Sécurisation de la migration des machines virtuelles

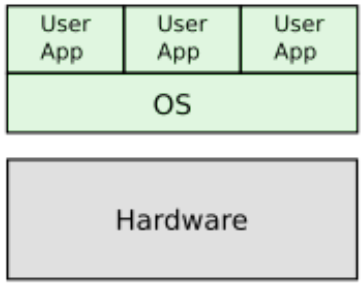
Salim NEDJAM

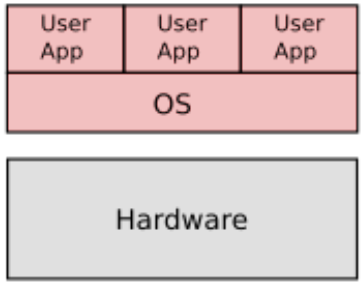
Réferent: Pierre SENS

Encadrant: Antoine BLIN

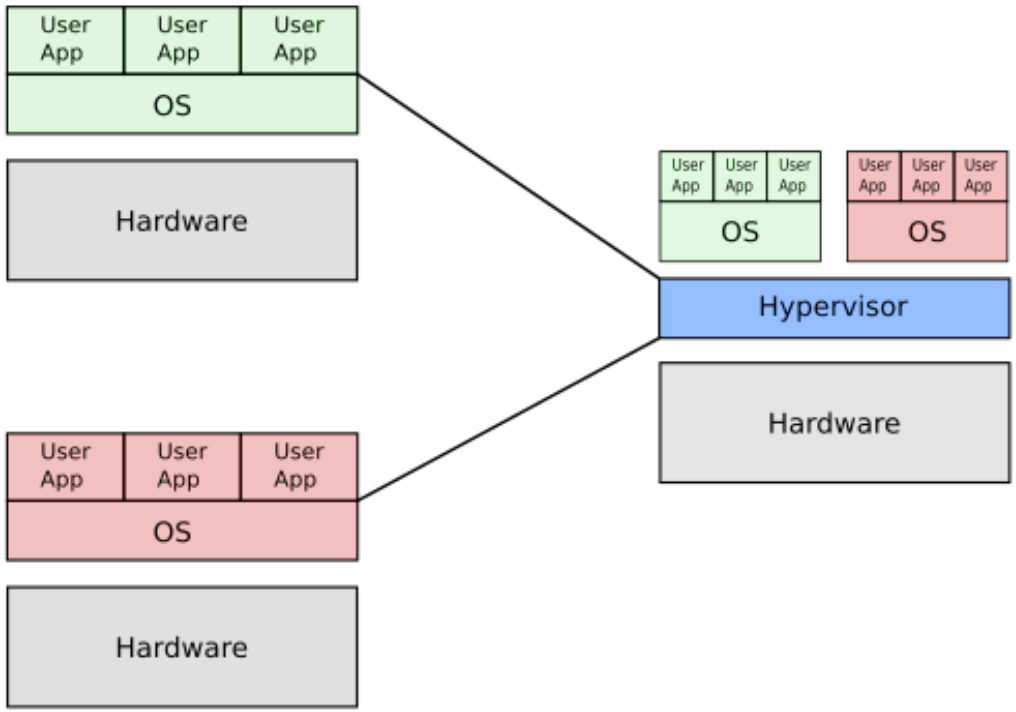
Septembre 14, 2021

Virtualisation





Virtualisation



Sécurisation des migrations de VM

Avantages:

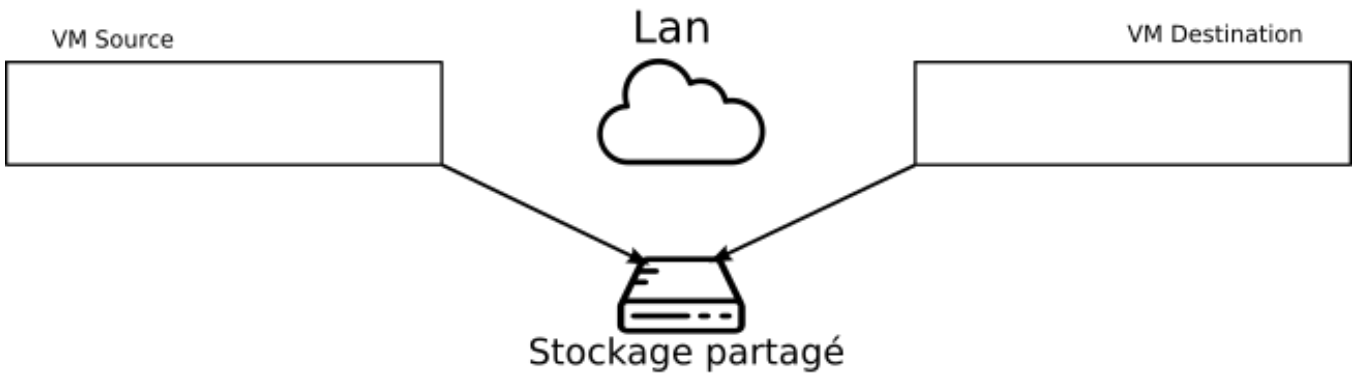
- La consolidation des serveurs.
- Équilibrage de la charge.
- Maintenance matérielle sans temps d'arrêt.

Sécurisation des migrations de VM

Problèmes:

- Sécuriser les VMs pendant la migration.
- Sécuriser l'intégrité des données des VMs.

Migration de VM: LAN

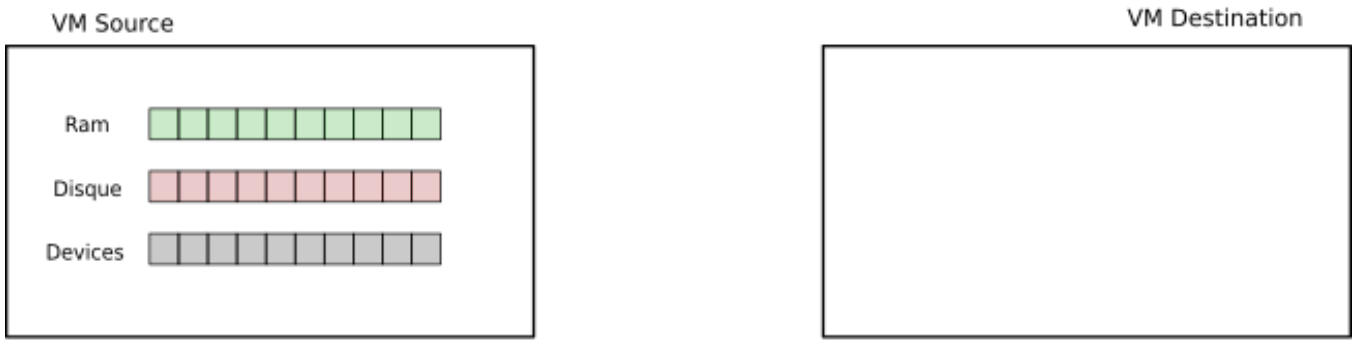


1. Les VMs sont sur le même réseau Lan.
2. Disque partagé (NFS/SAN).
3. Pas de transfert des données du disque.

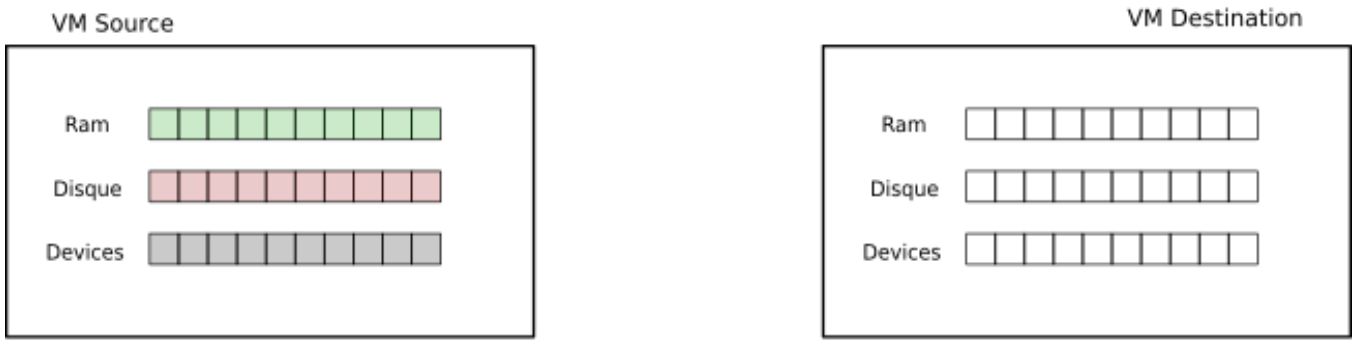
Migration de VM: WAN

1. Les VMs sont sur des machines distantes.
2. Pas de disque partagé (NFS/SAN).
3. Le transfert des données du disque est obligatoire.

Migration à froid

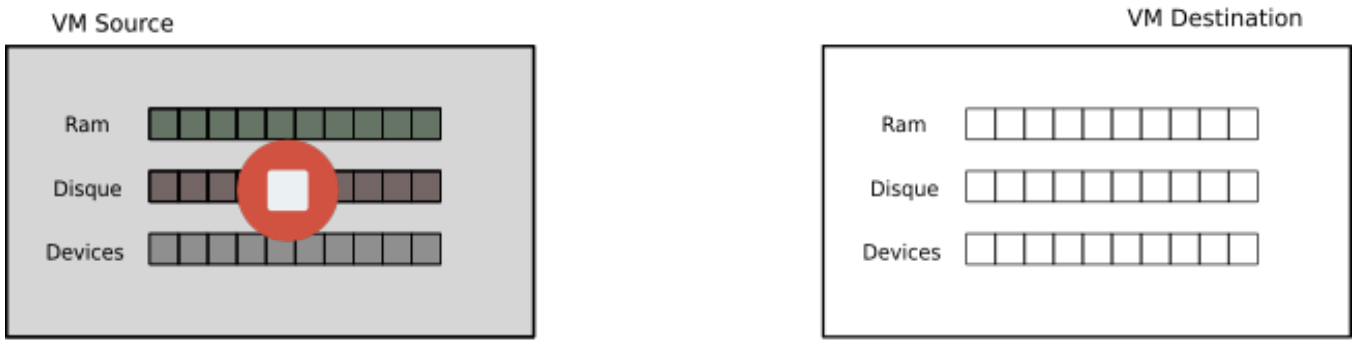


Migration à froid



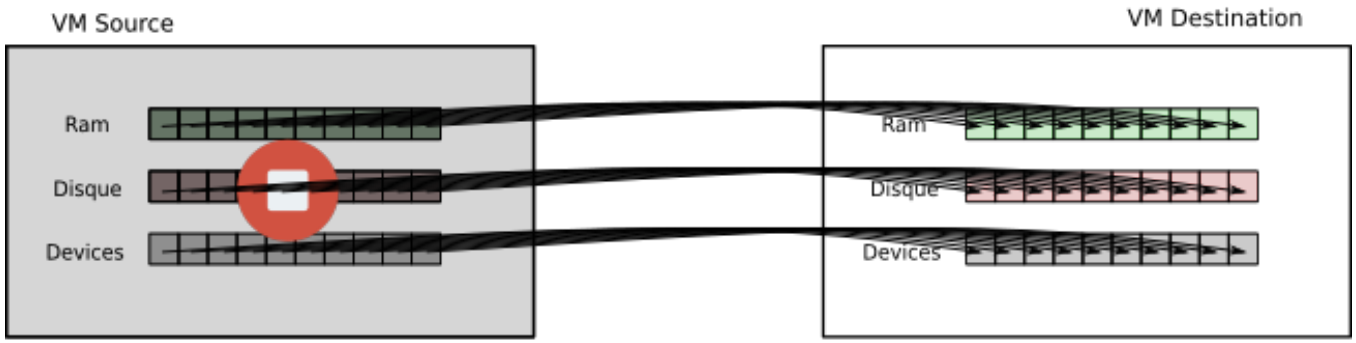
1. Allocation d'une VM de même caractéristiques.

Migration à froid



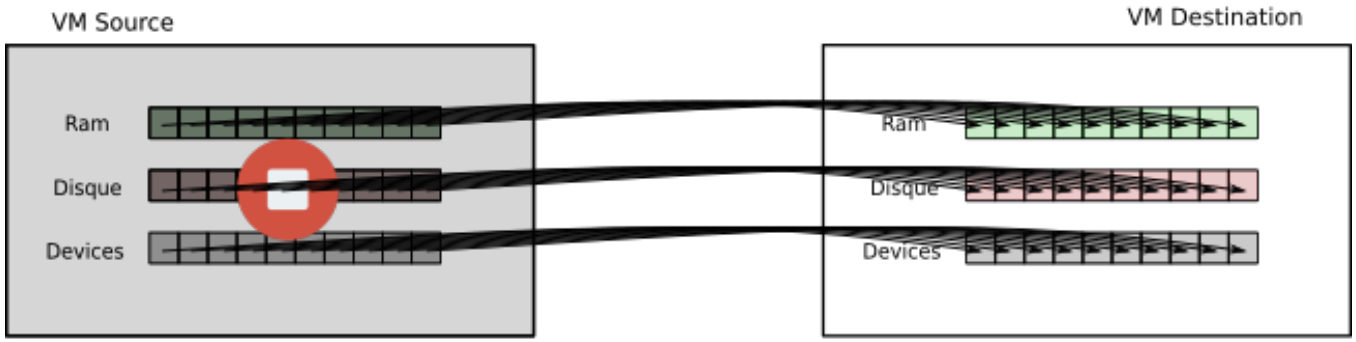
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.

Migration à froid



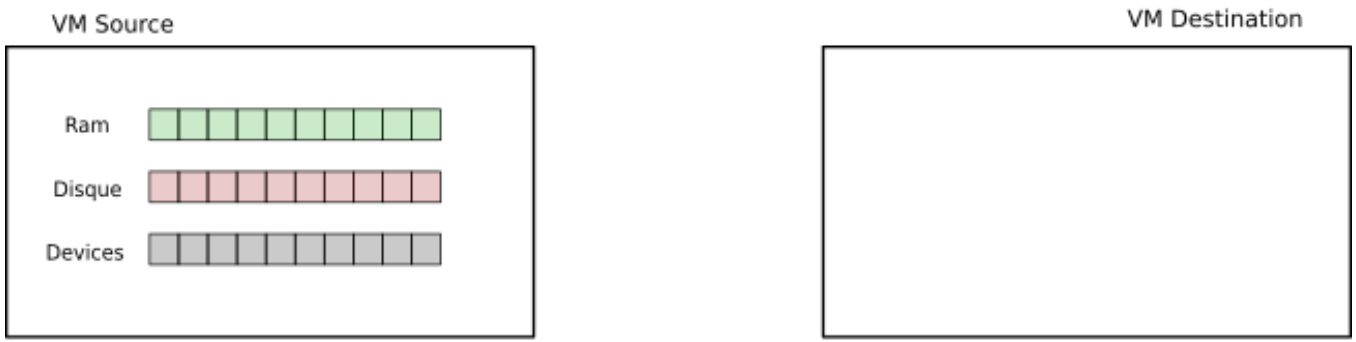
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert de tous les périphériques.

Migration à froid

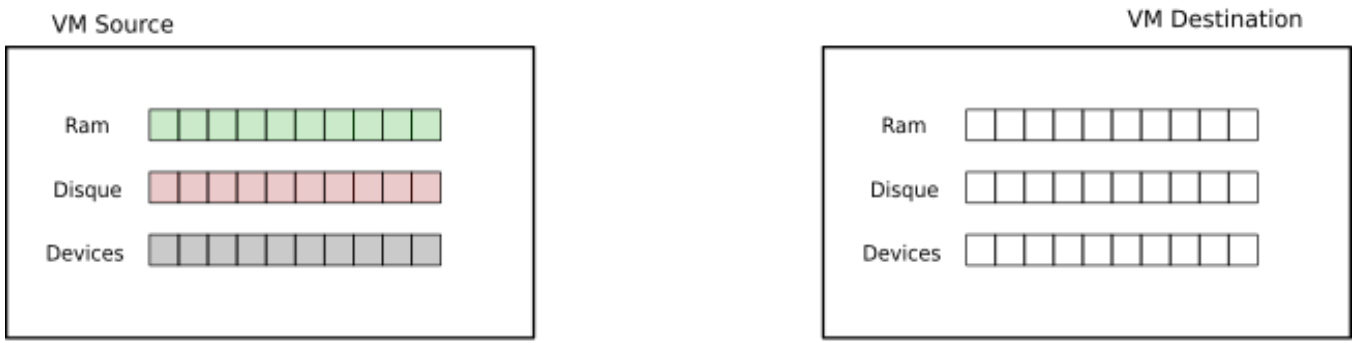


Temps d'arrêt = Temps total de migration.

Migration à chaud: pre-copie

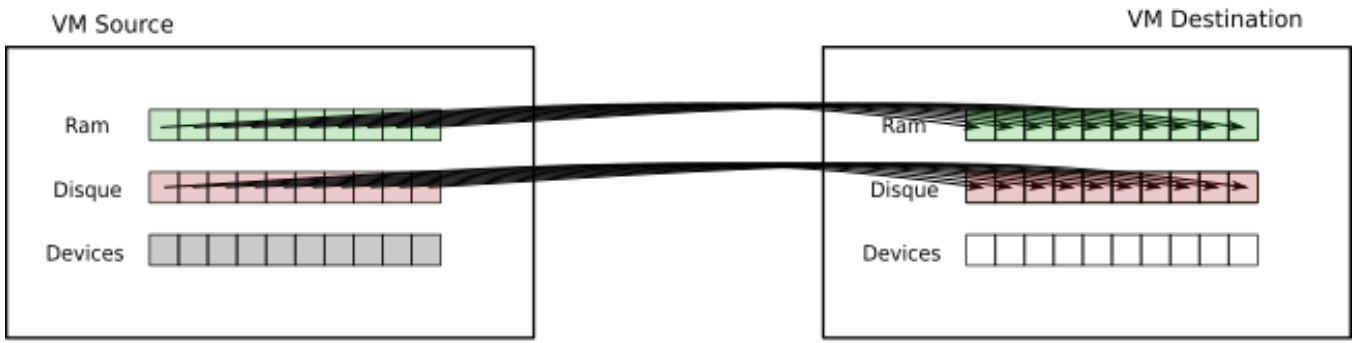


Migration à chaud: pre-copie



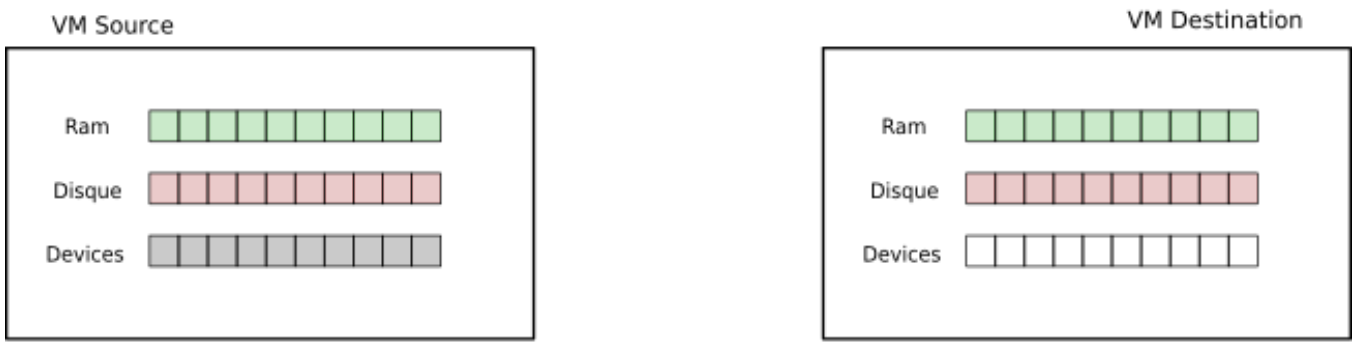
1. Allocation d'une VM de même caractéristiques.

Migration à chaud: pre-copie



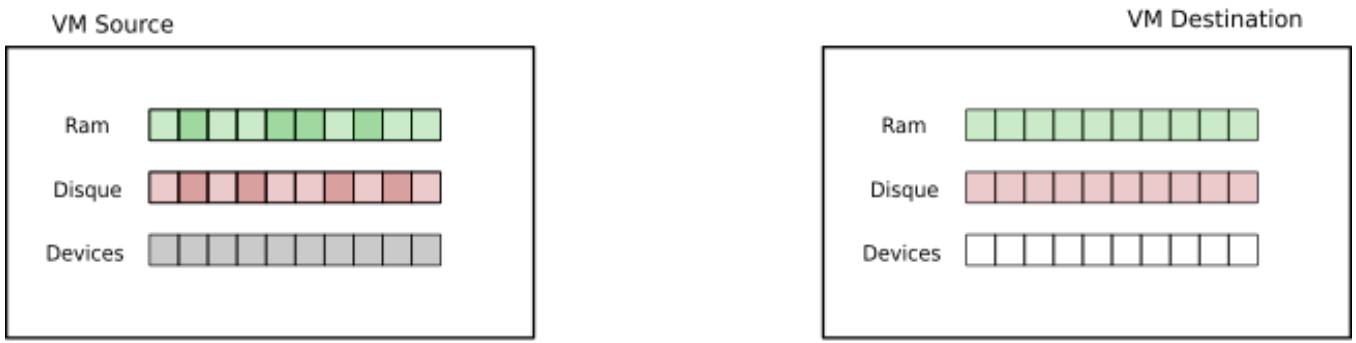
1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.

Migration à chaud: pre-copie



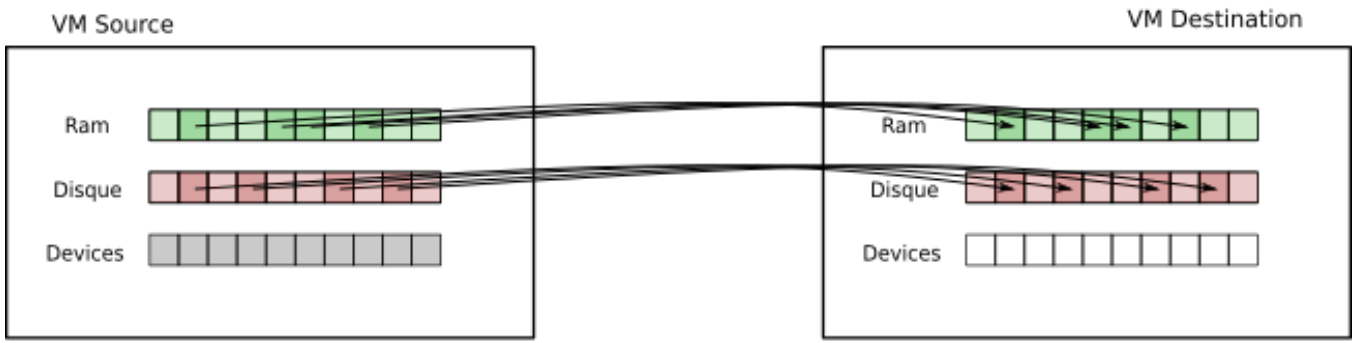
1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
    1. Première itération.

Migration à chaud: pre-copie



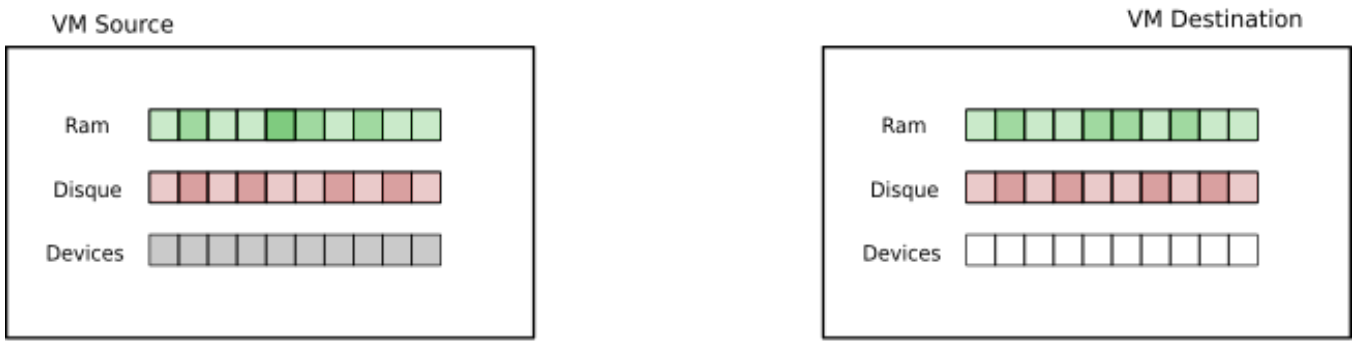
1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
   1. Première itération.
   2. Génération des pages dirty

Migration à chaud: pre-copie



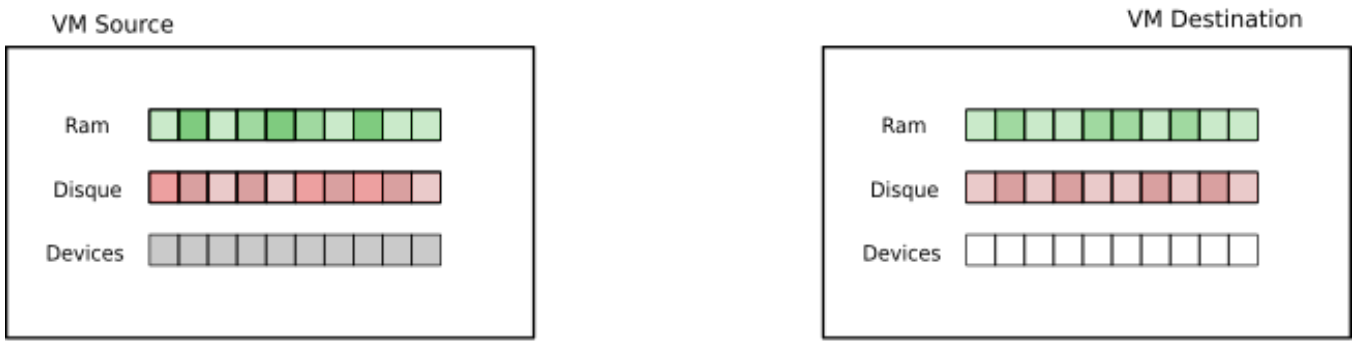
1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
   1. Première itération.
   2. Génération des pages dirty -> Copie des pages dirty

Migration à chaud: pre-copie



1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
   1. Première itération.
   2. Génération des pages dirty -> Copie des pages dirty
   3. Tester les critères de convergences.

Migration à chaud: pre-copie

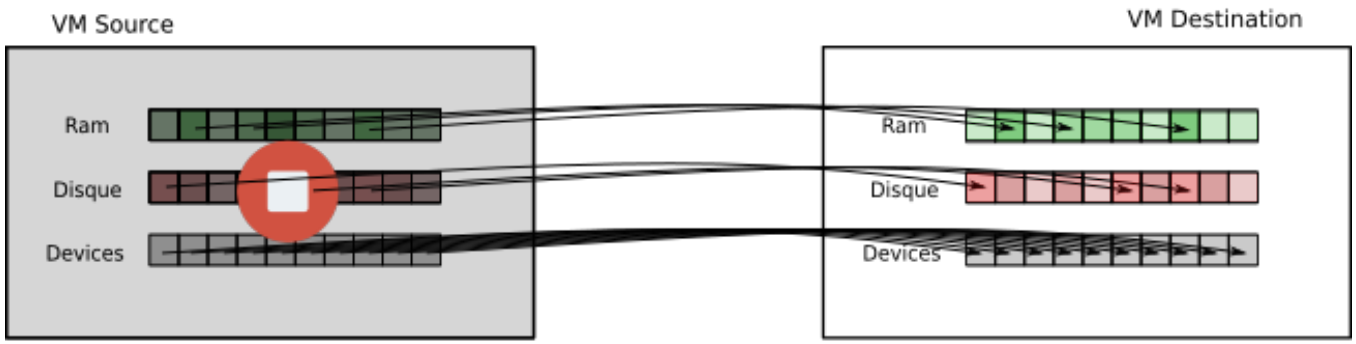


1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
   1. Première itération.
   2. Génération des pages dirty -> Copie des pages dirty
   3. Tester les critères de convergences.

Migration à chaud: pre-copie

1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
   1. Première itération.
   2. Génération des pages dirty -> Copie des pages dirty
   3. Tester les critères de convergences.
3. Stoper la machine.

Migration à chaud: pre-copie

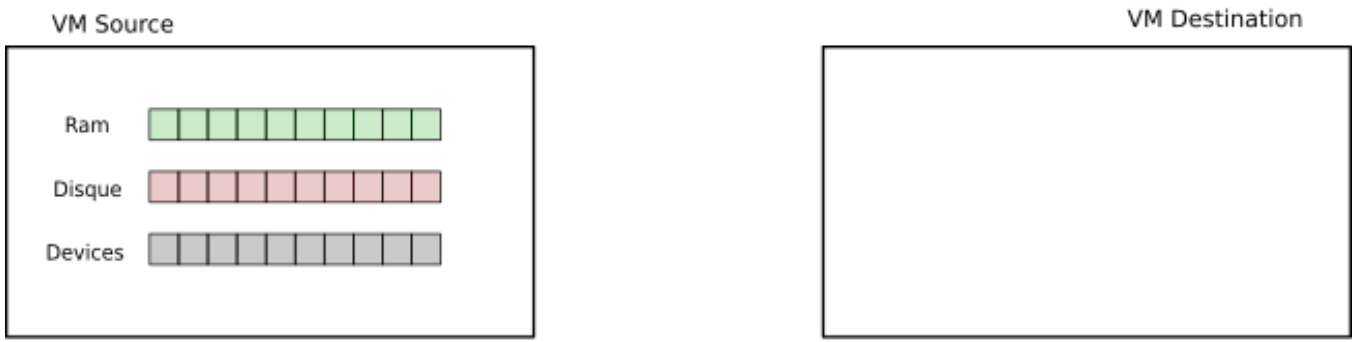


1. Allocation d'une VM de même caractéristiques.
2. Copie des périphériques itératifs.
   1. Première itération.
   2. Génération des pages dirty -> Copie des pages dirty
   3. Tester les critères de convergences.
3. Stoper la machine.
4. Copie de tous les périphériques.

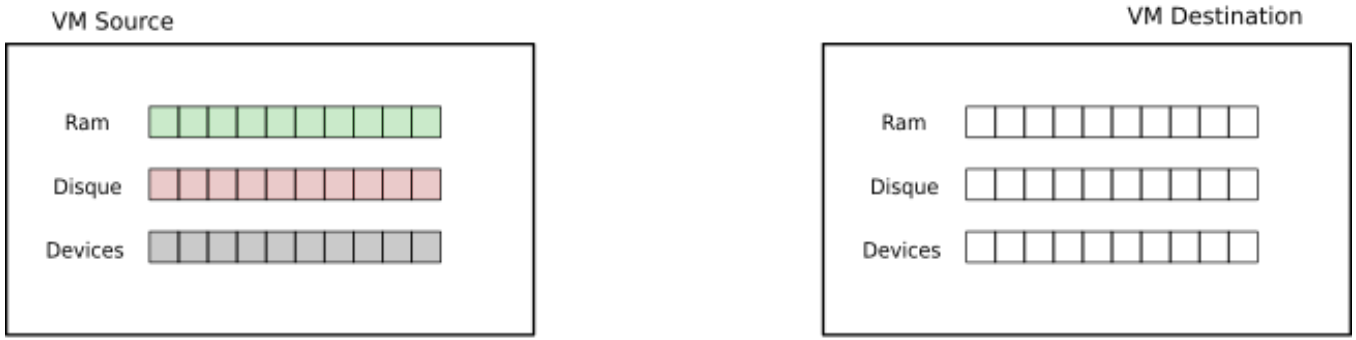
Migration à chaud: pre-copie

Temps d'arrêt = Temps de la dernière itération.

Migration à chaud: post-copie



Migration à chaud: post-copie

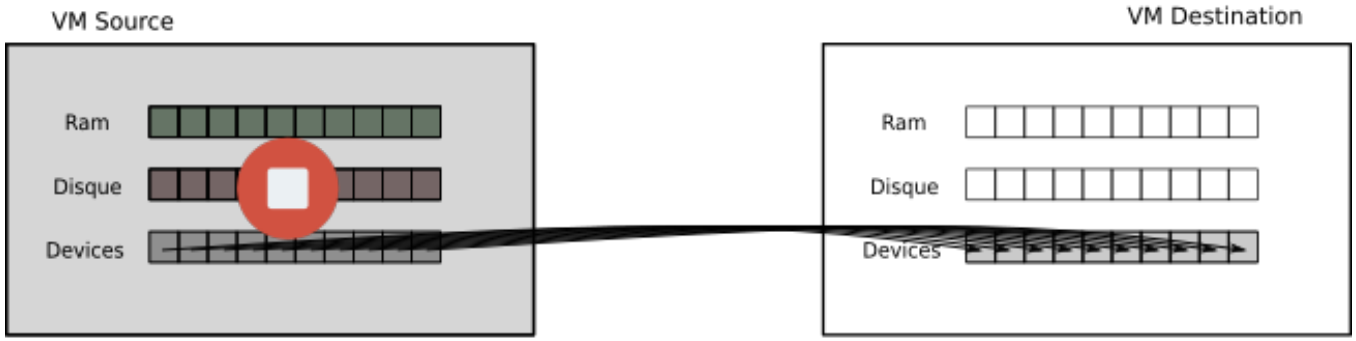


1. Allocation d'une VM de même caractéristiques.

Migration à chaud: post-copie

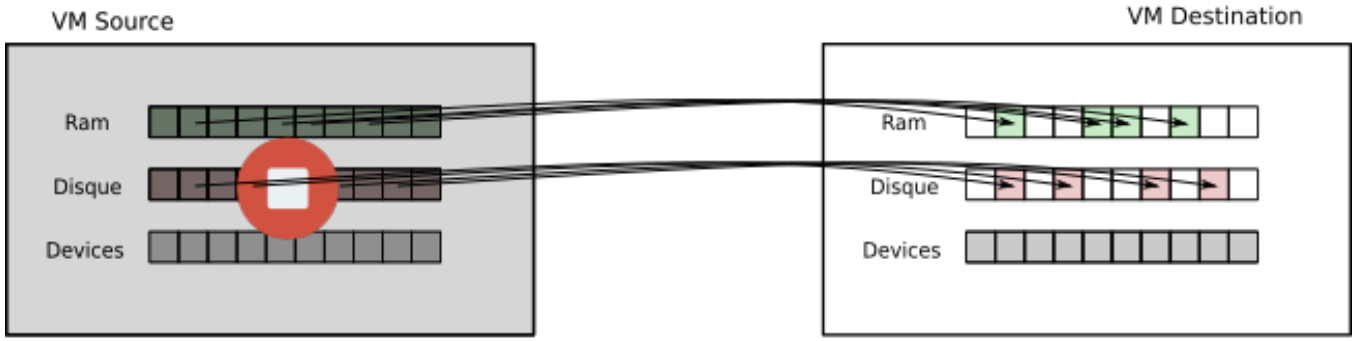
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.

Migration à chaud: post-copie



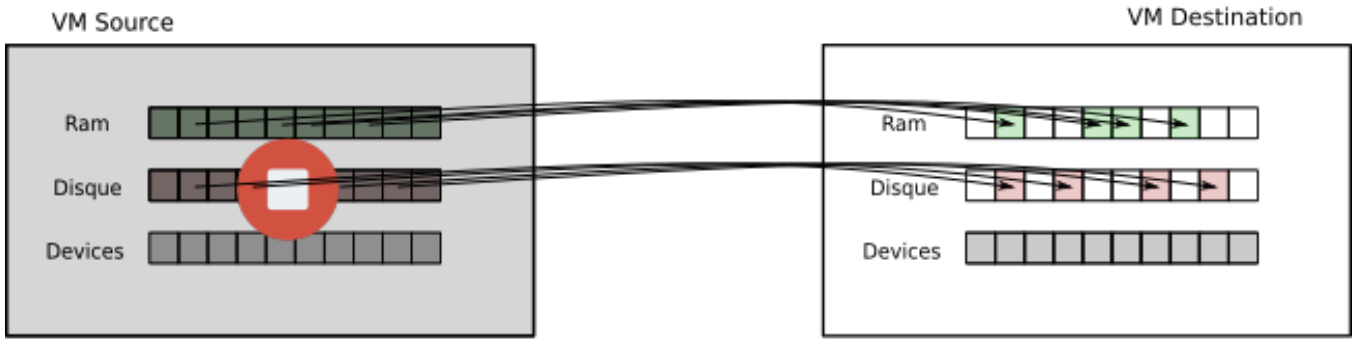
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert des structures de données essentielles.

Migration à chaud: post-copie



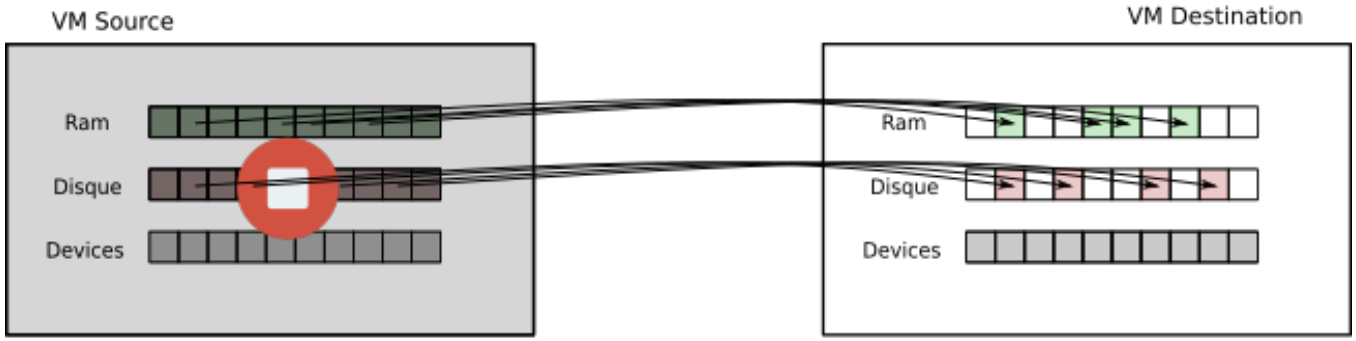
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert des structures de données essentielles.
4. Transfert des pages mémoire:

Migration à chaud: post-copie



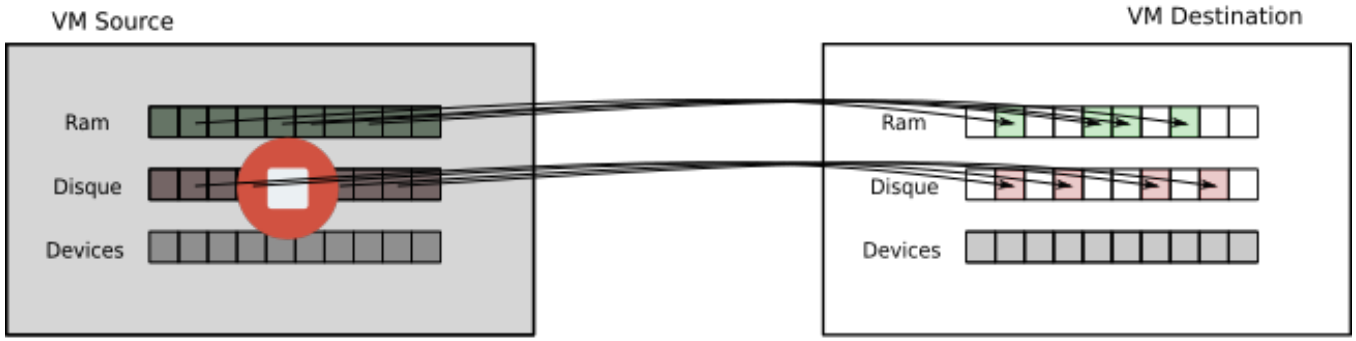
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert des structures de données essentielles.
4. Transfert des pages mémoire:
    1. Demand-paging

Migration à chaud: post-copie



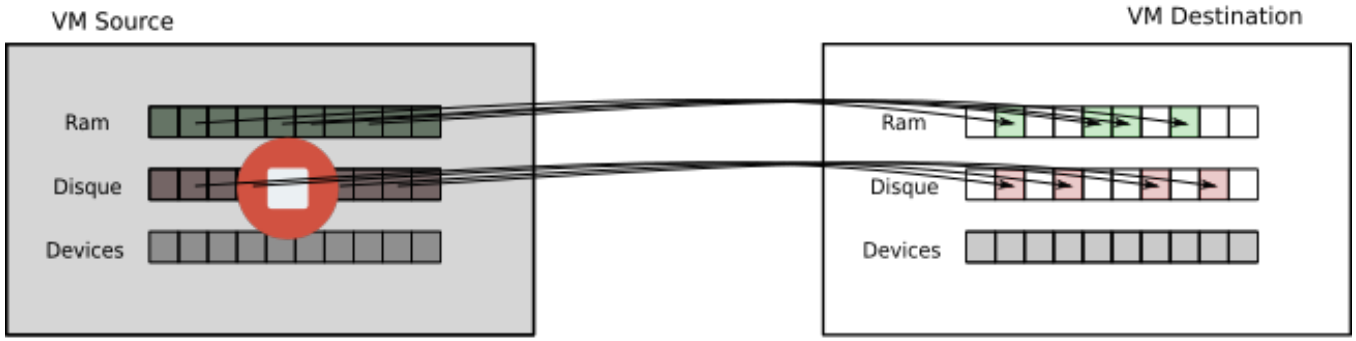
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert des structures de données essentielles.
4. Transfert des pages mémoire:
   1. Demand-paging
   2. Active-push

Migration à chaud: post-copie



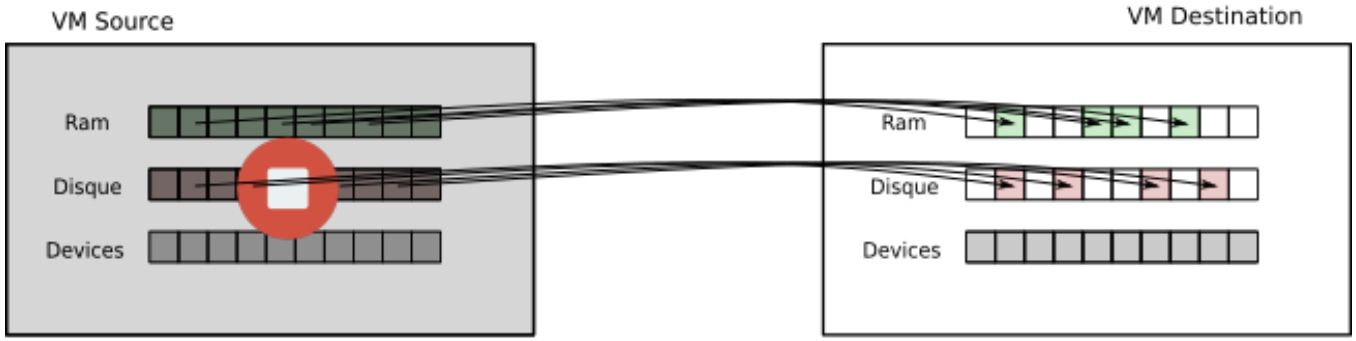
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert des structures de données essentielles.
4. Transfert des pages mémoire:
   1. Demand-paging
   2. Active-push
   3. Pre-paging

Migration à chaud: post-copie



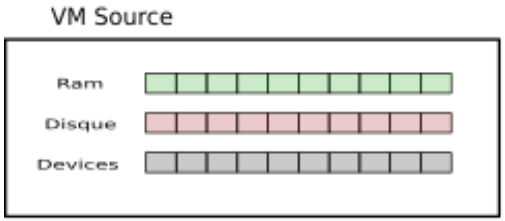
1. Allocation d'une VM de même caractéristiques.
2. Stoper la machine.
3. Transfert des structures de données essentielles.
4. Transfert des pages mémoire:
   1. Demand-paging
   2. Active-push
   3. Pre-paging
   4. Dynamic self balooning

Migration à chaud: post-copie



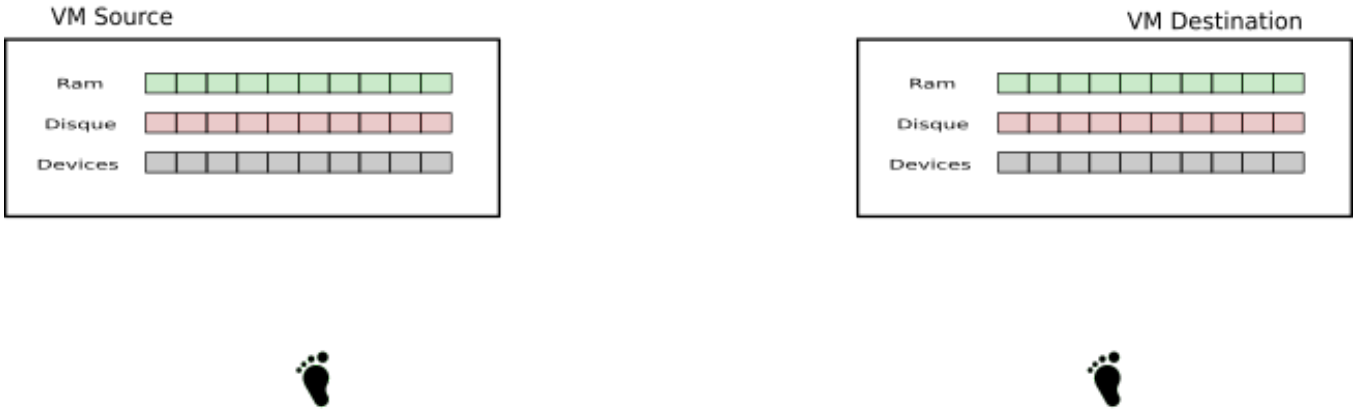
- Temps d'arrêt = Transfert des structures de données essentielles.
- Ralentissement de la VM destination.
- Risque de perte des données.

Calcul d'empreinte



Problématique S'assurer de l'intégrité des données.

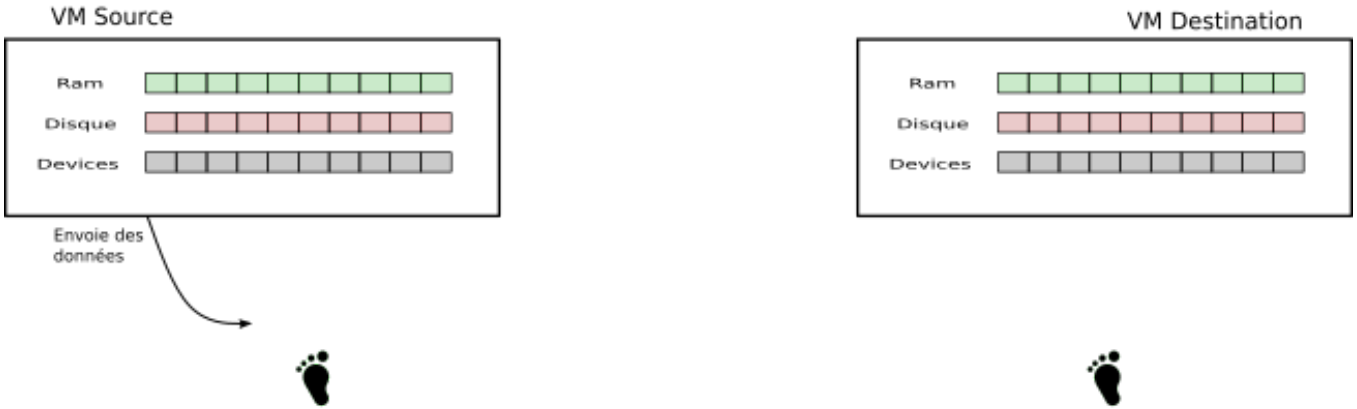
Calcul d'empreinte



Problématique S'assurer de l'intégrité des données.

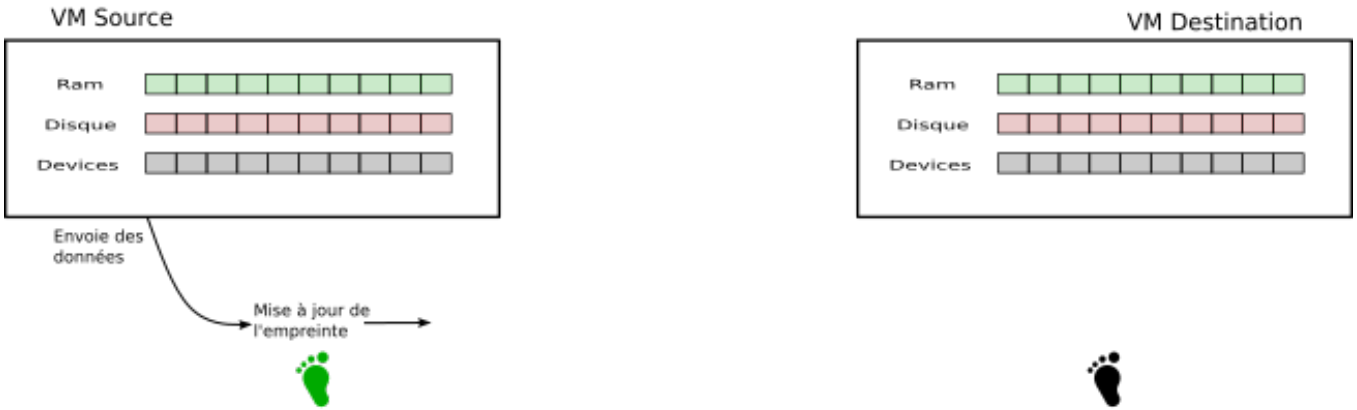
Solution Génération de l'empreinte de chaque VM.

Calcul d'empreinte



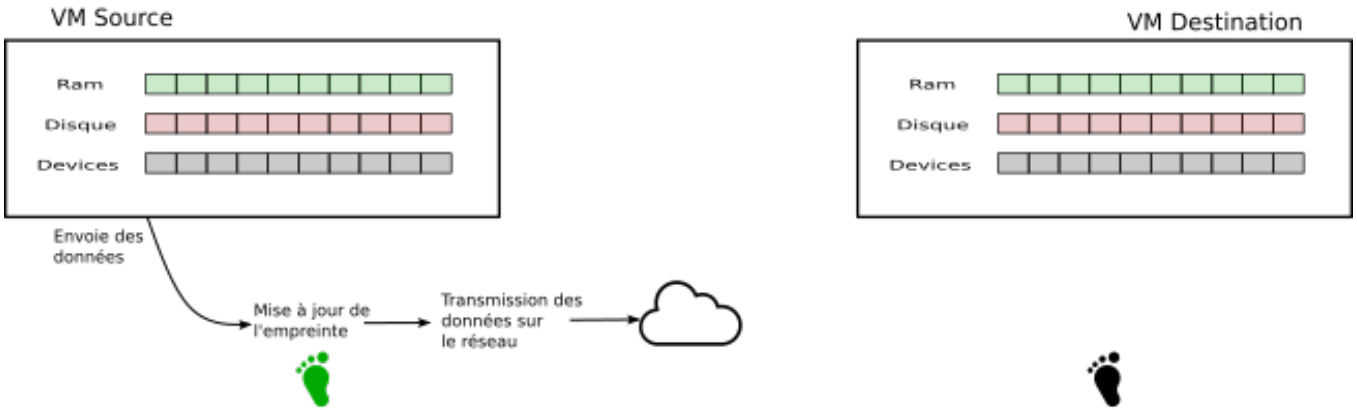
1. Envoie des données de la VM.

Calcul d'empreinte



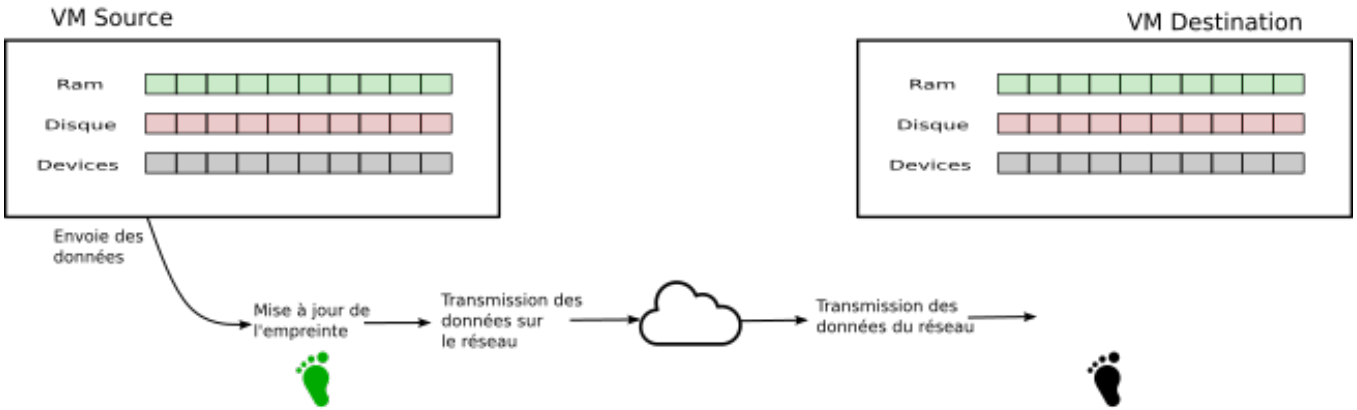
1. Envoie des données de la VM.
2. Calcul de la nouvelle empreinte de la VM source.

Calcul d'empreinte



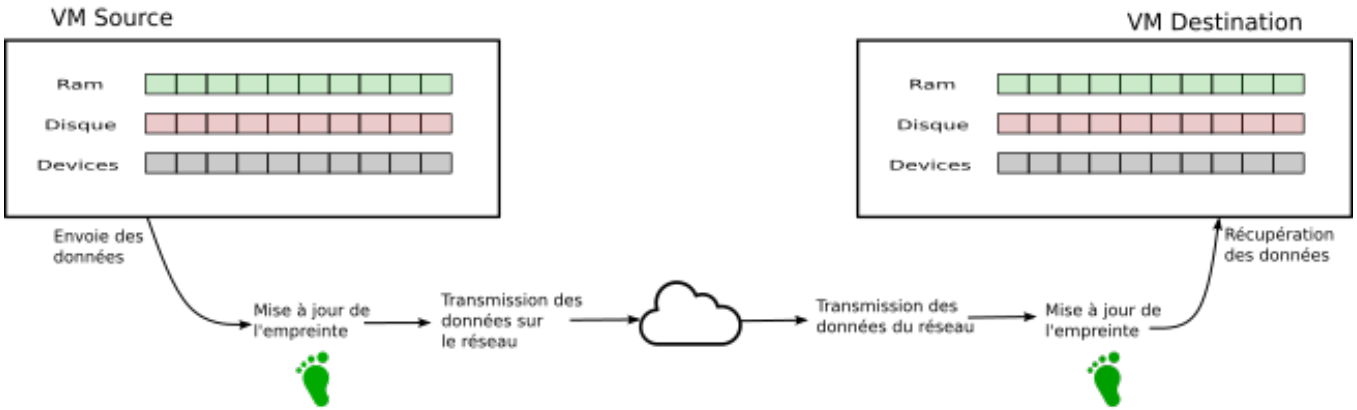
1. Envoie des données de la VM.
2. Calcul de la nouvelle empreinte de la VM source.
3. Transmission des données de la VM sur le réseau.

Calcul d'empreinte



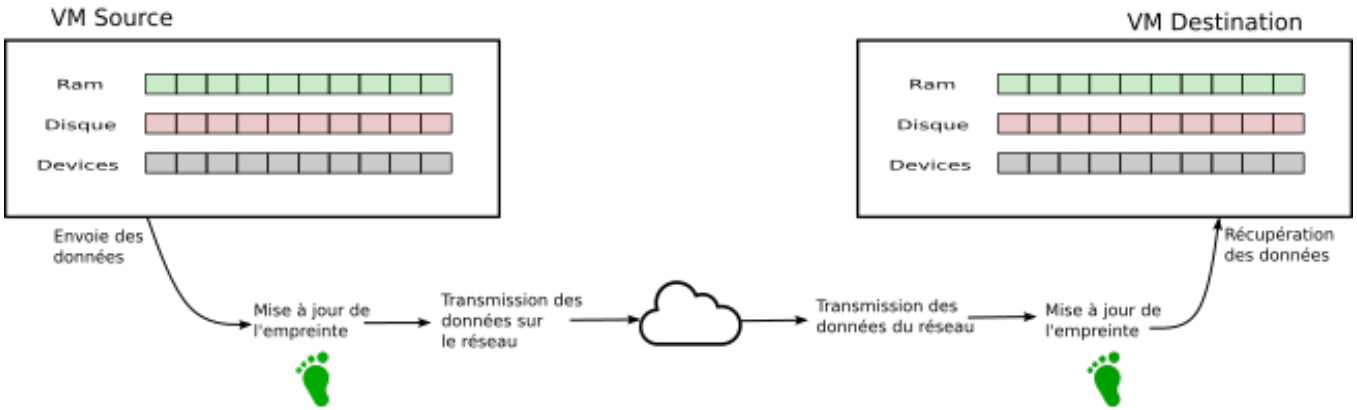
1. Envoie des données de la VM.
2. Calcul de la nouvelle empreinte de la VM source.
3. Transmission des données de la VM sur le réseau.
4. Réception des données de la VM du le réseau.

Calcul d'empreinte



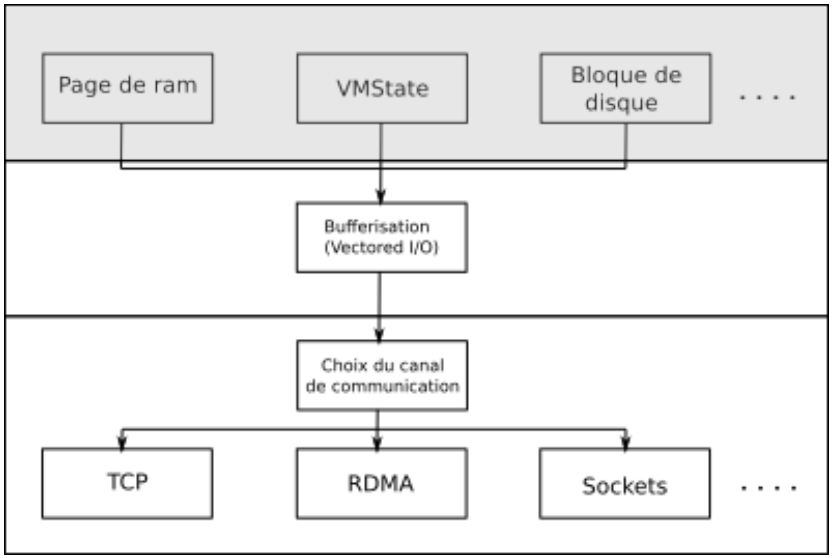
1. Envoie des données de la VM.
2. Calcul de la nouvelle empreinte de la VM source.
3. Transmission des données de la VM sur le réseau.
4. Réception des données de la VM du le réseau.
5. Calcul de la nouvelle empreinte de la VM destination.

Calcul d'empreinte



1. Envoie des données de la VM.
2. Calcul de la nouvelle empreinte de la VM source.
3. Transmission des données de la VM sur le réseau.
4. Réception des données de la VM du le réseau.
5. Calcul de la nouvelle empreinte de la VM destination.
6. Mise à jour des données de la VM.

Scénario 1



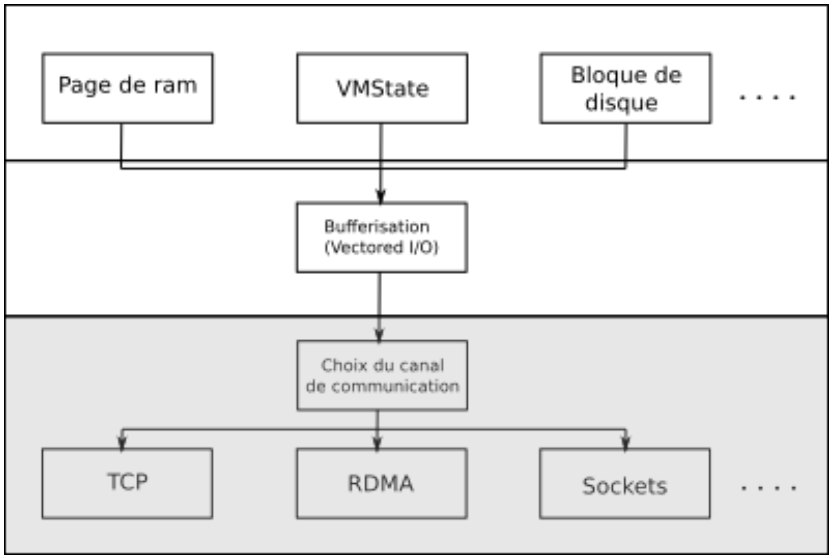
Avantages:

1. Connaissance du type de données envoyées.
2. Envoyer que les données importantes pour l'empreinte.

Inconvénients:

1. Non générique.
2. Rajout du code dans tout les périphériques

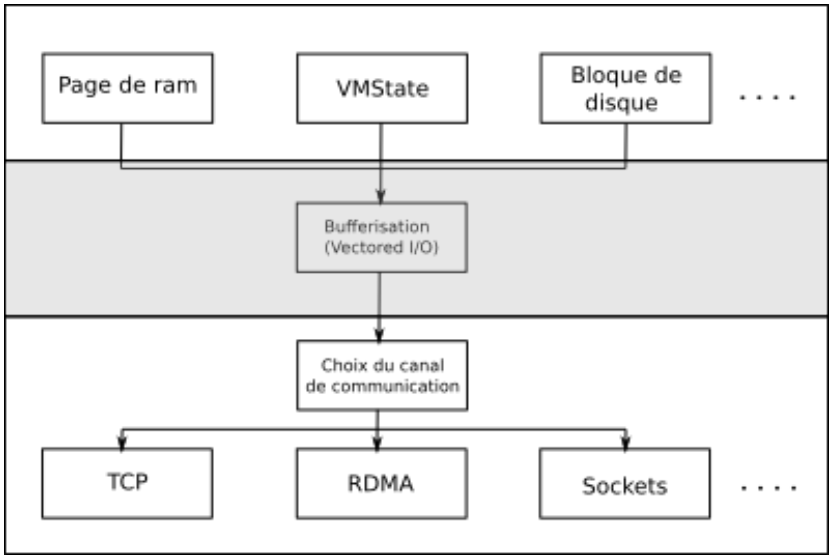
Scénario 2



Inconvénient:

1. Modifier le code de tout les protocoles réseau.
2. Pas de connaissance du type de données envoyées.

Scénario 3



Avantages:

1. Générique.
2. Facile, peu de code à rajouter.

Inconvénients:

1. Connaissance limitée du type de données envoyées.
2. Headers de section sont inclut dans le calcul de l'empreinte.

Métriques de performances

Temps de migration Temps entre le début de la migration et le moment où l'hôte source peut être désactivé.

Temps d'arrêt (Downtime) Phase indisponibilité du service perceptible par l'utilisateur.

Benchmark: Taille de la mémoire

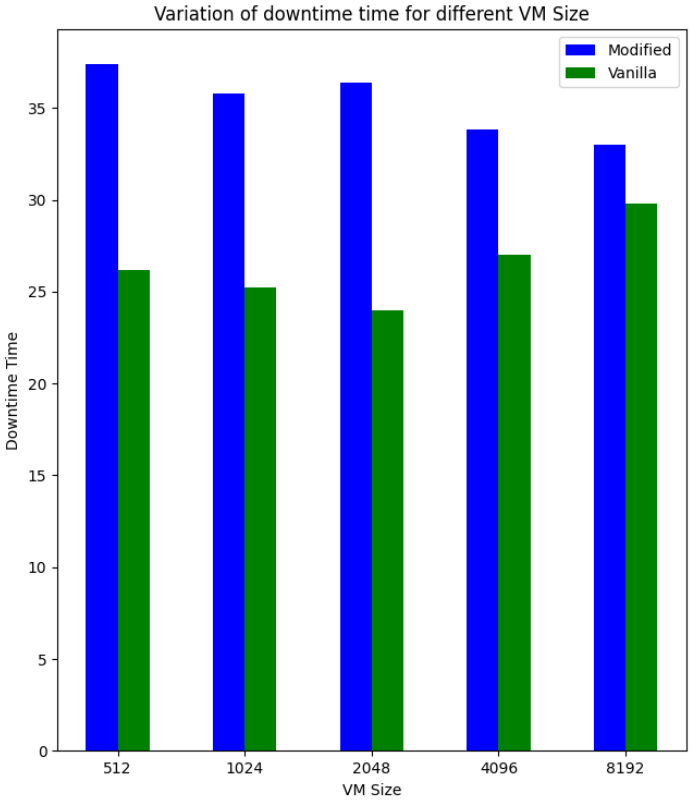
Varier la taille mémoire de la VM.

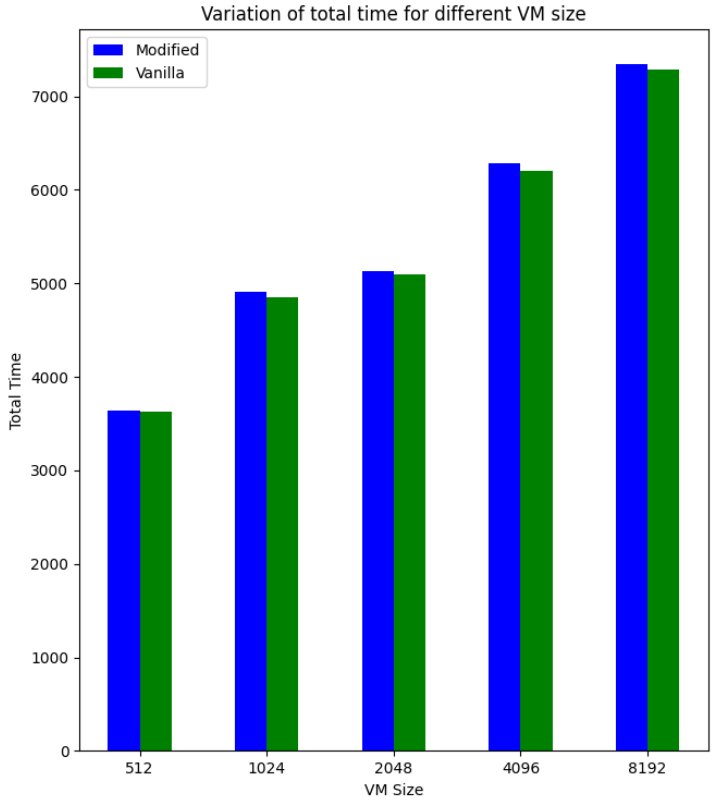
Benchmark: Taille de la mémoire

Varier la taille mémoire de la VM.

Configurations possible: 512 Mo, 1 Go, 2 Go, 4 Go et 8 Go.

Benchmark: Taille de la mémoire





Benchmark: Vitesse d'écriture

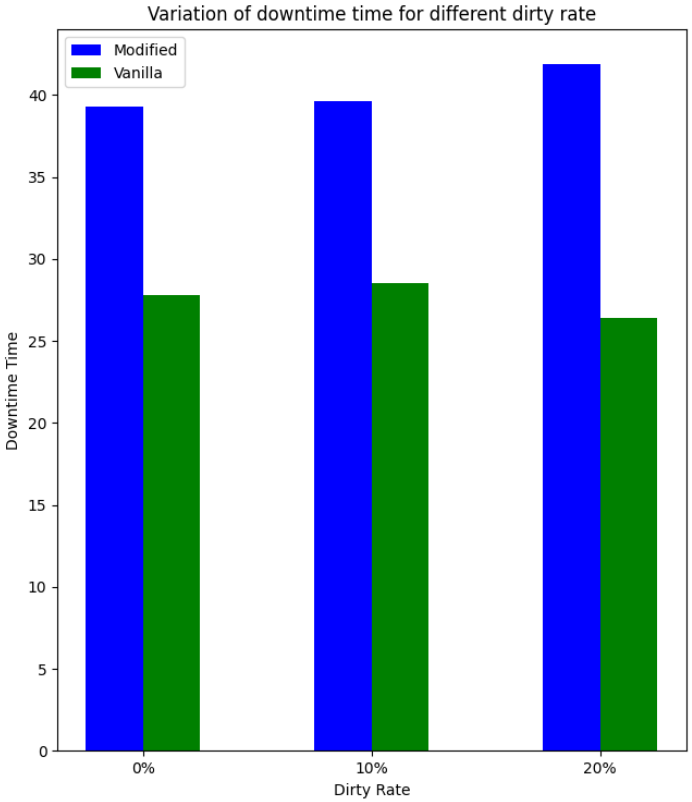
Création d'un processus dont le but est de salir la mémoire.

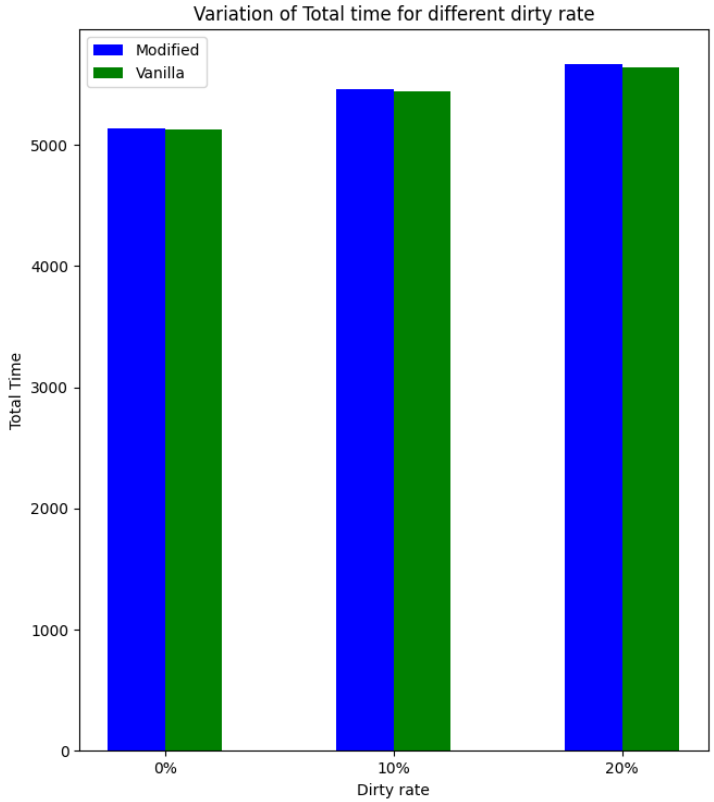
Benchmark: Vitesse d'écriture

Création d'un processus dont le but est de salir la mémoire.

Le but est de forcer plusieurs itération de la migration.

Benchmark: Vitesse d'écriture





Benchmark: Résultats

Overhead de 10ms pour le downtime.

Overhead en temps total est de l'ordre de moins de 1%.

Conclusion et Proposition d'optimisation

Conclusion

1. Génération d'une empreinte de VM.
2. Migration en direct avec/sans disque partagé.
3. Analyse du code de migration QEMU.
4. Analyse du flux réseau.
5. Problématique du mappage direct des données.

Proposition d'optimisation

1. Calcul du hash dans un thread différent (multi-threading).
2. Hashage intelligent des pages dirty.
3. Hashage intelligent des pages vides.
4. Hashage des données plus fin.