande `systemctl start httpd` pour démarrer le service Apache HTTP.
33. Exécutez la commande `systemctl enable httpd` pour assurer le démarrage du service Apache HTTP à l'amorçage.
34. Exécutez la commande `systemctl start mariadb` pour démarrer le service MariaDB.
35. Exécutez la commande `systemctl enable mariadb` pour assurer le démarrage du service MariaDB à l'amorçage.
36. Exécutez la commande `mysql_secure_installation` et suivez l'invite pour définir un mot de passe root, désactiver les utilisateurs anonymes et supprimer la base de données de test.
37. Exécutez la commande `mysql –u root –p` et connectez-vous avec les credentials root pour accéder à l'invite SQL Server.
38. À partir de l'invite SQL, entrez les lignes ci-dessous (en utilisant la touche Entrée pour les retours à la ligne) pour créer la base de données conceptuelle (lorsque vous répéterez l'opération pour LAMP2, changez le nom d'hôte de manière appropriée en fonction de LAMP1). Pour effectuer cette étape, vous devez vous connecter en tant qu'utilisateur authentifié pour accéder à la base de données à distance.

```
CREATE DATABASE testdb;
USE testdb;
GRANT REPLICATION SLAVE ON *.* TO testuser@LAMP2 IDENTIFIED BY 'password';
FLUSH PRIVILEGES;
CREATE TABLE testable (testname VARCHAR(100), testnumber DOUBLE);
INSERT INTO testable VALUES ('first', 100);
INSERT INTO testable VALUES ('second, 200);
exit;
```

39. Exécutez la commande `vim /etc/my.cnf` pour ouvrir le fichier de configuration de MariaDB.
40. Ajoutez les lignes suivantes au début du fichier (lorsque vous répéterez l'opération pour LAMP2, remplacez server-id par '2') :

```
server-id = 1
log_bin = /var/log/mariadb/mariad.log
binlog_do_db = testdb
```

41. Ajoutez les lignes suivantes à la fin du fichier (lorsque vous répéterez l'opération pour LAMP2, remplacez auto-increment-offset par '2' et master-host par 'LAMP2') :

```
replicate-same-server-id = 0
auto-increment-increment = 2
auto-increment-offset = 1
master-host = LAMP1
master-user = testuser
master-password = password
master-connect-retry = 60
replicate-do-db = testdb
```

42. Enregistrez les modifications et quittez VIM.
43. Exécutez la commande `systemctl restart mariadb` pour redémarrer MariaDB.
44. Exécutez la commande `mysql -u root -p` et connectez-vous avec les credentials root pour accéder à l'invite SQL Server.
45. À partir de l'invite SQL, entrez les lignes suivantes (en utilisant la touche Entrée pour les retours à la ligne) pour activer la réplication maître-maître (lorsque vous répéterez l'opération pour LAMP2, remplacez MASTER_HOST par 'LAMP1') :

```
CHANGE MASTER TO MASTER_HOST='LAMP2',
MASTER_USER='testuser', MASTER_PASSWORD='password',
MASTER_LOG_FILE='mariadb.log';
START SLAVE;
exit;
```

46. Répétez les étapes 31 à 45 une fois de plus pour configurer la pile LAMP pour les VM LAMP1 et LAMP2.
47. À partir de la connexion à distance de la console à la VM loadbalancer, exécutez la commande `yum -y install httpd php` pour installer le service Apache HTTP, PHP.
48. Par défaut, le module mod_proxy_balancer doit être installé et activé. Exécutez la commande `vim /etc/httpd/conf/httpd.conf` pour ajouter les paramètres de configuration de ce module.
49. Ajoutez les informations suivantes au fichier :

```
Allow from all

BalancerMember LAMP1
BalancerMember LAMP2

ProxyPass / balancer://mycluster
```

50. Exécutez la commande `systemctl restart httpd` pour redémarrer le service Apache HTTP.
51. Arrêtez toutes les VM.
52. Cliquez avec le bouton droit de la souris sur la VM, sélectionnez Template, puis cliquez sur Convert to Template.
53. Répétez l'étape 52 pour chacune des VM de la pile LAMP.

Création du blueprint dans vRealize Automation

1. Connectez-vous à vRealize Automation en tant qu'administrateur de l'infrastructure, puis sélectionnez l'onglet Design.
2. Sous Blueprints, cliquez sur New.
3. Sous l'onglet General, renseignez les champs Name, ID, Description, Archive days, Lease days, puis cliquez sur OK.
4. Sous Categories, sélectionnez Network and Security.
5. Glissez-déplacez l'icône Existing Network sur le modèle.
6. Sous l'onglet General, sélectionnez External Network pour Existing Network, puis cliquez sur OK.
7. Sous Categories, sélectionnez Machine Types.
8. Glissez-déplacez une machine vSphere sur le modèle.
9. Sous l'onglet General, entrez l'ID, le préfixe de la machine et le nombre d'instances.
10. Cliquez sur l'onglet Build Information, puis choisissez le type de blueprint Server, l'action Clone, le workflow de provisionnement CloneWorkflow et le modèle approprié pour Clone for.

11. Sélectionnez l'onglet Network, puis cliquez sur Next.
12. Dans le menu déroulant, sélectionnez External Network.
13. Sélectionnez la valeur appropriée pour Assignment Type, puis cliquez sur OK.
14. Répétez les étapes 8 à 13 deux fois de plus pour créer deux autres machines vSphere sur le modèle.
15. Cliquez sur Finish.
16. Mettez le blueprint en surbrillance, puis cliquez sur Publish.
17. Ajoutez le blueprint à un Entitlement et à un service pour l'ajouter au catalogue.

Annexe C : méthode de test

Nous avons commencé la comparaison à ce stade avec tous les autres composants configurés car il s'agit d'actions uniques non répétées. Nous avons déployé des services payants basés sur un abonnement comme le requiert le Cloud public AWS pour atteindre des configurations aussi proches que possible.

Création d'un nouvel utilisateur dans un tenant existant

VMware

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/`
2. Connectez-vous en tant qu'`administrateur`.
3. Sélectionnez le tenant dans lequel le nouvel utilisateur sera ajouté.
4. Cliquez sur Local users.
5. Cliquez sur New.
6. Entrez un prénom et un nom de famille pour le nouvel utilisateur.
7. Entrez une adresse e-mail et un nom d'utilisateur pour le nouvel utilisateur.
8. Entrez un mot de passe pour le nouvel utilisateur et confirmez-le.
9. Cliquez sur OK.
10. Cliquez sur Finish.
11. Cliquez sur Logout.
12. Cliquez sur Go back to login page.
13. Connectez-vous en tant que `configurationadmin`.
14. Sélectionnez Administration.
15. Cliquez sur Users & Groups.
16. Cliquez sur Business Groups.
17. Sélectionnez le groupe d'entreprises à modifier.
18. Cliquez sur Members.
19. Ajoutez le nouveau membre au rôle ou aux rôles appropriés.
20. Cliquez sur Finish.

AWS

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`.
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Sélectionnez IAM.
4. Cliquez sur Users.
5. Cliquez sur Add user.
6. Saisissez un nom d'utilisateur.
7. Sélectionnez l'accès à la console de gestion AWS.
8. Sélectionnez Custom password.
9. Saisissez un mot de passe.
10. Indiquez si l'utilisateur doit ou non créer un nouveau mot de passe lors de la prochaine connexion, puis cliquez sur Next: Permissions.
11. Cliquez sur Copy permissions from existing user.
12. Sélectionnez l'utilisateur à partir duquel copier les autorisations.
13. Cliquez sur Next: Review.
14. Cliquez sur Create User.
15. Retournez à la console principale.
16. Sélectionnez Service Catalog.
17. Sélectionnez le portefeuille dans lequel le nouvel utilisateur sera ajouté.
18. Cliquez sur Users, groups and roles.
19. Cliquez sur Add user, group or role.
20. Cliquez sur Users.
21. Sélectionnez l'utilisateur nouvellement créé.
22. Cliquez sur Add Access.

Déploiement d'une VM personnalisée à partir d'un catalogue

VMware

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/org/[tenant]`
2. Connectez-vous en tant qu'utilisateur du catalogue.
3. Sélectionnez Catalog.
4. Cliquez sur l'entrée de catalogue souhaitée.
5. Cliquez sur Request.
6. Cliquez sur Submit.
7. Cliquez sur OK.

AWS - Option 1 : utilisation du catalogue de services

1. Ouvrez un navigateur Web et accédez à `https://[service-catalog-user-IP].`
2. Connectez-vous en tant qu'utilisateur du catalogue.
3. Sélectionnez Service Catalog.
4. Cliquez sur le menu déroulant Service Catalog, puis sur Dashboard.
5. Sélectionnez le produit à lancer.
6. Cliquez sur Launch product.
7. Entrez un nom pour le produit provisionné, puis sélectionnez une version.
8. Cliquez sur Next.
9. Sélectionnez le nom d'une paire de clés EC2 existante et modifiez SSHLocation ou InstanceType si nécessaire.
10. Cliquez sur Next.
11. Entrez la clé et la valeur d'une balise existante.
12. Cliquez sur Next.
13. N'activez pas la diffusion de rubriques SNS, puis cliquez sur Next.
14. Vérifiez la configuration, puis cliquez sur Launch.

AWS - Option 2 : utilisation d'EC2 directement

1. Ouvrez un navigateur Web et accédez à `https://[service-catalog-user-IP].`
2. Connectez-vous en tant qu'utilisateur EC2.
3. Sélectionnez EC2.
4. Cliquez sur Launch Instance.
5. Cliquez sur My AMIs.
6. Choisissez l'AMI, puis cliquez sur Select.
7. Sélectionnez un type d'instance, puis cliquez sur Next: Configure Instance Details.
8. Modifiez les paramètres souhaités ou acceptez les valeurs par défaut en cliquant sur Next : Ajoutez un stockage.
9. Modifiez le volume root provisionné, ajoutez un nouveau volume ou acceptez les valeurs par défaut en cliquant sur Next: Add Tags.
10. Cliquez sur Add Tag.
11. Entrez une clé et une valeur, puis cliquez sur Next: Security Group.
12. Modifiez les paramètres souhaités ou acceptez les valeurs par défaut en cliquant sur Review and Launch.
13. Passez en revue les détails, puis cliquez sur Launch.
14. Choisissez une paire de clés existante, ou créez une nouvelle paire, puis cliquez sur Launch Instance.

Configuration et maintenance de la surveillance des opérations de Cloud

VMware

1. Ouvrez un navigateur Web et accédez à `https://[IP-address-of-vROM].`
2. Connectez-vous en tant qu'admin.
3. Examinez l'état du système et les correctifs suggérés.

AWS

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`.
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Sélectionnez CloudWatch.
4. Cliquez sur Dashboards.
5. Sélectionnez le tableau de bord souhaité.
6. Examinez les informations du tableau de bord.

Configuration et gestion de la surveillance des fichiers log

VMware

1. Ouvrez un navigateur Web et accédez à `https://[IP-address-of-vRLI]`.
2. Connectez-vous en tant qu'`admin`.
3. Examinez les événements, les erreurs et les notifications dans le tableau de bord.

AWS

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`.
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Sélectionnez CloudWatch.
4. Cliquez sur Logs.
5. Sélectionnez le Log Group souhaité.
6. Sélectionnez le Log Stream souhaité.
7. Examinez les événements trouvés dans le flux du log.

Configuration de rapports de refacturation personnalisés

VMware

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/`
2. Connectez-vous en tant que `configurationadmin`.
3. Sélectionnez Business Management.
4. Cliquez sur Reports.
5. Sélectionnez le rapport préconfiguré ou personnalisé souhaité.
6. Cliquez sur Export.

AWS

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`.
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Cliquez sur la flèche déroulante en regard du nom du compte.
4. Cliquez sur My Billing Dashboard.
5. Cliquez sur Cost Explorer.
6. Cliquez sur Launch Cost Explorer.
7. Cliquez sur Reports.
8. Sélectionnez le rapport préconfiguré ou personnalisé souhaité.
9. Cliquez sur Download CSV.

Configuration de la gestion de la capacité pour détecter, prédire et optimiser les VM surprovisionnées

VMware

1. Ouvrez un navigateur Web et accédez à `https://[IP-address-of-vROM]`.
2. Connectez-vous en tant qu'`admin`.
3. Examinez les actions suggérées dans le tableau de bord.

AWS

1. Ouvrez un navigateur Web et accédez à `https://console.aws.amazon.com`.
2. Connectez-vous en utilisant l'adresse e-mail et le mot de passe du compte principal.
3. Sélectionnez Trusted Advisor
4. Examinez les suggestions d'optimisation des coûts, de performances, de sécurité et de tolérance aux pannes.

Déploiement d'une pile LAMP à plusieurs VM

VMware

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/org/[tenant]`
2. Connectez-vous à vRealize Automation en tant qu'utilisateur de catalogue.
3. Sélectionnez l'onglet Catalog.
4. Sélectionnez All Services.
5. Localisez le blueprint et cliquez sur Request.
6. Examinez tous les composants du blueprint, puis cliquez sur Submit.

AWS - Option 1 : utilisation du catalogue de services

1. Ouvrez un navigateur Web et accédez à `https://[service-catalog-user-IP].`
2. Connectez-vous en tant qu'utilisateur du catalogue.
3. Sélectionnez Service Catalog.
4. Cliquez sur le menu déroulant Service Catalog, puis sur Dashboard.
5. Sélectionnez le produit à lancer.
6. Cliquez sur Launch product.
7. Entrez un nom pour le produit provisionné, puis sélectionnez une version.
8. Cliquez sur Next.
9. Sélectionnez le nom d'une paire de clés EC2 existante, sélectionnez les sous-réseaux souhaités et entrez un mot de passe de base de données.
10. Sélectionnez l'ID VPC et entrez un nom d'utilisateur de base de données.
11. Modifiez les valeurs par défaut souhaitées, puis cliquez sur Next.
12. Entrez la clé et la valeur d'une balise existante.
13. Cliquez sur Next.
14. N'activez pas la diffusion de rubriques SNS, puis cliquez sur Next.
15. Vérifiez la configuration, puis cliquez sur Launch.

AWS - Option 2 : utilisation d'EC2 directement

1. Ouvrez un navigateur Web et accédez à `https://[service-catalog-user-IP].`
2. Connectez-vous en tant qu'utilisateur EC2.
3. Sélectionnez EC2.
4. Cliquez sur Launch Instance.
5. Cliquez sur AWS Marketplace.
6. Recherchez `LEMP 7 Optimized` dans la zone de recherche.
7. Choisissez l'AMI, puis cliquez sur Select.
8. Examinez les détails de tarification, puis cliquez sur Continue.
9. Sélectionnez un type d'instance, puis cliquez sur Next: Configure Instance Details.
10. Modifiez les paramètres souhaités ou acceptez les valeurs par défaut en cliquant sur Next : Ajoutez un stockage.
11. Modifiez le volume root provisionné, ajoutez un nouveau volume ou acceptez les valeurs par défaut en cliquant sur Next: Add Tags.
12. Cliquez sur Add Tag.
13. Entrez une clé et une valeur, puis cliquez sur Next: Security Group.
14. Modifiez les paramètres souhaités ou acceptez les valeurs par défaut en cliquant sur Review and Launch.
15. Passez en revue les détails, puis cliquez sur Launch.
16. Choisissez une paire de clés existante, ou créez une nouvelle paire, puis cliquez sur Launch Instance.

Création d'un snapshot d'une VM gérée

VMware

1. Ouvrez un navigateur Web et accédez à `https://vra-ip/vcac/org/[tenant]`.
2. Connectez-vous en tant qu'utilisateur du catalogue.
3. Sélectionnez Items.
4. Cliquez Machines.
5. Sélectionnez la VM souhaitée.
6. Cliquez sur Actions.
7. Cliquez sur Create snapshot.
8. Si nécessaire, renommez le snapshot, entrez une description et choisissez si vous souhaitez inclure la mémoire. Sinon, cliquez sur Submit.
9. Cliquez sur OK.

AWS

1. Ouvrez un navigateur Web et accédez à `https://[service-catalog-user-IP]`.
2. Connectez-vous en tant qu'utilisateur EC2.
3. Sélectionnez EC2.
4. Dans la barre latérale, sélectionnez Volumes.
5. Sélectionnez le volume souhaité.
6. Cliquez sur Actions, puis sélectionnez Create Snapshot.
7. Saisissez le nom et la description du snapshot.
8. Cliquez sur Create.

Annexe D : Résultats

Nous avons enregistré les périodes médianes de trois séries consécutives et le nombre d'étapes établi à l'Annexe C'. Comme nos tests réalisés avec AWS utilisaient des réseaux publics, les durées peuvent légèrement varier en fonction du trafic réseau. Deux des scénarios ont abouti à deux méthodes similaires pour effectuer les tâches dans AWS. Nous avons donc noté la durée et les étapes pour chaque méthode.

Nous avons calculé la différence, en pourcentage, entre le nombre d'étapes requis pour chaque solution de Cloud, pour chacune des huit tâches de gestion testées. Ensuite, nous avons calculé la moyenne de ces différences, en pourcentage, pour les huit tâches, en utilisant le nombre d'étapes le plus bas possible pour effectuer ladite tâche. Cette moyenne a déterminé le gain global, en pourcentage.

	Dell EMC et VMware		AWS		AWS (avec EC2)		Pourcentage de gains/pertes
	Durée (min:sec)	Étapes	Durée (min:sec)	Étapes	Durée (min:sec)	Étapes	
Création d'un nouvel utilisateur	1:01	20	0:59	22	S/o	S/o	9,09 %
Déploiement d'une VM personnalisée	0:14	7	0:34	14	0:34	14	50 %
Configuration de la surveillance des opérations	0:10	3	0:12	6	S/o	S/o	50 %
Configuration de la surveillance des fichiers log	0:07	3	0:10	7	S/o	S/o	57,14 %
Configuration de rapports de refacturation personnalisés	0:23	6	0:18	9	S/o	S/o	33,33 %
Configuration de la gestion des capacités	0:08	3	0:08	4	S/o	S/o	25 %
Déploiement d'une pile LAMP	0:17	6	0:47	15	0:37	16	60 %
Création d'un snapshot	0:15	9	0:12	8	S/o	S/o	-12,5 %
						Gain moyen en pourcentage	34,01 %

Ce projet a été commandé par Dell EMC.