

RH299

COURS ACCÉLÉRÉ RHCE

Copyright © 2011 Red Hat, Inc.

Cours accéléré RHCE
Manuel d'exercices
Red Hat Enterprise Linux 6
Édition fr-2-20101223

COURS ACCÉLÉRÉ RHCE

Red Hat Enterprise Linux 6 RH300
Cours accéléré RHCE
Édition 2

Auteur	Forrest Taylor
Auteur	David Duffey
Auteur	George Hacker
Auteur	Joshua Hoffman
Auteur	Robert Locke
Auteur	Bowe Strickland
Éditeur	Steven Bonneville
Éditeur	Mark Howson

Copyright © 2010 Red Hat, Inc.

The contents of this course and all its modules and related materials, including handouts to audience members, are Copyright © 2010 Red Hat, Inc.

No part of this publication may be stored in a retrieval system, transmitted or reproduced in any way, including, but not limited to, photocopy, photograph, magnetic, electronic or other record, without the prior written permission of Red Hat, Inc.

This instructional program, including all material provided herein, is supplied without any guarantees from Red Hat, Inc. Red Hat, Inc. assumes no liability for damages or legal action arising from the use or misuse of contents or details contained herein.

If you believe Red Hat training materials are being used, copied, or otherwise improperly distributed please e-mail training@redhat.com or phone toll-free (USA) +1 (866) 626-2994 or +1 (919) 754-3700.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, Hibernate, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a registered trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Contributeurs: Brian Butler, Victor Costea, Andrew Dingman, Chris Negus

Conventions de la documentation vii
Remarques et avertissements vii

Introduction ix
Bienvenue dans ce cours ! ix
À propos de Red Hat Enterprise Linux ix
Logiciels Red Hat Enterprise Linux supplémentaires x
Contacter l'assistance technique de Red Hat xii

À propos de ce cours xv
Cours accéléré RHCE xv
Structure du cours xv
Orientation sur le réseau de la classe xvi

Internationalisation xix
Prise en charge linguistique xix
Langue par défaut du système xix
Sélection de la langue par utilisateur xix
Méthodes de saisie xx
Référence des codes de langue xx

1. Gestion des logiciels 1
Enregistrer un système avec Red Hat Network (RHN) 2
Utilisation de référentiels tiers 6
Utilisation de **yum** 10
Traitement de logiciels tiers 13
Conception de packages RPM 17
Spécifications d'un package RPM 19
Création et signature d'un package RPM 25
Publier des packages RPM 31
Test de critère 33

2. Gestion du réseau 37
Compréhension des fichiers de configuration réseau 38
Boîte à outils de résolution des problèmes 44
Configuration de l'interface réseau - Alias IP 47
Configuration de l'interface réseau - Liaison 49
Réglage des paramètres du noyau 53
Test de critère 1 56
Test de critère 2 57

3. Gestion du stockage 61
Partitions simples et systèmes de fichiers 62
Activation de la confidentialité des données avec le chiffrement des partitions 67
Gestion de l'espace swap 71
Accès au stockage iSCSI 74
Test de critère 78

4. Gestion des volumes logiques 81
Reconnaissance des composants de LVM 82
Implémentation du stockage LVM avec les outils en ligne de commande 85
Étendre un volume logique et un système de fichiers Ext4 88
Extension et réduction d'un groupe de volumes 92
Création d'un instantané pour faciliter la sauvegarde des données 95

Test de critère 98

5. Gestion de comptes **101**
Gestion des mots de passe 102
Gestion de listes de contrôle d'accès au système de fichiers 105
Test de critère 109

6. Gestion des authentifications **113**
Authentification réseau à l'aide d'un serveur LDAP 114
Configuration Kerberos 118
Résolution des problèmes de démon SSSD (System Security Services Daemon) 120
Montage de répertoires personnels sur le réseau 123
Test de critère 125

7. Installation, Kickstart et virtualisation **129**
Création d'un fichier Kickstart en modifiant un modèle 130
Introduction à la virtualisation KVM 134
Installation d'invités virtuels 137
Gérer des machines virtuelles 139
Test de critère 141

8. Gestion du démarrage **145**
Résolution des problèmes liés à GRUB 146
Modifications permanentes de GRUB 148
Modification du niveau d'exécution par défaut 150
Mode utilisateur unique 152
La séquence de démarrage et le mode de secours 154
Résolution des problèmes de démarrage 161
Test de critère 164

9. Gestion de SELinux **167**
Concepts de sécurité SELinux de base 168
Modes SELinux 171
Afficher et modifier les modes SELinux 174
Afficher et modifier les contextes de fichiers SELinux 176
Gestion des booléens SELinux 179
Contrôler les violations SELinux 181
Test de critère 184

10. Gestion du pare-feu **187**
Filtrage des paquets 188
Traduction d'adresses réseau 193
Test de critère 196

11. Configuration du serveur NTP **199**
Configuration d'un serveur NTP 200
Test de critère 204

12. Service de journalisation système **207**
Rapports d'utilisation 208
Configurer un service de journalisation distant 211
Test de critère 215

13. Service Web **219**
Sécurisation d'un serveur Apache avec le chiffrement 220

Configurer l'hébergement virtuel basé sur le nom 223
Activer un exécutable CGI 227
Configurer l'authentification utilisateur 230
Résolution des problèmes Apache/SELinux 234
Test de critère 1 239
Test de critère 2 240

14. Configuration SMTP de base **243**
Principes de base de la remise du courrier électronique 244
Configuration intranet 248
Test de critère 253

15. Serveur DNS cache uniquement **257**
Vue d'ensemble de DNS 258
Serveurs DNS cache uniquement 261
Test de critère 264

16. Partage de fichiers avec NFS **267**
Concepts et configuration NFS 268
Utilisation de NFS 273
Test de critère 275

17. Partage de fichiers avec CIFS **279**
Accès aux partages CIFS 280
Répertoires personnels fournis comme partages CIFS 283
Configuration des partages CIFS d'impression et de groupe 288
Test de critère 290

18. Partage de fichier avec FTP **293**
Zone de dépôt FTP de téléchargement anonyme 294
Test de critère 296

19. Service CUPS **299**
Configurer des imprimantes 300
Gérer les tâches d'impression 302
Test de critère 304

20. Service SSH **307**
Utilisation de clés SSH 308
Test de critère 311

21. Service VNC (Virtual Network Computing) **315**
Configuration d'un serveur VNC 316
Sécuriser l'accès à un bureau GNOME distant 318
Test de critère 320

22. Examen exhaustif **323**
Test d'examen exhaustif 324

A. Solutions **327**
Gestion des logiciels 327
Gestion réseau 333
Gestion du stockage 337
Gestion de volumes logiques 341
Gestion de comptes 347
Gestion de l'authentification 350

Installation, Kickstart et virtualisation 355
Gestion du démarrage 364
Gestion de SELinux 370
Gestion du pare-feu 374
Configuration du serveur NTP 379
Service de journalisation système 382
Service Web 385
Configuration SMTP de base 396
Serveur DNS de mise en cache uniquement 403
Partage de fichiers avec NFS 405
Partage de fichiers avec CIFS 408
Partage de fichier avec FTP 413
Service CUPS 415
Service SSH 417
Service VNC (Virtual Network Computing) 419
Examen exhaustif 422

Conventions de la documentation

Remarques et avertissements



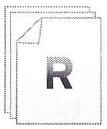
Remarque

Une « remarque» est un conseil, un raccourci ou une approche alternative pour la tâche considérée. L'ignorer ne devrait pas entraîner de conséquences négatives, mais vous pourriez passer à côté d'une astuce qui vous simplifierait la vie.



Comparaison

Les « comparaisons » étudient les similitudes et les différences entre la technologie ou le sujet traité et les technologies ou sujets similaires des autres environnements ou systèmes d'exploitation.



Références

Les « références » indiquent où trouver de la documentation externe se rapportant à un sujet.



Important

Les cadres « Important » détaillent des éléments qui pourraient aisément être négligés : des changements de configuration qui ne s'appliquent qu'à la session en cours ou des services qui doivent être redémarrés pour qu'une mise à jour soit appliquée. Ignorer les cadres « Important » ne vous fera perdre aucune donnée, mais cela pourrait être source de frustration et d'irritation.



Avertissement

Un « avertissement » ne doit pas être ignoré. Ignorer un avertissement risque d'entraîner une perte de données.

Introduction

Bienvenue dans ce cours !

Merci de votre participation à ce cours de formation Red Hat. N'hésitez pas à nous contacter pour toute question ou besoin particulier dans notre centre de formation.

Veuillez vous renseigner auprès de votre formateur si vous avez des questions sur l'établissement, notamment sur les heures d'ouverture et l'heure d'accès à la salle de classe, l'emplacement des toilettes et des salles de pause, la disponibilité des téléphones et de la connexion réseau ainsi que pour obtenir des informations sur les environs.

Par respect pour les autres participants, veuillez configurer votre biper ou votre téléphone portable en mode vibreur ou muet ou bien éteindre vos appareils pendant le cours. Nous vous demandons de limiter vos appels aux temps de pause.

Si vous vous trouvez face à une urgence personnelle et ne pouvez pas participer ou terminer le cours, veuillez nous en informer. Merci !

À propos de Red Hat Enterprise Linux

Ce cours est dispensé sur la base de Red Hat Enterprise Linux, une distribution Linux destinée aux entreprises, axée sur les logiciels open source aboutis conçus spécialement pour les organisations qui utilisent Linux dans un cadre de production.

Red Hat Enterprise Linux est vendu sous la forme d'un abonnement qui offre un accès continu à toutes les versions prises en charge du système d'exploitation aux formats binaire et source, et non pas uniquement à la dernière version, y compris toutes les mises à jour et les correctifs de bogues. Des services d'assistance étendue sont inclus : un contrat d'assistance et le droit d'accès au module de mise à jour pour le réseau Red Hat sont inclus pendant toute la durée de l'abonnement. Divers niveaux d'assistance (Service Level Agreements) sont disponibles pour bénéficier d'une couverture allant jusqu'à 24 heures sur 24, 7 jours sur 7 et une heure de temps de réponse garantie pour les problèmes de gravité 1. L'assistance sera disponible pour un maximum de sept ans après une version majeure précise (dix ans avec l'extension facultative « Assistance de mise à jour étendue »).

Red Hat Enterprise Linux est publié selon des cycles de plusieurs années entre les versions majeures. Les mises à jour mineures de versions majeures paraissent tous les six mois environ lors de la durée de vie du produit. La certification des systèmes certifiés sur une mise à jour mineure d'une version majeure se poursuit pour les futures mises à jour mineures ultérieures de la version majeure. De nombreuses autres bibliothèques partagées sont fournies, qui disposent d'API et d'ABI qui sont garanties au sein d'une version majeure (pour toutes les mises à jour mineures), mais dont la stabilité n'est pas garantie à travers les versions majeures. De nombreuses autres bibliothèques partagées sont fournies, qui disposent d'API et d'ABI qui sont garanties au sein d'une version majeure (pour toutes les mises à jour mineures), mais dont la stabilité n'est pas garantie à travers les versions majeures.

Red Hat Enterprise Linux est basé sur le code développé par la communauté open source, qui est souvent initialement inclus dans un package fourni avec la distribution Fedora disponible

gratuitement et commanditée par Red Hat (`http://fedoraproject.org/`). Red Hat ajoute ensuite des améliorations de performances, des tests poussés et la certification des produits proposés par des distributeurs de logiciels et des constructeurs de matériels indépendants. Red Hat Enterprise Linux garantit un niveau élevé de normalisation grâce à la prise en charge de quatre architectures de processeur (compatible Intel x86 32 bits, AMD 64/Intel 64 (x86-64), IBM POWER et ordinateur central IBM sur System z). En outre, nous prenons en charge les 4000 (et plus) certifications ISV sur Red Hat Enterprise Linux, que le système d'exploitation RHEL utilisant ces applications soit exécuté sur une machine « sans système d'exploitation » , sur une machine virtuelle, dans un logiciel monofonctionnel ou dans un cloud utilisant des technologies telles qu'Amazon EC2.

Actuellement, la famille de produits Red Hat Enterprise Linux comprend les éléments suivants :

- *Red Hat Enterprise Linux for Servers* : plate-forme de datacenter pour les serveurs stratégiques exécutant Red Hat Enterprise Linux. Ce produit inclut la prise en charge des plus gros serveurs x86-64 et compatibles x86 ainsi que les niveaux les plus élevés d'assistance technique, pouvant être déployés sur des machines sans système d'exploitation, en tant que client des principaux hyperviseurs ou dans le cloud. Les abonnements sont disponibles avec des droits d'invité flexibles pour un, quatre ou un nombre illimité d'invités par hôte physique. Les tarifs sont basés sur le nombre de paires de sockets remplies sur la carte mère du système, le nombre d'invités pris en charge, le niveau d'assistance souhaité et la longueur d'abonnement souhaitée.

  Red Hat Enterprise Linux for IBM POWER et *Red Hat Enterprise Linux for IBM System z* sont des variantes similaires destinées à ces architectures système.

- *Red Hat Enterprise Linux Desktop* : conçu pour les administrateurs et les utilisateurs finaux, Red Hat Enterprise Linux Desktop offre un environnement attirant et hautement productif pour les utilisateurs avancés des ordinateurs de bureau et portables. Les installations clientes peuvent être personnalisées jusqu'au moindre détail et verrouillées pour plus de simplicité et de sécurité pour toutes les tâches de station de travail.

  La variante *Desktop* de base est conçue pour les utilisateurs de tâches qui disposent d'un niveau limité de contrôle d'administration sur le système et qui utilisent principalement des applications de productivité telles que Firefox Evolution/Thunderbird, OpenOffice.org et Planner/TaskJuggler. La variante *Workstation* plus sophistiquée est conçue pour les utilisateurs Linux avancés qui ont besoin d'un environnement de développement autonome et qui disposent généralement de droits de superutilisateur locaux ou sélectionnés.

En outre, il existe d'autres variantes telles que *Red Hat Enterprise Linux for HPC Head Node* et *Red Hat Enterprise Linux for HPC Compute Node* (destinées aux clusters informatiques hautes performances) ainsi que *Red Hat Enterprise Linux for SAP Business Applications*. Pour plus d'informations, visitez `http://www.redhat.com/`.

Logiciels Red Hat Enterprise Linux supplémentaires

Deux canaux supplémentaires de mise à jour des logiciels sont fournis avec Red Hat Enterprise Linux en plus des packages logiciels principaux fournis :

- *Supplémentaire*: le canal « supplémentaire » offre des packages closed source sélectionnés, conçus pour Red Hat Enterprise Linux, à titre pratique pour le client. Il s'agit notamment d'éléments tels que Adobe Flash ou les machines virtuelles Java propriétaires.
- *Facultatif*: le canal « facultatif » offre des packages open source sélectionnés, également à titre pratique. Ils sont généralement inclus dans une autre variante de Red Hat Enterprise Linux en tant que package avec assistance complète ou constituent une exigence de version pour la distribution. Ces packages sont uniquement disponibles par le biais d'un canal enfant du réseau Red Hat.



Important

Les packages *supplémentaires* et *facultatifs* sont fournis avec une assistance limitée, uniquement à titre pratique pour le client.

Red Hat propose également un portefeuille d'*extensions pour Red Hat Enterprise Linux* avec assistance complète qui étendent les fonctionnalités de votre abonnement Red Hat Enterprise Linux. Ces extensions vous permettent d'ajouter des capacités et de personnaliser votre environnement informatique en fonction de vos besoins précis. Ces extensions incluent la prise en charge de la mise en cluster d'applications de disponibilité, de systèmes de fichiers de cluster et de systèmes de fichiers très volumineux, une gestion améliorée du système avec le réseau Red Hat, une assistance de mise à jour étendue et beaucoup d'autres choses encore.



Remarque

Veuillez visiter `http://www.redhat.com/rhel/add-ons/` pour plus d'informations sur les *extensions disponibles pour Red Hat Enterprise Linux*.

Pour plus d'informations sur d'autres produits fournis par Red Hat, notamment Red Hat Enterprise Virtualization, JBoss Enterprise Middleware, Red Hat Enterprise MRG et divers services de conseil et d'ingénierie personnalisés, le site `http://www.redhat.com/products/` dispose également d'informations utiles.

Le projet Fedora fournit également des packages supplémentaires pour Red Hat Enterprise Linux par le biais d'*EPEL (Extra Packages for Enterprise Linux)*. Il s'agit d'un dépôt géré par des volontaires au sein de la communauté Linux. Il inclut des packages additionnels de qualité pouvant être utilisés avec Red Hat Enterprise Linux et autres dérivés compatibles. Il accepte des logiciels Open Source libres et sans problèmes légaux, qui ne génèrent aucun conflit avec les packages Red Hat Enterprise Linux ou les produits additionnels de Red Hat. Les packages EPEL ont été conçus pour une version majeure spécifique de Red Hat Enterprise Linux et seront mis à jour par EPEL pour la durée de vie standard de la prise en charge de cette version majeure.

Red Hat ne fournit aucun support commercial de ces packages, ni les contrats de service correspondants. Bien que non pris en charge officiellement par Red Hat, EPEL fournit un moyen utile de réduction des coûts de prise en charge pour les packages non pris en charge que votre entreprise souhaite utiliser avec Red Hat Enterprise Linux. EPEL vous permet de répartir le

travail de prise en charge que vous devriez effectuer seul sur d'autres organisations qui utilisent aussi ce logiciel Open Source dans RHEL. Les packages sont eux-mêmes soumis aux mêmes processus que les packages Fedora, ce qui signifie que des développeurs Linux expérimentés ont examiné les packages à la recherche de problèmes. Comme EPEL ne remplace pas les packages logiciels livrés dans RHEL et ne génère aucun conflit avec ceux-ci, vous pouvez utiliser EPEL en sachant qu'il n'engendrera aucun problème avec vos packages logiciels normaux.

Pour les développeurs qui souhaitent que leur logiciel Open Source fasse partie de Red Hat Enterprise Linux, souvent, la première étape consiste souvent à le promouvoir dans EPEL, afin que les utilisateurs RHEL aient l'occasion de l'utiliser et de se familiariser avec la gestion de package pour une distribution Red Hat.

Pour en savoir plus sur les packages EPEL, voir `http://fedoraproject.org/wiki/EPEL/`.



Important

L'assistance relative à *EPEL* est assurée par le projet Fedora géré par la communauté et non pas par l'assistance de Red Hat.

Contacter l'assistance technique de Red Hat

Parmi les avantages de votre abonnement à Red Hat Enterprise Linux, vous pouvez accéder à l'assistance technique par le biais du portail client de Red Hat à l'adresse suivante: `http://access.redhat.com/`. Si vous ne possédez pas de compte Red Hat pour le portail client ou si vous ne parvenez pas à vous connecter, vous pouvez vous rendre sur le site `https://access.redhat.com/support/faq/LoginAssistance.html` ou contacter le service clientèle pour obtenir de l'aide.

Il se peut que vous parveniez à résoudre votre problème sans assistance technique formelle, simplement en consultant la base des connaissances (`https://access.redhat.com/kb/knowledgebase/`). Dans le cas contraire, l'assistance de Red Hat est joignable via un formulaire Web ou par téléphone, selon votre niveau d'assistance. Les numéros de téléphone et les horaires d'ouverture varient en fonction des régions; pour obtenir les dernières informations, rendez-vous sur `https://access.redhat.com/support/contact/technicalSupport.html`. Le site `https://access.redhat.com/support/policy/support_process.html` contient des informations sur le processus d'assistance.

Voici quelques conseils relatifs à la préparation de votre rapport de bogue afin que l'assistance de Red Hat puisse vous aider de la manière la plus efficace qui soit:

- *Définissez le problème.* Assurez-vous que vous pouvez décrire le problème et ses symptômes avant de contacter Red Hat. Soyez aussi précis que possible et détaillez les étapes que vous pouvez utiliser (le cas échéant) pour reproduire le problème.
- *Rassemblez des informations complémentaires.* Quelle version de notre logiciel exécutez-vous? Utilisez-vous la dernière mise à jour? Quelles étapes ont mené à l'échec? Le problème peut-il être recréé et quelles étapes sont nécessaires? De récentes modifications ont-elles été

apportées, ce qui peut avoir déclenché le problème ? Des messages ou autres messages de diagnostic se sont-ils affichés ? Quels étaient-ils *exactement* (la phraséologie exacte peut être essentielle) ?

- *Collectez des informations de diagnostic pertinentes.* Soyez prêt à fournir autant d'informations pertinentes que possible ; journaux, dumps principaux, traces, la sortie de **`sosreport`**, etc. Le support technique peut vous aider à déterminer ce qui est pertinent.
- *Déterminez le niveau de gravité de votre problème.* Red Hat utilise une échelle de quatre niveaux pour indiquer la gravité du problème ; les critères figurent sur `https://access.redhat.com/support/policy/GSS_severity.html`.



Avertissement

Bugzilla n'est pas un outil d'assistance ! Pour les problèmes d'assistance en rapport avec Red Hat Enterprise Linux, les clients doivent consigner leurs bogues en faisant appel aux canaux d'assistance présentés ci-devant afin d'avoir la garantie que Red Hat est parfaitement informé du problème et peut répondre dans le respect des conditions du contrat de niveau de service. Les clients ne doivent *pas* consigner de bogues directement dans l'interface Web `http://bugzilla.redhat.com/`.

Pour Red Hat Enterprise Linux, Bugzilla est utilisé par l'ingénierie pour assurer le suivi des problèmes et des modifications ainsi que pour communiquer au niveau technique avec les partenaires de l'ingénierie et les autres parties extérieures. Toute personne, y compris les utilisateurs qui ne sont pas clients, peut consigner un problème avec Bugzilla et Red Hat procédera au contrôle et à l'étude de ce problème en vue d'une intégration dans le cadre des errata.

Toutefois, Red Hat ne peut garantir aucun contrat de niveau de service pour les bogues consignés directement dans Bugzilla (qui est une procédure contraire à l'utilisation des canaux d'assistance habituels). Une étude peut avoir lieu immédiatement ou après une certaine période. Les problèmes transmis à l'assistance sont toujours placés en priorité par rapport aux problèmes ayant un impact et une gravité similaires, mais consignés dans Bugzilla. De plus, des solutions de contournement et des correctifs d'urgence, si disponibles et appropriés, peuvent être fournis aux clients par l'assistance, avant même qu'un correctif permanent ne soit diffusé sur le réseau Red Hat.

Red Hat considère les problèmes saisis directement dans Bugzilla comme des commentaires importants qui permettent d'offrir une interaction efficace avec la communauté de développement open source ainsi qu'une transparence maximale pour les clients en ce qui concerne le traitement des problèmes. Néanmoins, pour les clients rencontrant des problèmes de production avec Red Hat Enterprise Linux, Bugzilla ne constitue pas le canal adéquat.

À propos de ce cours

Cours accéléré RHCE

Le *Cours accéléré RHCE* (RH300) est une préparation rapide pour l'examen Red Hat Certified Engineer (RHCE) destiné aux administrateurs système Linux expérimentés maîtrisant déjà la plupart des points abordés dans ce cours. Ce cours accéléré réunit le *Cours accéléré RHCSA* (RH200) et le cours *Red Hat System Administration III* (RH255), qui normalement ont une durée de huit jours, en un cours de quatre jours seulement. Les étudiants doivent rapidement effectuer des tâches intermédiaires et avancées, en s'appuyant pour cela sur leur connaissance complète des meilleures pratiques en matière d'administration système basée sur les lignes de commande.

Objectifs

- Permettre aux administrateurs système Linux les plus expérimentés de revoir leurs connaissances en matière d'administration système et de combler leurs lacunes, mais aussi de se perfectionner notamment dans la configuration et la sécurisation des services réseau importants sur Red Hat Enterprise Linux
- Préparer des étudiants motivés et expérimentés en vue de l'examen RHCE validant leurs compétences

Public et conditions préalables

- Étudiants justifiant d'une expérience d'*au moins* trois ans en tant qu'administrateur système Linux à plein temps, de préférence sous Red Hat Enterprise Linux
- Les étudiants doivent être titulaires de la certification RHCT ou RHCSA *ou bien* posséder des compétences Linux équivalentes pour participer au cours

Structure du cours

Les cours de formation Red Hat sont interactifs, pratiques, basés sur les performances et concrets ; ils ont pour but de mobiliser votre esprit et vous offrent l'opportunité d'utiliser des systèmes réels afin de développer de véritables compétences. Nous encourageons les étudiants à participer et à poser des questions afin de tirer le meilleur parti de leurs sessions de formation.

Ce cours se divise en un certain nombre d'*unités* organisées autour d'un sujet donné. Chaque unité comprend plusieurs *sections* qui se concentrent sur une compétence ou une tâche spécifiques. Une unité commence par une introduction au sujet, avant de passer à la première section.

Chaque section comporte une *présentation* effectuée par l'instructeur. Pendant la présentation, il est conseillé de prendre des notes dans votre cahier d'exercices (ce cahier), comme l'instructeur ne manquera pas de vous le rappeler. La présentation est suivie par une brève activité ou *évaluation* afin de vous familiariser avec le matériel ou les procédures de révision. Après une révision de l'évaluation, l'instructeur passe à la section suivante. L'unité se termine normalement par un exercice pratique (un « *test de critère* ») qui vous donne la possibilité d'apprendre de manière concrète et de réviser votre compréhension du contenu de l'unité. N'hésitez pas à poser

des questions pendant le cours ou à demander conseil à l'instructeur pendant l'exercice final. Nous souhaitons que vous vous sentiez parfaitement à l'aise dans les cours et que vous n'hésitiez pas à poser des questions. Vous pouvez approfondir vos connaissances en fonction de ce qui fonctionne, mais surtout en fonction de ce qui n'est pas évident au départ.

Orientation sur le réseau de la classe

Deux sous-réseaux peuvent être utilisés pour ce cours. Le réseau principal de la classe est 192.168.0.0/24 et il appartient aux hôtes du domaine DNS "example.com" Ce réseau sera utilisé pour la plupart des activités en classe. Certains cours utilisent un deuxième sous-réseau, 192.168.1.0/24, qui appartient aux hôtes du domaine DNS "remote.test". Ce réseau peut être atteint à partir des hôtes dans example.com et est utilisé dans des exercices pratiques nécessitant des services de test ou des paramètres de sécurité à partir de machines (théoriquement) en dehors de votre contrôle administratif.

À chaque étudiant est affectée une machine physique (desktop*X*.example.com sur 192.168.0*X*) qui peut héberger au moins deux machines virtuelles pour les activités pratiques, server*X*.example.com et host*X*.example.com.

Dans certains cours, les étudiants peuvent également utiliser un compte d'utilisateur normal sur une machine de test dans le domaine remote.test, remote*X*.example.com (192.168.1.*X*) pour tester l'accès aux services de réseau sur leurs machines example.com dans le cadre des activités pratiques.

L'instructeur contrôle un certain nombre de machines que les étudiants voient également. La machine instructor.example.com (également appelée instructor.remote.test) est le serveur d'utilitaires de la classe et fournit des services de routage par défaut, DHCP, un service de noms DNS, un ou plusieurs référentiels YUM de logiciels utilisés en classe et d'autres services réseau. Il est également connecté au vidéoprojecteur de la classe pour permettre à l'instructeur d'afficher des diapositives et des démonstrations. Il fournit une machine virtuelle à l'instructeur, demo.example.com, que ce dernier utilise pour les démonstrations en classe.

Nom machine	Adresse IP	Rôle
desktop*X*.example.com	192.168.0.*X*	Station de travail physique étudiant
server*X*.example.com	192.168.0.*(X+100)*	Machine virtuelle principale étudiant
host*X*.example.com	192.168.0.*(X+200)*	Machine virtuelle secondaire étudiant
remote*X*.remote.test	192.168.1.*X*	Machine de test étudiant dans le domaine remote.test (partagé)
instructor.example.com	192.168.0.254	Machine physique de l'instructeur et serveur d'utilitaires
instructor.remote.test	192.168.1.254	Identité d'instructor.example.com sur le réseau remote.test

Nom machine	Adresse IP	Rôle
demo.example.com	192.168.0.250	Machine de démonstration virtuelle instructeur

Tableau 1. Machines de la classe

Internationalisation

Prise en charge linguistique

Red Hat Enterprise Linux 6 prend officiellement en charge vingt-deux langues : anglais, assamais, bengali, chinois (simplifié), chinois (traditionnel), français, allemand, gujrati, hindi, italien, japonais, kannada, coréen, malayalam, marathi, oriya, portugais (brésilien), punjabi, russe, espagnol, tamil et télougou. Les prises en charge du maithili, du népalais et du cingalais sont fournies en tant que présentations technologiques.

Langue par défaut du système

Par défaut, la langue du système d'exploitation est l'anglais (États-Unis) (en_US.UTF-8), mais vous pouvez la modifier pendant ou après l'installation.

Pour utiliser d'autres langues, il se peut que vous deviez installer des groupes de packages supplémentaires pour fournir les polices appropriées, les traductions, les dictionnaires, etc. Par convention, ces groupes de packages portent toujours le nom ***language*-support**. Vous pouvez sélectionner ces groupes de packages au moment de l'installation ou bien après à l'aide de PackageKit (**System** → **Administration** → **Add/Remove Software**) ou **yum**.

Vous pouvez changer la langue par défaut du système via **system-config-language** (**System** → **Administration** → **Language**), ce qui modifie le fichier **/etc/sysconfig/i18n**.

Sélection de la langue par utilisateur

Les utilisateurs peuvent, s'ils le souhaitent, utiliser une autre langue pour leur propre environnement de bureau ou dans des shells, différents de ceux définis par défaut pour le système. La variable d'environnement **LANG** exporte cela au système.

Ceci peut être défini automatiquement pour l'environnement de bureau GNOME, en sélectionnant une langue à partir de l'écran de connexion graphique, en cliquant sur l'élément **Language**, dans le coin inférieur gauche de cet écran immédiatement avant la connexion. Un message demande alors à l'utilisateur si la langue sélectionnée doit être utilisée juste pour cette session ou en tant que langue par défaut pour l'utilisateur à partir de maintenant. Le paramètre est enregistré dans le fichier **~/.dmrc** de l'utilisateur par GDM.

Si un utilisateur souhaite que son propre environnement de shell utilise le même paramètre **LANG** que son environnement graphique, même s'il s'est connecté via une console de texte ou à travers **ssh**, il peut définir du code similaire à celui qui suit dans son fichier **~/.bashrc**. Ce code définit leur langue favorite si elle est enregistrée dans **~/.dmrc** ou utilise la valeur système par défaut en l'absence de définition de cette langue :

```
i=$(grep 'Language=' ${HOME}/.dmrc | sed 's/Language=//')
if [ "$i" != "" ]; then
    export LANG=$i
```

```
fi
```

Les langues avec des caractères qui ne sont pas ASCII peuvent présenter des problèmes d'affichage dans certains environnements. Les caractères kanji, par exemple, risquent de ne pas apparaître comme souhaité sur une console virtuelle. Des commandes individuelles peuvent utiliser une autre langue en configurant **LANG** sur la ligne de commande :

```
[user@host ~]$ LANG=fr_FR.UTF-8 date
lun. oct. 24 10:37:53 CDT 2011
```

Les commandes suivantes utiliseront toujours la langue par défaut du système pour leur sortie. La commande **locale** peut être utilisée pour vérifier la valeur actuelle de **LANG**, ainsi que d'autres variables d'environnement connexes.

Méthodes de saisie

IBus (Intelligent Input Bus) peut être utilisé pour la saisie de texte dans différences langues sous X si les packages de prise en charge linguistique appropriés sont installés. Pour activer IBus, utilisez la commande **im-chooser** (**System** → **Preferences** → **Input Method**).

Référence des codes de langue

Langue	Valeur $LANG	Groupe de packages linguistiques
Anglais (États-Unis)	en_US.UTF-8	*(par défaut)*
Assamais	as_IN.UTF-8	assamese-support
Bengali	bn_IN.UTF-8	bengali-support
Chinois (simplifié)	zh_CN.UTF-8	chinese-support
Chinois (traditionnel)	zh_TW.UTF-8	chinese-support
Français	fr_FR.UTF-8	french-support
Allemand	de_DE.UTF-8	german-support
Gujrati	gu_IN.UTF-8	gujarati-support
Hindi	hi_IN.UTF-8	hindi-support
Italien	it_IT.UTF-8	italian-support
Japonais	ja_JP.UTF-8	japanese-support
Kannada	kn_IN.UTF-8	kannada-support
Coréen	ko_KR.UTF-8	korean-support
Malayalam	ml_IN.UTF-8	malayalam-support
Marathi	mr_IN.UTF-8	marathi-support
Oriya	or_IN.UTF-8	oriya-support

Langue	Valeur $LANG	Groupe de packages linguistiques
Portugais (brésilien)	pt_BR.UTF-8	brazilian-support
Punjabi	pa_IN.UTF-8	punjabi-support
Russe	ru_RU.UTF-8	russian-support
Espagnol	es_ES.UTF-8	spanish-support
Tamil	ta_IN.UTF-8	tamil-support
Télougou	te_IN.UTF-8	telugu-support
Présentations technologiques		
Maithili	mai_IN.UTF-8	maithili-support
Népalais	ne_NP.UTF-8	nepali-support
Cingalais	si_LK.UTF-8	sinhala-support

Tableau 2. Codes de langue



MODULE UN

GESTION DES LOGICIELS

Introduction

Sujets couverts dans cette unité :

- Enregistrement des systèmes avec Red Hat Network (RHN)
- Utilisation de `yum` pour gérer les packages logiciels
- Utilisation de `rpm` pour obtenir des informations sur les packages logiciels
- Création de vos propres packages logiciels RPM
- Création et utilisation d'un référentiel de packages yum

Enregistrer un système avec Red Hat Network (RHN)

Qu'est-ce que Red Hat Network ?

Red Hat Network est un service centralisé qui permet de déployer facilement des logiciels et des mises à jour de logiciel sur des systèmes Red Hat Enterprise Linux et de gérer, et surveiller, à distance ces derniers. Vous pouvez pour cela utiliser le service RHN « hébergé » géré par Red Hat, ou bien configurer et gérer votre propre RHN Satellite dans votre organisation. Dans un cas comme dans l'autre, pour obtenir des mises à jour de logiciels pour vos clients de RHN et les présenter dans votre interface de gestion Web, vous devez d'abord enregistrer ces systèmes avec le serveur RHN de votre choix.

Utilisation de la commande rhn_register

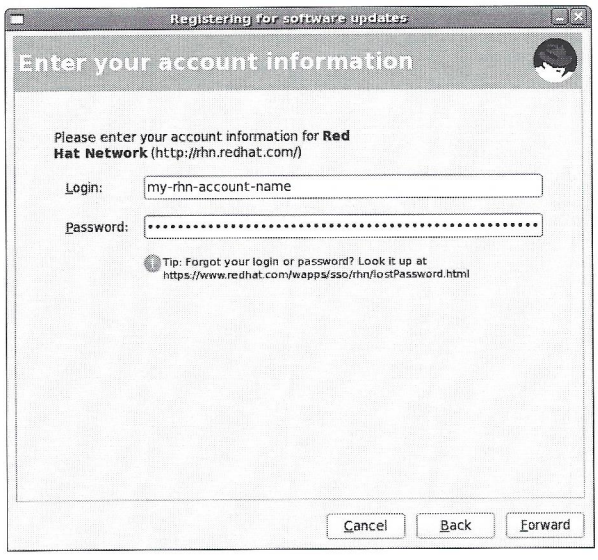
Lancez le processus d'enregistrement Red Hat Network (RHN) en exécutant la commande **`rhn_register`** depuis la ligne de commande ou en la sélectionnant dans le menu de l'interface utilisateur : **Système → Administration → Enregistrement RHN**

Si vous disposez d'un serveur RHN Satellite ou RHN Proxy, sélectionnez le bouton **Je dispose d'un accès à Red Hat Network Satellite...**de l'interface utilisateur. Indiquez le nom DNS du serveur RHN Satellite ou RHN Proxy.

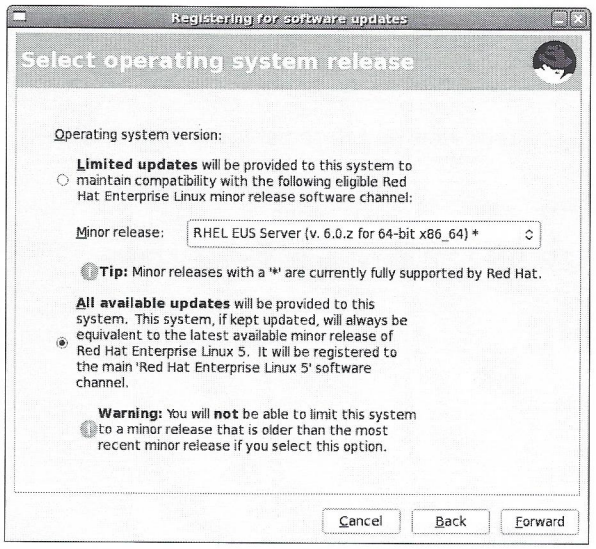
Si vous ne disposez pas d'un serveur RHN Satellite ou RHN Proxy, ou si vous souhaitez enregistrer un système avec le service RHN « hébergé », sélectionnez le bouton **Je voudrais recevoir des mises à jour de Red Hat Network.**

Si vous devez définir le paramètre de proxy pour la connexion, cliquez sur le bouton **Configuration réseau avancée...** et remplissez les champs appropriés.

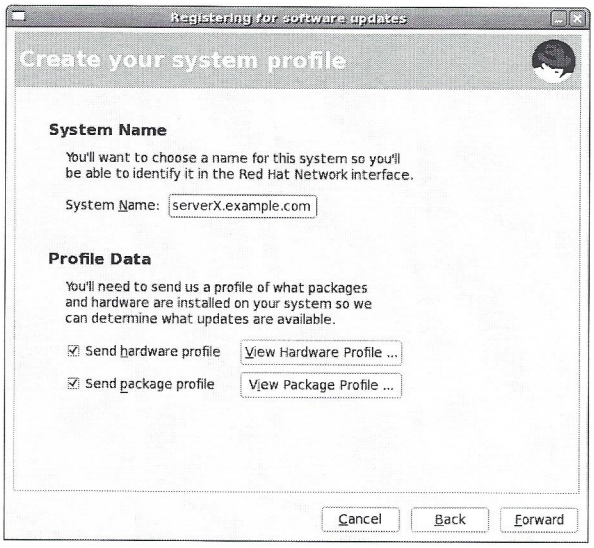
Fournissez les informations de votre compte Red Hat Network. Si vous avez oublié le nom ou le mot de passe utilisé pour votre compte ou si vous devez créer un nouveau compte, accédez à `https://www.redhat.com/wapps/sso/login.html`



L'écran suivant vous permet de limiter les mises à jour à celles compatibles avec les versions mineures de Red Hat Enterprise Linux. Si c'est ce que vous souhaitez faire, sélectionnez **Mises à jour limitées.** Si vous souhaitez bénéficier de toutes les mises à jour, sélectionnez **Toutes les mises à jour disponibles.**



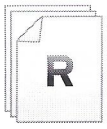
Entrez le nom de votre système (le nom de l'hôte courant sera ajouté par défaut) et envoyez éventuellement le profil du package et du matériel à RHN.





Note

La commande **`rhn_register`** fonctionne également bien dans un environnement graphique ou textuel. Si vous exécutez la commande **`rhn_register`** dans un environnement uniquement textuel, vous devrez fournir les mêmes informations que celles demandées par l'interface utilisateur.



Références

Pages man **`rhn_register`** et **`rhnplugin`**

Base de connaissances : « À quoi sert la commande rhn_register dans Red Hat Enterprise Linux ? »
https://access.redhat.com/kb/docs/DOC-11217

Bases de connaissances : "I had to re-install my system. How do I re-register my system with Red Hat Network (RHN)?"
https://access.redhat.com/kb/docs/DOC-8037

Red Hat Enterprise Virtualization for Servers 2.2: 5.5-2.2 Hypervisor Deployment Guide
- Section 5.1.7 : Enregistrer auprès de RHN



Exercice de Questionnaire

Enregistrement Red Hat Network

1. L'élément de menu qui lance l'enregistrement auprès de Red Hat Network est _____

2. Le premier choix d'enregistrement détermine si un système est enregistré avec _____ ou _____.

3. Un serveur _____ supplémentaire peut être requis en option et des informations d'authentification peuvent être demandées

4. Un _____ ainsi que le mot de passe correspondant doivent être fournis pour un enregistrement Red Hat Network correct.

5. Les dernières questions auxquelles vous devez répondre lors du processus d'enregistrement sont _____ et s'il faut télécharger les informations de profil relatives au _____ et aux _____.

Utilisation de référentiels tiers

Les référentiels tiers sont des répertoires réseau contenant des fichiers de packages logiciels accessibles à l'aide de **yum**, fourni en dehors de Red Hat Network. Les référentiels Yum sont utilisés par les distributeurs de logiciels autres que Red Hat ou pour de petits groupes de packages locaux. (Par exemple, Adobe fournit certains de ses logiciels gratuits pour Linux par le biais d'un référentiel yum.) Le serveur de la classe **instructor** héberge les répertoires yum prévus pour ce cours.

Placez un fichier dans le répertoire **/etc/yum.repos.d/** pour permettre la prise en charge d'un nouveau référentiel tiers. Les fichiers de configuration de référentiel doivent se terminer par ***.repo**. La définition du référentiel contient l'URL et le nom de ce dernier. Elle indique en outre si GPG doit être utilisé pour vérifier les signatures de package et, si tel est le cas, vérifier le fichier local contenant la clé GPG approuvée.

Exemples de fichiers de configuration /etc/yum.repos.d/*.repo :

Exemple avec un seul référentiel (les vérifications de sécurité des packages téléchargés étant désactivées) :

```
[GLS]
name=Instructor GLS Repository
baseurl=ftp://instructor.example.com/pub/gls
gpgcheck=0
```

Exemple avec plusieurs références de référentiel dans un seul fichier :

```
[base]
name=Instructor Server Repository
baseurl=http://instructor.example.com/pub/rhel6/dvd
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

# Optional rhel6
[optional]
name=Instructor Optional Repository
baseurl=http://instructor.example.com/pub/rhel6/Optional
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[client]
name=Instructor Client Repository
baseurl=http://instructor.example.com/pub/rhel6/Client
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
enabled=0

[kernel-extras]
name=Instructor Kernel Extras Repository
baseurl=http://instructor.example.com/pub/rhel6/Kernel-Extras
gpgcheck=1
```



Note

Notez que certains référentiels, comme EPEL (Extra Packages for Enterprise Linux), fournissent ce fichier de configuration dans un package RPM téléchargeable et dont l'installation s'effectue avec **yum localinstall**.

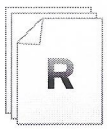
Installation du package du référentiel EPEL de Red Hat Enterprise Linux 6:

```
[root@serverX ~]# rpm --import http://download.fedora.redhat.com/pub/epel/RPM-GPG-KEY-
EPEL-6
[root@serverX ~]# yum install http://download.fedora.redhat.com/pub/epel/beta/6/x86_64/
epel-release-6-5.noarch.rpm
[root@serverX ~]# cat /etc/yum.repos.d/epel.repo

[epel]
name=Extra Packages for Enterprise Linux 6 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/6/$basearch
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-6&arch=$basearch
failovermethod=priority
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6

[epel-debuginfo]
name=Extra Packages for Enterprise Linux 6 - $basearch - Debug
#baseurl=http://download.fedoraproject.org/pub/epel/6/$basearch/debug
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-debug-6&arch=$basearch
failovermethod=priority
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
gpgcheck=1

[epel-source]
name=Extra Packages for Enterprise Linux 6 - $basearch - Source
#baseurl=http://download.fedoraproject.org/pub/epel/6/SRPMS
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-source-6&arch=$basearch
failovermethod=priority
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
gpgcheck=1
```



Important

Installez la clé GPG de RPM avant d'installer les packages signés. Cela permet de vérifier que le package appartient à une clé que vous avez importée. Sinon, **yum** demandera la clé manquante. (Vous pouvez utiliser l'option **--nogpgcheck** pour ignorer les clés GPG manquantes mais vous risquez alors d'installer des packages falsifiés ou dangereux sur votre système.)



Références

Pages man **yum**(1) et **yum.conf**(5)



Exercice de Exercice

Utilisation de référentiels YUM

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Vous allez configurer votre serveur pour utiliser un référentiel YUM distinct afin d'obtenir des mises à jour et de mettre à jour votre machine.

1. Créez le fichier **`/etc/yum.repos.d/errata.repo`** pour activer le référentiel « Mises à jour » qui se trouve sur la machine instructor. Il devrait accéder au contenu trouvé à l'adresse URL suivante : ftp://instructor.example.com/pub/rhel6/Errata

2. Mettez à jour tous les logiciels appropriés fournis par le référentiel à l'aide de **`yum update`**.

Utilisation de yum

yum est un outil de ligne de commande puissant qui peut être utilisé pour gérer les packages logiciels de manière plus flexible.

PackageKit utilise **yum** pour obtenir des packages. Les packages Red Hat officiels sont normalement téléchargés à partir de Red Hat Network (RHN). Lorsque vous enregistrez votre machine sur RHN, **yum** est automatiquement configuré pour l'utiliser. Vous pouvez également configurer **yum** pour obtenir des packages à partir de référentiels de packages tiers sur le réseau.

Commandes yum de base

1. **yum help** affiche les informations d'utilisation
2. **yum list** affiche les packages installés et disponibles
3. **yum search *KEYWORD*** répertorie les packages par mots-clés
4. **yum info *PACKAGENAME*** donne des informations détaillées sur un package
5. **yum install *PACKAGENAME*** obtient et installe un package logiciel, y compris toutes ses dépendances
6. **yum remove *PACKAGENAME*** supprime un package logiciel installé, y compris tous les packages pris en charge
7. **yum update *PACKAGENAME*** obtient et installe une version plus récente du package logiciel, y compris toutes les dépendances. En règle générale, le processus essaie de conserver les fichiers de configuration en place, mais dans certains cas ils doivent être renommés si le packager pense que l'ancienne version ne fonctionnera pas après la mise à jour. Sans PACKAGENAME spécifié, toutes les mises à jour pertinentes sont installées.

Utilisez cet espace pour vos notes.

Exemple de commandes yum :

Pour rechercher des packages dont la description, le nom ou le résumé comporte « serveur Web » :

```
[root@serverX ~]# yum search 'web server'
============================== Matched: web server ==============================
mod_auth_mysql.x86_64 : Basic authentication for the Apache web server using a
                      : MySQL database
webalizer.x86_64 : A flexible Web server log file analysis program
freeradius.x86_64 : High-performance and highly configurable free RADIUS server
hsqldb.x86_64 : Hsqldb Database Engine
htdig.x86_64 : ht://Dig - Web search engine
htdig-web.x86_64 : Scripts and HTML code needed for using ht://Dig as a web
```

```
                : search engine
httpd.x86_64 : Apache HTTP Server
...
```

Pour obtenir des informations sur le serveur Apache HTTP:

```
[root@serverX ~]# yum info httpd
Available Packages
Name        : httpd
Arch        : x86_64
Version     : 2.2.15
Release     : 5.el6
Size        : 811 k
Repo        : base
Summary     : Apache HTTP Server
URL         : http://httpd.apache.org/
License     : ASL 2.0
Description: The Apache HTTP Server is a powerful, efficient, and extensible
           : web server.
```

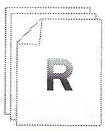
Pour installer, mettre à jour et supprimer le package **httpd**:

```
[root@serverX ~]# yum install httpd
[root@serverX ~]# yum update httpd
[root@serverX ~]# yum remove httpd
```



Avertissement

yum remove supprime les packages répertoriés *et les packages qui nécessitent les packages supprimés* (et les packages qui nécessitent ces packages et ainsi de suite). Cela peut entraîner la suppression non souhaitée de packages, par conséquent examinez attentivement la liste des packages à supprimer.



Références

Pages man **yum**(1), **yum.conf**(5)



Exercice de Exercice

Recherche et installation de packages

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Connectez-vous en tant que **root** sur le serverX et effectuez les tâches suivantes :

1. Essayez d'exécuter la commande **gnuplot**. Vous devez trouver qu'elle n'est pas installée.
2. Recherchez les packages de tracés.
3. Recherchez des informations supplémentaires sur le package **gnuplot**.
4. Installez le package **gnuplot**.
5. Tentez de supprimer le package **gnuplot**, mais sélectionnez non.

   Combien de packages seraient supprimés ? _____
6. Tentez de supprimer le package **gnuplot-common**, mais sélectionnez non.

   Combien de packages seraient supprimés ? _____

Traitement de logiciels tiers

L'utilitaire **rpm** est un outil de niveau bas permettant d'obtenir des informations sur le contenu des fichiers de package et sur les packages installés. **rpm** permet d'obtenir des informations détaillées sur les packages à partir des fichiers du package ou de la base de données locale d'informations sur les packages installés.

Requêtes RPM - Informations sur les versions des packages

- **-q -a** - tous les packages installés
- **-q *PACKAGENAME*** - NOMPACKAGE installé actuellement
- **-q -p *PACKAGEFILE.rpm*** - fichier de package FICHIERPACKAGE.rpm
- **-q -f *FILENAME*** - package qui fournit le NOMFICHIER

Requêtes RPM - Informations sur les versions des packages

- **-q** - indique le nom et la version du package par rapport à **yum list**
- **-q -i** - informations sur le package par rapport à **yum info**
- **-q -l** - répertorie les fichiers installés par le package spécifié
- **-q --configfiles** - répertorie uniquement les fichiers de configuration
- **-q --docfiles** - répertorie uniquement les fichiers de documentation
- **-q --scripts** - répertorie les scripts shell qui peuvent être exécutés une fois le package installé ou désinstallé



Note

La commande **repoquery** permet également d'obtenir des informations sur les packages et leur contenu. Elle est différente de **rpm**, car elle recherche ces informations dans les référentiels de yum et dans RHN et non pas dans la base de données locale des packages installées.

Utilisation de yum pour installer les fichiers de package locaux

yum localinstall *PACKAGEFILE.rpm* permet d'installer directement les fichiers de package. Il télécharge automatiquement toutes les dépendances du package à partir de RHN et de tout référentiel **yum** configuré. Les packages portent normalement une signature numérique pour garantir leur légitimité. Si le package n'a pas de signature de confiance pour votre système, il sera refusé. L'option **--nogpgcheck** peut désactiver la vérification de signature si vous êtes sûr que le package est légitime.



Note

rpm -ivh *PACKAGEFILE.rpm* permet également d'installer les fichiers de package. Cependant, **yum** permet de tenir à jour un historique des transactions conservé par **yum** (voir **yum history**).

Exemple de commandes de requête rpm :

Recherche des packages installés :

```
[root@serverX ~]# rpm -q samba-client
samba-client-3.5.4-68.el6.x86_64
[root@serverX ~]# rpm -ql zlib
/lib64/libz.so.1
/lib64/libz.so.1.2.3
/usr/share/doc/zlib-1.2.3
/usr/share/doc/zlib-1.2.3/ChangeLog
/usr/share/doc/zlib-1.2.3/FAQ
/usr/share/doc/zlib-1.2.3/README
[root@serverX ~]# rpm -q --scripts httpd
preinstall scriptlet (using /bin/sh):
# Add the "apache" user
getent group apache >/dev/null || groupadd -g 48 -r apache
getent passwd apache >/dev/null || \
  useradd -r -u 48 -g apache -s /sbin/nologin \
    -d /var/www -c "Apache" apache
exit 0
postinstall scriptlet (using /bin/sh):
# Register the httpd service
/sbin/chkconfig --add httpd
preuninstall scriptlet (using /bin/sh):
if [ $1 = 0 ]; then
        /sbin/service httpd stop > /dev/null 2>&1
        /sbin/chkconfig --del httpd
fi
posttrans scriptlet (using /bin/sh):
/sbin/service httpd condrestart >/dev/null 2>&1 || :
```

Recherche et installation de fichiers de package :

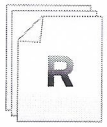
```
[root@serverX ~]# cd /net/instructor/var/ftp/pub/materials/
[root@serverX ~]# rpm -qpl wonderwidgets-1.0-4.x86_64.rpm
/etc/wonderwidgets.conf
/usr/bin/wonderwidgets
/usr/share/doc/wonderwidgets-1.0
/usr/share/doc/wonderwidgets-1.0/README.txt
[root@serverX ~]# rpm -qpi wonderwidgets-1.0-4.x86_64.rpm
Name        : wonderwidgets                Relocations: (not relocatable)
Version     : 1.0                               Vendor: Red Hat, Inc.
Release     : 4                            Build Date: Fri 03 Dec 2010 05:42:55 AM EST
Install Date: (not installed)              Build Host: station166.rosemont.lan
Group       : GLS/Applications             Source RPM: wonderwidgets-1.0-4.src.rpm
Size        : 4849                            License: GPL
Signature   : (none)
Summary     : Demonstration package for use in GLS training.
Description :
```

```
A demonstration package that installs an executable, and a config file.
[root@serverX ~]# rpm -qp --configfiles wonderwidgets-1.0-4.x86_64.rpm
/etc/wonderwidgets.conf
[root@serverX ~]# rpm -qp --docfiles wonderwidgets-1.0-4.x86_64.rpm
/usr/share/doc/wonderwidgets-1.0/README.txt
[root@serverX ~]# yum localinstall wonderwidgets-1.0-4.x86_64.rpm
...
Package wonderwidgets-1.0-4.x86_64.rpm is not signed
[root@serverX ~]# yum localinstall --nogpgcheck wonderwidgets-1.0-4.x86_64.rpm
[root@serverX ~]# rpm -q wonderwidgets
wonderwidgets-1.0-4.x86_64
```



Important

Procédez avec précaution en installant des packages tiers, non seulement en raison des logiciels qu'ils peuvent installer, mais aussi parce que RPM peut exécuter des scripts arbitraires en tant que **root** au cours du processus d'installation.



Références

Pages man **rpm**(8) et **repoquery**(1)



Exercice de Exercice

Traitement de logiciels tiers

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Dans cet exercice, vous allez collecter des informations sur un package tiers, en extraire des fichiers et l'installer en entier sur le système desktopX.

1. Téléchargez *wonderwidgets-1.0-4.x86_64.rpm* à partir de *http://instructor/pub/materials*.
2. Quels fichiers contient-il ?
3. Quels scripts contient-t-il ?
4. Quelle quantité d'espace disque utilise-t-il une fois installé ?
5. Utilisez **`yum localinstall`** pour installer le package

Conception de packages RPM

Il est bien plus simple de gérer des logiciels sous la forme de packages RPM que d'utiliser des logiciels qui ont été simplement extraits d'une archive et intégrés à un système de fichiers. Cela vous permet de savoir quels fichiers ont été installés par le package logiciel, quels fichiers doivent être supprimés si le logiciel est désinstallé et de vérifier que les packages complémentaires sont présents lorsque le logiciel est installé.

Par conséquent, il vous sera utile de savoir créer des packages RPM pour vos logiciels. Dans cette unité, nous examinerons la création d'un package RPM de base et nous vous indiquerons les ressources qui vous seront utiles pour créer des packages plus complexes à mesure que vous acquerrez de nouvelles compétences.

Conception/structure d'un package RPM

Chaque package RPM est constitué de trois composants de base :

- *métadonnées* - Données relatives au package : nom, version, build, créateur, date, dépendances, etc.
- *fichiers* - archive des fichiers fournis par le package (attributs des fichiers compris)
- *scripts* - les scripts s'exécutent lorsque le package est installé, mis à jour et/ou supprimé

Lors de la création d'un package RPM, vous devez spécifier les métadonnées relatives au package, fournir les fichiers dans l'archive et intégrer les scripts qui doivent s'exécuter lorsque le package est installé ou désinstallé.



Note

Les fichiers sont stockés en tant qu'archive **cpio** dans le fichier du package. La commande **rpm2cpio** permet d'extraire les fichiers dans le répertoire de travail courant sans installer le package : **rpm2cpio *package-1.2.3-4.el6.x86_64.rpm* | cpio -id**

Les requêtes **rpm** suivantes permettent de connaître la structure d'un package RPM :

- **rpm -qd** - répertorie les fichiers de documentation (**%doc**)
- **rpm -qc** - répertorie les fichiers de configuration (**%config**)
- **rpm -q --scripts** - répertorie les scripts **%pre**, **%post**, **%preun** et **%postun**



Références

Red Hat Enterprise Linux Deployment Guide, Section 3.2.6 : Interroger RPM

Pages man **rpm**(8), **rpm2cpio**(8) et **cpio**(1)

Spécifications d'un package RPM

Pour créer un package RPM, vous devez d'abord créer un fichier de spécification, également appelé *fichier spec*. Un fichier spec est en fait un fichier texte qui contient des informations sur la manière de créer le package RPM installable. Il est en général constitué de cinq parties :

- L'*introduction* ou *le préambule* répertorie les métadonnées relatives au package (nom, version, licence, etc.)
- Les *instructions de* création qui indiquent comment compiler et préparer le logiciel
- Les *scriptlets* qui spécifient les commandes à exécuter pour installer, désinstaller ou mettre à niveau le logiciel
- Le *manifeste* qui est une liste de fichiers à packager et de leurs autorisations pour l'installation du package
- Le *changelog* (journal des modifications) qui répertorie les modifications apportées au package RPM

Directives importantes relatives au préambule :

- **Name** - Nom du package, en général choisi par les développeurs. Pour plus d'instructions, reportez-vous aux conventions de dénomination Fedora sur le site *http://fedoraproject.org/wiki/Packaging:NamingGuidelines*
- **Version** - Version du package (sous forme numérique), en général choisie par les développeurs.
- **Release** - Numéro de build du package, choisi par le créateur du package. Ce numéro doit augmenter à chaque fois que vous lancez la distribution d'un nouveau package si vous utilisez toujours la même version du logiciel.
- **Group** - Groupe auquel le package appartient. Voir **/usr/share/doc/rpm-*/GROUPS** pour connaître les groupes par défaut ou utilisez un de vos groupes. Ce champ n'est pas obligatoire, il n'est lié à aucun groupe de packages **yum**.
- **License** - Identificateur court de la licence utilisée pour le logiciel. Vous trouverez des instructions détaillées pour définir cet identificateur de façon standard sur le site *http://fedoraproject.org/wiki/Packaging/LicensingGuidelines*
- **Summary** - Description brève en une ligne du logiciel. (50 caractères maximum.)
- **Source** - Fichier à utiliser comme code source. Si plusieurs fichiers de code source sont utilisés, numérotez les fichiers. Par exemple, Source0, Source1, Source2, etc.
- **BuildArch** - Architecture à utiliser pour créer le package. Il s'agit de l'architecture système par défaut. Un argument courant utilisé est **noarch**, qui indique que le package est indépendant de toute architecture (ce type de package est souvent constitué de scripts ou de fichiers de données).

- **Requires** - Liste de composants explicites dont dépend le package. Il peut s'agir d'une liste de fichiers ou d'autres packages. **rpmbuild** peut en général détecter automatiquement la plupart des dépendances de bibliothèque mais dans certains cas vous devrez indiquer une dépendance explicite. Voir *http://fedoraproject.org/wiki/Packaging/Guidelines#Requires* pour plus d'instructions concernant l'utilisation de **Requires**.
- **BuildRequires** - Liste de composants nécessaires pour *créer* le package. La syntaxe de cette liste est similaire à celle de **Requires**, par exemple **BuildRequires: /usr/bin/gcc, gimp-libs >= 2.6.11**. Voir le lien de **Requires** ci-dessus pour plus d'informations afin de déterminer si vous avez besoin de composants **BuildRequires** manquants.

Sections de fichier spec requises :

- Section **%description** - Longue description du logiciel. Chaque ligne ne peut comporter que 80 caractères, mais le fichier peut avoir plusieurs lignes.
- Section **%prep** -
- Section **%build** -
- Section **%install** -
- Section **%clean** -
- Section **%files** -
- Section **%changelog** -

Étapes de rpmbuild

Lorsque **rpmbuild** est exécuté, le processus de création s'effectue dans l'ordre de sections suivant :

1. %prep
2. %build
3. %install
4. Packager le RPM complet
5. %clean

Création d'un nouveau fichier spec

Sur Red Hat Enterprise Linux 6, **vim** comporte une macro qui permet de créer un fichier de spécification. Indiquez simplement un nom de fichier se terminant par **.spec** :

```
[student@serverX]$ vim foo.spec
```

vim utilisera le modèle de spécification pour fournir certaines entrées communes en vue de créer le RPM.



Note

Lorsqu'un package RPM est créé, un *package RPM source* (SRPM) est également créé, avec une architecture **src**. Il est également possible d'obtenir un fichier spec en installant un package source. Il suffit pour cela d'exécuter **rpm -ivh *package-1.2.3-4.src.rpm*** en tant qu'utilisateur classique, et *non super utilisateur*. Le fichier spec pour le package sera placé dans **~/rpmbuild/SPECS**.

Exemple de fichier spec

Voici ci-dessous un exemple de fichier spec annoté.

```
%define debug_package %{nil} (1)
%define product_family Red Hat Enterprise Linux
%define release_name Santiago
%define base_release_version 6
%define full_release_version 6.0
%define beta Beta

Name:           redhat-release (2)
Version:        %{base_release_version} (3)
Release:        6.0.0.24%{?dist} (4)
Summary:        %{product_family} release file (5)
Group:          System Environment/Base
License:        GPLv2
Obsoletes:      rawhide-release redhat-release-as redhat-release-es redhat-release-ws (6)
Source0:        redhat-release-6-4.tar.gz (7)

%description (8)
%{product_family} release files

%prep (9)
%setup -q

%build (10)
echo OK

%install (11)
rm -rf $RPM_BUILD_ROOT

# create /etc
mkdir -p $RPM_BUILD_ROOT/etc

# create /etc/system-release and /etc/redhat/release
echo "%{product_family} release %{full_release_version}%{?beta: %{beta}}
 (%{release_name})" > $RPM_BUILD_ROOT/etc/redhat-release
ln -s redhat-release $RPM_BUILD_ROOT/etc/system-release

# write cpe to /etc/system/release-cpe
echo "cpe:/o:redhat:enterprise_linux:%{version}:%{?beta:%{beta}}%{!?beta:GA}" >
 $RPM_BUILD_ROOT/etc/system-release-cpe
```

```
# create /etc/issue and /etc/issue.net
cp $RPM_BUILD_ROOT/etc/redhat-release $RPM_BUILD_ROOT/etc/issue
echo "Kernel \r on an \m" >> $RPM_BUILD_ROOT/etc/issue
cp $RPM_BUILD_ROOT/etc/issue $RPM_BUILD_ROOT/etc/issue.net
echo >> $RPM_BUILD_ROOT/etc/issue

# copy yum repos to /etc/yum.repos.d
mkdir -p $RPM_BUILD_ROOT/etc/yum.repos.d
for file in *.repo; do
    install -m 644 $file $RPM_BUILD_ROOT/etc/yum.repos.d
done

# copy GPG keys
mkdir -p -m 755 $RPM_BUILD_ROOT/etc/pki/rpm-gpg
for file in RPM-GPG-KEY* ; do
    install -m 644 $file $RPM_BUILD_ROOT/etc/pki/rpm-gpg
done

# set up the dist tag macros
install -d -m 755 $RPM_BUILD_ROOT/etc/rpm
cat >> $RPM_BUILD_ROOT/etc/rpm/macros.dist << EOF
# dist macros.

%%rhel %{base_release_version}
%%dist .el%{base_release_version}
%%el%{base_release_version} 1
EOF

%clean (12)
rm -rf $RPM_BUILD_ROOT

%files (13)
%defattr(-,root,root)
%doc EULA GPL autorun-template
%attr(0644,root,root) /etc/redhat-release
/etc/system-release
%config %attr(0644,root,root) /etc/system-release-cpe
%config(noreplace) %attr(0644,root,root) /etc/issue
%config(noreplace) %attr(0644,root,root) /etc/issue.net
%config %attr(0644,root,root) /etc/yum.repos.d/*
%dir /etc/pki/rpm-gpg
/etc/pki/rpm-gpg/*
/etc/rpm/macros.dist

%changelog (14)
* Mon Mar 29 2010 Dennis Gregorovic <dgregor@redhat.com> - 6-6.0.0.24
- Add beta debuginfo repos
- Resolves: rhbz#572308
```

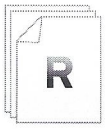
1. Macros (et variables) pouvant être utilisées dans le fichier spec
2. Nom du package
3. Version du package. Vous remarquerez qu'elle utilise la macro **%{base_release_version}** définie précédemment.
4. Build du package
5. Résumé bref
6. Liste de noms de package que ce package rend obsolète. Si l'un de ces packages est installé sur votre machine, une mise à jour de ce package le supprimera.

7. Fichier source
8. Longue description
9. Section **%prep**. Malheureusement, le fichier spec RPM utilise % pour les sections et les macros. **%prep** est une section, **%setup** est une macro.
10. Section **%build**
11. Section **%install**. **$RPM_BUILD_ROOT** est une variable qui s'applique à la « build root » (racine de la build). Les fichiers sont copiés du répertoire de la build à **$RPM_BUILD_ROOT**, comme si **$RPM_BUILD_ROOT** était **/** sur le système de fichiers dans lequel le logiciel sera installé. Puis le contenu de **$RPM_BUILD_ROOT** indiqué dans **%files** sera packagé dans le fichier RPM final. Vous devez créer tous les répertoires nécessaires dans **$RPM_BUILD_ROOT** avant d'y copier des fichiers. Les fichiers source peuvent être référencés à l'aide d'un chemin relatif depuis le répertoire source **%{name}-%{version}** de premier niveau. Par exemple, si vous voulez qu'un fichier soit placé dans **/root/bin/** (sous le répertoire **%{name}-%{version}/bin**), vous devez faire ce qui suit (ou quelque chose similaire) :

```
mkdir -p $RPM_BUILD_ROOT/root/bin
cp bin/my-script $RPM_BUILD_ROOT/root/bin
```

12. Section **%clean**. Normalement le nettoyage seulement requiert la commande **rm** ci-dessus.
13. Liste de fichiers à inclure dans ce package. Notez que **%defattr** définit les autorisations par défaut des fichiers, **%attr** peut remplacer ces autorisations fichier par fichier. **%config** et **%doc** marquent les fichiers de configuration et la documentation respectivement. **%dir** marque un répertoire appartenant au package. Voir *http://fedoraproject.org/wiki/Packaging:Guidelines#File_and_Directory_Ownership* et *http://fedoraproject.org/wiki/Packaging:Guidelines#Configuration_files* pour plus d'informations.
14. La section **%changelog** permet au créateur du package de répertorier les éléments qui ont changé dans cette build. Les entrées les plus récentes ajoutées au changelog sont placées au début de la section. Chaque entrée est présentée dans le format indiqué dans l'exemple. Les entrées sont séparées par une ligne vide.

L'exemple ci-dessus n'utilise aucune scriptlet. Pour plus d'informations sur les scriptlets, voir le document Fedora RPM Guide (à l'état d'ébauche) indiqué ci-dessous.



Références

Fedora RPM Guide -
http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/

Instructions de création de packages de Fedora -
http://fedoraproject.org/wiki/Packaging:Guidelines



Exercice de Questionnaire

Fichier spec RPM

1. Le package _____ est en général dérivé du projet open source tandis que le package _____ est la version du créateur.

2. La directive _____ indique la catégorie à laquelle appartient le type du package créé.

3. Le nom du tarball contenant les fichiers utilisés pour créer le package est spécifié avec la directive _____.

4. La directive _____ spécifie l'architecture cible pour laquelle le package est créé. _____ sera sa valeur lorsque le package peut être installé sur n'importe quelle architecture.

5. La directive _____ spécifie la description sur une ligne d'un package tandis que la section _____ fournit une explication plus complète de l'objectif du package.

6. La section _____ contient le code utilisé pour placer les fichiers dans la structure du répertoire chroot _____.

7. La section _____ définit quels fichiers et répertoires devront être intégrés au RPM.

8. Les sections _____, _____ et _____ contiennent le code shell utilisé pour assembler un package et le nettoyer après sa création.

Création et signature d'un package RPM

Les cinq étapes de création d'un package RPM :

1. *Tarball*

   Obtenez le fichier tar contenant la source. Par défaut, **rpmbuild** suppose que le répertoire de premier niveau de l'archive est nommé **%{name}-%{version}**. Placez ce fichier dans le répertoire **~/rpmbuild/SOURCES/**.

2. *Fichier spec*

   Créez un fichier spec et renseignez les champs requis. Placez ce fichier dans le répertoire **~/rpmbuild/SPECS/**.

3. *rpmbuild*

   Utilisez la commande **rpmbuild** pour créer des packages. Par exemple,

   ```
   rpmbuild -ba demo.spec
   ```

4. *Signature*

   Utilisez une clé GPG pour signer le package RPM. Vous pouvez utiliser **rpmbuild -ba --sign *demo*.spec** pour créer et signer le package en une seule étape. Si le package est déjà créé, utilisez **rpm --resign *demo-1.0-1.x86_64*.rpm** pour ajouter (ou modifier) une signature GPG.

5. *Test*

   Testez le package en l'installant sur un système de développement pour vérifier que sa charge utile est correcte, que les scripts s'exécutent correctement, etc.

Préparation d'une clé de signature GPG

Les packages RPM sont normalement signés de façon numérique pour que les utilisateurs puissent vérifier qu'il proviennent bien de la personne qui l'a préparé et auquel il appartient (comme il le déclare). Cela empêche l'installation de packages falsifiés si la fiabilité d'un répertoire yum a été compromise d'une manière ou d'une autre. Les étapes suivantes indiquent comment créer une clé de signature. Une fois que vous disposez d'une clé de signature vous pouvez l'utiliser pour signer de nombreux packages.

Si vous ne disposez pas encore d'une clé GPG, exécutez la commande **gpg --gen-key** pour en créer une.



Note

Une session graphique doit être ouverte pour exécuter **gpg --gen-key**. Cette commande utilise une zone graphique pour accepter la phrase de passe que vous fournissez.

```
[student@serverX ~]$ gpg --gen-key
gpg (GnuPG) 2.0.14; Copyright (C) 2009 Free Software Foundation, Inc. This is free
 software: you are free to change and redistribute it. There is NO WARRANTY, to the extent
 permitted by law. Please select what kind of key you want: (1) RSA and RSA (default) (2)
 DSA and Elgamal (3) DSA (sign only) (4) RSA (sign only) Your selection?   Enter
RSA keys may be between 1024 and 4096 bits long. What keysize do you want? (2048)  Enter
Requested keysize is 2048 bits Please specify how long the key should be valid. 0 = key
 does not expire <n> = key expires in n days <n>w = key expires in n weeks <n>m = key
 expires in n months <n>y = key expires in n years Key is valid for? (0)  Enter
Key does not expire at all Is this correct? (y/N) y
GnuPG needs to construct a user ID to identify your key. Real name: My Name
Email address: student@serverX.example.com
Comment:  Enter
You selected this USER-ID: "My Name <student@serverX.example.com>" Change (N)ame,
 (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key. Enter passphrase Passphrase: testing123
Please re-enter this passpassphrase. Passphrase: testing123
We need to generate a lot of random bytes. It is a good idea to perform some other action
 (type on the keyboard, move the mouse, utilize the disks) during the prime generation;
 this gives the random number generator a better chance to gain enough entropy.

gpg: /home/student/.gnupg/trustdb.gpg: trustdb created
gpg: key 54AF5285 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/54AF5285 2010-12-09
   Key fingerprint = 315F E90B 1745 2288 EBAE 4E7B 4BC6 4568 54AF 5285
uid    My Name <student@serverX.example.com>
sub    2048R/D08B2951 2010-12-09
```

Recherchez l'ID de la clé publique dans la sortie de **gpg --gen-key** ou exécutez **gpg --fingerprint**

```
[student@serverX ~]$ gpg --fingerprint
/home/student/.gnupg/pubring.gpg
--------------------------------
pub 2048R/54AF5285 2010-12-09
   Key fingerprint = 315F E90B 1745 2288 EBAE 4E7B 4BC6 4568 54AF 5285
uid    My Name <student@serverX.example.com>
sub    2048R/D08B2951 2010-12-09
```

L'ID de la clé publique est la chaîne de huit caractères hexadécimaux après **pub 2048R/** (54AF5285 dans l'exemple ci-dessus).

Exportez la clé publique (veillez à bien utiliser l'ID de votre clé) :

```
[student@serverX ~]$ gpg -a -o ~/RPM-GPG-KEY-student --export 54AF5285
```

Ajoutez ce qui suit au fichier **~/.rpmmacros** (en remplaçant l'ID de clé de huit caractères par l'ID de clé de votre système) pour que le RPM signe les packages avec la clé que vous avez créée précédemment.

```
[student@serverX ~]$ echo '%_gpg_name 54AF5285' > ~/.rpmmacros
```

Exemple de création d'un package RPM

L'exemple ci-dessous illustre la création d'un package RPM. Le nom du package est **test**, sa version est **1.0** et sa build est **1**. Il produit un seul fichier **/usr/local/bin/myscript** qui exécute simplement la commande **date**.

Créez le répertoire, le fichier et le tarball :

```
[student@serverX ~]$ mkdir test-1.0
[student@serverX ~]$ cat << EOF > test-1.0/myscript
#!/bin/bash
date
EOF
[student@serverX ~]$ tar czvf test-1.0.tar.gz test-1.0
```

Créez un fichier spec à l'aide de **vim** dans votre répertoire personnel :

```
[student@serverX ~]$ vim test.spec
```



Note

Dans Red Hat Enterprise Linux 6, **vim** crée automatiquement un fichier spec modèle lorsque vous ouvrez un nouveau fichier avec un nom se terminant par **.spec**.

Remplissez les champs comme suit.

```
Name:           test
Version:        1.0
Release:        1%{?dist}
Summary:        A test package

Group:          Testing
License:        GPL
URL:            http://www.example.com/testing
Source0:        %{name}-%{version}.tar.gz❶
BuildRoot:      %(mktemp -ud %{_tmppath}/%{name}-%{version}-%{release}-XXXXXX)

BuildRequires:  /bin/rm, /bin/mkdir, /bin/cp❷
Requires:       /bin/bash, /bin/date

%description
A testing package meant to deploy a single file.

%prep
%setup -q

%build
#configure❸
#make %{?_smp_mflags}


%install
```

```
rm -rf $RPM_BUILD_ROOT
#make install DESTDIR=$RPM_BUILD_ROOT
mkdir -p $RPM_BUILD_ROOT/usr/local/bin
cp myscript $RPM_BUILD_ROOT/usr/local/bin

%clean
rm -rf $RPM_BUILD_ROOT


%files
%defattr(-,root,root,-)
#%doc
%attr(0755,root,root)/usr/local/bin/myscript❹

%changelog
* Thu Dec 09 2010 Forrest <forrest@redhat.com> 1.0-1
- Initial RPM
- Added /usr/local/bin/myscript
```

❶ Les macros **%{name}** et **%{version}** sont définies à partir des lignes **Name:** et **Version:** ci-dessus. Vous auriez également pu utiliser **test-1.0.tar.gz**.

❷ Les commandes **rm**, **mkdir** et **cp** proviennent du package **coreutils**, vous auriez donc pu spécifier ce package à la place de ces commandes. Il s'agit des commandes qui sont utilisées dans la section **%install**.

❸ Certaines macros s'exécutent même si elles sont commentées, **%configure** est l'une d'elles. Si vous commentez **%configure** comme suit **#%configure**, la macro signalera qu'elle ne trouve pas **./configure**. Supprimez entièrement la ligne **%configure** ou supprimez **%** de **configure**.

❹ **%attr** a été ajouté pour que l'autorisation soit définie sur 0755. Vous pouvez constater que **%defattr** comporte un **-** à l'emplacement des autorisations. Cela signifie que les fichiers obtiendront les mêmes autorisations que celles figurant dans le tarball. Pour obtenir le même résultat, vous pouvez également exécuter **chmod 755 test-1.0/myscript** et recréer le tarball.

Installez le package **rpm-build** en tant que super utilisateur :

```
[root@serverX ~]# yum install -y rpm-build
```

Exécutez **rpmbuild** en tant qu'student. La première fois que vous l'exécuterez, vous obtiendrez une erreur. Vous résoudrez l'erreur plus loin. L'exécution de la commande **rpmbuild** crée la structure de répertoires nécessaire pour créer le package RPM.

```
[student@serverX ~]$ rpmbuild test.spec
error: File /home/student/rpmbuild/SOURCES/test-1.0.tar.gz: No such file or directory
```



Avertissement

Vous devez toujours exécuter **rpmbuild** pour créer des packages en tant qu'utilisateur normal, et *non super utilisateur. Ne créez pas de packages en tant que super utilisateur.* En effet, les erreurs dans le fichier spec, surtout dans les sections **%install** et **%clean**, risquent davantage d'endommager l'installation sur votre machine, lors d'une exécution en tant que super utilisateur.

Copiez les fichiers à l'emplacement approprié :

```
[student@serverX ~]$ cp test-1.0.tar.gz rpmbuild/SOURCES/
[student@serverX ~]$ cp test.spec rpmbuild/SPECS/
[student@serverX ~]$ cd rpmbuild/SPECS/
```

Créez et signez le package :

```
[student@serverX ~]$ rpmbuild --sign -ba test.spec
Enter pass phrase: testing123
Pass phrase is good.
...
```

Recherchez les erreurs dans la sortie de **rpmbuild** et corrigez-les. S'il n'y a aucune erreur, vous devriez obtenir :

```
...
Wrote: /home/student/rpmbuild/SRPMS/test-1.0-1.el6.src.rpm
Wrote: /home/student/rpmbuild/RPMS/x86_64/test-1.0-1.el6.x86_64.rpm
...
```

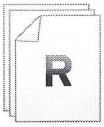
Testez le package en installant la clé, puis le package et en exécutant la commande :

```
[root@serverX ~]# rpm --import /home/student/RPM-GPG-KEY-student
[root@serverX ~]# cd /home/student/rpmbuild/RPMS/x86_64
[root@serverX ~]# yum localinstall test-1.0-1.el6.x86_64.rpm
[student@serverX ~]$ /usr/local/bin/myscript
Thu Dec 09 10:21:53 EST 2010
```



Note

Lors de la révision d'un package complet en vue de sa diffusion, les instructions de révision de packages formelles de Fedora (dans les références ci-dessous) peuvent vous être utiles.



Références

Fedora RPM Guide -
http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/

Instructions de création de packages de Fedora -
http://fedoraproject.org/wiki/Packaging:Guidelines

Instructions de révision de packages de Fedora -
http://fedoraproject.org/wiki/Packaging:ReviewGuidelines

Page man **rpmbuild**(8)

Publier des packages RPM

Une fois que vous avez créé un package RPM, vous devez disposer d'un moyen pour le distribuer à vos systèmes Red Hat Enterprise Linux. Dans l'idéal, vous disposez d'un serveur Red Hat Network Satellite qui vous permettra de déployer et de gérer vos packages personnalisés. Si ce n'est pas le cas, vous pouvez facilement rendre les packages disponibles pour les clients en configurant un référentiel yum.

Créer un référentiel yum

```
[root@serverX ~]# yum install -y createrepo
[root@serverX ~]# mkdir -p /var/www/html/repo/Packages
[root@serverX ~]# cp test-1.0-1.el6.x86_64.rpm /var/www/html/repo/Packages
[root@serverX ~]# createrepo -v /var/www/html/repo/
[root@serverX ~]# cp /home/student/RPM-GPG-KEY-student /var/www/html/repo/
```

Exemple de fichier de configuration yum

```
[example]
name=example
description=Example Yum Repository
baseurl=http://serverX.example.com/repo
enabled=1
gpgcheck=1
gpgkey=http://serverX.example.com/repo/RPM-GPG-KEY-student
```

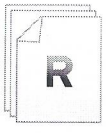
La ligne **gpgkey** peut également avoir l'aspect suivant, référençant un serveur FTP ou un fichier local:

```
gpgkey=ftp://serverX/pub/RPM-GPG-KEY-student
```

-OU-

```
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-student
```

Quel que soit votre choix, le fichier de clé GPG référencé est la clé publique correspondant à la clé GPG privée qui a été utilisée pour signer les packages dans le référentiel.



Références

Page man **createrepo**(8)



Exercice de Questionnaire

Créer un référentiel Yum - Questionnaire

1. Installez le package _____ si nécessaire.
2. Créez un répertoire pouvant être _____.
3. Créez un sous-répertoire appelé _____.
4. Copiez _____ à publier dans _____.
5. Exécutez _____ sur le répertoire de _____.



Test

Test de critère

Liste de contrôle des performances

Créer un RPM

- ☐ Téléchargez le fichier *ftp://instructor.example.com/pub/materials/hello.sh*.
- ☐ Créez un RPM simple qui installe **`hello.sh`** dans **`/root/bin`**. Veillez à ce que **`hello.sh`** soit installé avec le mode 755.
- ☐ Créez une clé GPG et signez le package avec la clé. Exportez la clé GPG publique.



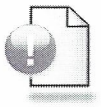
Note

Vous devez avoir une session graphique ouverte pour générer une clé GPG. **`gpg`** utilise maintenant une application graphique pour entrer et valider la clé.

- ☐ Déployez un serveur Web et créez un référentiel yum dans **`/var/www/html/Packages/`**. Créez un fichier de référentiel qui référence *http://serverX/Packages*. Servez la clé GPG à partir du serveur Web et incluez-la dans le fichier de référentiel.
- ☐ Installez votre rpm en utilisant le référentiel yum ci-dessus et exécutez **`/root/bin/hello.sh`**.



Notes personnelles



Résumé du module

Enregistrer un système avec Red Hat Network (RHN)

Dans cette section, vous avez appris à :

- Enregistrer un système avec Red Hat Network

Utilisation de référentiels tiers

Dans cette section, vous avez appris à :

- Gérer des fichiers de définition de référentiel dans **/etc/yum.repos.d/**

Utilisation de **yum**

Dans cette section, vous avez appris à :

- Répertorier les packages par nom, mot-clé ou fichier
- Obtenir la version et la description d'un package
- Installer, mettre à jour et supprimer des packages avec **yum**

Traitement de logiciels tiers

Dans cette section, vous avez appris à :

- Interroger des packages tiers à la recherche de fichiers avant l'installation
- Interroger le contenu du package rpm

Conception de packages RPM

Dans cette section, vous avez appris à :

- Utiliser **rpm** pour explorer la structure d'un fichier de package

Spécifications d'un package RPM

Dans cette section, vous avez appris à :

- Écrire un « fichier spec » pour créer un package logiciel RPM

Création et signature d'un package RPM

Dans cette section, vous avez appris à :

- Utiliser **rpmbuild** pour créer et signer un nouveau fichier de package RPM

Publier des packages RPM

Dans cette section, vous avez appris à :

- Créer votre propre référentiel **yum** pour déployer un petit nombre de fichiers de package



MODULE DEUX

GESTION DU RÉSEAU

Introduction

Sujets couverts dans cette unité :

- Utilisation d'outils de ligne de commande pour afficher des paramètres réseau
- Modification de paramètres réseau dans des fichiers de configuration
- Résolution des problèmes liés au réseau
- Configuration de plusieurs adresses IP sur une NIC unique
- Liaison Ethernet de deux cartes d'interface réseau ensemble
- Réglage de base de paramètres du noyau liés au réseau

Compréhension des fichiers de configuration réseau

Tandis que l'instructeur effectue une démonstration de la commande ou du fichier de configuration (ou à partir des notes qui suivent), remplissez le résumé ci-dessous concernant l'affichage et l'emplacement à partir duquel modifier la configuration réseau.

Catégorie de paramètre	*Affichage de la configuration actuelle*	*Modification de la configuration*
Adresse IP et masque de sous-réseau		
Routage/Passerelle par défaut		
Nom d'hôte du système		
Résolution de noms		

Tableau 2.1. Configuration réseau à partir de la ligne de commande

Noms d'interfaces réseau

Le noyau Linux nomme les interfaces en utilisant un préfixe spécifique au type d'interface. Par exemple, toutes les interfaces Ethernet commencent par **eth**, indépendamment du fabricant. Après le préfixe, chaque interface est numérotée, en commençant par zéro. Par exemple : **eth0**, **eth1** et **eth2** font référence à la première, seconde et troisième interfaces Ethernet. Les autres noms d'interface incluent **wlan0** pour le premier périphérique son fil, **virbr0** pour la passerelle interne configurée pour les hôtes virtuels, **bond0** pour le premier périphérique réseau associé, etc.

Configuration de l'interface réseau

/sbin/ip serre à afficher ou à modifier de manière temporaire des périphériques, le routage, le routage de stratégie et les tunnels.

```
[root@demo ~]# ip addr show eth0
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:00:00:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.250/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::5054:ff:fe00:fa/64 scope link
       valid_lft forever preferred_lft forever
[root@demo ~]# ip -s link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:00:00:fa brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    91449      520      0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    14020      99       0       0       0       0
[root@demo ~]# ip route
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.250  metric 1
default via 192.168.0.254 dev eth0  proto static
```



Note

ip -6 route affiche la table de routage IPv6.

Résolution du nom d'hôte

La commande **hostname** affiche ou modifie temporairement le nom d'hôte complet du système.

```
[root@demo ~]# hostname
demo.example.com
```

L'*interpréteur de stub* sert à convertir des noms d'hôte en adresses IP et vice versa. Le contenu du fichier **/etc/hosts** est vérifié en premier.

```
[root@demo ~]# cat /etc/hosts
192.168.0.250   demo.example.com        demo    # Added by NetworkManager
127.0.0.1       localhost.localdomain   localhost
::1             demo.example.com        demo    localhost6.localdomain6 localhost6
```

Si une entrée est introuvable dans ce fichier, l'interpréteur de stub recherche alors des informations à partir d'un serveur de noms DNS. Le fichier **/etc/resolv.conf** contrôle la formulation de cette requête :

- **nameserver** : adresse IP d'un serveur de noms à interroger. Trois directives de serveurs de noms maximum peuvent être attribuées pour fournir des sauvegardes, en cas de panne de l'un des serveurs.
- **search** : liste des noms de domaine à tester avec un nom d'hôte court. Cet élément et **domain** ne doivent pas être définisdans le même fichier ; si tel est le cas, la dernière instance prévaut. Consultez **resolv.conf**(5) pour plus de détails.

```
[root@demo ~]# cat /etc/resolv.conf
# Generated by NetworkManager
domain example.com
search example.com
nameserver 192.168.0.254
```

La commande **`getent hosts`** ***`hostname`*** peut servir à tester la résolution des noms d'hôte.

Modification de la configuration réseau

NetworkManager peut être installé sur Red Hat Enterprise Linux 6. Il est constitué d'un démon principal, d'une applet GNOME Notification Area qui fournit des informations d'état du réseau, ainsi que des outils de configuration graphiques qui peuvent créer, modifier et supprimer des connexions et des interfaces.

Pour modifier une interface eth0 gérée par NetworkManager afin qu'elle utilise une adresse IP statique au lieu de DHCP :

1. Cliquez avec le bouton droit de la souris sur l'icône NetworkManager dans le volet supérieur, puis sélectionnez **Modifier les connexions...**
2. Dans l'onglet **Câblé**, sélectionnez **Système eth0**, puis cliquez sur le bouton **Modifier...**
3. Sélectionnez l'onglet **Paramètres IPv4**
4. Dans le menu déroulant **Méthode**, passez de **Automatique (DHCP)** à **Manuel**
5. Sous **Adresses**, cliquez sur **Ajouter** et entrez l'adresse IPv4, le masque de réseau (selon la notation VLSN ou CIDR), le routeur de passerelle et le serveur DNS à utiliser
6. *IMPORTANT :* assurez-vous que l'option **Se connecter automatiquement** est activée, afin que l'interface démarre lors de l'initialisation (plutôt qu'à la connexion de l'utilisateur) et que l'option **Disponible à tous les utilisateurs** est activée pour une disponibilité au niveau du système
7. Cliquez sur **Appliquer** pour que vos modifications deviennent effectives.

Vous pouvez aussi configurer le réseau en modifiant les fichiers de configuration d'interface. Les fichiers de configuration d'interface gèrent les interfaces logicielles pour les périphériques réseau individuels. En général, ces fichiers sont nommés **`/etc/sysconfig/network-scripts/ifcfg-<name>`**, où <name> correspond au nom du périphérique géré par le fichier de configuration. Ci-dessous figurent des variables standard contenues dans le fichier utilisé pour la configuration statique ou dynamique.

Statique	*DHCP*	*Tous*
`BOOTPROTO=static`	`BOOTPROTO=dhcp`	`DEVICE=eth0`
`IPADDR=192.168.0.250`		`ONBOOT=yes`
`PREFIX=24`		`HWADDR=52:54:00:00:00:FA`
`GATEWAY=192.168.0.254`		`NM_CONTROLLED=yes`
`DNS1=192.168.0.254`		

Tableau 2.2. Options de configuration pour le fichier **`ifcfg`**



Note

Si vous devez configurer des routes statiques, la configuration est stockée par interface dans **/etc/sysconfig/network-scripts/route-<name>**. Pour plus d'informations, consultez le Manuel de déploiement de Red Hat Enterprise Linux ci-dessous.

/etc/sysconfig/network sert à spécifier le nom d'hôte complet et peut indiquer une route par défaut statique si DHCP n'est pas utilisé :

```
[root@demo ~]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=demo.example.com
GATEWAY=192.168.0.254
```

Comme nous l'avons vu précédemment, **/etc/resolv.conf** spécifie les adresses IP des serveurs DNS et du domaine de recherche.



Important

Si DHCP est utilisé, **/etc/resolv.conf** est automatiquement réécrit lors du démarrage des interfaces, sauf si vous spécifiez **PEERDNS=no** dans les fichiers de configuration d'interface pertinents.

Les interfaces réseau peuvent être arrêtées avec la commande **ifdown *eth0*** et réactivées avec la commande **ifup *eth0***, qu'elles soient gérées par NetworkManager ou par des fichiers de configuration non gérés.

Lors de la modification de la configuration du système, vous devez penser à :

1. Modifier un fichier de configuration
2. Redémarrer un service
3. Vérifier la modification



Références

Red Hat Enterprise Linux Deployment Guide
- Section 4.1: Fichiers de configuration réseau

Red Hat Enterprise Linux Deployment Guide
- Section 4.2: Fichiers de configuration d'interface

Red Hat Enterprise Linux Deployment Guide
- Section 4.4: Configuration de routes statiques

Red Hat Enterprise Linux Deployment Guide
- Chapitre 5: Configuration réseau

`/usr/share/doc/initscripts-*/sysconfig.txt`

Boîte à outils de résolution des problèmes

Indiquez comment TESTER, VÉRIFIER et CORRIGER chacune des catégories de résolution des problèmes liés au réseau ci-dessous, à partir de la liste de commandes qui suit.

Catégorie	*TEST*	*VÉRIFIER*	*CORRIGER*
Adresse IP et masque de sous-réseau	**ping** Accéder à un service	**ip addr**	Modifiez **ifcfg-***
Routage/Passerelle par défaut			
Résolution de noms			

Tableau 2.3. Résolution des problèmes réseau à partir de la ligne de commande

Commandes et fichiers utiles

- **ping**

```
[root@demo ~]# ping -c 2 instructor.example.com
PING instructor.example.com (192.168.0.254) 56(84) bytes of data.
64 bytes from instructor.example.com (192.168.0.254): icmp_seq=1 ttl=64 time=0.697 ms
64 bytes from instructor.example.com (192.168.0.254): icmp_seq=2 ttl=64 time=0.538 ms

--- instructor.example.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.538/0.617/0.697/0.083 ms
```

- **ip addr show eth0**

```
[root@demo ~]# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:00:00:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.250/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::5054:ff:fe00:fa/64 scope link
       valid_lft forever preferred_lft forever
```

- **/etc/sysconfig/network-scripts/ifcfg-<name>**

```
[root@demo ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="dhcp"
```

```
HWADDR="52:54:00:00:00:FA"
NM_CONTROLLED="yes"
ONBOOT="yes"
```

- **traceroute**

```
[root@demo ~]# traceroute -Tn www.redhat.com
traceroute to www.redhat.com (184.85.80.112), 30 hops max, 60 byte packets
 1  192.168.0.254  0.641 ms  0.606 ms  0.590 ms
 2  172.31.35.1  9.829 ms  9.531 ms  9.237 ms
 3  204.60.4.40  27.954 ms  27.726 ms  27.385 ms
 4  66.159.184.226  27.128 ms  49.156 ms  48.291 ms
 5  151.164.92.147  43.256 ms  42.995 ms  42.155 ms
 6  12.122.81.57  60.897 ms  60.041 ms  54.531 ms
 7  75.149.230.169  54.143 ms 75.149.231.45  46.412 ms 192.205.37.34  40.208 ms
 8  68.86.86.45  67.587 ms  54.599 ms  53.381 ms
 9  68.86.86.234  65.540 ms  62.189 ms  53.777 ms
10  68.86.87.166  57.084 ms  55.752 ms  57.154 ms
11  184.85.80.112  55.707 ms  58.702 ms  57.996 ms
```

- **ip route**

```
[root@demo ~]# ip route
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.250  metric 1
default via 192.168.0.254 dev eth0  proto static
```

- **host**

```
[root@demo ~]# host i
i.example.com is an alias for instructor.example.com.
instructor.example.com has address 192.168.0.254
```

- **dig**

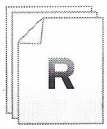
```
[root@demo ~]# dig i.example.com

; <<>> DiG 9.7.0-P2-RedHat-9.7.0-5.P2.el6 <<>> i.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17644
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;i.example.com.                 IN      A

;; ANSWER SECTION:
i.example.com.          86400   IN      CNAME   instructor.example.com.
instructor.example.com. 86400   IN      A       192.168.0.254

;; AUTHORITY SECTION:
example.com.            86400   IN      NS      instructor.example.com.

;; Query time: 2 msec
;; SERVER: 192.168.0.254#53(192.168.0.254)
;; WHEN: Mon Dec 13 15:50:21 2010
;; MSG SIZE  rcvd: 86
```

- **/etc/hosts**

```
[root@demo ~]# cat /etc/hosts
192.168.0.250 demo.example.com demo # Added by NetworkManager
127.0.0.1 localhost.localdomain localhost
::1 demo.example.com demo localhost6.localdomain6 localhost6
```

- **/etc/resolv.conf**

```
[root@demo ~]# cat /etc/resolv.conf
# Generated by NetworkManager
domain example.com
search example.com
nameserver 192.168.0.254
```



Références

Red Hat Enterprise Linux Deployment Guide
- Chapitre 4 : Interfaces réseau

Red Hat Enterprise Linux Deployment Guide
- Chapitre 5 : Configuration réseau

Configuration de l'interface réseau - Alias IP

L'attribution de plusieurs adresses IP à une interface unique est appelée définition d'alias. Cela se révèle utile dans certaines situations, comme avec l'hébergement Web où une machine unique peut exécuter différents services ou sites sur différentes adresses IP. DHCP ne prend pas en charge les alias.



Important

Dans ce ce cours, il est recommandé de désactiver NetworkManager lors de la configuration d'alias et de liaisons. NetworkManager prend en charge plusieurs adresses IP d'une manière qui empêche la compatibilité ascendante avec d'anciennes configurations d'alias réseau, comme celle de Red Hat Enterprise Linux 5. Actuellement, NetworkManager ne fonctionne pas avec une liaison NIC. Ces deux limitations devraient être résolues ultérieurement.

Pour plus d'informations sur la nouvelle méthode de configuration de plusieurs adresses IP de façon durable, consultez `http://live.gnome.org/NetworkManager/SystemSettings#ifcfg-rh`.

L'ajout d'un alias IP comporte trois étapes de base :

1. Désactivez NetworkManager de façon durable

```
[root@demo ~]# service NetworkManager stop ; chkconfig NetworkManager off
Stopping NetworkManager daemon:                            [  OK  ]
```

2. Ajoutez un alias de façon interactive

```
[root@demo ~]# ip addr add 10.1.1.250/24 dev eth0 label eth0:0
[root@demo ~]# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen
 1000
    link/ether 52:54:00:00:00:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.250/24 brd 192.168.0.255 scope global eth0
    inet 10.1.1.250/24 scope global eth0:0
    inet6 fe80::5054:ff:fe00:fa/64 scope link
       valid_lft forever preferred_lft forever
```

   Ajoutez de façon durable un alias en créant **`/etc/sysconfig/network-scripts/ifcfg-eth0:0`** avec le contenu suivant :

```
DEVICE=eth0:0
IPADDR=10.1.1.250
PREFIX=24
ONPARENT=yes
```

3. Relancez le service **`network`**.

```
[root@demo ~]# service network restart
Shutting down interface eth0:                              [  OK  ]
```

```
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0... done.
                                                           [  OK  ]
```



Important

Évitez d'utiliser la commande **ifconfig**, obsolète. Si un système dispose d'adresses IP secondaires du nouveau style sur une interface ne bénéficiant pas d'une étiquette d'alias IP de compatibilité ascendante, **ifconfig** n'affiche pas la ou les adresses secondaires. Utilisez plutôt la commande **ip addr**.



Références

Red Hat Enterprise Linux Deployment Guide

- Section 4.2.3: Fichiers d'alias et de clone

/usr/share/doc/initscripts-*/sysconfig.txt

> Paramères sytème de Network Manager
> http://live.gnome.org/NetworkManager/SystemSettings#ifcfg-rh

Configuration de l'interface réseau - Liaison

Red Hat Enterprise Linux permet aux administrateurs d'associer plusieurs interfaces réseau entre elles au sein d'un canal unique, à l'aide du module du noyau **bonding** et d'une interface réseau spéciale, appelée interface de liaison (ou interface bonding) de canal. La liaison de canaux permet à deux interfaces réseau ou plus d'agir comme une seule, en augmentant la bande passante et/ou en fournissant une redondance, en fonction du mode de liaison choisi.

Identification physique d'une NIC

Lors de l'utilisation de plusieurs cartes réseau, il est utile de pouvoir identifier physiquement chaque carte réseau. Une méthode d'identification physique d'une NIC consiste à entraîner le clignotement d'une ou de plusieurs de ses DEL. Afin que les DEL clignotent sur **eth0** pendant 30 secondes, exécutez **ethtool -p eth0 30**.

Modes de liaison Ethernet Linux sélectionnés

- Mode 0 (équilibre circulaire) - Stratégie circulaire, toutes les interfaces sont utilisées. Les paquets sont transmis de manière circulaire à travers l'ensemble des esclaves; n'importe quel esclave peut les recevoir.
- Mode 1 (sauvegarde active) - À tolérance de pannes. Une seule interface esclave est utilisée à la fois, mais en cas d'échec, une autre prend le relais.
- Mode 3 (diffusion) - À tolérance de pannes. Tous les paquets sont diffusés depuis l'ensemble des interfaces esclaves.

Le fichier **networking/bonding.txt** de documentation du noyau contient la description des autres modes de liaison.

Exemple de configuration de sauvegarde active

- **/etc/sysconfig/network-scripts/ifcfg-bond0**

  Ce fichier configure les informations réseau pour les interfaces liées, comme s'il s'agissait d'un fichier d'interface réseau normal:

```
DEVICE=bond0
IPADDR=10.1.1.250
PREFIX=24
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
BONDING_OPTS="mode=1 miimon=50"
```

- **/etc/sysconfig/network-scripts/ifcfg-<name>**

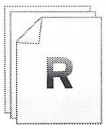
  Chaque interface esclave *<name>* nécessite un fichier contenant la configuration suivante:

```
DEVICE=<name>
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
```

```
SLAVE=yes
USERCTL=no
```

- **/etc/modprobe.d/bonding.conf**

```
alias bond0 bonding
```



Références

Red Hat Enterprise Linux Deployment Guide
- Section 4.2.2 : Interfaces de liaison de canaux

Red Hat Enterprise Linux Deployment Guide
- Section 22.7.2 : Utilisation de la liaison de canaux

/usr/share/doc/kernel-*/Documentation/networking/bonding.txt



Exercice de Questionnaire

Configuration avancée de l'interface réseau - Questionnaire

1. Quel mode de liaison Linux Ethernet utilise principalement une interface esclave et change d'interface en cas d'échec ?

   (sélectionnez une des réponses suivantes...)
   a. Mode 0 (balance-rr)
   b. Mode 1 (active-backup)
   c. Mode 3 (broadcast)

2. Quelle liaison Linux Ethernet utilise toutes les interfaces à tour de rôle pour obtenir plus de capacité ?

   (sélectionnez une des réponses suivantes...)
   a. Mode 0 (balance-rr)
   b. Mode 1 (active-backup)
   c. Mode 3 (broadcast)

3. Lors de la création d'une interface réseau liée, quel fichier de configuration contient les définitions d'adresse IP et de masque de réseau pour l'interface ?

   (sélectionnez une des réponses suivantes...)
   a. **`/etc/sysconfig/network`**
   b. **`/etc/sysconfig/network-scripts/ifcfg-bond0`**
   c. **`/etc/sysconfig/network-scripts/ifcfg-`*`iface`***
   d. Aucune des propositions ci-dessus

4. Lors de la création d'une interface réseau liée, quel fichier de configuration définit le type de la liaison ?

   (sélectionnez une des réponses suivantes...)
   a. **`/etc/sysconfig/network`**
   b. **`/etc/sysconfig/network-scripts/ifcfg-bond0`**
   c. **`/etc/sysconfig/network-scripts/ifcfg-`*`iface`***
   d. Aucune des propositions ci-dessus

5. Lors de la création d'une interface réseau liée, quelles définitions de variable doivent être spécifiées dans le fichier de configuration **`/etc/sysconfig/network-scripts/ifcfg-`*`iface`*** ?

   (sélectionnez une des réponses suivantes...)
   a. **`GATEWAY`**
   b. **`IPADDR`**
   c. **`MASTER`**

d. Aucune des propositions ci-dessus

Réglage des paramètres du noyau

Les paramètres du noyau fournissent un mécanisme permettant de régler le fonctionnement du noyau Linux. En général, lorsqu'un développeur de noyau sélectionne une constante arbitraire ou implémente des fonctionnalités qui ne sont pas forcément voulues, vous pouvez utiliser **sysctl** pour les ajuster. Les paramètres les plus utiles sont répertoriés en ligne, dans **kernel-doc**, dans ce cours, ou dans d'autres formations de Red Hat.

Ces paramètres peuvent être affichés ou définis via l'arborescence du répertoire **/proc/sys/** ou la commande **sysctl**.

Recherche et apprentissage du réglage du noyau

L'objectif est d'apprendre à régler la réponse du noyau au ping, à l'écho ICMP ou aux requêtes.

Étudiez la commande **sysctl** et parcourez la documentation du noyau à la recherche de paramètres du noyau pertinents, puis répondez aux questions contenues dans votre classeur. Consignez les étapes pour mener à bien les tâches suivantes:

1. Installez RPM **kernel-doc** s'il n'est pas déjà installé.

   ```
   [root@demo ~]# yum -y install kernel-doc
   ```

2. Comment utiliseriez-vous **sysctl** pour identifier des paramètres du noyau qui contrôlent le comportement du ping ou de l'écho ICMP ?

   ```
   [root@demo ~]# sysctl -a | grep icmp
   ```

3. Quels paramètres semblent prometteurs ?

   net.ipv4.icmp_echo_ignore_all ou **net.ipv4.icmp_echo_ignore_broadcasts**

4. Quelle commande utiliseriez-vous pour identifier et/ou examiner une documentation de noyau décrivant la fonction de ces paramètres ?

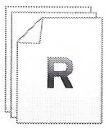
   ```
   [root@demo ~]# grep -A5 icmp /usr/share/doc/kernel-doc-*/Documentation/networking/ip-
   sysctl.txt
   ```

5. De quelle manière utiliseriez-vous **sysctl** pour régler des paramètres de noyau, afin de « masquer » votre système par rapport aux requêtes ping ?

   ```
   [root@demo ~]# sysctl -w net.ipv4.icmp_echo_ignore_all=1
   ```

6. Comment configureriez-vous **sysctl** pour régler de façon durable les paramètres du noyau, afin qu'ils survivent à un redémarrage ?

   ```
   [root@demo ~]# echo "net.ipv4.icmp_echo_ignore_all = 1" >> /etc/sysctl.conf
   ```



Références

Red Hat Enterprise Linux Deployment Guide
- Section 19.3.9.4 : /proc/sys/net/

Red Hat Enterprise Linux Deployment Guide
- Section 19.4 Utilisation de la commande sysctl

/usr/share/doc/kernel-doc-*/Documentation/sysctl/

/usr/share/doc/kernel-doc-*/Documentation/networking/ip-sysctl.txt

Page man **sysctl**(8)



Exercice de Liste de contrôle des performances

Activer la diffusion de ping

La configuration par défaut pour Red Hat Enterprise Linux 6 configure le noyau de manière à ignorer les requêtes de diffusion de ping. Vous collaborerez avec un partenaire pour régler le noyau sur serverX, afin qu'il réponde à ces requêtes.

- ☐ Recherchez un partenaire avec lequel collaborer. En cas de nombre impair d'étudiants, l'un des groupes sera composé de trois personnes.
- ☐ Envoyez un ping diffusé sur le réseau 192.168.0.0/24. Notez les hôtes qui répondent à la requête de ping.

```
[root@serverX ~]# ping -b 192.168.0.255
```

- ☐ Réglez serverX afin qu'il réponde aux diffusions de ping.

```
[root@serverX ~]# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=0
```

- ☐ Envoyez un ping autre diffusé sur le réseau 192.168.0.0/24. Vos hôtes ont-ils répondu ?

```
[root@serverX ~]# ping -b 192.168.0.255
```

- ☐ Configurez vos machines serverX de façon durable, de manière à ce qu'elles répondent aux diffusions de ping et redémarrent.

```
[root@serverX ~]# echo "net.ipv4.icmp_echo_ignore_broadcasts = 0" >> /etc/
sysctl.conf
[root@serverX ~]# reboot
```

- ☐ Envoyez une autre diffusion de ping. Vos modifications de ping ont-elles été conservées après le redémarrage ?

```
[root@serverX ~]# ping -b 192.168.0.255
```



Test

Test de critère 1

Étude de cas

Routage du trafic réseau : OSHU (Operation Strategic Holistic Unusual)

Avant de commencer...

Exécutez le script **`lab-setup-oshu`** sur desktopX.

Operation Strategic Holistic Unusual (ou OSHU) est un système de discussion en ligne pour les fans de complots à déjouer. Deux conditions sont requises pour rejoindre le site, elles sont indiquées ci-dessous.

1. Pour remplir la première condition, vous devez prouver que vous êtes capable de faire « disparaître » un serveur. Pour cela, vous devez modifier la configuration sur serverX pour qu'il ne réponde pas aux requêtes ping. Rendez cette modification permanente pour qu'elle soit toujours effective après chaque redémarrage.

2. La seconde condition est de rejoindre le réseau OSHU « secret ». Pour rejoindre le réseau, ajoutez une adresse IP supplémentaire à serverX, X correspondant au numéro de votre bureau/serveur :

   10.42.10.X/24

Lorsque c'est fait, exécutez **`lab-grade-oshu`** sur desktopX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Test

Test de critère 2

Exercice

Résolution des problèmes de configuration réseau à partir de la ligne de commande

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Toutes les opérations suivantes doivent être effectuées sur votre serveur virtuel, serverX. Vous commencez par exécuter un script qui « casse » la configuration réseau. Vous avez cinq minutes pour résoudre chacun des deux problèmes. Veillez à documenter vos découvertes, car nous effectuerons une analyse à la fin de l'exercice.

Les paramètres réseau pour serverX sont indiqués ci-dessous :

```
IP Address: 192.168.0.X+100
Netmask:  255.255.255.0  (/24)
DNS Server: 192.168.0.254
Default Gateway: 192.168.0.254
```

1. Exécutez le premier script pour effectuer une mauvaise configuration de votre mise en réseau :

   `lab-break-net 1`

2. Symptôme : un navigateur Web ne peut pas accéder à la page Web de l'adresse `http://instructor.remote.test`

3. Appliquez les étapes : TESTER, VÉRIFIER, CORRIGER pour identifier et résoudre le problème.

4. Documentez vos découvertes

   Utilisez cet espace pour vos notes.

5. Exécutez le deuxième script pour effectuer une mauvaise configuration de votre mise en réseau

   `lab-break-net 2`

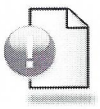
6. Symptôme : un navigateur Web ne peut pas accéder à la page Web de l'adresse `http://instructor.remote.test`

7. Appliquez les étapes : TESTER, VÉRIFIER, CORRIGER pour identifier et résoudre le problème.
8. Documentez vos découvertes

   Utilisez cet espace pour vos notes.



Notes personnelles



Résumé du module

Compréhension des fichiers de configuration réseau

Dans cette section, vous avez appris à :

- Modifier la configuration réseau avec des outils de ligne de commande
- Assurer la persistance des modifications apportées à la configuration réseau en modifiant des fichiers

Boîte à outils de résolution des problèmes

Dans cette section, vous avez appris à :

- Résolution des problèmes de base liés au réseau

Configuration de l'interface réseau - Alias IP

Dans cette section, vous avez appris à :

- Configurez manuellement plusieurs adresses IP sur une carte réseau

Configuration de l'interface réseau - Liaison

Dans cette section, vous avez appris à :

- Combiner deux interfaces réseau au sein d'une interface associée

Réglage des paramètres du noyau

Dans cette section, vous avez appris à :

- Modifier les paramètres de réglage du noyau qui affectent les paramètres du réseau



MODULE TROIS

GESTION DU STOCKAGE

Introduction

Sujets couverts dans cette unité :

- Création et formatage de partitions de disque simples avec un système de fichiers
- Activation de la confidentialité des données avec une partition chiffrée
- Création et formatage d'une partition de disque simple en tant qu'espace swap
- Connexion à une cible iSCSI distante et utilisation de celle-ci comme stockage

Partitions simples et systèmes de fichiers

Le stockage est un besoin de base de chaque système informatique. Red Hat Enterprise Linux inclut des outils puissants permettant de gérer un grand nombre de types de périphériques de stockage dans différents scénarios.

fdisk est un utilitaire permettant de gérer des partitions de disque. Vous pouvez afficher les disques et leurs partitions en exécutant l'utilitaire avec l'option **-l** et le nom du disque (**fdisk -cul /dev/vda**) Les modifications peuvent être apportées en exécutant l'utilitaire de manière interactive et en sélectionnant des options de menu appropriées (**fdisk -cu /dev/vda**). **-c** désactive le mode de compatibilité DOS hérité et **-u** affiche la sortie par secteurs (et non par cylindres, obsolètes).



Important

Red Hat Enterprise Linux 6 aligne automatiquement la première partition de manière à ce qu'elle commence au secteur 2048 au lieu du secteur 63 (le début « traditionnel » du cylindre 1). Cela afin d'assurer des performances maximales sur les nouveaux disques durs à secteurs de 4 KiB ainsi que sur les disques durs hérités à secteurs de 512 octets. De plus, cela est compatible avec le comportement des autres systèmes d'exploitation récents qui utilisent le schéma de partitionnement MBR. Un mauvais alignement des partitions peut entraîner une perte importante de performances, par conséquent procédez avec précaution lorsque vous ajustez ces paramètres.

Pour votre serveur virtuel, **serverX**, vérifiez la configuration actuelle du stockage. Recherchez des informations dans la sortie de la commande suivante: **fdisk -cul /dev/vda**

Disque principal:

1. Nom: **/dev/vda**
2. Taille: **6442 MB**
3. Nombre total de secteurs: **12582912**
4. Dernier secteur utilisé: **9914367**

```
[root@serverX ~]# fdisk -cul
Disk /dev/vda❶: 6442 MB❷, 6442450944 bytes
16 heads, 63 sectors/track, 12483 cylinders, total 12582912 sectors❸
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000a9b12

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048      526335      262144   83  Linux
/dev/vda2          526336     9914367❹    4694016   8e  Linux LVM
```

1. Nom du disque
2. Taille totale du disque
3. Nombre total de secteurs
4. Dernier secteur utilisé

Créer une nouvelle partition

```
[root@serverX ~]# fdisk -cu /dev/vda
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First sector (9914368-12582911, default 9914368):  Enter
Using default value 9914368
Last sector, +sectors or +size{K,M,G} (9914368-12582911, default 12582911): +1G

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@serverX ~]# reboot
```

Comparaison des systèmes de fichiers

- **ext4** est le système de fichiers standard pour Red Hat Enterprise Linux. Il est très robuste, fiable et dispose de nombreuses fonctions permettant d'améliorer les performances des charges de travail modernes.
- **ext2** est un système de fichiers plus ancien, généralement utilisé sous Linux : il est simple, fiable et fonctionne bien pour les petits périphériques de stockage, mais n'est pas aussi efficace que **ext4**.
- Le support **vfat** prend en charge une famille de systèmes de fichiers liés (VFAT/FAT16, FAT32), développée pour d'anciennes versions de Microsoft Windows et prise en charge sur une vaste gamme de systèmes et de périphériques.

Création et utilisation d'un nouveau système de fichiers

1. **mkfs -t *filesystem* /dev/*partition*** crée le type de système de fichiers requis.
2. **blkid** affiche les informations sur le contenu des périphériques de bloc (partitions et volumes logiques), y compris l'UUID du système de fichiers.
3. **mkdir */mountpoint*** crée un répertoire auquel le nouveau système de fichiers doit être connecté.
4. Ajoutez une entrée à **/etc/fstab** en utilisant l'UUID obtenu avec la commande **blkid** :

```
UUID=uuid  /mountpoint  ext4  defaults  1 2
```

5. Montez le nouveau système de fichiers avec **mount** ***/mountpoint***.



Avertissement

Lorsque vous ajoutez de nouveaux systèmes de fichiers à **/etc/fstab**, vous devez utiliser **blkid** pour déterminer leur UUID et procéder à leur montage par UUID. Il est *déconseillé* de monter des systèmes de fichiers sur des partitions simples par nom de service standard (tel que **/dev/sda3**). Les noms des périphériques de disque peuvent changer selon les périphériques visibles au démarrage. Votre système risque alors de monter le système de fichiers incorrect pour le mauvais objectif, ce qui peut entraîner au pire la perte de données. Cela est surtout important lorsque des périphériques SAN (iSCSI, Fiber Channel) sont impliqués, ce qui peut être détecté par le système dans un ordre différent d'un démarrage à un autre selon le trafic SAN, mais aussi quand des supports amovibles tels que des périphériques USB sont utilisés.

Notez que Red Hat Enterprise Linux 6 utilise UUID au lieu de LABEL dans **/etc/fstab** pour réduire les risques de conflits de noms. Le programme d'installation n'utilise plus **e2label** pour définir des étiquettes sur les systèmes de fichiers RHEL 6 par défaut.

Exemple de création d'un système de fichiers

```
[root@serverX ~]# mkfs -t ext4 /dev/vda3
[root@serverX ~]# blkid /dev/vda3
/dev/vda3: UUID="a11fadb0-2f5b-49e8-ba43-13de7990d3b9" TYPE="ext4"
[root@serverX ~]# mkdir /test
```

Ajoutez une entrée à **/etc/fstab**:

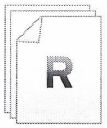
```
UUID="a11fadb0-2f5b-49e8-ba43-13de7990d3b9"  /test  ext4  defaults  1 2
```

Testez le montage:

```
[root@serverX ~]# mount /test
```

Suppression d'un système de fichiers existant

1. Démontez le système de fichiers en utilisant **umount** ***/mountpoint***.
2. Supprimez l'entrée correspondante dans **/etc/fstab**.
3. Supprimez le répertoire du point de montage: **rmdir** ***/mountpoint***.



Références

Pages manuel **fdisk**(8), **fstab**(5), **mkfs**(8), **blkid**(8), **partprobe**(8), **mount**(8)

> Base de connaissances : "How can I create a disk partition on a disk that is greater than 2 TB in size?"
> https://access.redhat.com/kb/docs/DOC-4282



Exercice de Questionnaire

Ajouter un nouveau système de fichiers

1. Identifiez un disque qui comporte de l'espace libre

2. Créez une nouvelle partition sur ce disque

3. Mettez à jour la table de partition du noyau

4. Créez un système de fichiers sur la partition

5. Ajoutez une entrée au fichier de la table du système de fichiers

6. Créez un point de montage

7. Montez le système de fichiers

Activation de la confidentialité des données avec le chiffrement des partitions

LUKS ("Linux Unified Key Setup") est un format standard de chiffrement des périphériques: LUKS chiffre la partition ou le volume: le volume doit être déchiffré pour que le système de fichiers qu'il contient puisse être monté.

Créer un nouveau fichier chiffré

1. Créez une nouvelle partition avec **fdisk**
2. **cryptsetup luksFormat /dev/*vdaN*** chiffre la nouvelle partition et définit le mot de passe de déchiffrement
3. **cryptsetup luksOpen /dev/*vdaN name*** déverrouille le volume chiffré /dev/*vdaN* en tant que **/dev/mapper/*name*** une fois que vous avez saisi le mot de passe de déchiffrement correct.
4. Créez un système de fichiers **ext4** sur le volume chiffré:**mkfs -t ext4 /dev/mapper/*name***
5. Créez le point de montage du répertoire et montez le système de fichiers: **mkdir /secret ; mount /dev/mapper/*name* /secret**
6. Lorsque vous avez terminé, démontez **umount /dev/mapper/*name*** et exécutez **cryptsetup luksClose *name*** pour verrouiller le volume chiffré

Monter la partition chiffrée de manière permanente

1. **/etc/crypttab** contient une liste de périphériques à déverrouiller pendant le démarrage du système.

```
❶name ❷/dev/vdaN ❸/path/to/password/file
```

/etc/crypttab répertorie un périphérique par ligne, avec les champs suivants séparés par des espaces:

❶ Nom que le mappeur de périphériques utilisera pour le périphérique
❷ Périphérique « verrouillé » sous-jacent
❸ Fichier de mot de passe à utiliser pour déverrouiller le périphérique. Si ce champ reste vide (ou s'il est défini sur **none**), l'utilisateur devra fournir le mot de passe de déchiffrement lors du démarrage

2. Créez une entrée dans **/etc/fstab**, similaire à l'exemple suivant:

```
/dev/mapper/name  /secret  ext4  defaults  1 2
```



Avertissement

Le périphérique répertorié dans le premier champ de **/etc/fstab** doit correspondre au nom choisi comme nom local à mapper dans **/etc/crypttab**. *Il s'agit d'une erreur de configuration commune.*

3. Créez le fichier de clé comprenant le mot de passe. Assurez-vous que son propriétaire est le super utilisateur (root) et que le mode utilisé est 600. Ajoutez la clé pour LUKS à l'aide de la commande suivante :

```
[root@serverX ~]# cryptsetup luksAddKey /dev/vdaN /path/to/password/file
```

Exemple de création d'un système de fichiers chiffré

Créer une nouvelle partition comme précédemment. Nous supposerons que le périphérique est **/dev/vda5**.

```
[root@serverX ~]# cryptsetup luksFormat /dev/vda5
WARNING!
========
This will overwrite data on /dev/vda5 irrevocably.

Are you sure? (Type uppercase yes): YES
Enter LUKS passphrase: testing123
Verify passphrase: testing123
[root@serverX ~]# cryptsetup luksOpen /dev/vda5 encdisk
Enter passphrase for /dev/vda5: testing123
[root@serverX ~]# mkfs -t ext4 /dev/mapper/encdisk
[root@serverX ~]# mkdir /encdisk
[root@serverX ~]# mount /dev/mapper/encdisk /encdisk
```

Pour que le disque soit persistant, commencez par ajouter ce qui suit à **/etc/fstab**:

```
/dev/mapper/encdisk  /encdisk  ext4  defaults  1 2
```

Créez **/etc/crypttab** et ajoutez la ligne suivante. Le mot de passe sera alors demandé à chaque fois que la machine démarre :

```
encdisk  /dev/vda5
```

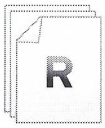
Entrée automatique du mot de passe de chiffrement

Si vous souhaitez que le démarrage soit automatisé, vous devez placer le mot de passe dans un fichier texte (pour des raisons de sécurité évidentes).

/etc/crypttab:

```
encdisk  /dev/vda5 /root/encdisk
```

```
[root@serverX ~]# echo "testing123" > /root/encdisk
[root@serverX ~]# chown root /root/encdisk
[root@serverX ~]# chmod 600 /root/encdisk
[root@serverX ~]# cryptsetup luksAddKey /dev/vda5 /root/encdisk
Enter any passphrase: testing123
```



Références

Pages man **cryptsetup**(8) et **crypttab**(5)



Exercice de Exercice de reclassement

Création d'un système de fichiers chiffré

Pour chaque nom de fichier ou répertoire ci-dessous, écrivez le numéro de sa définition dans la liste du bas.

__ Créez une nouvelle partition

__ Créer un système de fichiers **ext4**

__ Formater la nouvelle partition pour le chiffrement

__ Monter le système de fichiers sur le périphérique déverrouillé

__ Créer une entrée dans **/etc/fstab**

__ Créer un répertoire à utiliser comme point de montage

__ Déverrouiller la partition chiffrée

__ Créer une entrée dans **/etc/crypttab**

__ Informer LUKS de la présence du fichier de mot de passe

1. 1. **fdisk**
2. 2. **cryptsetup luksFormat /dev/vda*N***
3. 3. **cryptsetup luksOpen /dev/vda*N* *secret***
4. 4. **mkfs -t ext4 /dev/mapper/*secret***
5. 5. **mkdir /secret**
6. 6. **mount /dev/mapper/*secret* /secret**
7. 7. ***secret* /dev/vda*N* */password/file***
8. 8. **/dev/mapper/*secret* /secret ext4 defaults 1 2**
9. 9. **cryptsetup luksAddKey /dev/vda*N* */password/file***

Gestion de l'espace swap

L'espace swap ou zone swap est l'espace du disque utilisé comme espace de débordement pour des parties de mémoire qui ne sont pas utilisées. Il permet au système de libérer de l'espace dans la mémoire principale pour les données en cours de traitement et fournit un espace de débordement d'urgence si le système risque de manquer d'espace dans la mémoire principale.

Création et utilisation d'une partition swap supplémentaire

1. Créez une partition à l'aide de **fdisk**. *En outre*, changez le type de la partition et définissez-le sur « **0x82 Linux Swap** » avant d'enregistrer les modifications avec **fdisk**.
2. **mkswap /dev/*vdaN*** prépare la partition en vue de son utilisation comme espace swap.
3. **blkid /dev/*vdaN*** détermine l'UUID.
4. Ajoutez le nouvel espace swap à **/etc/fstab**:

   ```
   UUID=uuid  swap  swap  defaults 0 0
   ```

5. **swapon -a** active la nouvelle zone swap.

   swapon -s indique le statut des zones swap actuelles.

   swapoff /dev/*vdaN* désactive cette zone swap précise.

Exemple de création d'un espace swap

Créez une nouvelle partition et définissez son type sur 82:

```
[root@serverX ~]# fdisk /dev/vda
Command (m for help): n
First sector (12539904-12582911, default 12539904):  Enter
Using default value 12539904
Last sector, +sectors or +size{K,M,G} (12539904-12582911, default 12582911):  Enter
Using default value 12582911

Command (m for help): t
Partition number (1-6): 6
Hex code (type L to list codes): 82
Changed system type of partition 6 to 82 (Linux swap / Solaris)

Command (m for help): w

[root@serverX ~]# reboot
```

Inscrivez la signature swap sur le périphérique et recherchez l'UUID:

```
[root@serverX ~]# mkswap /dev/vda6
[root@serverX ~]# blkid /dev/vda6
/dev/vda6: UUID="4903c440-ffcb-4404-bc09-505c79c7a412" TYPE="swap"
```

Ajoutez une entrée à **/etc/fstab**:

```
UUID="4903c440-ffcb-4404-bc09-505c79c7a412"  swap  swap  defaults  0 0
```

Activez l'espace swap, vérifiez qu'il est disponible et désactivez l'espace swap :

```
[root@serverX ~]# swapon -a
swapon -s
/dev/dm-0                               partition       557048  0       -1
/dev/vda6                               partition       21496   0       -2
[root@serverX ~]# swapoff /dev/vda6
```

Le dimensionnement de l'espace swap total doit être basé sur la charge de travail de la mémoire sur le système et non sur la quantité totale de mémoire physique présente. Cependant, le tableau ci-dessous indique des règles générales pour dimensionner l'espace swap. Pour plus d'instructions sur le dimensionnement de l'espace swap, consultez l'article de la base de connaissances dans les références.

RAM système	*Espace swap minimal recommandé*
jusqu'à 4 Go	au moins 2 Go
4 Go à 16 Go	au moins 4 Go
16 Go à 64 Go	au moins 8 Go
64 Go à 256 Go	au moins 16 Go

Tableau 3.1. Instructions de base sur le dimensionnement de l'espace swap



Références

Base de connaissances : "If I add several hundred GB of RAM to a system, do I really need several hundred GB of swap space?"
https://access.redhat.com/kb/docs/DOC-15252

Pages man **mkswap** et **swapon**



Exercice de Exercice

Créer et utiliser une nouvelle partition swap.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Créez et utilisez une nouvelle partition swap de 256 Mo sur votre serveur virtuel serverX.

1. Démarrez **`fdisk`** et créez une nouvelle partition



Important

Veillez à créer une partition étendue au préalable afin d'avoir de l'espace pour créer des partitions supplémentaires ultérieurement.

2. Changez le type de partition sur **`swap`**.
3. Préparez la nouvelle partition pour l'utilisation comme swap
4. Déterminez l'UUID
5. Ajoutez la nouvelle partition à **`/etc/fstab`**
6. Déterminez la quantité actuelle de swap
7. Activez le nouveau swap
8. Vérifiez le nouveau swap activé

Accès au stockage iSCSI

iSCSI (Internet SCSI) prend en charge l'envoi de commandes SCSI par les clients (initiateurs) via IP aux périphériques de stockage SCSI (cibles) sur des serveurs distants. Un nom complet iSCSI est utilisé pour identifier les initiateurs et les cibles. Il suit le format suivant : **`iqn.yyyy-mm.{reverse domain}:label`**. La communication réseau par défaut s'effectue en texte clair sur le port 3260/tcp de la cible iSCSI.

- Initiateur iSCSI : client devant accéder à un stockage SAN brut
- Cible iSCSI : disque dur distant présenté à partir d'un serveur iSCSI ou « portail cible »
- Portail cible iSCSI : serveur qui fournit des cibles sur le réseau à un initiateur
- IQN : « iSCSI Qualified Name » (nom complet iSCSI). Chaque initiateur et chaque cible ont besoin d'un nom unique les identifiant ; il est conseillé d'utiliser un nom qui soit unique sur Internet.



Avertissement

Si vous autorisez deux initiateurs à se connecter simultanément à la même cible iSCSI (disque dur distant), il est important de ne pas les autoriser à monter simultanément le même système de fichiers à partir de la même cible. À moins, qu'un système de fichiers en cluster tel que GFS2 soit utilisé, vous risquez d'endommager le système de fichiers.

Pour accéder à une nouvelle cible avec un initiateur iSCSI :

- Installez le logiciel initiateur iSCSI : *iscsi-initiator-utils*
- Définissez l'IQN de l'initiateur dans **`/etc/iscsi/initiatorname.iscsi`**

  (En général, une étiquette unique dans un espace de noms correspondant à un nom DNS contrôlé par l'organisation. L'IQN est défini de façon aléatoire lorsque *iscsi-initiator-utils* est installé.)

- Détectez les cibles iSCSI fournies par le serveur iSCSI (portail cible)

```
iscsiadm -m discovery -t st -p 192.168.0.254
```

- Connectez-vous à l'une des cibles iSCSI ou à plusieurs sur le serveur

```
iscsiadm -m node -T iqn.2010-09.com.example:rdisks.demo -p 192.168.0.254 -l
```

- Identifiez le périphérique qui est la cible iSCSI

  Examinez la sortie de **`dmesg`** ou **`tail /var/log/messages`** ou regardez vers quoi pointent les symlinks iscsi avec **`ls -l /dev/disk/by-path/*iscsi*`**.

- À ce stade, le disque iSCSI peut être utilisé comme disque dur local.

Les systèmes de fichiers existants peuvent être montés. Si le disque n'est pas formaté, il peut être partitionné avec **fdisk** et les partitions doivent être formatées avec un système de fichiers ou en tant que volume physique LVM, par exemple.



Important

Pour monter un système de fichiers de manière permanente sur une cible iSCSI dans **/etc/fstab**:

1. Utilisez **blkid** pour déterminer l'UUID du système de fichiers et montez ce dernier en utilisant l'UUID et non le nom de périphérique**/dev/sd***. (Le nom du périphérique peut être différent d'un démarrage à un autre selon l'ordre dans lequel les périphériques iSCSI répondent sur le réseau. Le périphérique incorrect peut être utilisé si le montage s'effectue à partir du nom de périphérique.)
2. Utilisez **_netdev** comme option de montage dans **/etc/fstab**. (Cela empêche le client de tenter de monter le système de fichiers avant d'avoir activé la connexion réseau. Autrement, le système affichera des messages d'erreur au démarrage.)
3. Assurez-vous que les services **iscsi** et **iscsid** seront lancés au démarrage du système.

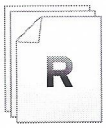
Pour interrompre l'utilisation d'une cible iSCSI:

- Assurez-vous qu'aucun des périphériques fournis par la cible n'est en cours d'utilisation.
- Assurez-vous que toutes les références permanentes devant utiliser la cible sont supprimées des emplacements tels que **/etc/fstab**.
- Déconnectez-vous de la cible iSCSI pour vous déconnecter temporairement.

```
iscsiadm -m node -T iqn.2010-09.com.example:rdisks.demo -p 192.168.0.254 -u
```

- Supprimez l'enregistrement local de la cible iSCSI pour vous déconnecter de façon permanente.

```
iscsiadm -m node -T iqn-2010-09.com.example:rdisks.demo -p 192.168.0.254 -o delete
```



Références

Red Hat Enterprise Linux Storage Administration Guide

- Chapitre 21: Gestion du stockage en ligne

/usr/share/doc/iscsi-initiator-utils-*/README

> Base de connaissances: "Can I put a swap device or file on iSCSI storage?"
> https://access.redhat.com/kb/docs/DOC-4135



Exercice de Liste de contrôle des performances

Configuration iSCSI - Exercice

Vous configurez votre serveur serverX pour utiliser le stockage iSCSI existant sur instructor.example.com.

- ☐ Connectez-vous à serverX en tant que super utilisateur.
- ☐ Vérifiez que le package *iscsi-initiator-utils* est installé. Installez-le, si besoin.
- ☐ Détectez les cibles iSCSI sur le serveur iSCSI sur 192.168.0.254.
- ☐ Connectez-vous à la cible iSCSI **`iqn.2010-09.com.example:rdisks.serverX`** sur 192.168.0.254.
- ☐ Identifiez le fichier de périphérique pour le nouveau disque iSCSI sur votre initiateur.
- ☐ Configurez une seule partition sur le nouveau périphérique de stockage, formatez la partition au format ext4 et configurez-la pour la monter de façon permanente sur /mnt au démarrage. *(Remarque : n'oubliez pas d'utiliser* **`_netdev`** *comme option de montage ou pour procéder à un montage par UUID de système de fichiers et non par nom de périphérique standard.)*
- ☐ Testez votre configuration.
- ☐ Démontez de façon permanente le nouveau système de fichiers.
- ☐ Déconnectez-vous et supprimez l'entrée pour la cible iSCSI.



Test

Test de critère

Exercice

Partitions et systèmes de fichiers - Exercice

Avant de commencer...

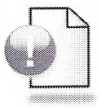
Réinitialisez serverX en exécutant **`lab-setup-server`** à partir de desktopX.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Sur serverX, connectez-vous à la cible iSCSI **`iqn.2010-09.com.example:rdisks.serverX`** à partir de &insIP et assurez-vous qu'elle est activée lors du démarrage.
2. Créez deux nouvelles partitions physiques de 10 Mo chacune sur le disque iSCSI.
3. Avec la première partition, créez un système de fichiers ext4 monté de manière permanente sur **`/test`**.
4. Avec la seconde, créez un système de fichiers ext4 monté de manière permanente sur **`/opt`** avec **`acl`** en tant qu'option de montage par défaut.



Notes personnelles



Résumé du module

Partitions simples et systèmes de fichiers

Dans cette section, vous avez appris à :

- Créer et formater une partition simple pour le stockage de données

Activation de la confidentialité des données avec le chiffrement des partitions

Dans cette section, vous avez appris à :

- Activer la confidentialité des données avec une partition chiffrée à partir de la ligne de commande.

Gestion de l'espace swap

Dans cette section, vous avez appris à :

- Créer et formater une partition simple pour le swap

Accès au stockage iSCSI

Dans cette section, vous avez appris à :

- Accéder à un périphérique de stockage iSCSI, à le formater et à le monter
- Déconnecter définitivement un périphérique de stockage iSCSI



MODULE QUATRE

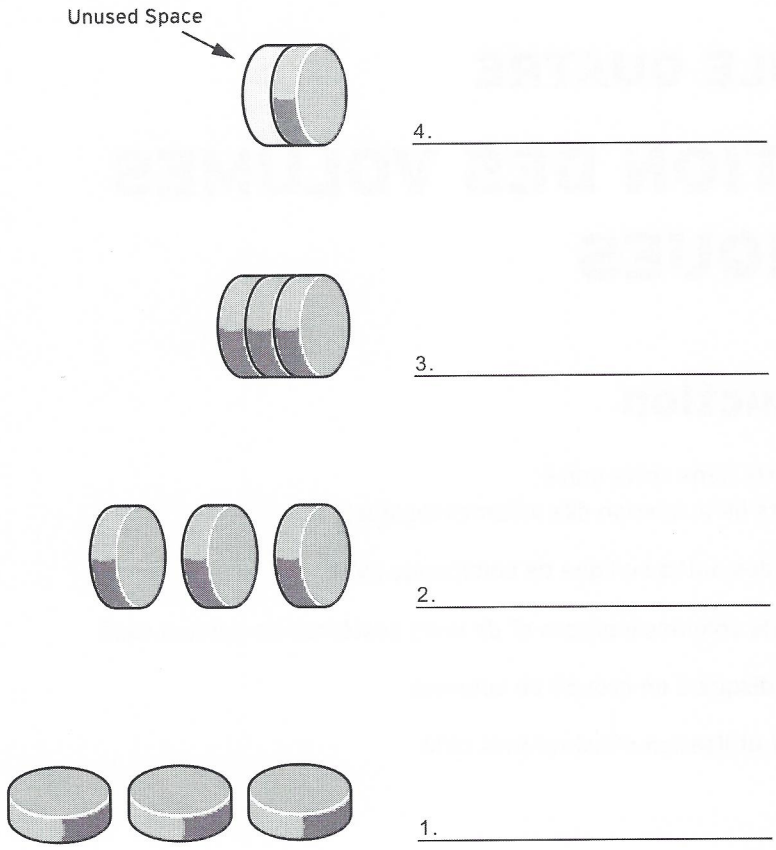
GESTION DES VOLUMES LOGIQUES

Introduction

Sujets couverts dans cette unité :

- Composants de la gestion des volumes logiques
- Utilisation des outils en ligne de commande LVM
- Extension de volumes logiques et de leurs systèmes de fichiers ext4
- Ajout d'un disque à un groupe de volumes
- Création et utilisation d'instantanés LVM

Reconnaissance des composants de LVM



Réviser les définitions LVM

- Les *partitions physiques ou disques* sont le premier composant de LVM (Logical Volume Manager, gestionnaire de volumes logiques. Il peut s'agir de partitions, de disques entiers, d'ensembles RAID ou de disques SAN.
- Les *volumes physiques* sont le stockage « physique » sous-jacent utilisé dans LVM. Il s'agit généralement d'un périphérique en mode bloc comme une partition ou un disque entier. Un périphérique doit être initialisé en tant que volume physique LVM pour pouvoir être utilisé avec LVM.
- Les *groupes de volumes* sont des pools de stockage constitués d'un ou de plusieurs volumes physiques.
- Les *extensions physiques* sont de petits morceaux de données stockés sur des volumes physiques qui agissent comme arrière-plan du stockage LVM.

- Les *extensions logiques* sont mappées sur les extensions physiques pour créer l'interface du stockage LVM. Par défaut, chaque extension logique est mappée sur une extension physique. L'activation de certaines options modifie ce mappage. La mise en miroir, par exemple, entraîne le mappage de chaque extension logique avec deux extensions physiques.
- Les *volumes logiques* sont des groupes d'extensions logiques. Un volume logique peut être utilisé de la même manière qu'une partition de disque dur.

Pourquoi utiliser des volumes logiques ?

Les volumes logiques, ainsi que la gestion de volumes logiques, aident à faciliter la gestion de l'espace disque. Si un système de fichiers nécessite davantage d'espace, cet espace peut être alloué à son volume logique depuis l'espace disponible de son groupe de volumes. Le système de fichiers peut-être redimensionné. En cas d'échec de démarrage d'un disque, un disque de remplacement peut être enregistré en tant que volume physique avec le groupe de volumes, tandis que les extensions du volume logique peuvent être déplacées sur le nouveau disque.



Références

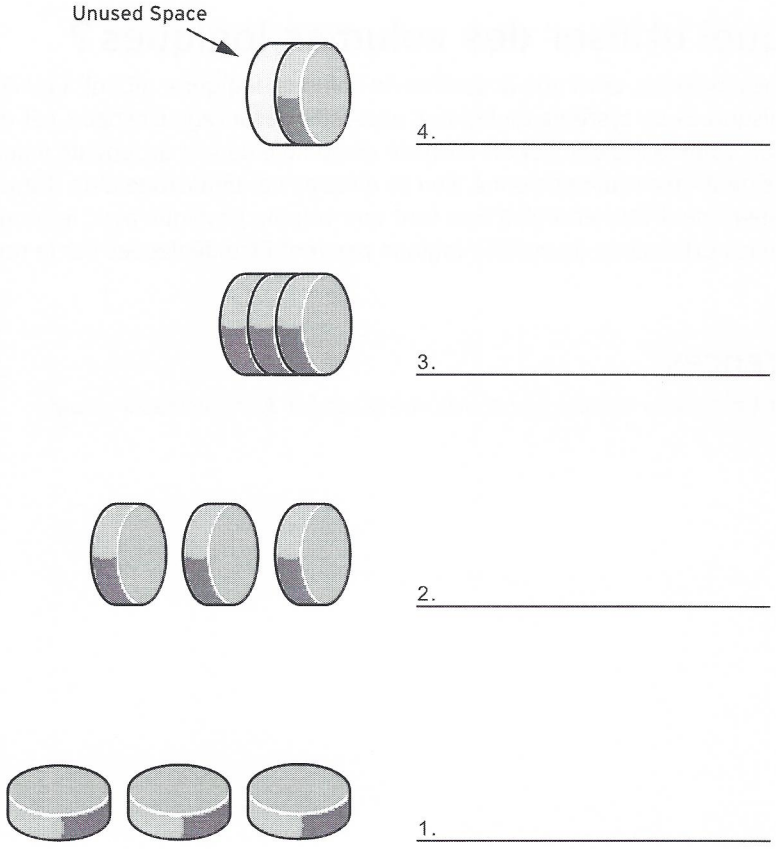
Red Hat Enterprise Linux Logical Volume Manager Administration Guide



Exercice de Questionnaire

Composants de LVM

1. Renseignez les deux graphiques suivants avec les noms des composants.



2. Quelles sont les plus petites pièces (morceaux ou blocs) du volume physique ?

3. Quelle est la plus petite taille possible pour un volume logique ?

4. Quel élément identifie les extensions physiques d'un volume logique ?

Implémentation du stockage LVM avec les outils en ligne de commande

Préparer un volume physique

1. **fdisk** permet de créer une nouvelle partition avec LVM. Définissez toujours le type sur **0x8e Linux LVM** sur une partition à utiliser avec LVM.



Note

Vous pouvez également utiliser un disque complet, une matrice RAID ou un disque SAN.

2. **pvcreate /dev/*vdaN*** permet d'initialiser la partition (ou un autre périphérique physique) pour l'utilisation avec LVM en tant que volume physique. Un en-tête de stockage des données de configuration de LVM est créé directement dans le volume physique.

Création d'un groupe de volumes

1. **vgcreate *vgname* /dev/*vdaN*** crée un groupe de volumes appelé *vgname* et constitué du volume physique */dev/vdaN*. Vous pouvez spécifier d'autres volumes physiques délimités par l'espace lors de la création ou en ajouter ultérieurement avec **vgextend**.

Créer et utiliser un nouveau volume logique

1. **lvcreate -n lvname -L 2G vgname** crée un volume logique de 2 Go appelé *lvname* à partir des extensions physiques disponibles sur *vgname*.



Important

Différents outils affichent le nom de volume logique en utilisant le nom traditionnel, **/dev/*vgname/lvname***, ou le nom de mappeur d'unité de noyau, **/dev/mapper/*vgname-lvname***.

2. **mkfs -t ext4 /dev/*vgname/lvname*** crée un système de fichiers **ext4** sur le nouveau volume logique.
3. **mkdir */data*** rend le répertoire requis comme point de montage.
4. Ajoutez une entrée au fichier **/etc/fstab**:

```
/dev/mapper/vgname-lvname  /data  ext4  defaults 1 2
```

5. **mount -a** monte le système de fichiers désormais répertorié dans **/etc/fstab**.

Consulter les informations de statut LVM

1. **pvdisplay /dev/*vdaN*** affiche les informations concernant le volume physique spécifique.

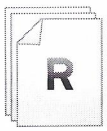
2. **vgdisplay *vgname*** affiche des informations concernant le groupe de volumes spécifique.

   Exemple de sortie de **vgdisplay**:

```
--- Volume group ---
VG Name ❶              vg1
System ID
Format                 lvm2
Metadata Areas         10
Metadata Sequence No   18
VG Access              read/write
VG Status              resizable
MAX LV                 0
Cur LV                 6
Open LV                6
Max PV                 0
Cur PV                 5
Act PV                 5
VG Size ❷              7.28 TB
PE Size ❸              4.00 MB
Total PE ❹             1907727
Alloc PE / Size ❺      1720587 / 6.56 TB
Free  PE / Size ❻      187140 / 731.02 GB
VG UUID                7FmScA-HJWa-<snip>
```

   ❶ Nom du groupe de volumes
   ❷ Taille totale du stockage « physique » dans le groupe de volumes
   ❸ Taille de l'extension physique
   ❹ Nombre total d'extensions physiques dans le groupe de volumes
   ❺ Nombre total d'extensions physiques utilisées par les volumes logiques
   ❻ Extensions physiques disponibles

3. **lvdisplay /dev/*vgname/lvname*** affiche des informations sur le volume logique spécifique.



Références

Red Hat Enterprise Linux Logical Volume Manager Administration Guide

Page man **lvm**(8)



Exercice de Exercice

Implémenter LVM et créer un volume logique

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Toutes ces étapes sont effectuées sur serverX.

1. Créez une partition de 512 Mo et préparez-la pour l'utilisation avec LVM en tant que volume physique.



Important

Veillez à créer une partition étendue au préalable pour avoir de l'espace pour créer des partitions supplémentaires ultérieurement.

2. Créez un groupe de volumes appelé **shazam** à l'aide du volume physique créé à l'étape précédente.
3. Créez et formatez avec **ext4** un nouveau volume logique de 256 Mo appelé **/dev/shazam/storage**.
4. Modifiez votre système pour que **/dev/shazam/storage** soit monté au moment du démarrage en tant que **/storage**.

Étendre un volume logique et un système de fichiers Ext4

La capacité d'augmenter la taille des volumes logiques sans interruption d'activité constitue l'un de leurs avantages. Des extensions physiques disponibles au sein d'un groupe de volumes peuvent être ajoutées à un volume logique pour « étendre » sa capacité. Le volume logique peut ensuite servir à étendre le système de fichiers qu'il contient.

Étapes de base du développement d'un volume logique

1. Vérifier la quantité d'espace disponible dans le _____
2. Étendre le _____
3. Étendre le _____

Extension du volume logique et du système de fichiers

1. Vérifiez la taille actuelle du système de fichiers */data* monté :

```
# df -h /data
```

2. Vérifiez que les « extensions physiques disponibles » sont suffisantes pour l'utilisation :

```
# vgdisplay vgname
```

3. Étendre le volume logique à l'aide de certaines ou de toutes les extensions disponibles :

```
# lvextend -l +128 /dev/vgname/lvname
```

4. Développer le système de fichiers associé monté sur */data* :

```
# resize2fs -p /dev/vgname/lvname
```

L'option **-p** affiche la progression de cette opération.



Note

Le système de fichiers peut rester monté et être utilisé lors de l'exécution de **resize2fs**.



Important

Une erreur courante consiste à exécuter **lvextend** en oubliant d'exécuter **resize2fs**.

5. Vérifiez la nouvelle taille du système de fichiers */data* monté :

```
# df -h /data
```

Réduction d'un système de fichiers et d'un volume logique

Ce processus est similaire à l'extension mais *inversé* : **resize2fs** puis **lvreduce**.



Avertissement

Il est essentiel de disposer d'une sauvegarde fiable avant d'entreprendre une réduction du volume logique, car les erreurs typographiques dans la ligne de commande peuvent entraîner une perte de données.

1. Alors que l'extension d'un volume logique peut être effectuée pendant que le système de fichiers est utilisé, la réduction d'un système de fichiers **ext4** doit être effectuée hors ligne.

   umount */data* permet de démonter le système de fichiers que vous voulez réduire.

2. **fsck -f /dev/mapper/***vgname-lvname* permet de vérifier que toutes les structures de données du système de fichiers sont nettoyées avant le redimensionnent.

3. **resize2fs -p /dev/mapper/***vgname-lvname 512M* redimensionne le système de fichiers à 512 Mo en supposant que le volume logique fait plus de 512 Mo.

   Remarque : si vous omettez la *taille* dans la commande **resize2fs**, elle prendra comme valeur par défaut la taille du volume logique, idéal pour étendre le volume logique comme précédemment.

4. **lvreduce -L** *512M* **/dev/mapper/***vgname-lvname* réduit le volume logique à 512 Mo.



Avertissement

lvreduce ne connaît pas les structures de données de votre système de fichiers et supprimera sans avertissement les éléments de ce système si vous n'avez pas utilisé **resize2fs** au préalable, afin de *réduire* le système de fichiers à une taille inférieure à celle du volume logique souhaité.

5. **mount -a** remonte votre volume logique désormais réduit en supposant qu'il est répertorié dans **/etc/fstab**.



Références

Red Hat Enterprise Linux Logical Volume Manager Administration Guide

Page man **lvm**(8)



Exercice de Exercice

Etendre un volume logique

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Toutes ces étapes sont effectuées sur serverX.

1. Déterminez la quantité d'espace libre dans le groupe de volumes **shazam**.
2. Étendez le volume logique **/dev/shazam/storage** avec *la moitié* des extensions disponibles dans le groupe de volume, à l'aide d'outils de ligne de commande.
3. Étendez le système de fichiers monté sur **/storage** à l'aide d'outils de ligne de commande.

Extension et réduction d'un groupe de volumes

Lorsque des volumes logiques au sein d'un groupe de volumes utilisent l'ensemble des extensions physiques disponibles de ce groupe, ils ne peuvent pas être étendus sans l'ajout d'espace supplémentaire au groupe de volumes. Heureusement, il est possible de créer et d'ajouter des volumes physiques supplémentaires à un groupe de volumes pour « étendre » sa capacité.

L'utilisation de LVM revêt un autre avantage. En effet, des données peuvent être déplacées entre des périphériques de stockage physiques sans interruption d'activité de l'utilisateur. Par exemple, des données peuvent être déplacées depuis un lecteur de disque plus lent vers un nouveau lecteur de disque plus rapide. Cela permet à un administrateur système de supprimer le périphérique de stockage physique inutilisé d'un groupe de volumes, le lecteur de disque lent dans ce cas.

Extension d'un groupe de volumes

1. Comme pour la création d'un groupe de volumes, une nouvelle partition doit être créée et préparée pour l'utilisation en tant que volume physique LVM.

   Utilisez **`fdisk`** pour créer une partition et définissez le type sur **`0x8e Linux LVM`**.

   Utilisez **`pvcreate /dev/vdaN`** pour initialiser la partition pour l'utilisation avec LVM en tant que volume physique.

2. **`vgextend vgname /dev/vdaN`** permet d'ajouter le nouveau volume physique, **`/dev/vdaN`**, au groupe de volumes existant ***vgname***.

3. **`vgdisplay`** permet de confirmer les « Extension physiques disponibles ».

Réduction d'un groupe de volumes

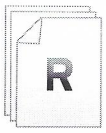
1. **`pvmove /dev/vdaN`** permet de déplacer des extensions physiques utilisées sur **`/dev/vdaN`** vers d'autres volumes physiques du groupe de volumes. Cette opération est uniquement possible si les extensions disponibles dans le groupe de volumes sont suffisantes et si elles proviennent toutes d'autres volumes physiques.



Avertissement

Avant d'utiliser **pvmove**, il est recommandé de sauvegarder les données sur des volumes logiques du groupe de volumes. Toute panne d'électricité au cours de l'opération peut laisser le groupe de volumes dans un état incohérent.

2. **`vgreduce vgname /dev/vdaN`** permet de supprimer le volume physique **`/dev/vdaN`** du groupe de volumes **vgname**.



Références

Red Hat Enterprise Linux Logical Volume Manager Administration Guide

Pages man **lvm**(8), **pvmove**(8), **vgreduce**(8)



Exercice de Exercice

Étendre un groupe de volumes

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Toutes ces étapes sont effectuées sur serverX.

1. Créez une partition de 512 Mo et préparez-la pour l'utilisation avec LVM en tant que volume physique.



Important

Veillez à créer une partition étendue au préalable pour avoir de l'espace pour créer des partitions supplémentaires ultérieurement.

2. Étendez le groupe de volumes **shazam** en ajoutant le volume physique créé à l'étape précédente.

Création d'un instantané pour faciliter la sauvegarde des données

Les volumes logiques d'instantanés constituent une autre fonctionnalité flexible du stockage LVM. Un instantané LVM est un volume logique qui conserve temporairement les données d'origine d'un volume logique qui évolue. L'instantané fournit une vue statique du volume d'origine, afin de pouvoir sauvegarder ces données dans un état cohérent.

Détermination de la taille de l'instantané

1. Taux de _____ prévu
2. _____ de l'instantané requise

Le volume de l'instantané doit uniquement être assez grand pour stocker les données qui seront modifiées pendant son existence.

Si la quantité de données modifiées est plus importante que la capacité de l'instantané, ce dernier devient automatiquement inutilisable. (Le volume initial reste inchangé et l'instantané mort devra toujours être démonté et supprimé manuellement du groupe de volumes.)

Création et utilisation d'un instantané pour la sauvegarde

1. Créez un nouveau volume de l'instantané appelé ***snaplvname*** de **/dev/*vgname/lvname*** dont la taille est de **20 MB**.

```
# lvcreate -s -n snaplv -L 20M /dev/vgname/lvname
```

2. Si votre logiciel de sauvegarde le requiert, montez l'instantané et pointez votre programme de sauvegarde vers le nouveau point de montage :

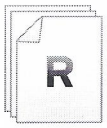
```
# mkdir /snapmount
# mount -ro /dev/vgname/snaplv /snapmount
```

3. Vérifiez le statut du volume logique de l'instantané :

```
# lvs /dev/vgname/snaplv
```

4. Lorsque vous avez terminé d'utiliser l'instantané, démontez-le et supprimez-le.

```
# umount /snapmount
# lvremove /dev/vgname/snaplv
```



Références

Red Hat Enterprise Linux Logical Volume Manager Administration Guide

Page man **lvm**(8)



Exercice de Exercice

Création d'un instantané LVM

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Comparez le contenu de notre volume logique existant, **/dev/shazam/storage**, avec un nouveau volume de l'instantané, **/dev/shazam/storagesnap**, tout en apportant des modifications au volume initial.

Toutes ces étapes sont effectuées sur serverX.

1. Copiez le fichier **/usr/share/dict/linux.words** dans **/storage** pour avoir des données à comparer.
2. Créez un volume logique d'instantané de 20 Mo de **/dev/shazam/storage**, appelé **storagesnap**.
3. Montez manuellement **/dev/shazam/storagesnap** en lecture seule sur **/storagesnap**
4. Répertoriez le contenu de **/storagesnap** et notez qu'il est identique à **/storage**.
5. Supprimez le fichier **/storage/linux.words** et notez qu'il existe encore dans **/storagesnap**.
6. Nettoyage : démontez **/storagesnap**, supprimez le répertoire et supprimez le volume logique **storagesnap**.



Test

Test de critère

Étude de cas

Étude de cas LVM

Avant de commencer...

Assurez-vous d'exécuter **`lab-setup-lvm`** à partir de votre système desktopX, qui prépare votre système serverX pour l'exercice.

Allison doit stocker des données pour son entreprise. La taille actuelle de sa base de données de clients est de 256 Mo. Les données qu'elle contient changent à un taux d'environ 10 Mo par heure au cours d'une journée normale. Le logiciel de sauvegarde prend 10 minutes pour terminer une exécution complète.

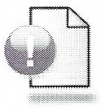
Créez un nouveau groupe de volumes appelé **`allison`** avec assez d'espace pour un volume de 512 Mo et un instantané de ce volume pour le logiciel de sauvegarde. Créez un volume logique de 512 Mo pour la base de données de clients d'Allison, appelée **`custdb`**. Créez un volume d'instantané de la base de données de clients d'Allison, appelé **`custdbsnap`** pour son logiciel de sauvegarde.

Lorsque vous êtes prêt, exécutez le script **`lab-grade-lvm`** sur le serverX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Reconnaissance des composants de LVM

Dans cette section, vous avez appris à :

- Identifier les composants de base du gestionnaire de volumes logiques

Implémentation du stockage LVM avec les outils en ligne de commande

Dans cette section, vous avez appris à :

- Créer des volumes physiques, des groupes de volumes et des volumes logiques via les outils de ligne de commande
- Réviser les informations de statut LVM

Étendre un volume logique et un système de fichiers Ext4

Dans cette section, vous avez appris à :

- Étendre un volume logique et le système de fichiers correspondant pour répondre aux besoins de données croissants

Extension et réduction d'un groupe de volumes

Dans cette section, vous avez appris à :

- Ajouter de nouveaux volumes physiques à un groupe de volumes existant
- Supprimer un volume physique existant d'un groupe de volumes

Création d'un instantané pour faciliter la sauvegarde des données

Dans cette section, vous avez appris à :

- Utiliser des instantanés de LVM temporaires pour faciliter les sauvegardes de données et réduire le temps d'arrêt des services



MODULE CINQ

GESTION DE COMPTES

Introduction

Sujets couverts dans cette unité :

- Gestion des stratégies de durée de vie des mots de passe des utilisateurs locaux
- Autorisation ou refus d'accès aux fichiers par les entrées ACL étendues
- Définition automatique des entrées ACL étendues sur les nouveaux fichiers

Gestion des mots de passe

Historiquement, les mots de passe étaient stockés dans **/etc/passwd**, mais ce fichier doit pouvoir être lu par tous afin de prendre en charge les mappages nom d'utilisateur à UID requis par les utilitaires comme **ls** pour afficher le nom d'utilisateur au lieu du numéro d'UID.

Les mots de passe ont été migrés vers un fichier plus sécurisé, **/etc/shadow**, dans lequel plusieurs algorithmes de chiffrement de mots de passe sont pris en charge. Tant que des mots de passe sont stockés dans un fichier dédié, la stratégie de durée de vie des mots de passe et les données peuvent également être stockées.

Quelles sont les 3 informations stockées dans un hachage de mot de passe ?

1gCjLa2/Z$6Pu0EK0AzfCjxjv2hoLOB/

1. **1** : l'algorithme de hachage (1 indique un hachage MD5).
2. **gCjLa2/Z** : la valeur salt qui sert à chiffrer le hachage.
3. **6Pu0EK0AzfCjxjv2hoLOB/** : le hachage chiffré.



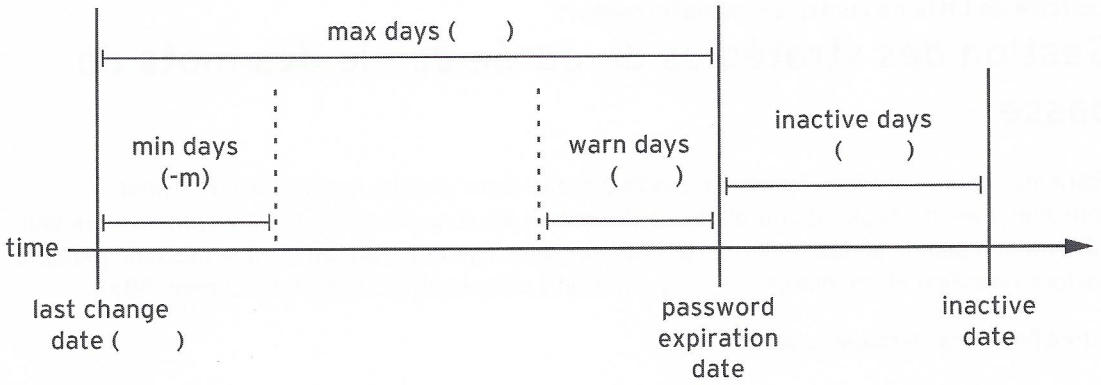
Note

Red Hat Enterprise Linux 6 prend en charge deux nouveaux algorithmes forts de hachage de mots de passe, SHA-256 (algorithme **5**) et SHA-512 (algorithme **6**). Ils peuvent être activés par défaut pour **/etc/shadow** en utilisant **system-config-authentication** pour les sélectionner dans le menu déroulant **Algorithme de hachage de mot de passe** de l'onglet **Options avancées**.

Champs /etc/shadow

1. Nom d'utilisateur
2. Hachage de mot de passe
3. Date de la dernière modification du mot de passe (nombre de jours depuis 1970.01.01)
4. Âge minimum du mot de passe (en jours, 0 = aucune condition d'âge minimum)
5. Âge maximum du mot de passe (en jours)
6. Période de préavis de mot de passe (en jours, 0 = aucun avertissement)
7. Période de mot de passe inactif (en jours)
8. Expiration du compte (nombre de jours depuis 1970.01.01)

Le diagramme suivant indique les paramètres de durée de vie du mot de passe pertinents, qui peuvent être réglés à l'aide de **chage** pour implémenter la stratégie de durée de vie du mot de passe.



Pendant que votre formateur présente ces paramètres, renseignez la parenthèse dans le diagramme ci-dessus avec le commutateur de ligne de commande (court) **chage** correspondant.

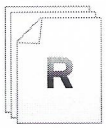
Par exemple, *-m* a été ajouté au paramètre *min days* pour démarrer.

```
# chage -m 0 -M 90 -W 7 -I 14 username
```

chage -d 0 *username* force une mise à jour du mot de passe lors de la prochaine connexion.

chage -l *username* liste les paramètres actuels du nom d'utilisateur.

usermod peut modifier un compte, y compris le « verrouiller » avec l'option **-L**.



Références

Red Hat Enterprise Linux Deployment Guide

- Section 15.6: Mots de passe en double

chage(1), **shadow**(5), **crypt**(3) (pages du manuel)



Exercice de Liste de contrôle des performances

Gestion des stratégies de durée de vie des mots de passe

Votre instructeur va vous répartir en petits groupes Dans chaque groupe, discutez pour déterminer les stratégies de durée de vie du mot de passe appropriées pour les *professeurs* (qui utilisent la machine pendant longtemps), les *étudiants diplômés* (qui utilisent la machine pendant quelques années) et les *internes d'été* (qui utilisent uniquement la machine pendant l'été).

- **`Professors`**: faraday, juliet
- **`Graduate Students`**: jack, kate, james
- **`Summer Interns`**: walt, ben, clair, hugo

☐ Si les utilisateurs et les groupes ne sont pas déjà définis, exécutez **`lab-add-users`** sur serverX.

☐ Pour chaque groupe d'utilisateurs, déterminez une stratégie de durée de vie du mot de passe appropriée, qui inclut

- Les dates d'expiration du compte (le cas échéant).
- Le délai avant la modification du mot de passe.
- Le délai avant que les mots de passe inchangés forcent l'inactivité d'un compte.

☐ Une fois déterminée, utilisez la commande **chage** pour implémenter votre règle pour les utilisateurs ajoutés dans la section précédente, en fonction de leur rôle.

De plus, obligez tous les utilisateurs à modifier leur mot de passe lors de la première connexion.

Gestion de listes de contrôle d'accès au système de fichiers

Des listes de contrôle d'accès (ACL) assurent des contrôles de sécurité plus fins que le schéma de sécurité UGO standard (utilisateur, groupe, autre). Elles peuvent servir à donner des privilèges, par exemple à accorder des privilèges d'écriture d'un fichier. Les ACL permettent également de restreindre les privilèges accordés pour un fichier, par exemple il est possible de retirer l'accès en lecture d'un membre spécifique d'un groupe doté d'un accès groupe en lecture à ce fichier.

Prise en charge de listes de contrôle d'accès

- Les systèmes de fichiers Linux standard (ext. 2/3/4) prennent en charge des ACL étendues, si elles sont montées avec l'option **`acl`**.
- Dans Red Hat Enterprise Linux, si le dernier caractère de la chaîne d'autorisation affichée dans **`ls -l`** est un **`+`**, une ACL est définie pour le fichier ou le répertoire.
- **`getfacl`** ***`file`*** permet d'afficher les ACL dans un fichier

```
u:elvis:rw-     # applies to user elvis
u:3142:---      # applies to user id 3142
u::rwx          # applies to file user owner

g:music:rwx     # applies to group music
g:10:r-x        # applies to group id 11
g::rw-          # applies to file group owner

o::rwx          # applies to everyone else
```

- **`setfacl`** permet de définir ou modifier les ACL dans un fichier

```
setfacl -m u:friend:rw filename  # grants rw to user friend
setfacl -m g:grads:rw filename   # grants rw to the group grads
setfacl -m g:profs:r filename    # grants r to the group profs

setfacl -x u:friend              # removes the existing ACL for friend

setfacl -m o::- filename         # changes normal "other" permissions
```

Utilisez cet espace pour vos notes.

Priorité de permission

1. Si l'UID de processus == propriétaire de l'utilisateur du fichier, utilisez les autorisations de l'utilisateur

2. Si l'UID de processus == une entrée ACL d'utilisateur explicite, utilisez ces autorisations (masquées)

3. Si l'un des groupes du processus correspond au propriétaire de groupe *ou* à une entrée ACL de groupe explicite, utilisez *n'importe quelle* autorisation (masquées) qui s'applique (en d'autres termes, elle est cumulative pour tous les groupes correspondants).

4. Sinon, utilisez les autres autorisations du fichier

Utilisez cet espace pour vos notes.

Entrées ACL et répertoires setgid par défaut (héritage)

- Les répertoires peuvent contenir des entrées « ACL par défaut », définies automatiquement sur les nouveaux fichiers créés dans ce répertoire

- **`setfacl -m d:u:elvis:rw directory`** définit une entrée ACL par défaut, qui autorise l'utilisateur **`elvis`** à accéder en lecture-écriture à l'ensemble des fichiers créés dans **`directory`**.

- Il en est de même avec l'autorisation setgid : lorsqu'elle est définie sur un répertoire, les fichiers créés dans ce répertoire appartiendront au groupe propriétaire du répertoire.

```
# chgrp staff /home/staff
# chmod 2775 /home/staff
# ls -ld /home/staff
drwxrwsr-x. 2 root staff 4096 2010-05-28 10:57 /home/staff
```

Utilisez cet espace pour vos notes.

Option de montage ACL

- Lors du montage du système de fichiers, la prise en charge des entrées ACL étendues doit être activée.

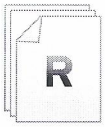
- Lorsque le programme d'installation crée des systèmes de fichiers **`ext4`**, il les configure en activant automatiquement la prise en charge ACL.

```
# dumpe2fs /dev/block-dev | grep 'Default mount'
Default mount options:    user_xattr acl
```

- Si vous avez formaté manuellement le système de fichiers, vous devrez le monter avec l'option de montage **acl**.
- Vous pouvez configurer un système de fichiers **ext4** formaté manuellement de façon à ce qu'il active automatiquement la prise en charge lors du montage, en utilisant **tune2fs** pour définir les options de montage par défaut::

```
# tune2fs -o acl,user_xattr /dev/block-dev
```

Utilisez cet espace pour vos notes.



Références

Red Hat Enterprise Linux Storage Administration Guide

- Chapitre 16: Listes de contrôle d'accès

acl(5), **getfacl**(1), **setfacl**(1) (pages du manuel)



Exercice de Questionnaire

Autorisations sur un répertoire collaboratif

1. Quelle commande permet de changer les autorisations d'un répertoire pour qu'il devienne un répertoire collaboratif de groupe unique privé ?

2. Quelle commande permet d'accorder l'accès au répertoire à un second groupe ?

3. Quelle commande permet d'accorder à ce deuxième groupe un accès en lecture-écriture à tout fichier créé dans ce répertoire ?



Test

Test de critère

Exercice

Utilisation de listes de contrôle d'accès (ACL) pour accorder et limiter l'accès

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Utilisation d'utilisateurs et de groupes créés précédemment sur serverX....

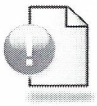
Si les utilisateurs et les groupes ne sont pas déjà définis, exécutez **`lab-add-users`** sur serverX.

Les étudiants diplômés ont besoin d'un répertoire /opt/recherche où ils pourront stocker les résultats de recherche générés. Les propriétés suivantes doivent être définies sur les fichiers créés dans le répertoire :

1. Le groupe des étudiants diplômés doit être propriétaire des fichiers.
2. Les professeurs (membres du groupe Professeurs) doivent avoir un accès en lecture/écriture au répertoire.
3. Les stagiaires saisonniers (membre du groupe Stagiaires) doivent avoir accès au répertoire en lecture seule.
4. En outre, les autres utilisateurs (non-membres des groupes Professeurs, Étudiants ou Stagiaires) ne doivent pas pouvoir accéder au répertoire.



Notes personnelles



Résumé du module

Gestion des mots de passe

Dans cette section, vous avez appris à :

- Personnaliser la stratégie de durée de vie des mots de passe pour les utilisateurs, afin de remplir les critères de sécurité de l'organisation

Gestion de listes de contrôle d'accès au système de fichiers

Dans cette section, vous avez appris à :

- Utiliser une entrée ACL pour autoriser ou bloquer l'accès à un fichier
- Lister les ACL sur un fichier
- Supprimer une entrée ACL
- Assigner une ACL ou une appartenance de groupe à de nouveaux fichiers créés automatiquement dans un répertoire



MODULE SIX

GESTION DES AUTHENTIFICATIONS

Introduction

Sujets couverts dans cette unité :

- Configuration de l'authentification centralisée des utilisateurs LDAP
- Configuration d'authentification par mot de passe à partir d'un serveur Kerberos
- Diagnostic des problèmes d'authentification LDAP/Kerberos gérée par le démon **sssd**
- Montage automatique des répertoires personnels des utilisateurs NFS

Authentification réseau à l'aide d'un serveur LDAP

Jusqu'à présent, nous avons examiné des comptes d'utilisateurs locaux gérés via des fichiers locaux sur chaque machine, **`/etc/passwd`**. Mais il est difficile de coordonner les comptes d'utilisateurs locaux pour qu'ils soient identiques sur un grand nombre de systèmes.

Dans cette section, nous étudierons comment configurer une machine comme client afin d'utiliser les comptes d'utilisateurs réseau fournis par un service d'annuaire LDAP existant. Cela permet à l'annuaire LDAP d'être notre autorité centrale pour tous les groupes et utilisateurs réseau dans notre organisation.

Les *informations de compte d'utilisateur* déterminent les caractéristiques et la configuration du compte. Les *méthodes d'authentification* permettent de déterminer si une personne qui tente de se connecter doit avoir accès au compte. Les *services d'annuaire réseau* peuvent fournir les informations de compte d'utilisateur et les méthodes d'authentification.

Les *serveurs d'annuaire LDAP* peuvent être utilisés comme service de gestion des utilisateurs réseau centralisé et distribué. Les entrées d'annuaire sont disposées en arborescence, dans laquelle des recherches peuvent être effectuées. Le *nom distinctif (DN, Distinguished Name) de base* se trouve à la base de l'arborescence dans laquelle les entrées d'annuaire pour les utilisateurs et groupes seront recherchées.

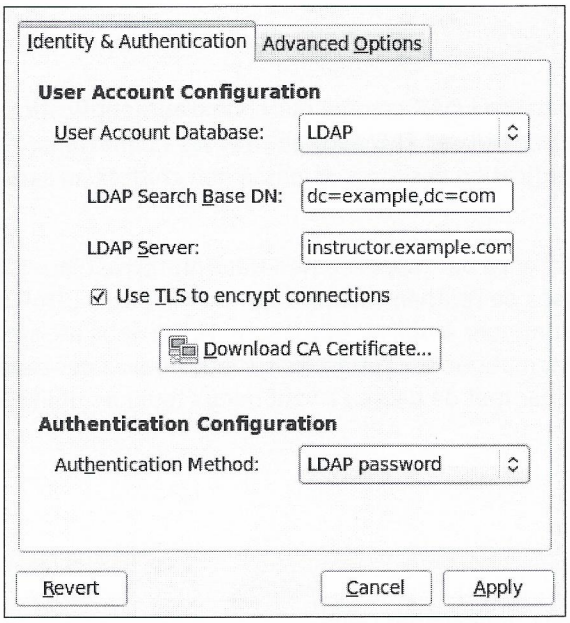
Éléments clés pour la configuration du client LDAP

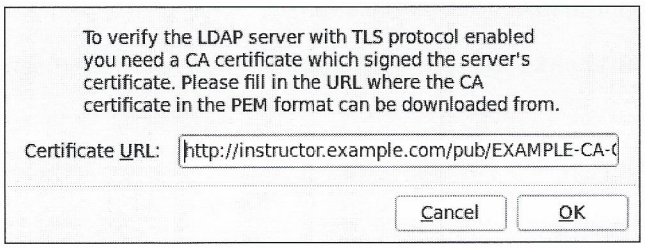
1. Nom d'hôte qualifié complet du serveur
2. DN de base à rechercher pour les définitions d'utilisateur
3. Autorité de certification (« CA », certificate authority) utilisée pour signer le certificat SSL du serveur LDAP

Utilisez cet espace pour vos notes.

Assurez-vous avant de commencer que le groupe de packages yum **`directory-client`** est installé, y compris les packages *sssd*, *authconfig-gtk* et *oddjob-mkhomedir*.

System → **Administration** → **Authentication** ou **`system-config-authentication`** permet de modifier la configuration d'*Identité & Authentification*.





system-config-authentication est exécuté automatiquement sur le service **sssd** qui recherche et met en mémoire cache les informations sur l'utilisateur et données d'authentification LDAP pour le client. Si le serveur LDAP est indisponible mais que **sssd** fonctionne, le système peut authentifier les utilisateurs réseau et obtenir des informations sur ces derniers à partir de la mémoire cache **sssd**.

Utilisez **getent passwd *username*** pour vérifier les informations de compte utilisées. Cette opération fonctionne que l'utilisateur soit un utilisateur local défini dans **/etc/passwd** ou un utilisateur réseau d'un service LDAP. La commande indique toujours la définition actuellement utilisée par le système si une duplication est effectuée entre les utilisateurs locaux et réseau. Par défaut, la définition d'utilisateur local prévaut sur la définition d'utilisateur réseau.



Note

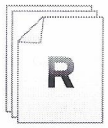
Dans Red Hat Enterprise Linux 6, la commande **getent passwd** (sans nom d'utilisateur spécifié) vide par défaut uniquement les noms d'utilisateurs en local, elle ne vide pas la liste de tous les utilisateurs LDAP comme c'était le cas dans Red Hat Enterprise Linux 5 dans un souci de performance. Pour de plus amples informations, consultez **sssd.conf**(5) sous l'option **enumerate**. (Pour modifier ce comportement, définissez **enumerate = True** dans la section **[domain/default]** de **/etc/sssd/sssd.conf**.)



Important

Si vous utilisez **Mot de passe LDAP** comme méthode d'authentification, vous *devez* sélectionner et configurer **Utiliser TLS pour chiffrer les connexions**. Vous évitez ainsi d'envoyer pour authentification des mots de passe non chiffrés au serveur LDAP via le réseau .

Ceci constitue une différence par rapport à Red Hat Enterprise Linux 5 qui permettait l'utilisation non sécurisée de l'authentification par mot de passe LDAP sans TLS. Avec RHEL 6, vous pouvez continuer à utiliser LDAP sans TLS si vous utilisez LDAP uniquement pour récupérer des informations sur l'utilisateur. (Vous pouvez par exemple utiliser Kerberos pour l'authentification par mot de passe.) Il vaut mieux toujours utiliser TLS.



Références

Red Hat Enterprise Linux Deployment Guide

- Chapitre 8 : Configuration de l'authentification

system-config-authentication(8), **sssd**(8) et **sssd.conf**(5) (pages du manuel)



Exercice de Questionnaire

Configuration du client LDAP

1. Quelles sont les sept informations généralement fournies par les services d'*information sur les comptes d'utilisateur* ?

2. Quel « autre » type d'information peut être fourni par un *service d'annuaire réseau* ?

3. Quelles sont les trois informations devant être configurées pour une machine client afin d'obtenir les informations sur l'utilisateur à partir d'un service d'annuaire LDAP ?

4. Que fait la commande **`getent passwd ldapuser1`** ? Pourquoi est-ce utile ?

Configuration Kerberos

Kerberos est une méthode d'authentification sécurisée sur un réseau non sécurisé développée à l'origine par le MIT. Kerberos authentifie les utilisateurs sans transmettre les mots de passe sur le réseau. L'intégrité des mots de passe est ainsi préservée et leur capture par des analyseurs de réseau empêchée. Dans ce cas, ce sont des *tickets* chiffrés avec le mot de passe de l'utilisateur comme clé de chiffrement qui sont transmis. Quand un utilisateur effectue sa première authentification dans un système avec un mot de passe Kerberos, le programme de connexion demande au serveur d'authentification Kerberos ou *au centre de distribution de clés*un ticket correspondant à cet utilisateur. Le centre de distribution de clés (KDC) envoie un ticket pour ledit utilisateur au programme de connexion. Ensuite, s'il saisit le mot de passe qui déchiffre le ticket, l'utilisateur est authentifié.

Kerberos ne stocke pas

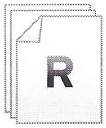
Nous allons examiner les étapes et les éléments de configuration principaux permettant de pointer un système vers une zone Kerberos existante.

Au lieu d'utiliser **`system-config-authentication`** pour procéder aux changements, nous allons nous concentrer sur l'outil en ligne de commande, **`authconfig`**. Notez les options dont cet outil a besoin à mesure qu'elles vous sont présentées.

- Zone Kerberos - L'ensemble de tous les serveurs qui utilisent les mêmes KDC (serveurs d'authentification Kerberos) pour l'authentification.

- Centre de distribution de clés (KDC) - Serveurs centraux qui stockent les informations sur les mots de passe Kerberos et émettent les tickets Kerberos (données d'authentification).

- Serveur d'administration Kerberos - Serveurs d'administration à distance (ces serveurs servent par exemple à la mise à jour des mots de passe). En principe, le centre de distribution de clés (KDC) est le serveur d'administration de la zone.



Références

Red Hat Enterprise Linux Deployment Guide

- Section 8.1: L'outil de configuration de l'authentification

`system-config-authentication`(8), **`kerberos`**(1) et **`sssd`**(8) (pages du manuel)



Exercice de Liste de contrôle des performances

Exercice de configuration Kerberos

Vous allez modifier votre configuration LDAP précédente pour utiliser uniquement Kerberos pour l'authentification. LDAP va uniquement servir à fournir les informations sur les comptes.

- ☐ Connectez-vous au serverX et étendez les privilèges au niveau super utilisateur.
- ☐ Vérifiez que les packages requis sont installés.
- ☐ Configurez le système de manière qu'il utilise les paramètres LDAP et Kerberos suivants :
  - Serveur LDAP : instructor.example.com (qui utilise TLS)
  - Certificat LDAP : `ftp://instructor.example.com/pub/EXAMPLE-CA-CERT`
  - DN de base LDAP : dc=example,dc=com
  - Zone Kerberos : EXAMPLE.COM
  - KDC Kerberos : instructor.example.com
  - Serveur d'administration Kerberos : instructor.example.com
  - Assurez-vous que le service **sssd** est activé.
- ☐ Connectez-vous au serveur serverX avec ssh pour tester la modification :
  - Nom d'utilisateur : **ldapuser*X*** (où X représente votre numéro de station)
  - Mot de passe : **kerberos**

Résolution des problèmes de démon SSSD (System Security Services Daemon)

Résolution des problèmes d'authentification

- Veuillez prendre des notes dans les espaces prévus ci-dessous à mesure que l'instructeur répond à chacune de ces questions :

1. Quel est l'inconvénient de l'authentification par LDAP ou Kerberos des utilisateurs d'ordinateur de bureau ou portables par rapport à une méthode où les comptes d'utilisateurs sont définis localement ?

2. Que peut-on implémenter pour résoudre ce problème ?

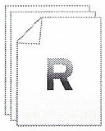
3. Comment configurer le démon SSSD ?

4. Et si je veux configurer le démon SSSD à partir de la ligne de commande ?

5. En quoi cela va-t-il affecter la résolution des problèmes du processus d'authentification ?

6. Où peut-on voir ce que fait le service SSSD ?

7. Que faire s'il m'est impossible de me connecter pour consulter les fichiers journaux ou de corriger une erreur de configuration de l'authentification ?



Références

Red Hat Enterprise Linux Deployment Guide

- Section 8.2: Le démon SSSD (System Security Services Daemon)

sssd.conf(5), **sssd-krb5**(5) **sssd-ldap**(5) (pages du manuel)



Exercice de Questionnaire

Questionnaire de résolution des problèmes d'authentification

1. Comment configure-t-on habituellement le démon SSSD ?

   _____

   _____

2. Quel répertoire contient les messages de journal de sssd ?

   _____

3. Comment augmenter le détail des enregistrements de journalisation générés ?

   _____

   _____

4. Face à l'impossibilité de vous connecter pour corriger une erreur de configuration de l'authentification, quelles approches s'offrent à vous ?

   _____

Montage de répertoires personnels sur le réseau

Gardez à l'esprit que le montage de partages réseau nécessite trois informations : nom du partage, point de montage et options de montage.

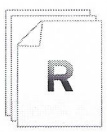
1. Utilisez **showmount -e nfsserver.domain** pour obtenir le chemin d'exportation qui, lorsqu'il est associé au nom d'hôte, nous donne le *nom du partage*.
2. **getent passwd username** permet d'obtenir le *point de montage* du répertoire personnel requis.
3. Comme répertoires personnels, nous souhaitons probablement utiliser **rw** comme *point de montage*.

La configuration de mappages indirects dans **autofs** serait similaire à l'exemple suivant :

```
# cat /etc/auto.master
/home/guests     /etc/auto.guests
# cat /etc/auto.guests
ldapuser1  -rw  instructor.example.com:/home/guests/ldapuser1
ldapuser2  -rw  instructor.example.com:/home/guests/ldapuser2
ldapuser3  -rw  instructor.example.com:/home/guests/ldapuser3
ldapuser4  -rw  instructor.example.com:/home/guests/ldapuser4
```

Et, à chaque création d'un utilisateur LDAP, ce fichier **/etc/auto.guests** doit être mis à jour pour inclure cet utilisateur supplémentaire. Notez toutefois le « modèle » des lignes : Nous souhaitons prendre en charge la connexion avec un nom d'utilisateur *quelconque*. Par conséquent, nous pouvons remplacer la première colonne par un « astérisque (*) », un caractère générique qui fait correspondre tout nom de sous-répertoire auquel le processus de connexion peut tenter d'envoyer une commande **cd**. Ensuite, nous utilisons le métacaractère « perluète (&) » pour remplacer le nom d'utilisateur du partage qui transmet le nom du mappage correspondant au caractère générique.

```
# cat /etc/auto.master
/home/guests /etc/auto.guests
# cat /etc/auto.guests
* -rw instructor.example.com:/home/guests/&
```



Références

Red Hat Enterprise Linux Storage Administration Guide

- Section 10.3 : **autofs**

autofs(5), **auto.master**(5) (pages du manuel)



Exercice de Liste de contrôle des performances

Utiliser un serveur NFS de répertoires personnels pour monter automatiquement des répertoires personnels.

L'université fournit aussi un serveur NFS de répertoires personnels pour ses étudiants. Utilisez le serveur NFS de répertoires personnels pour monter automatiquement les répertoires personnels des utilisateurs préalablement définis.

Informations sur le serveur de répertoires personnels.

- Nom d'hôte : *instructor.example.com*
- Répertoire exporté : **/home/guests/**

- ☐ Étendez la configuration de votre automonteur afin de monter le répertoire **/home/guests**.
- ☐ Configurez l'automonteur pour qu'il tente de mapper tout répertoire cible spécifié comme le répertoire miroir du serveur de répertoires personnels.

  Par exemple, une demande d'accès au répertoire local **/home/guests/ldapuser1** doit essayer de monter le répertoire **/home/guests/ldapuser1** de instructor.example.com.
- ☐ Assurez-vous que le service d'automonteur charge à nouveau ses fichiers de configuration.
- ☐ À partir d'un autre terminal, essayez d'émettre une commande shell sur votre serveur distant en tant que l'utilisateur **ldapuserX** avec le mot de passe de **password**. Le répertoire personnel de l'utilisateur doit être monté automatiquement.
- ☐ Une fois que vous avez terminé, exécutez le script **lab-grade-autofshomes** pour vérifier votre travail.



Test

Test de critère

Étude de cas

Renforcement de la sécurité des utilisateurs

Avant de commencer...

Assurez-vous d'exécuter **`lab-setup-taylorlocke`** à partir de votre système desktopX, qui prépare votre système serverX pour l'exercice.

Taylor and Locke, prestigieux cabinet d'avocats, a récemment fait appel à un consultant en sécurité pour ses serveurs. Comme les serveurs renferment des informations confidentielles des clients du cabinet, leur sécurité est une priorité !

Le consultant en sécurité a recommandé que tous les serveurs utilisent LDAP pour les comptes centralisés et Kerberos pour l'authentification. Globalement, le déploiement LDAP/Kerberos s'est bien passé Toutefois, un des serveurs que vous gérez semble contenir une erreur de configuration.

Corrigez la configuration de serverX de manière que tous utilisateurs LDAP puissent se connecter avec l'authentification Kerberos (voir les détails ci-dessous).

- Serveur LDAP : instructor.example.com (qui utilise TLS)
- Certificat LDAP : ftp://instructor.example.com/pub/EXAMPLE-CA-CERT
- DN de base LDAP : dc=example,dc=com
- Zone Kerberos : EXAMPLE.COM
- KDC Kerberos : instructor.example.com
- Serveur d'administration Kerberos : instructor.example.com

Connectez-vous au serveur serverX avec ssh pour tester la modification :

- Nom d'utilisateur : ldapuserX (où *X* représente votre numéro de station)
- Mot de passe : kerberos

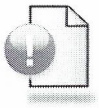
Une fois que les utilisateurs LDAP peuvent se connecter, configurez autofs pour les répertoires personnels soient automatiquement montés. Les répertoires personnels sont partagés à partir de instructor.example.com.

Lorsque vous êtes prêt, exécutez le script **`lab-grade-taylorlocke`** sur le serverX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Authentification réseau à l'aide d'un serveur LDAP

Dans cette section, vous avez appris à :

- Configurer le système pour authentifier les utilisateurs gérés dans un service d'annuaire LDAP central.

Configuration Kerberos

Dans cette section, vous avez appris à :

- Utiliser un serveur Kerberos pour vérifier les mots de passe des utilisateurs.

Résolution des problèmes de démon SSSD (System Security Services Daemon)

Dans cette section, vous avez appris à :

- Corriger les problèmes avec le service **sssd** et l'authentification réseau.

Montage de répertoires personnels sur le réseau

Dans cette section, vous avez appris à :

- Monter automatiquement des répertoires personnels NFS existants pour les utilisateurs distants à l'aide de métacaractères de mappage indirect



MODULE SEPT

INSTALLATION, KICKSTART ET VIRTUALISATION

Introduction

Sujets couverts dans cette unité :

- Création d'un fichier Kickstart en modifiant `/root/anaconda-ks.cfg` à l'aide d'un éditeur de texte
- Introduction à la virtualisation KVM
- Installation d'invités virtuels
- Gestion de machines virtuelles

Création d'un fichier Kickstart en modifiant un modèle

À l'aide de *Kickstart*, un administrateur système peut créer un fichier unique contenant les réponses à toutes les questions généralement posées pendant une installation. Le programme d'installation peut ensuite accéder au fichier pour automatiser l'installation de Red Hat Enterprise Linux.



Comparaison

Kickstart sous Red Hat Enterprise Linux est similaire à Jumpstart pour Oracle Solaris ou à une installation sans assistance sous Microsoft Windows.

Étapes de base :

1. Créer un fichier kickstart
2. Mettre le fichier kickstart à disposition du programme d'installation
3. Démarrer le programme d'installation
4. Pointer le programme d'installation vers le fichier kickstart

Utilisez cet espace pour vos notes.

Le fichier Kickstart

Au moment de l'installation, le programme d'installation, **Anaconda**, crée le fichier **`/root/anaconda-ks.cfg`**, qui contient les paramètres de configuration utilisés pour installer ce système.



Note

Par défaut, les informations de partitionnement sont exclues de **/root/anaconda-ks.cfg**.

```
# Kickstart file automatically generated by anaconda.

#version=RHEL6
install
url --url=ftp://instructor.example.com/pub/rhel6/dvd
lang en_US.UTF-8
keyboard us
network --device eth0 --bootproto dhcp
rootpw  --iscrypted $1$UaJVgaTh$KrpFf3K04r9hCZ2hsaa
# Reboot after installation
reboot
firewall --disabled
authconfig --useshadow --enablemd5
selinux --enforcing
timezone --utc America/New_York
bootloader --location=mbr --driveorder=vda --append="crashkernel=auto rhgb quiet"
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
#clearpart --all --drives=vda

#part /boot --fstype=ext4 --size=100
#part pv.ZS1CDM-iUYu-Gfua-YX0W-MSzd-ftBY-7qTB1E --size=28000
#part swap --size=512
#volgroup vol0 --pesize=32768 pv.ZS1CDM-iUYu-Gfua-YX0W-MSzd-ftBY-7qTB1E
#logvol /home --fstype=ext4 --name=home --vgname=vol0 --size=500
#logvol / --fstype=ext4 --name=root --vgname=vol0 --size=8192
repo --name="Red Hat Enterprise Linux"  --baseurl=ftp://instructor.example.com/pub/rhel6/
dvd/ --cost=100

%packages
@Base
@Console internet tools
@Core
@Desktop
@Desktop Platform
@General Purpose Desktop
@Graphical Administration Tools
@Internet Browser
@Network file system client
@Printing client
@X Window System
lftp
mutt
ntp
%end

%post
# Turn on graphical login
perl -pi -e 's,id:3:initdefault,id:5:initdefault,' /etc/inittab
%end
```

Principales sections d'un fichier Kickstart

- Options de spécifications relatives à l'installation
- **%packages** (package et listes de groupes yum)
- **%pre** (script exécuté avant le démarrage de l'installation)
- **%post** (script exécuté après l'installation)

Raisons de modification manuelle d'un fichier Kickstart :

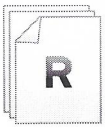
1. L'interface graphique et/ou **system-config-kickstart** est indisponible.
2. Des instructions LVM sont requises.
3. Des packages individuels doivent être inclus ou omis (pas uniquement des groupes).



Note

Avant d'utiliser votre fichier Kickstart, il est utile de vérifier sa syntaxe avec **ksvalidator *file.ks***. Les erreurs de frappe grossières et des problèmes avec les options sont ainsi vérifiés ; les packages, les listes de groupes ou les scripts **%pre**/**%post** arbitraires ne sont pas validés. **ksvalidator** appartient au package *pykickstart*.

Utilisez cet espace pour vos notes.



Références

Red Hat Enterprise Linux Installation Guide

- Chapitre 32 : Installations Kickstart



Exercice de Liste de contrôle des performances

Modification d'un fichier Kickstart sans system-config-kickstart

Une fois que vous avez terminé cet exercice, vous avez suivi toutes les étapes nécessaires à l'utilisation de Kickstart pour un nouveau système, sorte de version allégée de l'installation réelle. Vous effectuerez une installation Kickstart ultérieurement dans cette unité. Suivez les étapes ci-dessous sur desktopX :

- ☐ Créez une copie de **/root/anaconda-ks.cfg** appelée **~/projman.cfg**. À l'aide d'un éditeur de texte uniquement, modifiez ce fichier pour qu'il remplisse les critères suivants. L'installation doit être entièrement automatisée et identique à celle du poste de travail de base, sauf...
  - Partitionnez le disque comme suit :
    - Initialisez le moteur de recherche, le cas échéant
    - Effacez toutes les partitions existantes
    - /boot (ext4) : 200 Mo
    - swap : 512 Mo
    - / (ext4) : tout l'espace restant (5 Go minimum)
  - Le groupe de packages **E-mail server** doit être installé.
  - Le package **fetchmail**, non inclus avec le groupe **E-mail server** par défaut, doit être installé
  - Assurez-vous de supprimer les scripts existants de **%pre** et de **%post**
  - Utilisez **echo** pour ajouter le texte suivant à la fin de **/etc/issue** :

    ```
    PROJECT MANAGEMENT
    ```

- ☐ **ksvalidator** doit être en mesure de valider le fichier.
- ☐ Une fois l'opération terminée, publiez le fichier afin qu'il puisse être utilisé dans le cadre d'une installation. Déployez un serveur Web sur desktopX et copiez **projman.cfg** sur **/var/www/html/**.
- ☐ Utilisez un navigateur Web pour vous assurer que votre fichier Kickstart est accessible en lecture. L'URL que vous utilisez pour afficher le fichier est celle que vous transmettriez au programme d'installation avec l'argument **ks=*URL***.

Introduction à la virtualisation KVM

La virtualisation est une fonctionnalité qui permet à une machine physique unique d'être divisée en plusieurs machines *virtuelles*, qui peuvent chacune exécuter un système d'exploitation indépendant. Red Hat Enterprise Linux 6 pour x86-64 prend en charge *KVM*, qui permet au noyau de fonctionner en tant qu'hyperviseur prenant en charge les machines virtuelles invitées, tant que certaines conditions requises sont respectées.

Faits concernant la virtualisation KVM

- KVM = _____
  (machine virtuelle basée sur le noyau)
  - Implémenté sous forme de modules du noyau
  - Permet à un noyau Linux _____ de fonctionner en tant qu'hyperviseur
- Exigences en matière de KVM :
  - Processeurs 64 bits AMD ou Intel
  - Extensions _____
  - Système d'exploitation 64 bits
- Prise en charge VirtIO =
  _____ utilisés par les invités KVM (améliorent les performances E/S)
- Les avantages de KVM comprennent :
  - Des performances _____
  - Un concept _____
  - Une _____ par les développeurs de noyau en amont

Comment vérifier si une machine prend en charge KVM

- _____
- Les indicateurs pertinents comprennent :
  - **`lm`** = _____ (64-bit x86)
  - **`svm`** = _____
    (AMD)
  - **`vmx`** = _____
    (Intel)



Note

Red Hat Enterprise Linux 6 ne peut pas fonctionner comme un hyperviseur Xen, même s'il peut être exécuté en tant qu'invité Xen paravirtualisé ou entièrement virtualisé sur un hôte Xen RHEL 5. Pour plus d'informations, consultez *Red Hat Enterprise Linux Virtualization Guide* au chapitre 8, « Installation de Red Hat Enterprise Linux 6 en tant qu'invité paravirtualisé sur Red Hat Enterprise Linux 5 ».

Les machines invitées Xen existantes provenant d'un hôte Red Hat Enterprise Linux 5 peuvent faire l'objet d'une migration pour être exécutées en tant que machines invitées KVM sur un hôte Red Hat Enterprise Linux 6. Consultez *Red Hat Enterprise Linux Virtualization Guide* au chapitre 23, « Migration vers KVM depuis d'autres hyperviseurs à l'aide de virt-v2v », pour plus d'informations.



Important

Le terme *paravirtualisation* correspond à deux utilisations différentes dans le domaine de la virtualisation Linux, ce qui peut porter à confusion.

Dans Red Hat Enterprise Linux 5, l'hyperviseur Xen prenait en charge *les invités paravirtualisés*. Dans ce scénario, les pilotes et le noyau des invités ont été modifiés afin de pouvoir les exécuter sur un hyperviseur Xen, exécuté sur un système qui ne prenait pas en charge les extensions de virtualisation de matériel complètes. Le système d'exploitation lui-même devait être modifié pour prendre en charge la virtualisation paravirtualisée Xen. KVM ne prend pas en charge la paravirtualisation dans ce sens.

KVM prend en charge *les pilotes paravirtualisés*. Les pilotes paravirtualisés sont des pilotes de périphérique spéciaux, qui peuvent « tricher » en s'adressant directement à l'hyperviseur. Ainsi, avec l'hyperviseur, l'invité n'a pas besoin d'utiliser une interface moins efficace qui agit comme un périphérique matériel existant, tel qu'un contrôleur de disque ou une carte réseau. Ces *pilotes paravirtualisés virtio* sont plus rapides que les pilotes normaux présentés à l'invité par KVM pour le matériel virtuel. De manière identique, inutile de modifier le noyau du système d'exploitation pour profiter des périphériques paravirtualisés. Vous avez uniquement besoin de l'écriture de nouveaux pilotes qui les prennent en charge.



Références

Red Hat Enterprise Linux Virtualization Guide

- Chapitre 5 : Installation des packages de virtualisation



Exercice de Questionnaire

Introduction à la virtualisation KVM

1. La virtualisation matérielle nécessite l'activation dans le BIOS d'un processeur spécial doté de capacités de virtualisation.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

2. KVM est une technologie de virtualisation basée sur le noyau qui permet d'installer à la fois Linux et Windows en tant que machine virtuelle sans avoir à utiliser de noyau special.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

3. KVM est très prisé en raison de ses performances élevées et de sa conception complexe.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

4. Les indicateurs de CPU **`lm`** et **`svm`** ou **`vmx`** sont requis pour la virtualisation basée sur le noyau.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

5. KVM fonctionne à la fois sur des machines 32 et 64 bits.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

6. Les développeurs de logiciels en amont ont intégré KVM dans le code source du noyau Linux.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

Installation d'invités virtuels

Lors de l'installation d'une machine virtuelle, plusieurs éléments doivent être choisis avant de passer à la suite de l'installation via **Anaconda**.

Spécifications des machines virtuelles

1. Un nom de domaine doit être spécifié
2. Pointez sur le support d'installation pour prendre en compte les deux étages d'Anaconda.
3. Les éléments matériels virtuels doivent être spécifiés :
   - Nombre et type de CPU
   - Taille de la RAM
   - Lecteur de disque virtuel (fichier ou volume ?)
   - Connexion réseau et adresse MAC

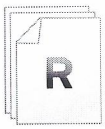
L'outil graphique **`virt-manager`** permet d'installer, de gérer et d'accéder à des machines virtuelles. L'instructeur enseigne l'utilisation de **`virt-manager`** en classe avant que vous l'utilisiez lors de l'exercice pratique suivant.



Note

Les disques durs paravirtualisés (qui utilisent les pilotes virtio) apparaissent comme invités en tant que **`/dev/vd*`** au lieu de **`/dev/sd*`**.

Utilisez cet espace pour vos notes.



Références

Red Hat Enterprise Linux Virtualization Guide
- Chapitre 6 : Présentation de l'installation des invités virtualisés

Red Hat Enterprise Linux Virtualization Guide
- Chapitre 7 : Installation de Red Hat Enterprise Linux 6 en tant qu'invité virtualisé

Page man **`virt-manager`**(1)



Exercice de Liste de contrôle des performances

Installation d'invités virtuels

Au cours de cet exercice, vous allez installer une nouvelle machine virtuelle avec Red Hat Enterprise Linux à l'aide de **`virt-manager`** et du programme d'installation graphique. Lorsque vous avez terminé l'exercice, vous devez supprimer la machine virtuelle et son volume logique afin de restaurer les ressources système requises pour d'autres exercices.

Suivez les étapes ci-dessous sur desktopX :

- ☐ Fermez correctement votre machine virtuelle serverX pour restaurer les ressources CPU et RAM du système.
- ☐ Créez un volume logique de 10 Go à partir du groupe de volumes **`vol0`** et appelez-le **`guest`**.
- ☐ Créez une machine virtuelle Red Hat Enterprise Linux 6 avec les caractéristiques suivantes :
  - Nom = invité
  - Support d'installation = installation réseau à partir de http://instructor.example.com/pub/rhel6/dvd
  - Mémoire (RAM) = 768 Mo
  - CPU = 1
  - Périphérique de stockage = le volume logique créé lors de l'étape précédente
  - Réseau - utiliser DHCP pour obtenir une adresse IP
- ☐ Une fois **Anaconda** lancé, structurez votre système invité en fonction des spécifications suivantes :
  - Utilisez la totalité de l'unité périphérique avec un schéma de partitionnement du disque par défaut
  - Affectez **`redhat`** comme mot de passe root
  - Installez le groupe de packages Desktop
- ☐ Restaurez les ressources système utilisées au cours de cet exercice. Supprimez la machine virtuelle que vous avez créée, ainsi que le stockage qu'elle utilise.

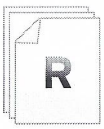
Gérer des machines virtuelles

Commandes utilisées pour gérer des machines virtuelles

Jusqu'à maintenant, **virt-manager** a servi à gérer des machines virtuelles. Il existe un outil en ligne de commande, **virsh**, qui implémente la même fonctionnalité que **virt-manager** sans nécessiter d'interface utilisateur graphique. Ces deux utilitaires ont recours à la bibliothèque **libvirt**, de sorte qu'ils peuvent être utilisés de manière interchangeable pour la gestion de machines virtuelles.

1. Mettre une machine virtuelle sous tension : **virsh** _____
2. Éteindre correctement une machine virtuelle : **virsh** _____
3. Mettre une machine virtuelle hors tension : **virsh** _____
4. Se connecter à une console de machine virtuelle : **virsh** _____
5. Se déconnecter d'une console de machine virtuelle : _____
6. Démarrer une machine virtuelle à l'initialisation : **virsh** _____

Utilisez cet espace pour vos notes.



Références

Red Hat Enterprise Linux Virtualization Guide

- Chapitre 30 : Gestion d'invités avec **virsh**

Page man **virsh**(1)



Exercice de Liste de contrôle des performances

Commandes de virtualisation

Effectuez l'ensemble des tâches suivantes à partir de la ligne de commande sur desktopX. Au cours de cet exercice, n'utilisez pas **`virt-manager`** ni **`virt-viewer`**.

- ☐ Utilisez **`virsh list --all`** pour déterminer l'ID de domaine virtuel (ou le nom) de serverX. Pour effectuer les étapes suivantes, vous aurez besoin du nom de domaine.
- ☐ Si serverX n'est pas exécuté, mettez-le sous tension.
- ☐ Éteignez correctement serverX.
- ☐ Mettez serverX sous tension.
- ☐ Connectez-vous à la console de serverX.
- ☐ La machine virtuelle n'est peut-être pas configurée de manière à présenter une console sur la console virtuelle. Déconnectez-vous de la console.
- ☐ Mettez serverX hors tension.
- ☐ Assurez-vous que serverX démarre à l'initialisation.



Test

Test de critère

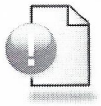
Liste de contrôle des performances

Utilisez Kicktart pour une machine virtuelle

- ☐ Copiez le fichier **`/root/anaconda-ks.cfg`** depuis serverX vers desktopX et appelez-le **`~/test.cfg`**. Éteignez serverX une fois que vous avez copié le fichier pour restaurer les ressources système pour le reste de l'exercice.
- ☐ Modifiez **`test.cfg`** en fonction des critères suivants :
  - Stockage de partition d'après les éléments suivants :
    - /boot (ext4) 200 Mo
    - swap 512 Mo
    - / (ext4) 8 Go
  - Ajoutez le package **`gimp`**
  - Créez un fichier **`/root/install-date`** avec la date et l'heure.
- ☐ Copiez **`test.cfg`** vers **`/var/www/html/`** sur desktopX. Assurez-vous le fichier est accessible en lecture pour Apache. Démarrez le démon **`httpd`** s'il n'est pas déjà exécuté.
- ☐ Créez un volume logique dans le groupe de volumes **`vol0`** appelé **`test`** et d'une taille suffisamment importante pour faire office de disque pour votre machine virtuelle.
- ☐ Démarrez une installation de machine virtuelle à l'aide de votre fichier Kickstart **`test.cfg`**. Attribuez le nom **`test`** à la machine virtuelle. Utilisez le support d'installation depuis http://instructor/pub/rhel6/dvd et fournissez à la machine virtuelle 768 Mo de RAM et 1 CPU. Utilisez le volume logique que vous avez créé lors de l'étape précédente comme stockage pour votre machine virtuelle.
- ☐ Réinitialisez votre machine virtuelle une fois l'installation terminée et confirmée.
- ☐ *IMPORTANT :* supprimez votre machine virtuelle ainsi que le volume logique qu'elle utilise pour le stockage, afin de restaurer les ressources requises lors de futurs exercices.



Notes personnelles



Résumé du module

Création d'un fichier Kickstart en modifiant un modèle

Dans cette section, vous avez appris à :

- Modifier une configuration Kickstart existante avec un éditeur de texte

Introduction à la virtualisation KVM

Dans cette section, vous avez appris à :

- Décrire les fonctions de base, les composants et les avantages de la virtualisation KVM

Installation d'invités virtuels

Dans cette section, vous avez appris à :

- Installer un invité virtuel selon des spécifications

Gérer des machines virtuelles

Dans cette section, vous avez appris à :

- Gérer les machines virtuelles à l'aide de l'outil **`virsh`** en ligne de commande



MODULE HUIT

GESTION DU DÉMARRAGE

Introduction

Sujets couverts dans cette unité :

- Résolution des problèmes liés au chargeur de démarrage GRUB
- Apport de modifications de façon durable à la configuration du chargeur de démarrage GRUB
- Modification du niveau d'exécution par défaut
- Utilisation du mode utilisateur unique pour corriger des problèmes d'initialisation
- Résolution des problèmes liés au processus de démarrage
- Utilisation du mode de secours du programme d'installation
- Résolution des problèmes courants liés au démarrage

Résolution des problèmes liés à GRUB

Le GRUB (GRand Unified Bootloader) fournit la passerelle entre le matériel et le noyau Linux lors du processus de démarrage. Lors du démarrage du système, le BIOS démarre et charge normalement GRUB par étapes depuis le disque dur ; d'abord à partir des 446 premiers octets du disque, ensuite depuis l'espace entre le premier secteur et le démarrage de la première partition, enfin, à partir des fichiers de **/boot**. GRUB lit ensuite son fichier de configuration, **/boot/grub/grub.conf**, qui contrôle les systèmes d'exploitation et les noyaux disponibles pour le démarrage.

L'écran de démarrage GRUB

Lors du démarrage du GRUB, un écran d'accueil graphique est accessible en appuyant sur Entrée, la barre d'espace ou toute autre touche. Cet écran comprend une liste de menus, qui correspondent généralement à des images amorçables. Vous pouvez choisir entre différentes images en utilisant les touches de direction haut et bas ; appuyez sur Entrée pour en sélectionner une. Pour transmettre des arguments aux images amorçables via le mode édition du menu ou accéder à la ligne de commande GRUB, vous devez indiquer « p », puis le mot de passe GRUB, s'il est défini.

Correction GRUB temporaire

1. Arrêtez le compte à rebours GRUB : touche **Esc**
2. Utilisez "e" pour éditer la configuration actuelle.
3. Sélectionnez les lignes à corriger à l'aide des touches fléchées.
4. Saisissez "e" à nouveau pour éditer la ligne actuelle.



Note

La touche **Esc** permet de retourner au menu initial sans enregistrer les modifications.

5. La commande « b » démarre avec les modifications actuelles



Références

Red Hat Enterprise Linux Installation Guide

- Annexe technique E.5 : Interfaces GRUB



Exercice de Liste de contrôle des performances

Résoudre les problèmes liés à GRUB

- ☐ Exécutez le script **`lab-setup-bootbreak`** sur desktopX, afin de préparer votre serveur virtuel concernant les problèmes de démarrage.
- ☐ Une fois serverX démarré, exécutez le script **`lab-setup-bootbreak-5`** dessus pour provoquer un problème dans le processus de démarrage.
- ☐ Redémarrez serverX et modifiez temporairement le chargeur de démarrage, afin que le système puisse démarrer et vous, vous connecter.

Modifications permanentes de GRUB

La seconde étape de GRUB utilise **/boot/grub/grub.conf**, qui dispose d'un format d'options globales suivi de stanzas de démarrage. Voici un exemple de fichier **grub.conf**:

```
[root@demo ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/vgsrv-root
#          initrd /initrd-[generic-]version.img
#boot=/dev/vda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux (2.6.32-71.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-71.el6.x86_64 ro root=/dev/mapper/vgsrv-root
 rd_LVM_LV=vgsrv/root rd_LVM_LV=vgsrv/swap rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=en_US.UTF-8
 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=pc KEYTABLE=us crashkernel=auto rhgb quiet
        initrd /initramfs-2.6.32-71.el6.x86_64.img
```

- Les lignes de commentaire commencent par le caractère **#**.
- **default=*number*** - *number* est l'instance de démarrage par défaut (en commençant par 0)
- **timeout=*number*** - spécifie le délai avant le démarrage du compte à rebours
- **hiddenmenu** - masque l'affichage de menu jusqu'à l'utilisation d'une touche
- **rhgb quiet** - envisagez de supprimer ces arguments de noyau pour afficher davantage d'informations de diagnostic au cours du démarrage



Références

Red Hat Enterprise Linux Installation Guide
- Annexe technique E.7 : Fichier de configuration du menu GRUB

Red Hat Enterprise Linux Deployment Guide
- Section 23.6: Vérification du chargeur de démarrage

info grub

e pour éditer
Ajout de "single" pour modifier mot de passe root



Exercice de Liste de contrôle des performances

Résoudre de façon durable un problème lié à GRUB

- ☐ Redémarrez et assurez-vous que le problème précédement traité est persistant. Comme précédemment, vous devrez appliquer le correctif pour démarrer le système.
- ☐ Modifiez le fichier de configuration pour corriger définitivement le problème.
- ☐ Installez un nouveau noyau à partir du référentiel **Errata**.
- ☐ Rétablissez l'ancien noyau. En d'autres termes, en conservant le nouveau noyau disponible, assurez-vous que, lors du redémarrage, le noyau plus ancien est celui par défaut.
- ☐ Redémarrez le système pour confirmer que l'ancien noyau démarre correctement et que vous pouvez vous connecter.

Modification du niveau d'exécution par défaut

Le niveau d'exécution détermine les services qui sont démarrés automatiquement sur votre système Linux. La plupart des systèmes de bureau Linux sont définis pour démarrer au niveau d'exécution 5 (multiutilisateurs, mise en réseau, interface graphique). De nombreux systèmes de serveur démarrent au niveau d'exécution 3 (multi-utilisateur, mise en réseau, aucune connexion graphique), où le système apparaît avec une interface en mode texte.

La commande **who -r** renvoie le niveau d'exécution actuellement utilisé par le système, tout comme le nombre figurant à droite dans la sortie de **runlevel**.

Le niveau d'exécution est lu à partir du fichier **/etc/inittab**. La ligne ci-dessous, par exemple, entraîne le démarrage du système au niveau d'exécution 5 par défaut.

```
id:5:initdefault:
```



Note

Dans Red Hat Enterprise Linux 6, le nouveau système de démarrage **Upstart** est configuré de manière à lire le niveau d'exécution par défaut depuis **/etc/inittab**, à des fins de compatibilité descendante. Aucun des autres services précédemment contrôlés à partir de ce fichier, y compris les invites de connexion, ne peut être défini dans ce fichier depuis RHEL 6. Ces paramètres sont plutôt conservés dans le répertoire **/etc/init/**. Leur fonctionnement sera traité plus en détail ultérieurement dans cette unité.

Modification des niveaux d'exécution

- Exécutez **init *rlnum*** à l'invite du shell, *rlnum* correspondant au numéro du niveau d'exécution. Cela modifie immédiatement le niveau d'exécution.
- Transmettez le numéro du niveau d'exécution en tant qu'argument au noyau via GRUB, lors du démarrage. Le niveau d'exécution par défaut est alors remplacé.



Références

Red Hat Enterprise Linux Installation Guide

- Annexe technique E.8 : Changement du niveau d'exécution au démarrage

Commentaires dans **/etc/inittab**



Exercice de Liste de contrôle des performances

Modifier le niveau d'exécution par défaut

Vous configurez un nouveau système auquel vous accèderez à distance. Le système démarre actuellement au niveau d'exécution 5 par défaut, mais cette machine est hébergée dans un centre de données auquel vous ne vous connecterez qu'à distance. Vous souhaitez modifier le système serverX pour qu'il démarre par défaut au niveau d'exécution 3.

- ☐ Configurez le système pour qu'il démarre par défaut au niveau d'exécution 3.

- ☐ Réinitialisez, puis vérifiez le niveau d'exécution actuel.

Mode utilisateur unique

Le mode utilisateur unique correspond à un niveau d'exécution spécial, qui arrête le processus de démarrage juste avant le démarrage des services système, puis ouvre une invite de shell comme super utilisateur. Il se révèle utile pour le dépannage, lorsqu'un système se bloque uniquement lors du démarrage d'un service. Cela peut être dû à une configuration incorrecte d'un service système ou, dans certains cas, au réseau.

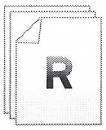
Pour démarrer en mode utilisateur unique, transmettez l'argument **single** au noyau au lieu d'un numéro de niveau d'exécution sur la ligne de commande du noyau depuis le menu GRUB.



Remarque

Dans Red Hat Enterprise Linux 6, lors du démarrage en mode utilisateur unique, le processus **init** lit son fichier **/etc/init/rcS.conf** normalement, qui exécute **/etc/rc.d/rc.sysinit**. Cependant, **init** lit ensuite **/etc/init/rcS-sulogin.conf** (qui interrompt le processus de démarrage et ouvre l'invite de shell racine), au lieu de lire **/etc/init/rc.conf** et d'exécuter des scripts de démarrage de service. (Voir la section suivante pour un diagramme du processus de boot Upstart **init**.)

Dans Red Hat Enterprise Linux 5 et les versions antérieures, le mécanisme de démarrage diffère légèrement. Cependant, le mode utilisateur unique est démarré de manière identique, puis il interrompt le démarrage après l'exécution de **/etc/rc.d/rc.sysinit**, juste avant l'exécution normale des scripts de démarrage de service.



Références

Red Hat Enterprise Linux Installation Guide

- Section 36.1.3 : Démarrage en mode utilisateur unique



Exercice de Liste de contrôle des performances

Modification du mot de passe root

Cet exercice est destiné à vous apprendre à modifier le mot de passe root dans un système avec mot de passe root inconnu.

- ☐ Commencez par exécuter le script **`lab-setup-bootbreak-4`** sur serverX. Cela modifiera le mot de passe en un élément inconnu et indiquera l'heure du jour.
- ☐ Entrez dans le système et réinitialisez le mot de passe root en **`redhat`**.



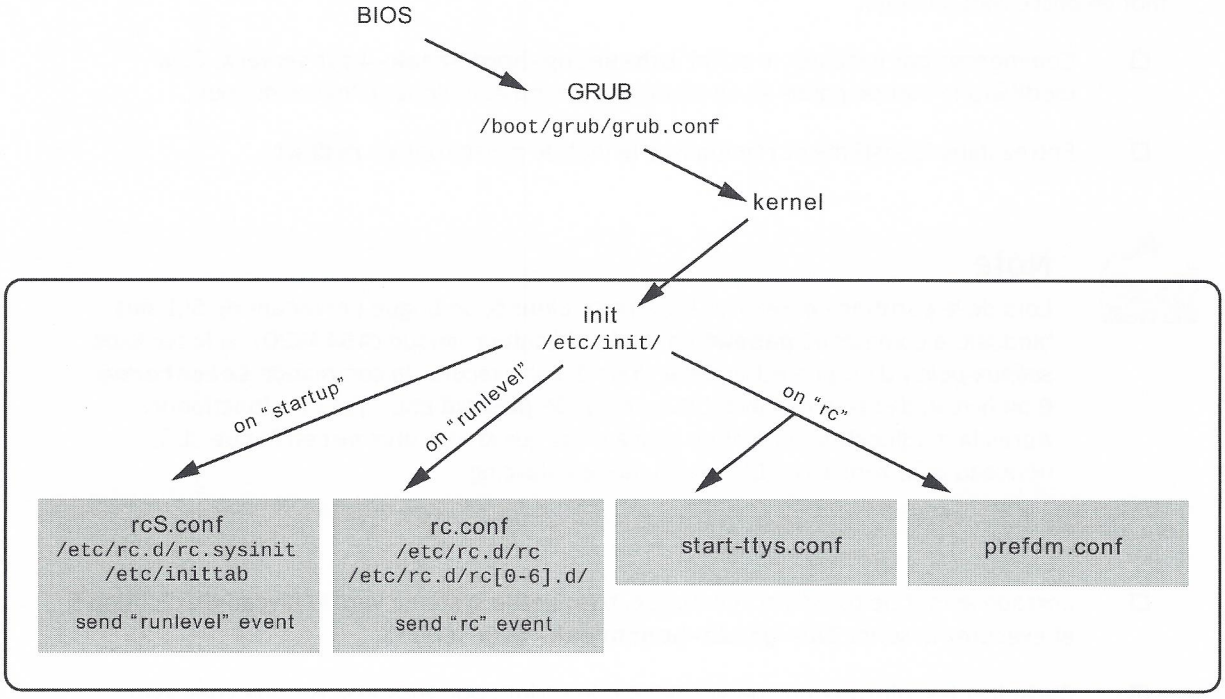
Note

Lors de la parution de Red Hat Enterprise Linux 6, un bogue provenant de SELinux bloquait la commande **`passwd`** en mode utilisateur unique (#644820). Si le package *selinux-policy* d'origine est installé, vous devez exécuter la commande **`setenforce 0`** au niveau d'exécution1 avant la commande **`passwd`** pour que cela fonctionne. Après la modification du mot de passe, vous devez exécuter **`setenforce 1`** à nouveau pour remettre SELinux en mode enforcing.

- ☐ Lorsque le mot de passe est réinitialisé, basculez le système vers le niveau d'exécution 5 et exécutez le script **`lab-grade-bootbreak-4`** sur serverX.
- ☐ Consultez les informations renvoyées par le script pour vous assurer que vous avez correctement mené à bien la tâche. Le script de notation affiche une heure, notez-la.
- ☐ Répétez au moins cinq fois ce processus.
- ☐ Entourez votre meilleur temps.

La séquence de démarrage et le mode de secours

La séquence de démarrage de Red Hat Enterprise Linux 6 figure dans le diagramme simplifié ci-dessous, depuis la mise sous tension jusqu'à l'invite de connexion apparaissant à l'écran.



BIOS

Le BIOS, ou Basic Input/Output System, correspond à l'interface de microprogramme intégrée au matériel x86/x86-64 standard, qui place le matériel dans un état connu et prépare le système en vue du chargement d'un système d'exploitation.

Que se passe-il ?

- Détecte et démarre le matériel
- Détermine le périphérique à partir duquel effectuer le démarrage

Quelle peut être la cause ?

- Des paramètres BIOS incorrects ou étranges
- Un ordre de démarrage de périphériques incorrect

De quelle manière peut-il être interrompu ou influencé ?

- Utilisation d'une touche spécifique au fabricant
- Utilisation d'un utilitaire de configuration spécifique au fabricant
- Souvent, <F12> peut effectuer un remplacement unique de l'ordre de démarrage

GRUB

GRUB (GRand Unified Bootloader) est chargé par le BIOS et sert à sélectionner et à démarrer le système d'exploitation, comme nous l'avons déjà expliqué.

Que se passe-il ?

- Charge le système de fichiers RAM initial (« initramfs »)
- Charge et exécute un noyau
- Fournit une ligne de commande du noyau

Quelle peut être la cause ?

- Configuration incorrecte du chargeur de démarrage
- Image ou initramfs de noyau incorrect
- Ligne de commande de noyau incorrecte

De quelle manière peut-il être interrompu ou influencé ?

- Choisissez un autre élément de menu pré-configuré
- Utilisez « e » ou « a » pour sélectionner une autre image de noyau ou modifier la ligne de commande du noyau
- Modifiez la ligne de commande du noyau pour démarrer à partir du mode utilisateur **`single`**
- Démarrez avec **`init=/bin/bash`**

Noyau

Le noyau Linux constitue le coeur du système d'exploitation. Il est responsable de la gestion de l'accès au matériel pour les processus d'espace utilisateur. Les pilotes et l'hyperviseur KVM sont des pièces intégrées du noyau.

Que se passe-il ?

- Détecter les périphériques matériels
- Charger les pilotes (modules) pour les périphériques



Note

Où le noyau obtient-il les modules à charger au démarrage ?

1. Initialement, il utilise le disque de mémoire vive d'origine configuré pour le noyau dans **`/boot/grub/grub.conf`**: **`/boot/initramfs-<VERSION>.img`**
2. Une fois le système de fichiers racine monté, il utilise **`/lib/modules/<VERSION>/`**

- Monter le système de fichiers racine en lecture seule

- Démarrer le processus initial, **init**

Quelle peut être la cause ?

- Image du système de fichiers RAM initial incorrecte
- Système de fichiers racine incorrectement identifié
- Système de fichier racine corrompu

De quelle manière peut-il être interrompu ou influencé ?

- En général, uniquement via les options GRUB

init et Upstart

Le premier processus d'espace utilisateur démarré sur la machine est **/sbin/init**. Le processus **init** est responsable du démarrage de tous les processus d'espace utilisateur restants, de manière directe ou indirecte.

Que se passe-il ?

- Une fois que le noyau est en cours d'exécution, il démarre **init**. Le programme **init** est chargé de terminer la séquence de démarrage en lançant tous les processus système autres que le noyau.

  Avec **Upstart**, **init** démarre des « tâches » lorsque différents « événements » se produisent, comme le démarrage du système, l'entrée d'un niveau d'exécution ou le démarrage ou l'arrêt d'une autre tâche**init** Ces tâches sont stockées sous forme de scripts dans le répertoire **/etc/init/**. Lors du démarrage, l'événement de démarrage provoque l'exécution par **init** de la tâche **/etc/init/rcS.conf** qui :

  - Exécute **/etc/rc.d/rc.sysinit** pour démarrer LVM, monter et vérifier les systèmes de fichiers, régler l'heure système et effectuer d'autres opérations générales.
  - Recherche le niveau d'exécution dans **/etc/inittab**.
  - Envoie un événement à **init** pour lui indiquer de passer à ce niveau d'exécution.

  L'événement de niveau d'exécution entraîne l'exécution par **init** de la tâche **/etc/init/rc.conf** qui exécute le script **/etc/rc.d/rc** avec le niveau d'exécution souhaité comme argument :

  - Exemple : **rc.conf** exécute **rc 5**, qui exécute **/etc/rc.d/rc5.d/K* stop** et **/etc/rc.d/rc5.d/S* start**.
  - Les scripts sont exécutés par ordre numérique, d'abord les K puis les S.
  - Les scripts **/etc/rc.d/rc5.d/** sont des liens symboliques vers les scripts utilisés par le service.
  - La première lettre des liens, K ou S, dépend de l'état **on** ou **off** défini avec **chkconfig**.

  Des versions plus anciennes de Red Hat Enterprise Linux ont une autre implémentation de **init** qui fonctionne différemment.

Quelle peut être la cause ?

- **/etc/fstab** ou **/etc/crypttab** mutilé
- Configuration incorrecte du réseau ou d'un service entraînant le blocage des services
- Nombreuses autres causes probables...

De quelle manière peut-il être interrompu ou influencé ?

- Appuyez sur « Alt-D » depuis l'environnement graphique pour afficher les messages d'erreur
- Appuyez sur « I » (i majuscule) pendant le démarrage du service pour sélectionner des services de manière interactive



Note

Red Hat Enterprise Linux 5 et les versions antérieures utilisaient une implémentation différente de **init**, **SysVinit**, gérée par des directives du fichier **/etc/inittab**. La séquence de démarrage de base et les scripts exécutés par **init** étaient cependant similaires.



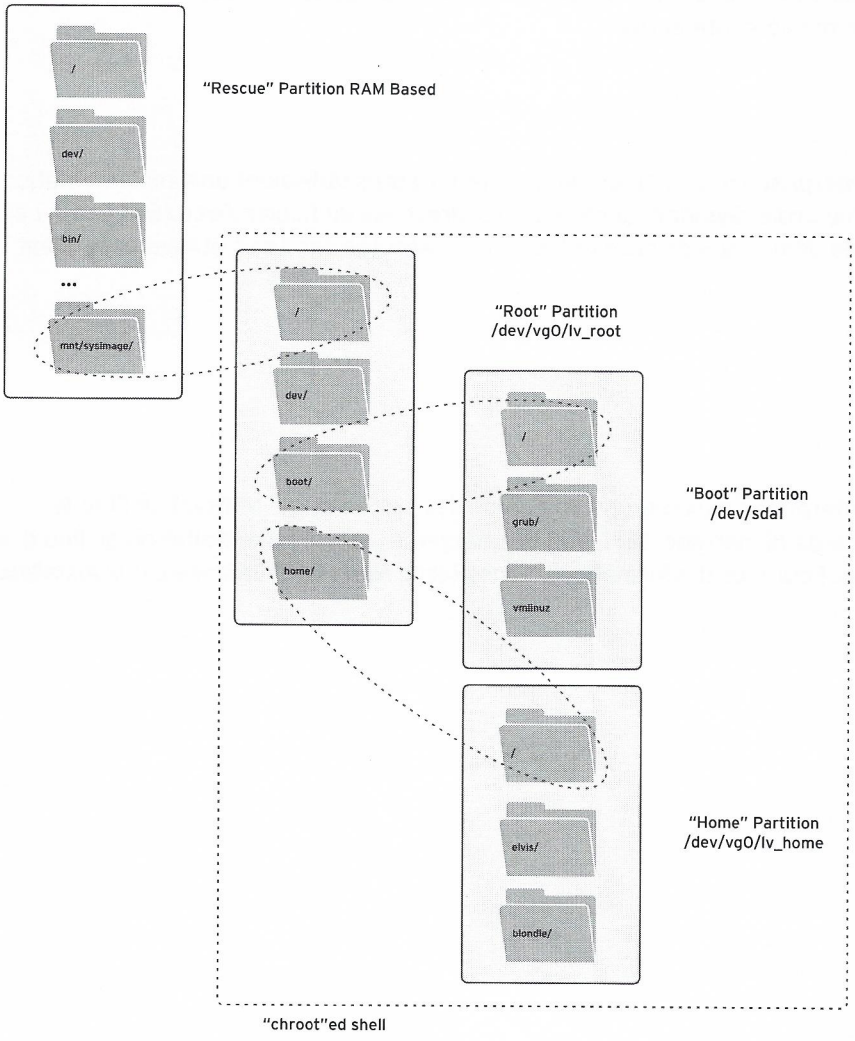
Note

Red Hat Enterprise Linux 6 prend en charge des systèmes qui utilisent UEFI et le gestionnaire de démarrage UEFI, afin de charger le système d'exploitation au lieu d'un BIOS et de GRUB. Pour plus d'informations, consultez le *Red Hat Enterprise Linux Installation Guide*.

Le shell de secours

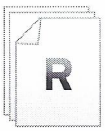
Les modes de récupération se révèlent utiles lorsque vous pouvez utiliser le GRUB, mais que se passe-t-il si ce dernier ne fonctionne plus ? Le shell de secours, qui correspond à un mode spécial du programme d'installation, vous permet de démarrer et de récupérer le système lorsque cela est impossible autrement.

Pour accéder au shell de secours, démarrez une installation, puis choisissez *Rescue installed system* (Dépanner le système installé) à partir du menu initial ou ajoutez **rescue** comme argument au noyau.



Souvent, la première chose que vous souhaitez faire dans le shell de secours est d'accéder ou de récupérer des systèmes de fichiers sur votre disque dur local. Le mode de secours tente de monter le système de fichiers racine de votre système (et d'autres) sous **/mnt/sysimage**, tel que cela est illustré ci-dessus.

Une astuce utile consiste à utiliser **chroot /mnt/sysimage** pour démarrer un sous-shell, où **/** correspond au système de fichiers racine de votre disque dur.



Références

Red Hat Enterprise Linux Deployment Guide
- Section 3.2.2: Utilisation de RPM - Installation et mise à niveau

Red Hat Enterprise Linux Deployment Guide
- Section 23.6: Vérification du chargeur de démarrage

Red Hat Enterprise Linux Installation Guide
- Section 36.1: Mode de secours

Red Hat Enterprise Linux Installation Guide
- Annexe technique E: Chargeur de démarrage GRUB

Red Hat Enterprise Linux Installation Guide
- Annexe technique F: Séquence de démarrage, init et arrêt

`info chroot`

`info grub`



Exercice de Exercice

Utilisation du mode de secours

Avant de commencer...

Exécutez **`lab-setup-bootbreak`** sur desktopX.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Cette exploration automatique a été conçue de manière à vous exercer à l'accès au mode de secours. Le chemin d'installation est *http://instructor.example.com/pub/rhel6/dvd*. Le chemin pour les packages individuels est *http://instructor.example.com/pub/rhel6/dvd/Packages/*

1. Une fois que serverX a démarré, exécutez le script **`lab-setup-bootbreak-0`**. Ce script modifiera votre système et entraînera des problèmes de démarrage.
2. Démarrez en mode de secours pour diagnostiquer et résoudre le problème.
3. Confirmez que celui-ci a été résolu en redémarrant le système.
4. Répétez ce processus aussi souvent que possible au cours de la période allouée.

Résolution des problèmes de démarrage

Réinstallation de GRUB

La première étape du GRUB correspond à un petit binaire installé dans le bloc de démarrage d'un disque amorçable. En général, le GRUB est installé par le programme d'installation Anaconda et ne doit jamais être réinstallé. Parfois, lors de l'endommagement ou du déplacement d'un disque, vous devez éventuellement procéder à la réinstallation manuelle du GRUB.

Procédure de réintallation du GRUB

1. Appelez GRUB

```
[root@serverX ~]# grub
```

2. Identifiez le partitionnement de **/boot**

```
grub> root (hd0,0)
```

GRUB fait référence aux disques durs tels que **(hd0)** ou **(hd1)**, qui correspondent à « BIOS drive #0 » ou « BIOS drive #1 ». Le lecteur réel peut varier en fonction du BIOS. La première partition sur **(hd0)** serait **(hd0,0)**, qui peut être **/dev/sda1** ou **/dev/vda1**.

3. Installez le grub de la première étape dans le bloc de démarrage

```
grub> setup (hd0)
```

4. Quittez grub

```
grub> quit
```

Réparation de systèmes de fichiers endommagés

Lors du fonctionnement normal, le noyau conserve les informations de système de fichiers fréquemment consultées en mémoire. En outre, il valide uniquement de manière périodique les informations sur le disque. Si un système de fichiers devient indisponible de manière inattendue (en raison d'une panne d'alimentation électrique ou d'un problème de connectivité physique), le système de fichiers sur disque contiendra des incohérences. Si ces erreurs ne sont pas corrigées, elles risquent d'engendrer des données corrompues.

La commande **fsck** tentera de restaurer un système de fichiers dans un état auto-cohérent. **fsck** ne garantit pas une récupération complète des données, mais une cohérence du système de fichiers. Lors du démarrage, les scripts de démarrage utiliseront automatiquement **fsck** pour tous les systèmes de fichiers (s'ils sont marqués dans **/etc/fstab**). Les problèmes mineurs seront résolus sans interaction. Si la réparation automatique d'un système de fichiers peut entraîner la perte de données, la séquence de démarrage permet d'accéder à un shell, afin qu'un administrateur puisse exécuter **fsck** de manière interactive. Si la partition racine est endommagée, le mode de secours doit éventuellement être initialisé pour exécuter **fsck**

1. Démontez le système de fichiers **/boot** sur **/dev/vda1**.

```
[root@demo ~]# umount /dev/vda1
```

2. Vérifiez le système de fichiers sur **/dev/vda1**.

```
[root@demo ~]# fsck /dev/vda1
```

3. Remontez le système de fichiers **/boot**.

```
[root@demo ~[# mount /dev/vda1
```

Procédure de modification de fichiers à partir du shell de maintenance

Cette opération est parfois nécessaire lorsqu'un système ne peut pas monter de systèmes de fichiers, en raison d'erreurs de frappe dans **/etc/fstab**, **/etc/crypttab**, ou des fichiers connexes, et que le système accède à un shell de maintenance avec / monté en lecture seule.

1. Remontez le système de fichiers racine en lecture-écriture :

```
(Repair filesystem 1)# mount -o remount,rw /
```

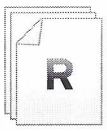
2. Montez tous les autres systèmes de fichiers (le cas échéant) :

```
(Repair filesystem 2)# mount -a
```

3. Modifiez tout fichier qui le nécessite.

4. Quittez le shell de maintenance :

```
(Repair filesystem 4)# exit
```



Références

Red Hat Magazine : « Utilisation de GRUB pour résoudre les problèmes de démarrage »
http://magazine.redhat.com/2007/03/21/using-grub-to-overcome-boot-problems/



Exercice de Questionnaire

Questionnaire de résolution des problèmes

1. En mode maintenance, exécutez mount -o remount,rw / pour marquer la partition / comme accessible en écriture.

2. En supposant que vous disposiez d'un seul disque dur, et que la première partition contienne /boot, en cas de corruption mineure du bloc de démarrage, corrigez ce problème en démarrant en mode de _____, puis exécutez la commande _____. Tapez _____, suivi de _____, puis quittez.

3. Si vous rencontrez des problèmes de corruption de système de fichiers, la machine démarre alors en mode _____.

4. En mode maintenance, exécutez _____ pour résoudre les problèmes de corruption du _____.



Test

Test de critère

Exercice

Dépannage de la séquence de démarrage

Avant de commencer...

Exécutez la commande **`lab-setup-bootbreak`** sur desktopX pour configurer l'exercice.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Cet exercice pratique inclut trois défis de provocation/réparation de panne. Pour chacun d'entre eux, votre machine virtuelle serverX est modifiée de manière à empêcher son démarrage correct, vous devez ensuite diagnostiquer et corriger le problème.

1. Exécutez **`lab-setup-bootbreak-1`** sur serverX. Après l'exécution du script, serverX ne doit plus démarrer correctement. Diagnostiquez et corrigez le problème. Lorsque serverX démarre de nouveau normalement, cela signifie que vous avez trouvé la solution.

2. Lorsque vous avez résolu le premier scénario, répétez la séquence avec **`lab-setup-bootbreak-2`** et **`lab-setup-bootbreak-3`**.

Notes personnelles



Résumé du module

Résolution des problèmes liés à GRUB

Dans cette section, vous avez appris à :

- Utiliser GRUB pour corriger une configuration GRUB défectueuse et démarrer le système

Modifications permanentes de GRUB

Dans cette section, vous avez appris à :

- Corriger en permanence un défaut de configuration GRUB
- Configurer et démarrer le système en utilisant un noyau par défaut différent

Modification du niveau d'exécution par défaut

Dans cette section, vous avez appris à :

- Utiliser GRUB pour démarrer le système en utilisant un niveau d'exécution spécifique

Mode utilisateur unique

Dans cette section, vous avez appris à :

- Passer en mode utilisateur unique
- Utiliser le mode utilisateur unique pour réparer les problèmes de démarrage

La séquence de démarrage et le mode de secours

Dans cette section, vous avez appris à :

- Décrire la séquence de démarrage pour Red Hat Enterprise Linux 6

Résolution des problèmes de démarrage

Dans cette section, vous avez appris à :

- Réinstaller GRUB
- Vérifier et réparer des erreurs sur des systèmes de fichiers
- Modifier des fichiers à partir du shell de maintenance du système de fichiers en lecture seule



MODULE NEUF

GESTION DE SELINUX

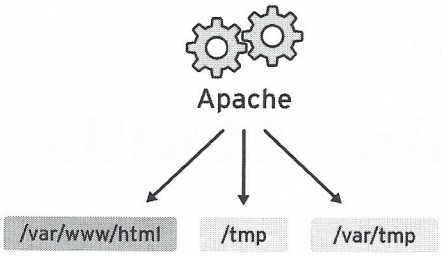
Introduction

Sujets couverts dans cette unité :

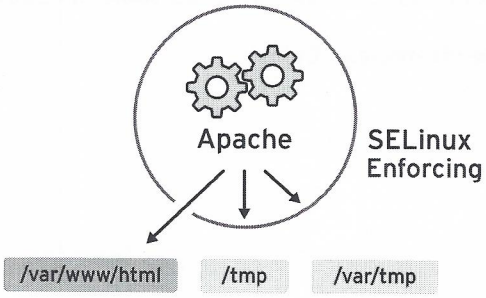
- Révision des concepts SELinux de base
- Affichage et configuration des modes SELinux
- Affichage et configuration des contextes de fichiers SELinux
- Affichage du comportement des stratégies avec les booléens SELinux
- Contrôle des violations de stratégies SELinux

Concepts de sécurité SELinux de base

SELinux, Security-Enhanced Linux, est une méthode complémentaire pour protéger votre système.



Si nous voulons permettre l'accès anonyme à distance à un serveur Web, nous devons alors ouvrir les ports via le pare-feu. Cependant, cela risque de permettre à des personnes mal intentionnées de s'introduire dans le système via une faille de sécurité, et si elles parviennent à compromettre le processus du serveur Web, elles pourront s'approprier ses autorisations, c'est-à-dire les autorisations de l'utilisateur apache et du groupe apache. Cet utilisateur/groupe dispose d'un accès en lecture pour des éléments tels que la racine des documents (**`/var/www/html`**), ainsi que d'un accès en écriture pour **`/tmp`**, **`/var/tmp`** et autres fichiers/répertoires universels.



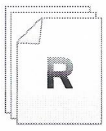
SELinux est un ensemble de règles de sécurité qui déterminent quel processus peut accéder à quels fichiers, répertoires, ports, etc. Chaque fichier, processus, répertoire et port dispose d'une étiquette de sécurité spéciale appelée contexte SELinux. Un contexte est simplement un nom utilisé par la stratégie SELinux pour déterminer si un processus peut ou non accéder à un fichier, un répertoire ou un port. Par défaut, la stratégie n'autorise aucune interaction, se sont donc les règles explicites qui autorisent les accès. S'il n'existe aucune règle d'accès, aucun accès n'est autorisé.

Les étiquettes SELinux ont différents contextes, mais celui qui nous intéresse est le troisième : le contexte de type. Les noms des contextes de types se terminent généralement par **`_t`**. Le contexte de type pour le serveur Web est **`httpd_t`**. Le contexte de type pour les fichiers et répertoires qui se trouvent généralement dans **`/var/www/html`** est **`httpd_sys_content_t`**. Les contextes de types pour les fichiers et répertoires qui se trouvent généralement dans **`/tmp`** et **`/var/tmp`** est **`tmp_t`**. Le contexte de type pour les ports de serveur Web est **`http_port_t`**.

Il existe une règle dans la stratégie qui permet à Apache (le processus du serveur Web qui s'exécute comme **`httpd_t`**) d'accéder à des fichiers et des répertoires avec un contexte

que l'on trouve généralement dans **/var/www/html** et d'autres répertoires de serveur Web (**httpd_sys_content_t**). La stratégie ne contient aucune règle d'accès pour les fichiers qui se trouvent généralement dans **/tmp** et **/var/tmp**, de sorte que l'accès n'est pas autorisé. Avec SELinux, un utilisateur malveillant ne peut pas accéder au répertoire **/tmp**, et encore moins y enregistrer des fichiers. SELinux dispose même de règles pour les systèmes de fichiers distants tels que NFS et CIFS, bien que tous les fichiers de ces systèmes de fichiers aient le même contexte.

L'un des objectifs de SELinux est de protéger les données utilisateur des services système qui ont été compromis.



Références

Red Hat Enterprise Linux SELinux Guide

- Section 2 : Introduction



Exercice de Questionnaire

Concepts SELinux de base

1. Parmi les éléments suivants SELinux, auxquels applique-t-il des contextes de sécurité (sélectionnez toutes les réponses correctes) ?

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. Ports
   b. Processus
   c. Fichiers
   d. Répertoires
   e. Systèmes de fichiers distants

2. SELinux peut être utilisé pour :

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. Empêcher un service de s'exécuter sur d'autres ports.
   b. Protéger les données de l'utilisateur d'applications telles que le serveur Web.
   c. Bloquer les systèmes distants afin qu'ils n'accèdent pas à des ports locaux.
   d. Garder le système à jour.
   e. Accéder à un serveur Web.

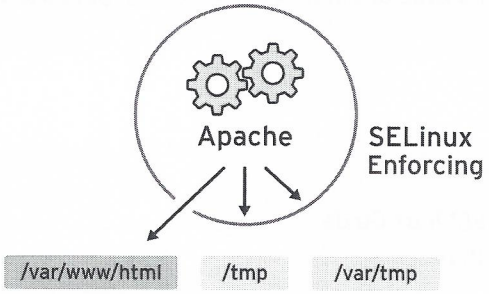
3. Parmi les éléments suivants, lesquels sont des types de contextes SELinux standard ?

   (sélectionnez une ou plusieurs des réponses suivantes...)

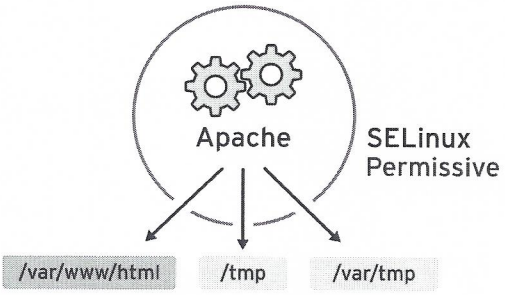
   a. selinux_type
   b. object_r
   c. httpd_sys_content_t
   d. tmp_t
   e. user_u

Modes SELinux

À des fins de dépannage, nous pouvons désactiver temporairement la protection SELinux à l'aide des modes SELinux.



En *mode enforcing*, SELinux refuse activement l'accès au serveur Web qui tente de lire les fichiers avec le contexte de type **`tmp_t`**. En mode enforcing, SELinux connecte et protège.



Le mode permissif est souvent utilisé pour résoudre les problèmes. En mode permissif, SELinux autorise toutes les interactions même sans règle explicite et connecte toutes les interactions refusées. Ce mode peut être utilisé pour déterminer si vous avez des problèmes avec SELinux. Aucun redémarrage n'est requis pour passer du mode enforcing au mode permissif et réciproquement.

Un troisième mode, *désactivé*, désactive complètement SELinux. Vous devez redémarrer pour désactiver complètement SELinux, ou pour basculer du mode désactivé au mode enforcing ou permissif.



Important

Si vous envisagez de réactiver les restrictions SELinux, il est préférable d'utiliser le mode permissif au lieu de désactiver SELinux complètement. La raison étant que même en mode permissif, le noyau mettra automatiquement à jour les étiquettes du système de fichiers SELinux comme il convient, ce qui évite de devoir réétiqueter le système de fichiers lorsque vous redémarrez le système avec SELinux réactivé, ce qui peut s'avérer fastidieux.



Références

Red Hat Enterprise Linux SELinux Guide

- Section 5.5: Modes SELinux



Exercice de Questionnaire

Modes SELinux

1. Le mode _____ de SELinux permet la connexion, mais pas la protection.

2. Le mode _____ de SELinux protège le système.

3. Parmi les éléments suivants, lesquels sont des modes SELinux valides ?

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. enforcing
   b. testing
   c. permissive
   d. disabled
   e. logging

Afficher et modifier les modes SELinux

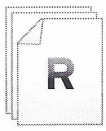
Comme vous pouvez le constater, **/etc/sysconfig/selinux** contient des commentaires utiles :

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Utilisez **/etc/sysconfig/selinux** pour modifier le mode SELinux par défaut lors du démarrage du système. Dans l'exemple ci-dessus, le mode enforcing est activé.

Pour afficher le mode SELinux actif, utilisez **getenforce**. Pour modifier le mode SELinux actif, utilisez **setenforce**.

```
[root@serverX ~]# getenforce
Enforcing
[root@serverX ~]# setenforce
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
[root@serverX ~]# setenforce 0
[root@serverX ~]# getenforce
Permissive
[root@serverX ~]# setenforce Enforcing
[root@serverX ~]# getenforce
Enforcing
```



Références

Red Hat Enterprise Linux SELinux Guide

- Section 5.5 : Modes SELinux

Pages man **selinux**(8), **getenforce**(1), **setenforce**(1)



Exercice de Exercice

Modification des modes enforcing et permissif

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Sur serverX, activez le mode permissif comme mode SELinux par défaut et redémarrez le système.
2. Une fois le système redémarré, vérifiez qu'il est en mode permissif.
3. Activez le mode enforcing comme mode SELinux par défaut.
4. Activez le mode enforcing comme mode SELinux actif.

Afficher et modifier les contextes de fichiers SELinux

De nombreuses commandes qui s'appliquent aux fichiers ont une option (en général **-Z**) pour afficher ou définir des contextes SELinux. Par exemple, **ps**, **ls**, **cp** et **mkdir** utilisent toutes l'option **-Z** pour afficher ou définir des contextes SELinux.

```
[root@serverX ~]# ps axZ
LABEL                               PID TTY      STAT   TIME COMMAND
system_u:system_r:init_t:s0           1 ?        Ss     0:00 /sbin/init
system_u:system_r:kernel_t:s0         2 ?        S      0:00 [kthreadd]
system_u:system_r:kernel_t:s0         3 ?        S      0:00 [migration/0]
...
[root@serverX ~]# service httpd start
[root@serverX ~]# ps -ZC httpd
LABEL                               PID TTY          TIME CMD
unconfined_u:system_r:httpd_t:s0 27672 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 27675 ?        00:00:00 httpd
...
[root@serverX ~]# ls -Z /home
drwx------. root    root    system_u:object_r:lost_found_t:s0 lost+found
drwx------. student student unconfined_u:object_r:user_home_dir_t:s0 student
drwx------. visitor visitor unconfined_u:object_r:user_home_dir_t:s0 visitor
[root@serverX ~]# ls -Z /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
```

Quel élément détermine le contexte SELinux initial d'un fichier ? Normalement, il s'agit du répertoire parent. Le contexte du répertoire parent est affecté au fichier nouvellement créé. Cela fonctionne pour les commandes telles que **vim**, **cp** et **touch**, cependant, si un fichier est créé ailleurs et si les autorisations sont conservées (comme avec **mv** ou **cp -a**), le fichier conservera également le contexte SELinux. La stratégie comporte des règles spéciales, appelées règles de transition de type, qui peuvent changer le contexte de type par défaut. Ces règles ne sont pas abordées dans ce cours.

```
[root@serverX ~]# ls -Zd /var/www/html/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
[root@serverX ~]# touch /var/www/html/index.html
[root@serverX ~]# ls -Z /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/
index.html
```

semanage fcontext peut être utilisée pour afficher ou modifier les règles que **restorecon** utilise pour définir les contextes de fichier par défaut. Elle utilise les expressions régulières étendues pour spécifier le chemin d'accès et le nom des fichiers. L'expression régulière étendue la plus courante utilisée dans les règles **fcontext** est **(/.*)?**, ce qui signifie *éventuellement, avec un / suivi de n'importe quel nombre de caractères.* Essentiellement, elle recherche le répertoire avant l'expression et tout ce qui se trouve dans ce répertoire de façon récursive.

restorecon fait partie du package **policycoreutil** et **semanage** fait partie du package **policycoreutil-python**.

```
[root@serverX ~]# touch /tmp/file1 /tmp/file2
[root@serverX ~]# ls -Z /tmp/file*
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/file2
[root@serverX ~]# mv /tmp/file1 /var/www/html/
[root@serverX ~]# cp /tmp/file2 /var/www/html/
[root@serverX ~]# ls -Z /var/www/html/file*
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
[root@serverX ~]# semanage fcontext -l
...
/var/www(/.*)?                                     all files
 system_u:object_r:httpd_sys_content_t:s0
...
[root@serverX ~]# restorecon -Rv /var/www/
restorecon reset /var/www/html/file1 context unconfined_u:object_r:user_tmp_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
[root@serverX ~]# ls -Z /var/www/html/file*
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/file1
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
```

L'exemple suivant montre comment utiliser **semanage** pour ajouter un contexte pour un nouveau répertoire.

```
[root@serverX ~]# mkdir /virtual
[root@serverX ~]# touch /virtual/index.html
[root@serverX ~]# ls -Zd /virtual/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual/
[root@serverX ~]# ls -Z /virtual/
-rw-r--r--. root root unconfined_u:object_r:default_t:s0 index.html
[root@serverX ~]# semanage fcontext -a -f "" -t httpd_sys_content_t '/virtual(/.*)?'
[root@serverX ~]# restorecon -RFvv /virtual
[root@serverX ~]# ls -Zd /virtual/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /virtual/
[root@serverX ~]# ls -Z /virtual/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 index.html
```



Références

Red Hat Enterprise Linux SELinux Guide

- Section 5.7 : Contextes SELinux - Étiquetage de fichiers

Pages manuel **restorecon** et **semanage**



Exercice de Exercice

Correction de contextes de fichiers SELinux

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Vous avez été invité à régler la configuration DNS de votre machine distante pour qu'elle corresponde exactement à la configuration de votre machine de bureau. Vous déterminez la manière la plus facile de copier le fichier **/etc/resolv.conf** de votre machine locale vers la machine distante.

1. Transférez le fichier **/etc/resolv.conf** depuis votre machine de bureau vers le répertoire personnel de *root* sur serverX.

2. Émettez une commande shell sur serverX en tant que **root**. Toutes les étapes suivantes doivent être effectuées sur votre serveur.

3. Observez le contexte SELinux du fichier **/etc/resolv.conf** initial.

   Contexte **/etc/resolv.conf** initial :
   net_conf_t

4. Déplacez **resolv.conf** du répertoire personnel du *root* vers **/etc/resolv.conf**.

5. Observez le contexte SELinux du fichier **/etc/resolv.conf** récemment copié.

   Nouveau contexte **/etc/resolv.conf** :
   admin_home_t

6. Restaurez le contexte SELinux de votre fichier **/etc/resolv.conf** récemment positionné.

7. Observez le contexte SELinux du fichier **/etc/resolv.conf** restauré.

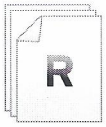
   Contexte **/etc/resolv.conf** restauré :

Gestion des booléens SELinux

Les booléens SELinux sont des commutateurs qui modifient le comportement de la stratégie SELinux. Les booléens SELinux sont des règles pouvant être activées ou désactivées. Ils peuvent être utilisés par les administrateurs pour affiner la stratégie afin de procéder à des ajustements sélectifs. De nombreux packages comportent des pages man ***_selinux(8)** qui peuvent détailler certains des booléens qu'ils utilisent. **man -k '_selinux'** permet de trouver ces pages man facilement.

getsebool permet d'afficher les booléens et **setsebool** permet de les modifier. **setsebool -P** modifie la stratégie SELinux pour que la modification soit permanente. **semanage boolean -l** indique si un booléen est permanent ou non.

```
[root@serverX ~]# getsebool -a
abrt_anon_write --> off
allow_console_login --> on
allow_corosync_rw_tmpfs --> off
...
[root@serverX ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
[root@serverX ~]# setsebool httpd_enable_homedirs on
[root@serverX ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          -> off   Allow httpd to read home directories
[root@serverX ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
[root@serverX ~]# setsebool -P httpd_enable_homedirs on
[root@serverX ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          -> on    Allow httpd to read home directories
```



Références

Red Hat Enterprise Linux SELinux Guide

- Section 5.6: Booléens

Pages manuel **booleans**(8), **getsebool**(8), **setsebool**(8), **semanage**(8)



Exercice de Questionnaire

Booléens SELinux :

Quelle commande répertorie l'état actuel de tous les booléens SELinux ?

getsebool -a

Quelle commande active immédiatement le booléen *httpd_enable_cgi* ?

setsebool httpd_enable_cgi on

Quelle commande active le booléen *ftp_home_dir* immédiatement et lors des redémarrages ?

setsebool ftp_home_dir on

Quelle commande affiche la configuration actuelle des booléens SELinux, ainsi que les annotations abrégées du booléen ?

semanage boolean -l

Contrôler les violations SELinux

Le package **setroubleshoot-server** doit être installé pour envoyer les messages SELinux à **/var/log/messages**. **setroubleshoot-server** écoute les messages d'audit dans **/var/log/audit/audit.log** et envoie un court résumé à **/var/log/messages**. Ce résumé comprend les identificateurs uniques (*UUIDs*) des violations SELinux. Ces identificateurs sont utiles pour recueillir des informations complémentaires. **sealert -l *UUID*** permet de produire un rapport pour un incident spécifique. **sealert -a /var/log/audit/audit.log** permet de produire des rapports pour tous les incidents dans ce fichier.

```
[root@serverX ~]# touch /root/file3
[root@serverX ~]# mv /root/file3 /var/www/html
[root@serverX ~]# service httpd start
[root@serverX ~]# elinks -dump http://serverX/file3
                                 Forbidden
   You don't have permission to access /file3 on this server.
[root@serverX ~]# tail /var/log/audit/audit.log
...
type=AVC msg=audit(1292526292.144:952): avc:  denied  { getattr } for
  pid=27675 comm="httpd" path="/var/www/html/file3" dev=dm-1 ino=54545
 scontext=unconfined_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0
 tclass=file
...
[root@serverX ~]# tail /var/log/messages
...
Dec 16 14:04:59 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd "getattr"
 access to /var/www/html/file3. For complete SELinux messages. run sealert -l e6e1d1d6-
d716-4e2e-863c-bba4d2b2407a
[root@serverX ~]# sealert -l e6e1d1d6-d716-4e2e-863c-bba4d2b2407a
Summary:

SELinux is preventing /usr/sbin/httpd "getattr" access to /var/www/html/file3.

Detailed Description:

SELinux denied access requested by httpd. /var/www/html/file3 may be a
mislabeled. /var/www/html/file3 default SELinux type is httpd_sys_content_t, but
its current type is admin_home_t. Changing this file back to the default type,
may fix your problem.
...
Allowing Access:

You can restore the default system context to this file by executing the
restorecon command. restorecon '/var/www/html/file3', if this file is a
directory, you can recursively restore using restorecon -R
'/var/www/html/file3'.

Fix Command:

/sbin/restorecon '/var/www/html/file3'
...
```



Note

La section « Allowing Access » suggère **`restorecon /var/www/html/file3`**. Il peut y avoir d'autres fichiers devant être ajustés, **`restorecon`** peut redéfinir de façon récursive le contexte : **`restorecon -R /var/www/`**.



Références

Red Hat Enterprise Linux SELinux Guide
- Chapitre 8 : Résolution des problèmes

Red Hat Enterprise Linux SELinux Guide
- Section 8.3.7 : Messages **`sealert`**

Page man **`sealert`**(8)



Exercice de Questionnaire

Contrôle des violations SELinux

1. Quel fichier contient les entrées de journal qui fournissent les identificateurs uniques des violations SELinux ?

   _____.

2. Avec l'UUID d'une violation SELinux, quelle commande génère un rapport texte sur le problème ?

   _____



Test

Test de critère

Exercice

Gestion de SELinux

Avant de commencer...

Avant de commencer, exécutez la commande **`lab-setup-selinux`** sur desktopX

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Connectez-vous à serverX en tant que **`student`**. Ouvrez un terminal et basculez vers l'utilisateur **`root`**.
2. Copiez l'archive *web_content.tgz* de *instructor:/var/ftp/pub/materials* vers **`/tmp`**.
3. Extrayez l'archive dans **`/tmp`**.
4. Déplacez le répertoire extrait vers **`/var/www/html`**.
5. Démarrez le service Web.
6. Essayez d'observer le nouveau répertoire avec votre navigateur Web en accédant à l'adresse URL *http://serverX/web_content*.
7. Recherchez dans votre système les UUID de toute violation SELinux que votre tentative de parcours du nouveau contenu installé peut avoir générée.
8. Générez les rapports texte des violations.
9. Suivez le conseil dans le rapport et restaurez les contextes SELinux du nouveau contenu installé.
10. Vérifiez que vous pouvez afficher le contenu dans votre navigateur Web en accédant à l'adresse URL *http://serverX/web_content*.



Notes personnelles



Résumé du module

Concepts de sécurité SELinux de base

Dans cette section, vous avez appris à :

- Identifier les concepts de sécurité SELinux de base, comme contexte, user/role/type et stratégie

Modes SELinux

Dans cette section, vous avez appris à :

- Décrire les différences fonctionnelles entre les modes enforcing et permissif lorsque la sécurité SELinux est activée

Afficher et modifier les modes SELinux

Dans cette section, vous avez appris à :

- Afficher et modifier le mode SELinux actif d'un système
- Définir le mode SELinux par défaut d'un système

Afficher et modifier les contextes de fichiers SELinux

Dans cette section, vous avez appris à :

- Afficher le contexte de sécurité SELinux des processus et fichiers
- Définir le contexte de sécurité SELinux des fichiers de la règle
- Restaurer le contexte de sécurité SELinux des fichiers

Gestion des booléens SELinux

Dans cette section, vous avez appris à :

- Utiliser les booléens SELinux pour apporter des ajustements au comportement de la stratégie

Contrôler les violations SELinux

Dans cette section, vous avez appris à :

- Déployer les outils d'analyse de fichier SELinux



MODULE DIX

GESTION DU PARE-FEU

Introduction

Sujets couverts dans cette unité :

- Filtrage des paquets
- Traduction d'adresses réseau (NAT)

Filtrage des paquets

Ci-dessous figure une liste des principaux concepts que vous devez connaître pour définir un pare-feu. Soyez attentif lorsque la classe traite de chacun de ces concepts et prenez des notes, car vous devrez utiliser l'ensemble de ces mots-clés lors de la création de votre pare-feu pour l'exercice.

- _____: critère désignant les paquets qui doivent correspondre, ainsi qu'une cible, ou une action, qui détermine ce qui doit être effectué avec ces paquets.
- _____: liste de *règles* qui seront vérifiées selon un ordre. La première correspondance devient effective.
- _____: action par défaut, **ACCEPT** ou **DROP**, entreprise si aucune *règle* ne correspond dans une *chaîne* incorporée.
- _____: ensemble de *chaînes* utilisées dans un but précis: **`filter`** pour bloquer le trafic, **`nat`** pour modifier la destination ou la source apparente d'un paquet.

Chaînes incorporées (table filter)

- _____: paquets adressés au pare-feu
- _____: paquets provenant d'un service sur le pare-feu (non transmis)
- _____: paquets provenant d'une autre machine, qui ne sont pas destinés au pare-feu mais qui sont transmis (routés) vers un autre emplacement (lorsque **`net.ipv4.ip_forward=1`**)

Cibles

(Actions à entreprendre lorsque des paquets correspondent à des règles)

- _____: le paquet transmet la chaîne
- _____: le paquet est coupé comme s'il n'avait jamais été détecté
- _____: le paquet est rejeté et le pare-feu envoie un message d'erreur (un message de port ICMP injoignable par défaut)
- _____: les informations relatives aux paquets sont consignées dans syslog; passons à la règle suivante dans la chaîne

Commande iptables

Vous avez éventuellement utilisé **system-config-firewall**, un outil graphique de Red Hat Enterprise Linux 6, pour configurer des pare-feu simples. Il est possible de créer et de gérer des configurations plus avancées à l'aide de l'outil en ligne de commande **iptables**.

iptables sert à définir ou à afficher des règles dans la mémoire du noyau.

Options iptables	*Définition*
-vnL --line-numbers	répertorie toutes les règles, de manière intégrale, en mode numérique
-A CHAIN <rule> -j <target>	ajoute une *règle* à la fin de *CHAIN*
-I CHAIN # <rule> -j <target>	insère une *règle* en tant que # (n°) de règle dans *CHAIN*; si aucun # n'apparaît, alors cette règle constitue la première règle
-D CHAIN #	supprime le # de règle de *CHAIN*
-F CHAIN	supprime toutes les règles de *CHAIN*

Tableau 10.1. Exemple de syntaxe iptables

Syntaxe de règle (critères de concordance)

Une règle iptables contient des critères de concordance qui peuvent être comparés à des informations d'en-tête trouvées dans le paquet.

Concept	*Directive*
IP ou réseau source	**-s 192.0.2.0/24**
IP ou réseau de destination	**-d 10.0.0.1**
UDP/TCP et ports	**-p udp --sport 68 --dport 67**
ICMP et types	**-p icmp --icmp-type echo-reply**
Interface de réseau entrant	**-i eth0**
Interface de réseau sortant	**-o eth0**
Suivi d'état	**-m state --state ESTABLISHED,RELATED**

Tableau 10.2. Critères de concordance iptables

Le suivi d'état stocke des informations concernant des communications précédemment observées, afin de prendre des décisions de concordance. Une fois la connexion autorisée, les informations placées dans une table de suivi d'état jusqu'à l'expiration d'un délai entraînent la fermeture des connexions, ou l'affichage d'un trafic de concordance accru (réinitialisez la minuterie). Si cette opération nécessite une mémoire du noyau supplémentaire, son avantage est de simplifier la conception des règles.

État	*Définition*
NEW	le paquet démarre une nouvelle communication, ajoute une règle à la table de suivi d'état
ESTABLISHED	tout paquet qui correspond à une règle dans la table de suivi d'état

État	*Définition*
RELATED	trafic « associé » d'une certaine manière au trafic ESTABLISHED ; des protocoles tels que FTP
INVALID	le paquet ne peut pas être identifié ; normalement, ceux-ci doivent être rejetés ou supprimés

Tableau 10.3. États de suivi des connexions

Pour aider au fonctionnement des règles RELATED, vous devez éventuellement activer les modules de l'assistant dans **`/etc/sysconfig/iptables-config`**

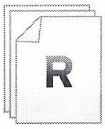


Important

L'exécution de la commande **`iptables`** modifie les règles du module du noyau netfilter, mais ne persiste PAS après une réinitialisation.

L'exécution de **`service iptables save`** place les règles actuelles en mémoire et les inscrit dans **`/etc/sysconfig/iptables`**, lu lors du démarrage.

Certains administrateurs peuvent aussi modifier (ou copier) directement le fichier **`/etc/sysconfig/iptables`**, puis exécuter **`service iptables restart`** pour l'activation.



Références

Red Hat Enterprise Linux Security Guide
- Section 2.5 : pare-feu

Red Hat Enterprise Linux Security Guide
- Section 2.6 : IPTables

Page man **`iptables`**(8)

Page d'accueil Netfilter
http://www.netfilter.org/



Exercice de Exercice

Implémenter un pare-feu

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Au cours de cet exercice, vous allez implémenter un pare-feu sur serverX qui rejette tous les paquets, sauf que le trafic ICMP sera autorisé pour example.com et SSH pour tous, à l'exception de remote.test.

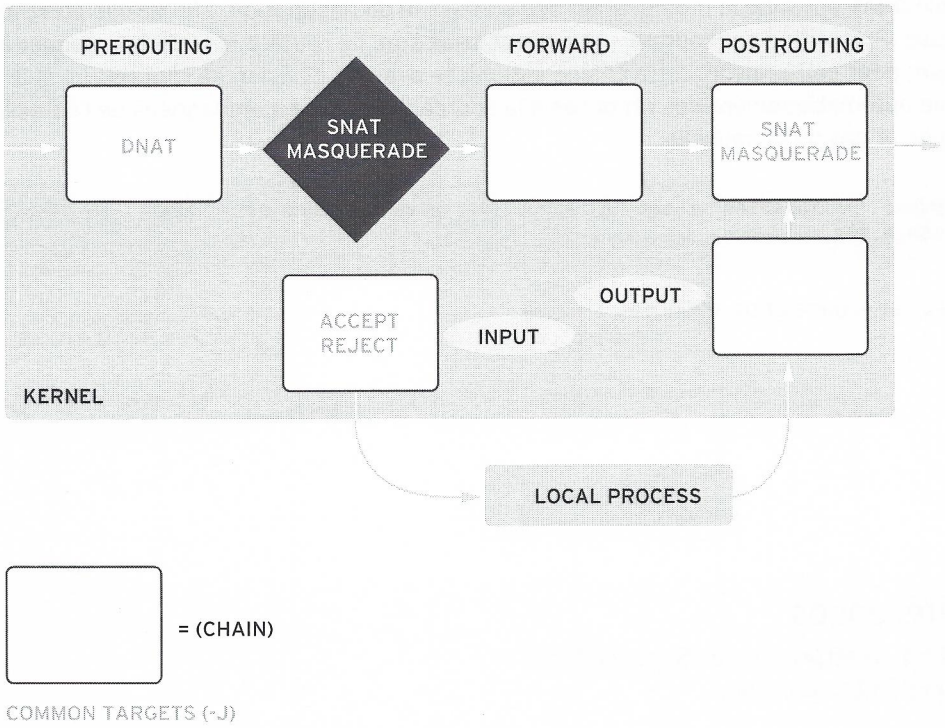
1. Connectez-vous à serverX en tant que **root** à l'aide de **virt-viewer** ou de **virt-manager**.
2. Créez un pare-feu simple qui refuse tout (sauf le loopback) en créant un fichier **/root/bin/resetfw.sh** qui
   1. définit la stratégie par défaut de la chaîne **INPUT** par **DROP**,
   2. vide toutes les règles dans la table de filtres et
   3. appliquera **ACCEPT** à tous les paquets à partir de l'interface loopback
3. Exécutez votre script et enregistrez les résultats des éléments suivants :
   - Utilisez **ping** et **ssh** serverX depuis desktopX et depuis remoteX.remote.test
4. Que se passe-t-il lorsque vous utilisez **ping** desktopX et 192.168.0.X depuis &sr maintenant ? Pour quelle raison ? Tout est rejeté
5. Activez un pare-feu avec état en appliquant une règle à votre script qui
   - utilisera **ACCEPT** pour tous les paquets **ESTABLISHED, RELATED**
6. Exécutez votre script et enregistrez les résultats des éléments suivants :
   - **ping** desktopX et 192.168.0.X depuis serverX
7. Rejetez tous les paquets depuis remote.test en appliquant une règle à votre script qui
   - appliquera **REJECT** à tous les paquets provenant du réseau 192.168.1.0/24
8. Exécutez votre script et enregistrez les résultats des éléments suivants :
   - Utilisez **ping** et **ssh** serverX depuis desktopX et depuis remoteX.remote.test
9. Activez le trafic ICMP pour example.com en appliquant une règle à votre script qui
   - appliquera **ACCEPT** à l'ensemble du trafic **icmp** depuis 192.168.0.0/24
10. Exécutez votre script et enregistrez les résultats des éléments suivants :
    - **ping** et **ssh** serverX depuis desktopX
11. Activez le trafic SSH pour tous les hôtes en modifiant votre script par

- **ACCEPT** toutes les connexions **NEW** au port **tcp 22**

12. Exécutez votre script et enregistrez les résultats des éléments suivants:
    - **ssh** vers serverX depuis desktopX et depuis remoteX.remote.test
13. Rejetez les paquets par défaut au lieu de supprimer des paquets en appliquant une règle à votre script qui appliquera
    - **REJECT** à tout autre trafic
14. Exécutez votre script et enregistrez les résultats des éléments suivants:
    - Utilisez **ping** et **ssh** serverX depuis desktopX et depuis remoteX.remote.test

Traduction d'adresses réseau

La traduction d'adresses réseau sert à manipuler la source apparente ou l'adresse de destination souhaitée des paquets réseau. Le diagramme ci-dessous illustre l'ordre de traitement des chaînes Netfilter présentes sur les tables **filter** **nat**:



Les pare-feu basés sur l'hôte simples peuvent posséder des règles dans la chaîne **INPUT** uniquement pour appliquer **ACCEPT** ou **REJECT** aux paquets. Cependant, sur une passerelle ou un routeur de réseau privé (non routable), l'utilisation de la chaîne **PREROUTING** et **POSTROUTING** est courante pour modifier des paquets.

La table **nat** utilise trois chaînes: **PREROUTING**, **OUTPUT** et **POSTROUTING**. La traduction d'adresses réseau se produit lorsqu'un routeur modifie l'adresse IP ou le port source ou de destination du trafic réseau qui transite par lui. Elle est utilisée pour le mappage d'un réseau de machines derrière une adresse IP, afin que celles-ci puissent partager une adresse publique unique et masquer leur réseau interne (**MASQUERADE** ou **SNAT**). Elle sert également à la redirection du trafic provenant d'une adresse IP et destiné à une autre. Cette *traduction*

d'adresses réseau de destination est utilisée pour le *transfert de port* (transfert d'un port en-dehors d'un pare-feu vers un service à l'intérieur de ce dernier) et la redirection transparente vers des services proxy.

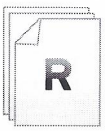
La cible **MASQUERADE** entraîne la modification de l'adresse IP source pour qu'elle corresponde à l'IP de l'interface sur laquelle le pare-feu est laissé. La destination renvoie une réponse à l'adresse IP de cette interface. Le suivi d'état démasque l'adresse IP avec la source d'origine correcte (suivis basés sur les adresses IP et les ports des deux extrémités de la connexion). La cible **SNAT** entraîne la modification de l'adresse IP source en adresse IP spécifique, avec l'option **`--to-source`**

```
[root@demo ~]# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

La cible **DNAT** entraîne la modification de l'adresse IP de destination, afin qu'elle corresponde à l'adresse IP spécifiée par l'option **`--to-destination`**. Le routeur transfère le paquet à cette adresse ; pour cette raison, cette chaîne est placée avant la décision de routage. Le suivi d'état renvoie automatiquement des réponses à la source d'origine, accompagnées de l'adresse IP d'origine et pas de la nouvelle.

```
[root@demo ~]# iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
 192.168.0.254
```

Utilisez cet espace pour vos notes.



Références

Red Hat Enterprise Linux Security Guide
- Section 2.5 : pare-feu

Red Hat Enterprise Linux Security Guide
- Section 2.6 : IPTables



Exercice de Questionnaire

Questionnaire sur la traduction d'adresses réseau

1. Les chaînes disponibles dans la table **filter** sont _____, _____ et _____

2. Les chaînes disponibles dans la table **nat** sont _____, _____ et _____

3. **iptables -t** _____ **-A** _____ **-o eth0 -j MASQUERADE**

4. **iptables -t** _____ **-A** _____ **-o eth0 -j SNAT** _____ **192.168.0.1**

5. **iptables -t** _____ **-A** _____ **-i eth0 -m tcp -p tcp --dport 80 -j DNAT** _____ **192.168.0.100:8080**

6. La cible **DNAT** peut être utilisée uniquement dans la chaîne _____ et la chaîne _____ de la table _____

7. Pour activer le transfert de manière permanente tout au long des réinitialisations, ajoutez **net**_____**=1** à **/etc/**_____ et exécutez _____ **-p**



Test

Test de critère

Étude de cas

L'entreprise Morris Worm and Fish Supply

Avant de commencer...

Important : veillez à exécuter le script **`lab-setup-morrisworm`** sur desktopX avant de commencer ! Le script **`lab-setup-morrisworm`** configurera serverX pour une exécution sur un réseau privé.

L'entreprise Morris Worm and Fish Supply cherche finalement à moderniser son activité en ouvrant un site Web. Le serveur Web sera exécuté sur un réseau privé, derrière un pare-feu. Le pare-feu transférera l'ensemble du trafic TCP du port 80 vers le serveur Web et utilisera la traduction d'adresses réseau, afin que le serveur Web puisse contacter des hôtes externes.

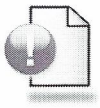
- desktopX.example.com sera le pare-feu et serverX.example.com le serveur Web.
- Configurez Apache en vue d'une exécution sur serverX.example.com. Placez du contenu personnalisé dans **`/var/www/html/index.html`** qui identifiera de manière unique le serveur.
- Configurez le pare-feu sur desktopX pour effectuer une traduction d'adresses réseau qui autorisera le serveur Web à contacter le réseau externe. Vous serez en mesure de faire un **`ping`** à instructor.example.com depuis serverX pour confirmer que cela fonctionne.
- Enfin, configurez le pare-feu pour transférer l'ensemble du trafic TCP du port 80 qu'il reçoit vers le serveur Web exécuté sur serverX. Vous devrez identifier l'adresse IP de serverX's pour compléter cette étape. Confirmer que cela fonctionne en utilisant un navigateur Web depuis une machine externe et PAS desktopX, pour accéder à http://desktopX.example.com.

Une fois que vous avez réussi à terminer cet exercice, exécutez **`lab-cleanup-morrisworm`** sur desktopX pour réinitialiser votre réseau à son état d'origine.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Filtrage des paquets

Dans cette section, vous avez appris à :

- Définir des règles de pare-feu avec **`iptables`**
- Bloquer ou autoriser le trafic réseau en fonction de critères spécifiques
- Bloquer ou autoriser le trafic réseau en fonction du trafic précédent observé

Traduction d'adresses réseau

Dans cette section, vous avez appris à :

- Utiliser **`iptables`** pour définir la traduction d'adresses réseau IPv4
- Faites en sorte que les paquets qui transitent via le routeur Linux semblent provenir de son adresse IP sortante
- Redirigez les paquets qui transitent via le routeur Linux vers une autre adresse IP de destination



MODULE ONZE

CONFIGURATION DU SERVEUR NTP

Introduction

Sujets couverts dans cette unité :

- Configuration des serveurs de temps

Configuration d'un serveur NTP

NTP est le protocole de temps du réseau (Network Time Protocol). Il définit un mode standard d'échange des heures correctes entre machines sur Internet. Une machine peut obtenir des informations précises des heures de services NTP publics sur Internet, par exemple du Réservoir NTP, ou d'horloges matérielles de haute qualité, et peut ensuite les diffuser à ses clients locaux.

Pour configurer un serveur et un client NTP, il vous faut comprendre trois paramètres principaux du fichier **/etc/ntp.conf**: **server**, **peer** et **restrict**.

Le premier argument de la ligne **server** est l'adresse IP ou le nom DNS du serveur NTP. L'accès de votre adresse IP au serveur doit être autorisé par une ligne **restrict**, comme indiqué ci-dessous. Après l'adresse IP ou le nom du serveur, vous pouvez énumérer une série d'options pour le serveur. La page de manuel **ntp.conf(5)** recommande l'utilisation de l'option **iburst**.

Comme la ligne **server**, la ligne **peer** prend un serveur NTP et les options prennent des arguments. **server** est dans la strate immédiatement au-dessus de votre serveur NTP et **peer** dans la même strate. Vous pouvez spécifier plus d'un serveur **server** et plus d'un pair**peer**, un par ligne.

La ligne **restrict** prend généralement une adresse IP ou un nom DNS comme premier argument. Toutefois, le premier argument peut être **default** pour indiquer que les restrictions sont les paramètres appliqués par défaut . Si le premier argument est **-6**, les restrictions suivantes (y compris **default**) s'appliquent uniquement aux adresses IPv6. Plusieurs balises peuvent être utilisées dans la ligne **restrict**. Vous trouverez ci-dessous des explications, reprises de la page de manuel **ntp_acc(5)**, pour les plus courantes d'entre elles:

- **ignore**: interdit les paquets de toute sorte, y compris les requêtes **ntpq** et **ntpdc**
- **kod**: si cet indicateur est défini quand une violation d'accès se produit, le paquet KoD (Kiss-of-death) est envoyé. L'envoi de paquets KoD est limité à un taux d'un par seconde au plus. Si un autre paquet KoD se produit dans la seconde qui suit le précédent, le paquet est ignoré.
- **nomodify**: interdit les requêtes **ntpq** et **ntpdc** qui tentent de modifier la strate du serveur (c.-à-d. les tentatives de reconfiguration au lancement). Les requêtes qui renvoient des informations sont autorisées.
- **noquery**: interdit les requêtes **ntpq** et **ntpdc**. Le service de temps n'est pas affecté.
- **nopeer**: interdit les paquets qui entraîneraient une nouvelle association. Ces paquets comprennent les paquets clients Broadcast, Manycast et le mode symétrique actif quand une association configurée n'existe pas.
- **notrap**: refuse de fournir le service d'interruption en mode de contrôle (6) aux hôtes correspondants. Le service d'interruption est un sous-système du protocole de messages de contrôle ntpdq conçu pour être utilisé par des programmes distants de journalisation des événements.

Si le temps du client a un décalage de plus de quelques minutes, la synchronisation du client NTP avec le serveur échoue. Vous pouvez utiliser la commande **ntpdate -v *ntpserver* command to roughly set the clock once so that it can synchronize.**

Si vous voulez inclure une horloge matérielle dans le service NTP, utilisez une adresse IP spéciale dans la plage **127.127.1**. L'horloge peut être un récepteur GPS ou grandes ondes de grande précision ou une imprécise horloge en temps réel intégrée au système.

Par exemple, l'horloge en temps réel (RTC) sert à mesurer le temps sur la carte mère. Cette horloge est généralement plutôt imprécise. C'est pourquoi, si vous l'utilisez, il est recommandé de la forcer à annoncer une strate inférieure (habituellement 10). La section correspondante dans **/etc/ntp.conf** doit ressembler à :

```
server          127.127.1.
fudge           127.127.1.0       stratum 10
```



Références

Red Hat Enterprise Linux Deployment Guide

- Section 13.2.2 : Configuration de Network Time Protocol

ntp.conf(5) et **ntp_acc**(5) (pages du manuel)

/usr/share/doc/ntp-*/html (du package **ntp-doc**)

> Réservoir NTP (NTP Pool Project)
> http://www.ntp.pool.org/



Exercice de Questionnaire

Questionnaire sur la configuration NTP

Répondez aux questions ci-dessous à l'aide du fichier de configuration NTP ci-dessous:

```
#/etc/ntp.conf

restrict default kod nomodify notrap nopeer noquery
restrict -6 default ignore

restrict 192.168.0.0 mask 255.255.255.0 nomodify notrap nopeer
restrict 192.168.0.101 kod nomodify notrap
restrict 192.168.0.200

server 192.168.0.2
server 192.168.0.3
peer 192.168.0.101
```

1. Le temps du client NTP a 15 minutes de décalage, il va finalement se désynchroniser d'avec les serveurs.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

2. Le client NTP va utiliser l'horloge en temps réel (RTC) de l'ordinateur (BIOS) comme source de synchronisation.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

3. L'adresse 192.168.0.200 peut modifier le temps sur ce server NTP.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

4. L'adresse 192.168.0.4 peut interroger ce serveur NTP.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

5. 192.168.0.3 peut utiliser ce serveur NTP comme pair.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

6. Toute personne dotée d'une adresse IPv4 peut utiliser ce serveur NTP comme source de synchronisation.

(sélectionnez une des réponses suivantes...)

a. Vrai
b. Faux

7. Toute personne dotée d'une adresse IPv6 peut utiliser ce serveur NTP comme source de synchronisation.

(sélectionnez une des réponses suivantes...)

a. Vrai
b. Faux



Test

Test de critère

Étude de cas

Configuration du serveur NTP

Avant de commencer...

Exécutez **`lab-setup-howsonclock`** sur desktopX.

Howson Heavy Machine and Clock Manufacture, fabricant de Pièces et accessoires d'horloges, a récemment mené un audit de tous ses systèmes informatiques. L'audit a révélé que plusieurs systèmes dont les horloges ne sont plus synchronisées, y compris votre machine serverX.example.com.

Configurez NTP sur votre serveur serverX en tant que client du service NTP qui s'exécuter sur instructor.example.com.

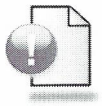
Pour avoir des sources de synchronisation supplémentaires, travaillez avec vos voisins afin que tous vos systèmes serverX se synchronisent comme des pairs NTP.

Lorsque vous avez fini, exécutez **`lab-grade-howsonclock`** sur desktopX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Configuration d'un serveur NTP

Dans cette section, vous avez appris à :

- Installez une grappe de serveurs NTP en tant que pairs et utilisez un service de strates inférieures.
- Configurez les clients de manière qu'ils utilisent votre grappe locale de serveurs NTP.



MODULE DOUZE

SERVICE DE JOURNALISATION SYSTÈME

Introduction

Sujets couverts dans cette unité :

- Scripts de suivi du système
- Journalisation centralisée

Rapports d'utilisation

Dans cette section, nous commencerons par examiner certains outils qui sont utiles pour écrire des scripts ou des tâches automatisées afin de générer des rapports sur l'utilisation du système.

Rapports d'utilisation - Travail en groupe

1. **df** permet d'afficher l'utilisation du disque. L'option **-h** imprime la sortie sous une forme « lisible ».

```
[root@serverX ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vgsrv-root
                      3.3G  2.2G  935M  71% /
tmpfs                 246M  112K  246M   1% /dev/shm
/dev/vda1             248M   30M  206M  13% /boot
/dev/mapper/vgsrv-home
                      248M   11M  225M   5% /home
```

   Utilisez cet espace pour vos notes.

2. Créez un rapport de l'utilisation des E/S disque à l'aide de **iostat**

   Quelles informations fournit l'option **-d** ?

   Quelles informations fournit l'option **-N** ?

   Montre les noms des LVM

   Quelles informations fournit l'option **-k** ?

   en Ko

   Que fait **iostat** si deux arguments numériques lui sont transmis (par exemple **iostat 2 10**) ?

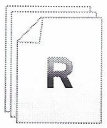
   Une fois que vous avez répondu aux questions ci-dessus, reportez-vous à l'étude de cas pratique des rapports d'utilisation et suivez les instructions qui s'y trouvent.

3. Créez un rapport d'utilisation de l'espace swap à l'aide de **vmstat**

   Que représente la première sortie lorsque la commande **vmstat** est exécutée ?

Que fait **vmstat** si deux arguments numériques lui sont transmis (par exemple **vmstat 2 10**) ?

Une fois que vous avez répondu aux questions ci-dessus, reportez-vous à l'étude de cas pratique des rapports d'utilisation et suivez les instructions qui s'y trouvent.



Références

Pages man **df**(1), **iostat**(1) et **vmstat**(8)



Exercice de Étude de cas

Rapports d'utilisation

Utilisez l'outil que vous avez examiné pour créer un rapport simple qui consigne les informations dans un fichier.

Une fois que vous avez utilisé l'outil pour générer un rapport, l'instructeur vous demandera de présenter la commande que vous avez utilisée et le résultat que vous avez obtenu au reste de la classe.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.

Configurer un service de journalisation distant

La collecte centralisée des messages de journaux système peut être très utile pour contrôler l'état de vos systèmes et identifier rapidement les problèmes. Elle fournit également un emplacement de sauvegarde pour les messages de journaux si un système subit une panne sérieuse de disque dur ou un autre problème grave, empêchant ainsi l'accès aux journaux locaux pour dresser un diagnostic du problème ou de la panne de disque.

La journalisation système standardisée est mise en œuvre dans Red Hat Enterprise Linux 6 par le service **rsyslog**. Les programmes du système peuvent envoyer des messages syslog au service **rsyslogd** local, qui redirige ensuite ces messages vers des fichiers dans **/var/log**, des serveurs de journaux distants ou des bases de données selon les paramètres de son fichier de configuration, **/etc/rsyslog.conf**.

Les messages de journaux ont deux caractéristiques permettant de les trier ; une *fonction* qui indique le type du message et une *priorité* qui indique l'importance de l'événement consigné.

Priorité	*Signification*
emerg	Système inutilisable
alert	Action immédiate exigée
crit	Condition critique
err	Condition d'erreur
warning	Condition d'avertissement
notice	Condition normale mais significative
info	Messages d'information
debug	Messages de débogage

Tableau 12.1. Niveaux de priorité syslog

Voir **logger**(1) et **syslog**(3) pour plus d'informations et obtenir une liste des fonctions.

La configuration d'un service de journalisation distant s'effectue en deux parties : d'une part la configuration de **rsyslog** sur le serveur de journalisation distant pour qu'il accepte les messages de journaux du réseau et d'autre part la configuration des systèmes **rsyslog** clients pour qu'ils envoient les journaux au serveur de journalisation distant.

- Pour configurer **rsyslog** afin qu'il accepte les journaux distants, supprimez les commentaires des lignes de réception TCP ou UDP dans la section des modules du fichier **/etc/rsyslog.conf**. Pour la réception UDP :

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514
```

ou pour la réception TCP :

```
# Provides TCP syslog reception
$ModLoad imtcp.so
$InputTCPServerRun 514
```

Le protocole TCP permet une livraison plus fiable des messages de journaux distants mais UDP est pris en charge par un plus grand nombre de systèmes d'exploitation et de périphériques réseau.



Important

Le transport TCP ordinaire des messages syslog est plutôt largement mis en œuvre mais il n'est pas encore la norme. La plupart des implémentations du protocole TCP utilisent actuellement le port 514/TCP, qui est le port **rshd** hérité. Si vous avez installé le package *rsh-server* et si vous utilisez l'ancien service **rshd** peu fiable, celui-ci sera en conflit avec l'utilisation du port 514/TCP pour la réception syslog TCP ordinaire. Vous pouvez configurer le serveur de journalisation pour qu'il utilise un autre port en changeant le paramètre pour **$InputTCPServerRun**.

Une fois que vous avez supprimé les commentaires d'une section de réception syslog, redémarrez le service **rsyslog**.

- Pour configurer une machine de sorte qu'elle envoie des journaux à un serveur **rsyslog** distant, ajoutez une ligne à la section des règles du fichier **/etc/rsyslog.conf**. À la place du nom de fichier, utilisez l'adresse IP du serveur **rsyslog** distant. Pour utiliser UDP, faites précéder l'adresse IP du signe @. Pour utiliser TCP, faites précéder l'adresse IP de deux signes @ (@@).

  Par exemple, si vous voulez que tous les messages avec **info** ou une priorité supérieure soient envoyés à 192.168.0.1 à l'aide d'UDP, utilisez la ligne suivante :

```
*.info    @192.168.0.1
```

  Si vous voulez que *tous* les messages soient envoyés à 192.168.0.101 à l'aide de TCP, utilisez la ligne suivante :

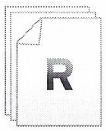
```
*.*    @@192.168.0.101
```

  Vous pouvez également ajouter **:*PORT*** après l'adresse IP, *PORT* étant le port que le serveur **rsyslog** distant utilise. Si aucun port n'est indiqué, le port 514 par défaut sera utilisé.

  Une fois que vous avez ajouté les règles, redémarrez le service **rsyslog** et envoyez un message test à l'aide de la commande **logger** :

```
[root@serverX ~]# logger "Test from serverX
```

  Consultez les journaux sur le serveur distant pour vérifier que vous avez bien reçu le message.



Références

Red Hat Enterprise Linux Deployment Guide

- Chapitre 17 : Fichiers journaux

Documentation **rsyslog** générale :

/usr/share/doc/rsyslog-*/manual.html

Documentation du fichier de configuration de **rsyslog** :

/usr/share/doc/rsyslog-*/rsyslog_conf_actions.html

Pages man **rsyslog.conf**(5), **rsyslogd**(8), **logger**(1), **syslog**(3)



Exercice de Exercice

Journalisation distante

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Configurez serverX pour qu'il accepte les messages de journaux distants à l'aide de TCP.
2. Configurez desktopX pour qu'il envoie tous les événements de priorité **`info`** et supérieure à serverX à l'aide de TCP .
3. Testez votre configuration.



Test

Test de critère

Étude de cas

Contrôle du système et journaux

Avant de commencer...

Avant de commencer, exécutez le script **`lab-setup-blossoms`** sur desktopX.

Blossoms, Inc. est une coopérative de floriculteurs aux États-Unis. La coopérative assure notamment des services informatiques pour tous ses membres. Son responsable informatique a décidé de renforcer la sécurité en exigeant la mise en œuvre de la journalisation distante sur tous les serveurs, y compris le vôtre (serverX).

Configurez rsyslog sur desktopX pour accepter les messages de journaux distants provenant de serverX via UDP. Puis configurez **`rsyslog`** sur serverX pour envoyer tous les messages de journaux **`*.info`** à desktopX via UDP.

Avant de vérifier votre travail, exécutez **`lab-grade-blossoms`** sur serverX, puis exécutez **`lab-grade-blossoms`** sur desktopX.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Rapports d'utilisation

Dans cette section, vous avez appris à :

- Vérifier et contrôler l'intégrité du système de fichiers avec des outils tels que **df**, **iostat** et **vmstat**

Configurer un service de journalisation distant

Dans cette section, vous avez appris à :

- Configurer la journalisation distante pour un serveur de journalisation
- Rediriger les messages de journaux système vers un serveur de console centralisée



MODULE TREIZE

SERVICE WEB

Introduction

Sujets couverts dans cette unité :

- Déployer des services Web SSL
- Configurer un serveur Web avec des hôtes virtuels
- Configurer un serveur Web avec du contenu dynamique
- Configurer un serveur Web avec des répertoires authentifiés

Sécurisation d'un serveur Apache avec le chiffrement

Configuration d'un serveur Apache HTTP - Révision

Vous devez normalement déjà connaître les principes de base pour configurer un serveur **Apache HTTP Server** simple. Dans cette unité, nous examinerons en détail certaines configurations plus complexes mais courantes utilisées avec des déploiements de serveurs Web, en commençant par la configuration du support pour les connexions TLS/SSL.

Apache HTTP Server est installé par le groupe yum **`web-server`**, le package le plus important étant *httpd*, qui fournit les principaux composants du serveur Web. Le script du service **`httpd`** sert à démarrer le serveur autant de fois qu'il est nécessaire et il écoute les connexions sur le port TCP 80 par défaut. Il est confiné par la stratégie SELinux pour plus de sécurité, sujet dont nous avons déjà parlé et qui est documenté dans la page man **`httpd_selinux`**(8). Son fichier de configuration principal est **`/etc/httpd/conf/httpd.conf`**, qui intègre automatiquement tous les fichiers correspondant à **`/etc/httpd/conf.d/*.conf`**. Par défaut, le contenu Web est servi à partir des sous-répertoires de **`/var/www`**, avec le « **`DocumentRoot`** » des pages Web dans **`/var/www/html`**, bien que cela puisse être modifié dans le fichier de configuration.

Étapes pour déployer le chiffrement TLS/SSL

La prise en charge des sites Web TLS/SSL est assurée par le package RPM *mod_ssl*. Son fichier de configuration est **`/etc/httpd/conf.d/ssl.conf`**. Il suffit d'installer ce fichier et de redémarrer le serveur Web pour qu'une version chiffrée SSL du site Web par défaut sur le serveur soit disponible avec un certificat de test auto-signé pour l'hôte local.



Important

Pour contacter un site Web chiffré TLS/SSL sur votre serveur à l'aide d'une URL **`https://`**, vous devez vous assurer que les clients peuvent se connecter au port TCP 443 sur votre serveur Web. Vérifiez pour cela les paramètres du pare-feu.

Si vous utilisez un navigateur Web pour vous connecter au site Web sécurisé, vous obtiendrez probablement un avertissement vous indiquant que le certificat SSL pour le site Web ne correspond pas au nom d'hôte du site et qu'il n'est pas signé par une autorité de certification de confiance. Pour résoudre ce problème, vous devez vous procurer un certificat SSL pour le nom d'hôte du site Web signé par une autorité de certification publique et modifier la configuration dans **`/etc/httpd/conf.d/ssl.conf`**. Les directives essentielles sont **`SSLCertificateFile`**, qui doit normalement pointer vers un fichier dans **`/etc/pki/tls/certs/`** contenant le certificat SSL public et **`SSLCertificateKeyFile`**, qui doit pointer vers un fichier dans **`/etc/pki/tls/private/`** contenant la clé SSL privée. Nous n'aborderons pas en détail la manière d'obtenir un certificat SSL signé dans ce cours.

Les étapes de base sont les suivantes :

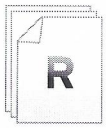
1. Assurez-vous que le groupe yum **`web-server`** est installé :

```
yum groupinstall web-server
```

2. Installez le package *mod_ssl*:

```
yum install mod_ssl
```

3. Si vous remplacez le certificat de test par un certificat signé:
   - Copiez le certificat et la clé privée aux emplacements appropriés dans **/etc/pki/tls/**
   - Assurez-vous que les deux fichiers sont de type SELinux **cert_t** et que la clé privée n'est pas lisible par tous
   - Ouvrez **/etc/httpd/conf.d/ssl.conf** dans un éditeur
   - Pointez **SSLCertificateFile** vers le certificat SSL
   - Pointez **SSLCertificateKeyFile** vers la clé privée SSL
   - Enregistrez les modifications et fermez **/etc/httpd/conf.d/ssl.conf**
4. Redémarrez le service **httpd**



Références

Red Hat Enterprise Linux Deployment Guide
- Section 11.6: Configuration d'un serveur SSL

Apache.org: « Apache TLS/SSL Encryption »
http://httpd.apache.org/docs/2.2/ssl/
(si ***httpd-manual*** est installé et **httpd** est exécuté):
http://localhost/manual/ssl/



Exercice de Liste de contrôle des performances

Principes de base Apache avec mod_ssl

Déployez un serveur Web Apache encapsulé avec SSL sur serverX. Il doit utiliser le certificat SSL auto-signé par défaut.

- ☐ Connectez-vous à serverX en tant que super utilisateur.
- ☐ Installez le package (**`httpd`**) du serveur Web Apache, si nécessaire.
- ☐ Installez le package **`mod_ssl`**.
- ☐ Examinez le fichier de configuration **`/etc/httpd/conf.d/ssl.conf`** fourni par le package **`mod_ssl`**.
  - Quelle directive Apache pointe vers le certificat SSL ?
  - Quelle est sa valeur ?
- ☐ Relancez le service **`httpd`**.
- ☐ Lancez Firefox et accédez à https://serverX.example.com. Lorsque Firefox affiche un avertissement, effectuez les opérations suivantes pour examiner le certificat avec ce navigateur.
  - Cliquez sur le lien « Je comprends les risques ».
  - Cliquez sur le bouton « Ajouter des exceptions... », puis cliquez sur « Afficher... » lorsque l'option devient active.
  - Consultez les informations présentées dans les onglets « Général » et « Détails ».
  - Cliquez sur « Fermer » lorsque vous avez fini d'examiner les informations relatives au certificat.

Configurer l'hébergement virtuel basé sur le nom

Les hôtes virtuels vous permettent de servir plusieurs sites Web simultanément à partir d'un seul serveur **httpd**. Dans cette section, nous allons examiner *les hôtes virtuels basés sur le nom.* Avec les hôtes virtuels basés sur le nom, plusieurs noms d'hôte pointent vers la même adresse IP et le serveur Web fournit un site Web différent avec du contenu différent selon le nom d'hôte utilisé pour atteindre le site.

Cela fonctionne comme suit : une adresse IP particulière ou des adresses IP sur le serveur Web sont identifiées comme étant partagées par les hôtes virtuels basés sur le nom. Le serveur Web recherche dans ses fichiers de configuration le premier bloc **VirtualHost** pour l'adresse IP de chaque requête entrante dans laquelle **ServerName** ou **ServerAlias** correspond au nom d'hôte utilisé par la requête. Puis, il sert le contenu en fonction de la configuration du bloc **VirtualHost** correspondant au nom d'hôte. Si le nom d'hôte ne correspond à aucun bloc, alors le premier bloc **VirtualHost** pour l'adresse IP de la requête est utilisé par défaut.



Important

Lorsque vous ajoutez des hôtes virtuels à la configuration de votre serveur Web, vous devez vous assurer qu'un bloc **VirtualHost** correspond à votre site Web principal d'origine si vous envisagez de continuer à lui servir du contenu. Les directives pour le site Web principal sont utilisées *par défaut* pour les hôtes virtuels, qui peuvent être remplacés par chaque bloc **VirtualHost**.

La liste suivante contient les principaux concepts et paramètres que vous devez connaître afin de configurer des hôtes virtuels basés sur le nom. Écoutez attentivement les explications de l'instructeur concernant chacun d'eux et prenez des notes sur les conditions de leur utilisation illustrées par des exemples . Il vous sera demandé de configurer des hôtes virtuels à la fin de cet exposé.

```
# Name-based virtual hosts defined in /etc/httpd/conf/httpd.conf
NameVirtualHost *:80

<VirtualHost *:80>
    ServerName www.wonka-chocolates.com
    ServerAlias wonka-chocolates.com
    ServerAdmin webmaster@wonka-chocolates.com
    DocumentRoot /var/www/wonka-chocolates.com/html
</VirtualHost>
```

- VirtualHost

- NameVirtualHost

- ServerName/ServerAlias

- ServerAdmin

- DocumentRoot

- **semanage fcontext**

Configuration d'un **DocumentRoot** devant être administré par un groupe :

L'utilisation de répertoires set-GID est judicieuse, car cela permet aux administrateurs Web de gérer plus facilement du contenu sous un **DocumentRoot**. Utilisez **chgrp -R *webadmins* *DocumentRoot*** pour que tous les fichiers dans **DocumentRoot** appartiennent au groupe *webadmins*, c'est-à-dire le groupe auquel vos administrateurs Web appartiennent. Puis, pour ce groupe, assurez-vous que set-GID est défini sur **DocumentRoot**: **chmod 2775 *DocumentRoot***. (Un moyen plus judicieux de définir set-GID et d'écrire pour le groupe sur *tous* les sous-répertoires de **DocumentRoot** est d'utiliser **find *DocumentRoot* -type d -exec chmod g +ws '{}'\;**, où *DocumentRoot* est remplacé par le répertoire **DocumentRoot**.)

Vous devez également vous assurer que le type SELinux sur le contenu de **DocumentRoot** est **httpd_content_t** ou **public_content_t** pour permettre au serveur Web de servir le contenu.



Note

Un autre type d'hôte virtuel existe. Il s'agit de *l'hôte virtuel basé sur l'adresse IP*. Chaque hôte virtuel de ce type possède sa propre adresse IP sur le serveur. Ces hôtes virtuels fonctionnent mieux avec les sites TLS/SSL ; notez que le service SSL par défaut configuré dans **/etc/httpd/conf.d/ssl.conf** est un hôte virtuel basé sur l'adresse IP. Pour plus d'informations sur les hôtes virtuels basés sur l'adresse IP, voir la documentation relative à **Apache HTTP Server**.



Références

Red Hat Enterprise Linux Deployment Guide
- Section 11.5 : Hôtes virtuels

Red Hat Enterprise Linux Deployment Guide
- Section 15.5.1 : Répertoires de groupe

> Apache.org : « Support Apache des serveurs virtuels par nom »
> http://httpd.apache.org/docs/2.2/vhosts/name-based.html
> (si ***httpd-manual*** est installé et **`httpd`** est exécuté)
> http://localhost/manual/vhosts/name-based.html



Exercice de Liste de contrôle des performances

Configurer des hôtes virtuels basés sur le nom

Pour cet exercice, wwwX.example.com est déjà configuré en tant qu'alias **CNAME** de serverX.example.com.

Au terme de la liste de contrôle, vous exécuterez un script de notation, par conséquent assurez-vous que votre serveur Web sert le contenu exactement comme il est décrit dans la procédure.

- ☐ Créez **`/var/www/html/index.html`** contenant le texte « **`this is serverX`** ».
- ☐ Sur desktopX, utilisez Firefox pour vérifier que les sites Web wwwX, wwwX.example.com, serverX et serverX.example.com affichent tous l'**`index.html`** personnalisé.
- ☐ Créez **`/wwwX/html/index.html`** contenant le texte « **`this is wwwX`** ».
- ☐ Modifiez la configuration d'Apache pour activer l'hébergement virtuel basé sur le nom. serverX et serverX.example.com doivent servir **`/var/www/html/index.html`** comme page principale wwwX et wwwX.example.com doivent servir **`/wwwX/html/index.html`** comme page principale.
- ☐ Ne désactivez pas SELinux (conseil : il peut être nécessaire de modifier la base de données des contextes de fichiers SELinux ou de changer le type SELinux de certains fichiers).
- ☐ Lorsque vous avez terminé, exécutez le script d'évaluation **`lab-grade-virthost`** à partir de serverX pour vous assurer que tout est correct.

Activer un exécutable CGI

CGI ou Common Gateway Interface (Interface passerelle commune) constitue le moyen le plus facile de placer du contenu dynamique sur un site Web. Le serveur Web sert de passerelle entre les applications et un *script CGI* qui s'exécute sur le serveur et génère une sortie HTML dans sa réponse que le serveur renvoie au navigateur.

Bien que les scripts CGI puissent servir à plusieurs choses, il est important de déterminer soigneusement les scripts CGI à utiliser et qui est autorisé à les ajouter et à les exécuter. Un script CGI mal écrit peut permettre à un pirate de compromettre la sécurité du site Web et de son contenu. Par conséquent, des paramètres au niveau du serveur Web et de la stratégie SELinux sont appliqués pour restreindre l'utilisation des scripts CGI.

Installez une copie locale du How-To en installant le RPM **`httpd-manual`** avec **`yum`** sur serverX. Redémarrez Apache après avoir installé le package pour que la documentation Apache puisse être consultée. Consultez le didacticiel Apache.org « Dynamic Content with CGI » dans les références ci-dessous pour découvrir des exemples et des exemples de commandes permettant d'effectuer la procédure suivante.

Prenons l'exemple d'un script CGI à placer dans **`/wwwX/cgi-bin/hostinfo.cgi`**, quelle syntaxe de configuration, quelles autorisations du système de fichiers et quel type de contexte SELinux devez-vous connaître ?

1. Créez un répertoire hors du **`DocumentRoot`** du site Web :

```
[root@serverX ~]# mkdir -p /wwwX/cgi-bin
```

2. Configurez Apache de sorte qu'il reconnaisse ce répertoire comme source des programmes CGI :

3. Définissez le contexte SELinux du répertoire du script CGI sur **`httpd_sys_script_exec_t`** :

4. Redémarrez Apache pour que les modifications prennent effet :

Assurez-vous que vous avez bien compris comment activer CGI sur un répertoire si l'on vous donne un script CGI.

1. Copiez le script dans le répertoire de script CGI :

2. Assurez-vous que le script n'est pas modifiable par le démon **`httpd`** :

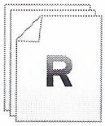
3. Rendez-le script exécutable :



Avertissement

Les problèmes pouvant compromettre la sécurité d'un site Web sont le plus souvent dus à des bogues dans les applications Web. Procédez avec précaution lorsque vous écrivez du code pour des applications CGI !

Les programmes CGI doivent être écrits de manière à produire le contenu que le serveur Web Apache attend. Étant donné qu'il est du ressort des développeurs Web d'écrire des scripts produisant une sortie CGI valide, ce sujet n'est pas abordé dans ce cours.



Références

> Apache.org : « Didacticiel Apache : Dynamic Content with CGI »
> http://httpd.apache.org/docs/2.2/howto/cgi.html
> (si ***httpd-manual*** est installé et **`httpd`** est exécuté)
> http://localhost/manual/howto/cgi.html

Red Hat Enterprise Linux Managing Confined Services
- Chapitre 3 : Le Serveur HTTP Apache

Page man **`httpd_selinux`**(8)



Exercice de Questionnaire

Questionnaire CGI Apache

1. CGI signifie

   (sélectionnez une des réponses suivantes...)
   a. Content Generated Interface
   b. Command Gateway Interface
   c. Common Generated Interface
   d. Common Gateway Interface

2. Le dernier argument dans **`ScriptAlias /cgi-bin/ /my/private/cgi-bin/`** est

   (sélectionnez une des réponses suivantes...)
   a. relatif à **`DocumentRoot`**
   b. relatif à **`/var/www/`**
   c. relatif à **`ServerRoot`**
   d. un chemin absolu sur le système de fichiers

3. Le **`ScriptAlias`** par défaut dans **`/etc/httpd/conf/httpd.conf`** pointe sur ...

   (sélectionnez une des réponses suivantes...)
   a. /var/www/cgi-bin
   b. /var/html/cgi-bin
   c. /cgi-bin
   d. /var/www/html/cgi-bin

4. L'un des types de contexte SELinux intégré pour un programme CGI générique est

   (sélectionnez une des réponses suivantes...)
   a. **`httpd_t`**
   b. **`httpd_sys_script_exec_t`**
   c. **`script_t`**
   d. **`httpd_content_t`**

5. Le processus Apache nécessite que les autorisations du système de fichiers suivantes soient sur les programmes CGI

   (sélectionnez une des réponses suivantes...)
   a. **`---`**
   b. **`r--`**
   c. **`r-x`**
   d. **`rwx`**

Configurer l'authentification utilisateur

Il peut être utile d'accorder l'accès à certaines parties d'un site Web uniquement aux utilisateurs autorisés. Un moyen pour cela consiste à configurer *l'authentification utilisateur* basée sur le nom des utilisateurs et leur mot de passe ; le serveur Web demande alors à l'utilisateur de s'authentifier pour accéder à certaines pages.

Il existe plusieurs façons d'implémenter l'authentification. Nous en examinerons deux dans ce cours : *l'authentification par fichier plat,* dans laquelle les utilisateurs sont définis dans un fichier de mots de passe local, et *l'authentification LDAP,* dans laquelle les utilisateurs sont définis dans un serveur de répertoires LDAP.

L'instructeur vous montrera comment configurer l'authentification utilisateur. Notez bien les explications, car vous devrez configurer votre serveur Web pour faire la même chose au cours de l'exercice.

Authentification utilisateur par fichier plat d'Apache

Dans cette configuration, les comptes d'utilisateur et les mots de passe sont stockés dans un fichier **.htpasswd** local. Pour des raisons de sécurité, ce fichier ne doit pas être conservé dans le **DocumentRoot** du site Web mais dans un répertoire que le site Web n'expose pas. La commande **htpasswd** est spécialement prévue pour gérer les utilisateurs dans le fichier **.htpasswd**.

Exemple de procédure de configuration :

- Créez un fichier de mots de passe Apache avec deux comptes :

```
[root@serverX]# htpasswd -cm /etc/httpd/.htpasswd bob
[root@serverX]# htpasswd -m /etc/httpd/.htpasswd alice
```

- En supposant que le bloc **VirtualHost** a déjà été défini, ajoutez une section similaire à la section suivante au bloc **VirtualHost** :

```
<Directory /var/www/virtual/wwwX/html>
    AuthName "Secret Stuff"
    AuthType  basic
    AuthUserFile /etc/httpd/.htpasswd
    Require valid-user
</Directory>
```

- Testez l'accès à l'aide d'un navigateur Web ; vérifiez que l'accès réussit pour les utilisateurs authentifiés mais qu'il échoue pour les autres.

Authentification utilisateur LDAP d'Apache

Dans cette configuration, les comptes d'utilisateur et les mots de passe sont stockés dans un service d'annuaire LDAP distant. L'avantage de cette configuration est que plusieurs serveurs Web peuvent utiliser le même service d'annuaire pour stocker des comptes d'utilisateur et des mots de passe, ce qui facilite leur synchronisation. Pour cette configuration, vous devez connaître l'emplacement du serveur LDAP contenant les informations de votre compte, et savoir s'il utilise les protocoles TLS/SSL et sous quel préfixe LDAP se trouvent vos entrées d'utilisateur.

Votre administrateur LDAP devra gérer de la manière appropriée les informations relatives aux comptes dans l'annuaire. Pour les besoins de ce cours, nous nous concentrerons sur la partie serveur Web de cette configuration et ignorerons la manière dont les informations sont gérées dans l'annuaire LDAP.

Exemple de procédure de configuration :

- Téléchargez le certificat LDAP, si nécessaire. Dans la salle de classe, vous pouvez le télécharger depuis *ftp://instructor.example.com/pub/example-ca.crt*
- Ajoutez **`LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/example-ca.crt`** et **`AuthBasicProvider ldap`** à **`httpd.conf`**.
- Ajoutez un bloc **`Directory`** dans le bloc **`VirtualHost`** comme vous l'avez fait précédemment pour l'authentification par fichier plat. Vous devez cependant remplacer la ligne **`AuthUserFile`** par une ligne **`AuthLDAPUrl`** pointant vers l'annuaire LDAP dans lequel rechercher des informations utilisateur :

```
AuthLDAPUrl "ldap://instructor.example.com/dc=example,dc=com" TLS
```

par exemple,

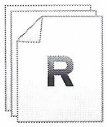
```
LDAPTrustedGlobalCert CA_BASE64 cert-path

<Directory /var/www/html/private>
    AuthName "A very private place"
    AuthType basic
    AuthBasicProvider ldap
    AuthLDAPUrl "ldap://fqdn/prefix" TLS
    Require valid-user
</Directory>
```

où

- *`cert-path`* est le nom de chemin du certificat CA
- *`fqdn`* est le nom de domaine complet du serveur LDAP
- *`prefix`* est le préfixe LDAP (**`dc=example,dc=com`** par exemple)

- Faites un test pour vérifier que les utilisateurs LDAP peuvent s'authentifier à Apache.

Utilisez cet espace pour vos notes.



Références

Apache.org : « Authentification, autorisation et contrôle d'accès »
http://httpd.apache.org/docs/2.2/howto/auth.html
(si ***httpd-manual*** est installé et **`httpd`** est exécuté)
http://localhost/manual/howto/auth.html

Documentation du module Apache mod_authnz_ldap
http://localhost/manual/mod/mod_authnz_ldap.html



Exercice de Liste de contrôle des performances

Configurer l'authentification LDAP

Vous allez configurer le serveur Web sur serverX avec une URL **/private** à laquelle les utilisateurs dans l'annuaire LDAP sur instructor.example.com peuvent accéder.

- ☐ Configurez l'authentification LDAP sur serverX en utilisant instructor.example.com comme serveur LDAP et **dc=example,dc=com** comme nom distinctif de base, et utilisez le certificat trouvé dans *ftp://instructor/pub/example-ca.crt*. Choisissez des mots de passe LDAP.

- ☐ Connectez-vous en tant que **root** (super utilisateur) sur serverX. Créez un nouveau répertoire **/var/www/html/private**.

- ☐ Dans le répertoire **private**, créez un **index.html** contenant le texte **Private Data**.

- ☐ Téléchargez **ftp://instructor/pub/example-ca.crt** et placez-le dans **/etc/httpd**.

- ☐ Modifiez **/etc/httpd/conf/httpd.conf** et ajoutez l'authentification LDAP pour le répertoire **private**.

```
LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/example-ca.crt

<Directory /var/www/html/private>
    AuthName "Secret Stuff"
    AuthType  basic
    AuthBasicProvider ldap
    AuthLDAPUrl "ldap://instructor.example.com/dc=example,dc=com" TLS
    Require valid-user
</Directory>
```

- ☐ Redémarrez Apache.

- ☐ Accédez à http://serverX.example.com/private. Une boîte de dialogue d'authentification doit normalement s'afficher. Si ce n'est pas le cas, fermez toutes les fenêtres du navigateur, vérifiez votre configuration et réessayez.

- ☐ Connectez-vous en tant qu'utilisateur **ldapuserX** avec le mot de passe **password**.

Résolution des problèmes Apache/SELinux

- Répertorier les contextes SELinux affectés aux ports

```
[root@serverX ~]# semanage port -l | grep http
http_cache_port_t              tcp      3128, 8080, 8118, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      80, 443, 488, 8008, 8009, 8443
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
```

- Affecter un contexte SELinux à un port

  Si vous configurez Apache pour qu'il s'exécute sur un port non standard, vous devrez probablement affecter le contexte SELinux **http_port_t** à ce port. Par exemple, si vous avez configuré Apache pour qu'il s'exécute sur le port 777, vous devrez faire ce qui suit pour permettre à Apache de s'exécuter :

```
[root@serverX ~]# semanage port -a -t http_port_t -p tcp 777
```

- Fichiers journaux Apache et niveaux de journalisation

  Vous pouvez définir le niveau de journalisation et les fichiers journaux à l'aide du **LogLevel**, **ErrorLog** et **CustomLog** dans **/etc/httpd/conf/httpd.conf**. Le **LogLevel** (niveau de journalisation) par défaut est **warn**. Par défaut, le **ErrorLog** est envoyé à **/var/log/httpd/error_log** et **CustomLog** est envoyé à **/var/log/httpd/access_log**. Ces directives peuvent servir à définir des directives pour le site Web principal ou pour les hôtes virtuels.

- Configurer SELinux pour que les fichiers journaux SELinux soient plus détaillés

  Des règles dans la stratégie SELinux empêchent les messages d'erreur d'être envoyés aux journaux. Ces règles sont appelées *règles* dontaudit. Elles empêchent les journaux de recevoir des messages inutiles mais elles peuvent aussi vous empêcher de détecter un problème à résoudre. Pour désactiver ces règles **donaudit**, exécutez la commande suivante :

```
[root@serverX ~]# semanage dontaudit off
```



Avertissement

La désactivation des règles **dontaudit** désactive aussi **setroubleshoot-server**. Aucun message ne sera envoyé à **/var/log/messages** et **sealert** sera désactivé. Tous les messages d'erreur SELinux seront envoyés à **/var/log/audit/audit.log**.

- Restaurer ou changer le type de contexte SELinux d'un fichier ou d'un répertoire html

  Si vous stockez des données Web dans un nouvel emplacement, utilisez **semanage fcontext** pour ajouter le nouvel emplacement à la base de données des contextes et **restorecon** pour définir les contextes des fichiers et des répertoires :

```
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/virtual(/.*)?'
[root@serverX ~]# restorecon -RFvv /virtual/
```

Si vous obtenez des erreurs de refus d'autorisation, alors que le contenu se trouve dans un emplacement approuvé (par exemple, **/var/www/html/**), exécutez la commande **restorecon** sur le répertoire comme précédemment. La commande **restorecon** peut s'exécuter avec l'option **-F** qui changera les types *personnalisables* que **restorecon** ignore normalement (**/etc/selinux/targeted/contexts/customizable_types** contient la liste de ces types).



Note

Si vous obtenez des erreurs de refus d'autorisation, gardez à l'esprit qu'il peut s'agir d'un problème d'autorisation Linux et non SELinux. Assurez-vous que l'utilisateur ou le groupe **apache** dispose au moins d'un accès en lecture aux fichiers et aux répertoires en question.

- Documentation SELinux sur les types de contexte et les booléens Apache

  La page man **httpd_selinux**(8) décrit les contextes de fichiers et les booléens les plus courants pour le serveur Web.

  httpd_sys_content_t est utilisé pour n'importe quel fichier/répertoire général pour le serveur Web. **httpd_sys_script_exec_t** est utilisé pour les scripts (par exemple, CGI) exécutés par le serveur Web. **public_content_t** est le contexte pour les fichiers qui seront partagés avec d'autres services restreints par SELinux tels que FTP, rsync, Samba, etc.

- Répertorier les booléens Apache/SELinux

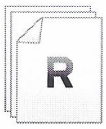
  Utilisez la commande **getsebool** pour afficher les booléens :

```
[root@serverX ~]# getsebool -a
abrt_anon_write --> off
allow_console_login --> on
allow_corosync_rw_tmpfs --> off
allow_cvs_read_shadow --> off
...
[root@serverX ~]# getsebool httpd_enable_cgi
httpd_enable_cgi --> on
```

- Rendre les booléens SELinux persistants

  Pour rendre les booléens persistants, utilisez **setsebool -P**:

```
[root@serverX ~]# setsebool -P httpd_enable_cgi off
[root@serverX ~]# getsebool httpd_enable_cgi
httpd_enable_cgi --> off
[root@serverX ~]# semanage boolean -l | grep httpd_enable_cgi
httpd_enable_cgi               -> off    Allow httpd cgi support
```



Références

Red Hat Enterprise Linux SELinux Guide
- Section 5.6 : Booléens

Red Hat Enterprise Linux SELinux Guide
- Chapitre 8 : Résolution des problèmes

Red Hat Enterprise Linux Managing Confined Services
- Chapitre 3 : Le Serveur HTTP Apache

Pages man **semanage**(8), **httpd_selinux**(8)



Exercice de Questionnaire

Résolution des problèmes liés à Apache - Questionnaire

1. Complétez la commande suivante pour répertorier tous les contextes de port : **semanage** _____ **-l**.

2. Complétez la commande suivante pour qu'Apache utilise le port TCP 8001 : **semanage** _____ _____ **-t httpd_port_t** _____ _____ **8001**.

3. Les deux directives du fichier de configuration Apache pour spécifier la gravité (détails) des messages d'erreur et le fichier dans lequel consigner les erreurs sont _____ et _____.

4. La directive du fichier de configuration Apache pour spécifier le format et l'emplacement du contenu auquel les clients peuvent accéder est _____.

5. Les messages AVC complets (bruts) SELinux sont transmis à **/var/log**_____.

6. Pour que SELinux fournisse plus de détails, vous pouvez exécuter **semanage** _____ **off**.

7. Les commandes pour obtenir et définir les booléens SELinux sont _____ et _____.

8. **man** _____ présente une page man SELinux spécifique à Apache.

9. **man -k** _____ répertorie toutes les pages man SELinux spécifiques aux services.

10. L'option **-F** de la commande **restorecon** réinitialise les types _____.



Test

Test de critère1

Étude de cas

Services Web encapsulés dans SSL

Avant de commencer...

Exécutez le script **`lab-setup-hacker`** sur desktopX.

Marcelo Hacker est un détective privé réputé. En fait, cela marche tellement bien pour lui qu'il lui est difficile de trouver le temps de rencontrer des clients potentiels. M. Hacker a décidé de créer un site Web sur lequel ses clients potentiels pourront lui envoyer des messages. La confidentialité étant un élément essentiel dans le secteur de l'enquête privée, le site Web doit utiliser un certificat SSL signé.

- Configurez Apache sur serverX pour qu'il chiffre le site Web de Marcelo Hacker avec SSL.
- Vous trouverez un certificat SSL signé pour le serveur et la clé correspondante à l'emplacement suivant : **`/net/instructor/var/ftp/pub/materials/tls`**. Sous ce répertoire, **`certs/serverX.crt`** contient le certificat signé pour le serveur et **`private/serverX.key`** contient la clé privée correspondante.

  Déployez le certificat signé pour Apache sur serverX. Laissez le site Web par défaut réservé pour le contenu. M. Hacker téléchargera ce contenu personnalisé ultérieurement.

Une fois toutes ces opérations effectuées, exécutez le script **`lab-grade-hacker`** sur desktopX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Test

Test de critère 2

Étude de cas

Configuration supplémentaire du serveur Web

Avant de commencer...

Exécutez le script **`lab-setup-website`** sur desktopX.

Example Industries, une entreprise performante, a besoin d'un nouveau site Web. En fait, elle en a besoin de deux ! L'un sera le site Web de l'entreprise et l'autre servira au test du contenu. En outre, le site Web de l'entreprise devra comporter une zone protégée par mot de passe et une application CGI spéciale devra y être installée.

Sur la machine serverX, déployez un serveur Web avec deux hôtes virtuels.

Hôte virtuel1 : *http://serverX.example.com*

- Créez une page simple réservée à l'URL de base

Hôte virtuel2 : *http://wwwX.example.com*

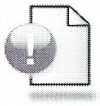
- Créez une page simple réservée à l'URL de base différente de celle utilisée sur l'hôte virtuel1.
- Protégez la zone *http://wwwX.example.com/private* par un mot de passe
- Ajoutez l'utilisateur **`forrest`** avec le mot de passe **`trees`** à **`/private`**
- Téléchargez le fichier CGI ftp://instructor.example.com/pub/gls/special.cgi et installez-le en tant que *http://wwwX.example.com/cgi-bin/special.cgi*

Avant de vérifier votre travail, exécutez le script de notation **`lab-grade-website`** sur desktopX.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Sécurisation d'un serveur Apache avec le chiffrement

Dans cette section, vous avez appris à :

- Installer un certificat pour le serveur Web Apache et activer l'encapsulation SSL

Configurer l'hébergement virtuel basé sur le nom

Dans cette section, vous avez appris à :

- Configurer un hôte virtuel basé sur le nom (DocumentRoot, ServerAdmin et ServerName distincts)
- Établir un alias de serveur
- Configurer un DocumentRoot à gérer par un groupe

Activer un exécutable CGI

Dans cette section, vous avez appris à :

- Activer un exécutable CGI

Configurer l'authentification utilisateur

Dans cette section, vous avez appris à :

- Limiter les informations à un petit groupe d'utilisateurs à l'aide de l'authentification par fichier plat
- Limiter les informations à un groupe centralisé d'utilisateurs ayant recours à un serveur LDAP ou une base de données relationnelle

Résolution des problèmes Apache/SELinux

Dans cette section, vous avez appris à :

- Contrôler et analyser l'activité Web
- Ajouter un contexte de fichiers SELinux persistant correspondant à la stratégie
- Modifier SELinux pour permettre à un service d'utiliser un port non standard
- Résoudre les conflits de contextes et de booléens SELinux

Test de critère 2

Dans cette section, vous avez appris à :

-



MODULE QUATORZE

CONFIGURATION SMTP DE BASE

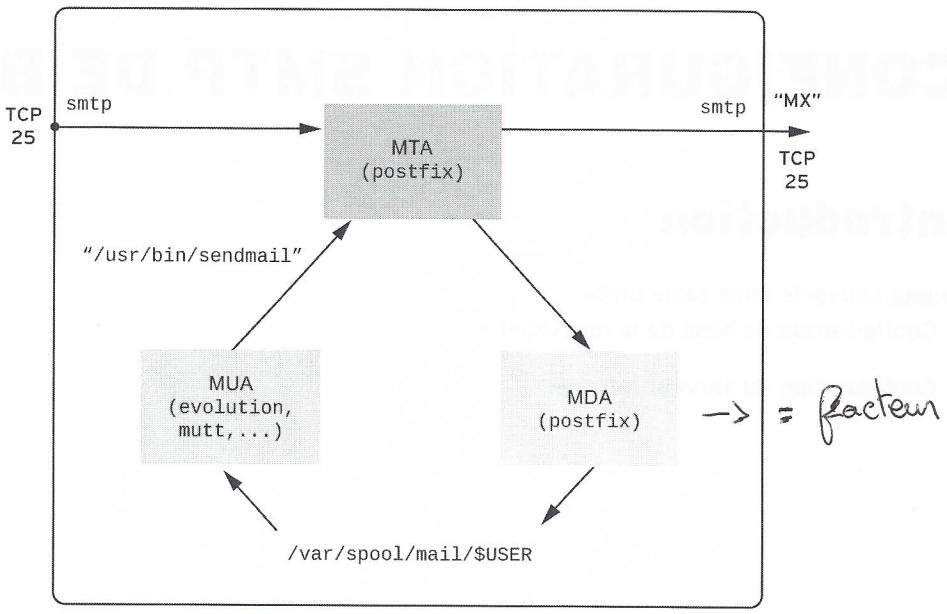
Introduction

Sujets couverts dans cette unité :

- Configuration de base de la messagerie
- Configuration du serveur intranet

Principes de base de la remise du courrier électronique

Remise du courrier électronique



- *MTA* : « Mail Transfer Agent », l'agent de transfert de courrier. Les MTA transmettent le courrier d'un point à un autre jusqu'à la remise à sa destination. L'email est envoyé par d'autres serveurs au moyen du protocole SMTP au port TCP 25 ou par des clients locaux via le programme **`/usr/bin/sendmail`**. Si l'agent MTA est la destination finale, le message est transmis à l'agent de remise de courrier (MDA). Sinon, l'agent MTA utilise les enregistrements MX pour trouver le MTA suivant dans le DNS et y envoie le message par SMTP.

- *MDA* : « Mail Delivery Agent», l'agent de remise du courrier. L'agent MDA distribue le courrier dans la base de messages locale du destinataire (par défaut, **`/var/spool/mail/`*`user`***). Postfix fournit son propre MDA de remise vers la base de messages locale par défaut basé sur les fichiers, **`/usr/libexec/postfix/local`**.

- *MUA* : « Mail User Agent », l'agent de gestion de courrier. Les clients utilisés pour l'envoi des emails et leur consultation dans la base de messages de l'utilisateur.

Concepts clés de la remise des emails :

- *Relais* : quand un serveur de messagerie (MTA) transfère l'email envoyé à un autre serveur, pour la remise du courrier.

- *File d'attente* : la remise a échoué ou une tentative de relais se trouve dans une file d'attente ; la remise est retentée régulièrement par l'agent MTA. (Par défaut, Postfix effectue une tentative toutes les heures.)
- *Refusé* : quand un serveur refuse un email au cours de l'envoi initial.
- *Non remis* : quand un email est renvoyé par un serveur distant au serveur de messagerie et/ou l'utilisateur d'origine après que le serveur distant a accepté de distribuer ledit email.

Agent MTA Postfix

Il existe un certain nombre de serveurs de messagerie open source, y compris Postfix, Sendmail et Exim. Dans cette unité, nous allons nous concentrer sur Postfix, un puissant MTA relativement facile à configurer, qui est utilisé par défaut dans Red Hat Enterprise Linux 6.



Note

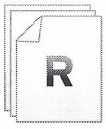
Sendmail était le MTA par défaut fourni jusqu'à la version 5 de Red Hat Enterprise Linux incluse.

Postfix est fourni par le package RPM *postfix* et contrôlé par le script de service **postfix**. Ce programme modulaire est constitué de plusieurs programmes qui coopèrent entre eux. Ses composants sont contrôlés par le processus **master**.

Le principal fichier de configuration de Postfix est **/etc/postfix/main.cf**. Il peut être modifié dans un éditeur de texte ou avec la commande **postconf**. La commande **postconf** peut aussi servir à déterminer les paramètres de configuration actuels ou par défaut, soit pour Postfix dans son ensemble, soit individuellement pour chaque option.

Par défaut, Postfix écoute uniquement le courrier entrant à partir de l'hôte local. Pour modifier la configuration de Postfix afin de recevoir le courrier à distribuer localement et qui a été envoyé par des hôtes distants, **inet_interfaces = all** doit être défini dans **/etc/postfix/main.cf**.

Pour la résolution des problèmes d'email, un journal de toutes les opérations liées au courrier est conservé dans **/var/log/maillog**. Il comprend des informations sur les remises refusées et réussies. La commande **mailq** (ou **postqueue -p**) affiche une liste des emails sortants ayant été mis en file d'attente. Pour tenter de redistribuer immédiatement les messages en file d'attente, vous pouvez exécuter la commande **postfix flush** (ou **postqueue -f**) ; dans le cas contraire, Postfix fera une nouvelle tentative environ une fois toutes les heures jusqu'à ce que les messages soient acceptés ou arrivent à expiration.



Références

Red Hat Enterprise Linux Deployment Guide

- Section 12.3.1: Postfix

postconf(5) et **postfix**(1) (pages du manuel)



Exercice de Liste de contrôle des performances

Principes de base de la remise du courrier électronique

- ☐ Démarrez deux shells de terminal, l'un en tant que **root** sur desktopX, et l'autre en tant que **root** sur serverX.
- ☐ Sur chaque machine, vérifiez que *postfix* est installé et que le service *postfix* est en cours d'exécution.
- ☐ Sur serverX, ajoutez l'utilisateur **elvis**. Connectez-vous en tant qu'**elvis** et ouvrez l'agent MUA **mutt** pour surveiller le courrier entrant d'Elvis.
- ☐ Utilisez l'agent **mutt** MUA sur desktopX pour composer et envoyer le courrier à elvis@serverX.example.com.
- ☐ **elvis** a-t-il reçu l'email sur serverX ? Hum...
- ☐ Sur desktopX, utilisez **mailq** pour examiner la file d'attente de remise. Regardez aussi dans **/var/log/maillog** s'il y a des problèmes.
- ☐ Sur serverX, n'oubliez pas que **postfix** se lie uniquement à **localhost** par défaut selon la politique de Red Hat. Utilisez **netstat** pour vérifier que c'est bien le cas.
- ☐ Examinez les paramètres actuels de la directive **inet_interfaces** du principal fichier de configuration **postfix**, **/etc/postfix/main.cf**.
- ☐ Modifiez **/etc/postfix/main.cf** et définissez **inet_interfaces=all**. Redémarrez le service **postfix** et vérifiez que le démon écoute toutes les interfaces.
- ☐ Sur desktopX, utilisez **postfix flush** pour vider manuellement la file de remise en attente. Vérifiez que la file d'attente est maintenant vide et que le courrier a été distribué.
- ☐ Sur serverX, utilisez l'agent MUA **mutt** pour vérifier que les emails sont effectivement remis. Vérifiez aussi que **/var/log/maillog** contient une preuve du succès de la remise du courrier.

Configuration intranet

Dans la pratique aujourd'hui, la plupart des entreprises n'ont plus uniquement un serveur de messagerie qui gère tous les emails entrants et sortants. Pour des raisons de sécurité, les serveurs de messagerie sont plutôt spécialisés dans des rôles précis, de façon à affiner encore les performances des applications souhaitées qui leur sont propres.

Certains rôles standard comprennent :

- *client null* : une machine cliente qui exécute un agent MTA local, mais uniquement afin d'envoyer tout le courrier à un serveur de messagerie central qui assure la remise. Un client null n'accepte pas la remise locale des emails *quels qu'ils soient*. Les utilisateurs peuvent exécuter des agents MUA sur le client null pour la consultation et l'envoi d'emails. La plupart des machines sont des clients null .

  Dans le schéma ci-dessous, nous utilisons desktop*X*.example.com pour figurer tous ces clients null.

- *serveur de réception de courrier uniquement* : un serveur de messagerie qui gère les emails entrants pour les utilisateurs sur le site et les fait passer à un agent MDA qui va les distribuer aux bases de messages des utilisateurs. Le courrier sortant est envoyé à un serveur de messagerie central comme pour un client null. Le serveur de courrier entrant peut être intégré à un serveur IMAP ou POP3 afin de permettre aux agents utilisateurs de messagerie (MUA) d'accéder à leur bases de messages ou un hôte distinct avec un accès à la base de messages peut exécuter le serveur IMAP ou POP3.

  Dans un environnement de production, on trouve généralement un serveur ou un mécanisme anti-courrier indésirable avant le serveur de réception de courrier uniquement qui filtre les courriers indésirables et envoie uniquement les bons messages vers le serveur de courrier entrant. La configuration de cet équipement n'est pas l'objet de ce cours.

  Dans le schéma ci-dessous, mail.example.com est le serveur de réception de courrier uniquement et il exécute également le serveur IMAP.

- *relais de courrier sortant* : le relais de courrier sortant, ou « hôte actif », accepte tous les messages sortants et les relaie vers leur destination en utilisant les enregistrements MX et le protocole SMTP. Un relais de courrier sortant doit uniquement relayer le courrier des hôtes autorisés ; un « relais de messagerie ouvert » sera exploité par les spammeurs et les autres serveurs de messagerie bloqueront probablement les messages en provenance d'un relais ouvert connu.

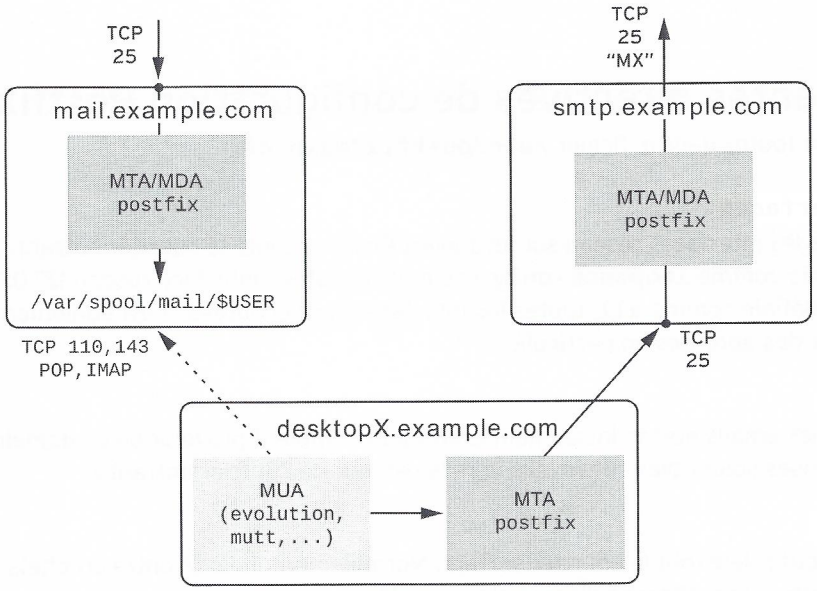
  Par souci de simplicité, nous allons nous intéresser pendant la présente formation à un relais interne de courrier sortant de groupe de travail qui accepte les messages envoyés au port 25/TCP à partir d'adresses IP internes vers toutes les destinations sans autre authentification, mais qui refuse les messages en provenance d'adresses IP externes.

  Dans le schéma ci-dessous, smtp.example.com est le relais de courrier sortant utilisé par les clients null.



Note

Une variante plus sophistiquée du relais de courrier sortant est l' *agent d'envoi du courrier.* Un agent d'envoi du courrier (MSA) relaie les messages des machines externes ou internes authentifiées par nom d'utilisateur et mot de passe sur une connexion SMTP protégée par SSL vers le port 587/TCP. Ainsi, les utilisateurs hors du réseau local peuvent relayer en toute sécurité les emails par le relais de courrier sortant. Cette configuration est plus complexe et ne sera pas abordée plus avant au cours de notre formation.



DNS externe

```
example.com.        IN MX 10    mail.example.com.
```

envoie->smtp delivre aucun mail envoie -> smtp no delivery

Concept	Directive	*mail.example.com*	*desktop.example.com*	*smtp.example.com*
Interface de liaison	*inet_interfaces*	all	loopback only	mynetwork all
Domaine fictif	*myorigin*	example.com	example.com	example.com
Remise indirecte	*relayhost*	smtp.example.com	smtp.example.com	none

		mail	Desktop	smtp
Recevoir le courrier pour...	*mydestination*	example.com	example.com	none
Remise locale	*local_transport*	error	default	error
Relais depuis...	*mynetworks*	~~localhost~~ all	~~all~~ localhost	

Tableau 14.1. Serveur de messagerie Intranet, client null et relais sortant

Importantes directives de configuration Postfix

On les trouve toutes dans le fichier **`/etc/postfix/main.cf`**.

`inet_interfaces`
: Contrôle les interfaces réseau sur lesquelles Postfix écoute le courrier entrant. Si la directive est définie comme **`loopback-only`**, seule est écoutée l'interface réseau 127.0.0.1 et ::1, et elle est définie comme **`all`**, toutes les interfaces sont écoutées. Il est également possible de spécifier des adresses en particulier.

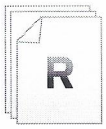
`myorigin`
: Réécrit les emails postés localement pour qu'ils semblent provenir de ce domaine. (Pour que les réponses soient bien renvoyées vers le serveur de courrier entrant.)

`relayhost`
: L'hôte actif relaie tout le courrier sortant. Normalement indiqué entre crochets carrés afin de supprimer la recherche d'enregistrement MX.

`mydestination`
: Les emails adressés à ces domaines sont transmis à l'agent MDA pour une remise locale.

`local_transport`
: Procédure de remise des messages adressés à **`$mydestination`**. Par défaut, la directive est définie avec **`local:$myhostname`** qui utilise l'agent MDA **`local`** pour la remise des emails entrants à la base de messages locale dans **`/var/spool/mail`**.

`mynetworks`
: Listes d'adresses IP et de réseaux séparés par des virgules (en notation CIDR) qui peuvent relayer partout via cet agent MTA, sans authentification supplémentaire.



Références

postconf(5), **postconf**(1) et **transport**(5) (pages du manuel)

/usr/share/doc/postfix-*/README_FILES/BASIC_CONFIGURATION_README

/usr/share/doc/postfix-*/README_FILES/STANDARD_CONFIGURATION_README



Exercice de Étude de cas

Configuration intranet

Avant de commencer...

Le DNS a déjà été configuré pour recouvrir vos hôtes comme des membres du domaine **`domainX.example.com`**.

nom d'hôte	adresse IP	aussi connu comme
mail.domainX.example.com	192.168.0.X+100	(serverX.example.com)
smtp.domainX.example.com	192.168.0.X+200	(hostX.example.com)
desktop.domainX.example.com	192.168.0.X	(desktopX.example.com)

Tableau 14.2. domainX.example.com

L'hôte mail.domainX.example.com est également le destinataire **`MX`** de tout le domaine domainX.example.com.

Complétez le tableau ci-dessous avec les directives appropriées pour configurer ces hôtes respectivement comme serveur de boîte aux lettres Intranet, hôte smtp et station cliente.

Essayez d'utiliser uniquement les fichiers **`BASIC_CONFIGURATION_README`**, **`STANDARD_CONFIGURATION_README`** et **`main.cf`** pour référence.

Une fois que vous avez terminé, demandez à un autre participant de vérifier votre travail.

DNS externe

```
domainX.example.com.      IN MX 10    mail.domainX.example.com.
```

Concept	Directive	*mail.domainX*	*desktop.domainX*	*smtp.domainX*
Interface de liaison	*inet_interfaces*			
Domaine fictif	*myorigin*			
remise indirecte	*relayhost*			
Recevoir le courrier pour...	*mydestination*			
remise locale	*local_transport*			
Relais de...	*mynetworks*			

Tableau 14.3. Configuration de la messagerie Intranet pour domainX.example.com

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Test

Test de critère

Étude de cas

Configuration de messagerie Intranet

Avant de commencer...

Avant de commencer, exécutez le script **`lab-setup-email`** sur desktopX

La société Hoffman Hair Supply, un fabricant de produits de soin capillaire, veut centraliser la gestion de ses emails internes.

Le serveur DNS est déjà configuré de sorte que vos machines soient des membres du domaine DNS **`domainX.example.com`** avec les adresses suivantes :

```
192.168.0.X      desktop.domainX.example.com   (a.k.a.  desktopX.example.com)
192.168.0.X+100     mail.domainX.example.com   (a.k.a.   serverX.example.com)
192.168.0.X+200     smtp.domainX.example.com   (a.k.a. hostX.example.com)
```

Le serveur **`mail.domainX.example.com`** est également le destinataire **`MX`** de l'ensemble du domaine **`domainX.example.com`**.

Configurez l'hôte **`mail.domainX.example.com`** comme serveur de courrier entrant uniquement de façon que tout courrier distribué au domaine **`@domainX.example.com`** soit stocké sur ce serveur.

Configurez le serveur **`smtp.domainX.example.com`** comme serveur SMTP sortant qui accepte de relayer les emails des membres du domaine **`domainX.example.com`** vers les réseaux extérieurs.

Configurez l'hôte **`desktop.domainX.example.com`** comme « client null ». Il ne peut pas recevoir de courrier provenant du réseau , la remise de courrier locale est désactivée et tout le courrier sortant est envoyé indirectement via **`smtp.domainX.example.com`**.

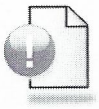
Pour les trois hôtes, assurez-vous que tout courrier d'origine masque le domaine de l'expéditeur comme **`domainX.example.com`**.

Une fois que vous avez terminé, exécutez le script **`lab-grade-email`** pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Principes de base de la remise du courrier électronique

Dans cette section, vous avez appris à:

- Configurer postfix pour recevoir les emails du réseau pour les tâches administratives du système.
- Surveiller la remise des emails et diagnostiquer les problèmes potentiels de remise du courrier.

Configuration intranet

Dans cette section, vous avez appris à:

- Déterminer si un serveur de boîtes aux lettres et/ou un serveur SMTP est adapté.
- Masquer le domaine des adresses de l'expéditeur.
- Relayer tout le courrier vers un serveur de messagerie du domaine.
- Désactiver la remise locale.
- Relayer uniquement le courrier destiné au réseau local.



MODULE QUINZE

SERVEUR DNS CACHE UNIQUEMENT

Introduction

Sujets couverts dans cette unité :

- Serveurs DNS ne faisant pas autorité

Vue d'ensemble de DNS

Dans cette section, nous allons passer en revue les connaissances de la classe sur le DNS et nous allons nous assurer que tout le groupe comprend les types de serveurs DNS, d'enregistrements de ressources DNS et les bases de fonctionnement du système DNS. Un jeu clôturera la discussion en groupe : n'hésitez pas à poser des questions maintenant et à prendre des notes pour vous y préparer.

Serveurs de noms faisant autorité
: Ils stockent et diffusent les données réelles d'une zone (tout ou partie d'un domaine DNS). Les serveurs de noms faisant autorité comprennent les types suivants :

  - *Serveur maître*, qui contient les données de zone d'origine. On parle parfois de serveur de noms « principal » ou « primaire ».
  - *Serveur esclave*, un serveur de sauvegarde qui récupère des copies des données de zone du serveur maître par des *transferts de zone*. On parle parfois de serveur de noms « secondaire ».

Serveurs de noms récursifs/ne faisant pas autorité
: Les clients les utilisent pour rechercher des données provenant des serveurs de noms faisant autorité. Les serveurs de noms récursifs comprennent les types suivants :

  - *Serveur de noms cache uniquement*, qui sert uniquement aux recherches et ne fait pas autorité pour quoi que ce soit, sauf des données triviales.

Recherches DNS

- *Le résolveur stub* du client envoie une requête au serveur de noms dans **`/etc/resolv.conf`**.
- Si le serveur de noms fait *autorité* pour l'information demandée, il envoie une *réponse faisant autorité* au client.
- Dans le cas contraire, si le serveur de noms a en cache les informations demandées, il envoie une réponse *ne faisant pas autorité* au client.
- Si les informations ne sont pas dans le cache, le serveur de noms les recherche sur le serveur de noms qui fait autorité en commençant par la zone racine, puis en descendant dans la hiérarchie DNS jusqu'au serveur de noms qui fait autorité pour ces informations, et enfin récupère la réponse pour le client. Dans ce cas, le serveur de noms transmet les informations au client et garde également une copie des informations dans son cache qui servira lors de recherches ultérieures.

Utilisez cet espace pour vos notes.

Enregistrements de ressources DNS

Une zone DNS stocke ses informations sous forme d' *enregistrements de ressources*. Chaque enregistrement de ressource a un *type* qui indique la sorte de données qu'il contient :

- A : nom vers adresse IPv4.
- AAAA : nom vers adresse IPv6.
- CNAME : nom vers « nom canonique » (un autre nom avec un enregistrement A/AAAA).
- PTR : adresse IPv4/IPv6 vers nom.
- MX : serveur de messagerie pour un nom (l'endroit où l'email doit être envoyé).
- NS : serveur de noms d'un nom de domaine.
- SOA : l'enregistrement de début d'autorité « start of authority » contient les informations administratives d'une zone DNS).

Résolution des problèmes des recherches DNS

L'outil **dig** est l'un des plus utiles dans la résolution des problèmes liés aux recherches DNS.

```
[student@student ~]$ dig example.com
; <<>> DiG 9.7.0-P2-RedHat-9.7.0-5.P2.el6 <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41645
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;server3.example.com.           IN      A

;; ANSWER SECTION:
server3.example.com.    86400   IN      A       192.168.0.103

;; AUTHORITY SECTION:
example.com.            86400   IN      NS      instructor.example.com.

;; ADDITIONAL SECTION:
instructor.example.com. 86400   IN      A       192.168.0.254

;; Query time: 2 msec
;; SERVER: 192.168.0.254#53(192.168.0.254)
;; WHEN: Mon Dec 13 10:06:48 2010
;; MSG SIZE  rcvd: 94
```

Il fournit des informations détaillées sur une recherche DNS, y compris les raisons possibles de l'échec de l'interrogation :

- **NOERROR** : la requête a abouti.
- **NXDOMAIN** : le serveur DNS répond que ce nom n'existe pas.

- **SERVFAIL** : le serveur DNS est indisponible *ou* la validation DNSSEC de la réponse a échoué.
- **REFUSED** : le serveur DNS refuse de répondre (peut-être pour des raisons de contrôle d'accès).

Quelques informations de sortie **dig** :

- L'en-tête donne des informations sur l'interrogation et la réponse, y compris l'état de la réponse et toute indication spéciale définie (**aa** pour une réponse faisant autorité, etc.).
- **QUESTION** : l'interrogation de DNS elle-même.
- **ANSWER** : la réponse, le cas échéant.
- **AUTHORITY** : les serveurs de noms responsables du domaine ou de la zone.
- **ADDITIONAL** : informations supplémentaires qui concernent généralement les serveurs de noms.
- Les commentaires dans la partie inférieure indiquent le serveur de noms récursif auquel la requête a été envoyée et le temps qu'il a fallu pour obtenir une réponse.



Références

Red Hat Enterprise Linux Deployment Guide
- Section 10.1: Introduction au DNS

> Administrateur BIND : Guide de référence, Chapitre 1
> /usr/share/doc/bind-9.7.0/arm/

host(1), **dig**(1) et **resolv.conf**(5) (pages du manuel)

Serveurs DNS cache uniquement

Dans cette section, le groupe va apprendre à configurer BIND 9.7 fourni avec Red Hat Enterprise Linux 6 en tant que serveur de noms cache uniquement. Un jeu clôturera la discussion en groupe : n'hésitez pas à poser des questions sur BIND et sa configuration et à prendre des notes pour vous y préparer.

Le serveur de noms BIND est le plus largement utilisé en open source. Dans Red Hat Enterprise Linux, il fait partie du package logiciel *bind*. Toutefois, le principal service qu'il fournit est le programme **named**, contrôlé par le script de service **named**.



Important

Pour que BIND fonctionne correctement, le pare-feu doit autoriser les connexions aux ports 53/UDP et 53/TCP sur le serveur de noms Si le port 53/TCP est bloqué, les grandes requêtes et les transferts de zone risquent de s'interrompre. Cette erreur de configuration est très courante.

Le fichier de configuration principal de BIND est **`/etc/named.conf`**. Le répertoire **`/var/named`** contient des fichiers de données supplémentaires que le serveur de noms utilise.

Syntaxe de **`/etc/named.conf`** :

- `//` ou # à la fin d'une ligne indique un commentaire ; du texte entre `/*` et `*/` constitue aussi un commentaire qui peut s'étendre sur plusieurs lignes.
- Les directives se terminent par un point-virgule (`;`).
- Beaucoup de directives ont des *listes de correspondances d'adresses* entre accolades ; une liste d'adresses IP ou de sous-réseaux en notation CIDR, ou des ACL nommées comme **`any;`** (tous les hôtes) et **`none;`** (aucun hôte).
- Le fichier commence par un bloc **`options`** contenant des directives qui contrôlent le fonctionnement de **named**.
- Les blocs **`zone`** contrôlent la façon dont **named** trouve le serveur de noms racine et les zones où ce serveur fait autorité.

Quelques directives **`options`** importantes :

- **`listen-on`** définit les adresses IPv4 que **named** écoute.
- **`listen-on-v6`** définit les adresses IPv6 que **named** écoute.
- **`allow-query`** définit les clients qui peuvent interroger le serveur DNS et obtenir des informations.
- **`forwarders`** contient une liste de serveurs de noms auxquels les requêtes DNS vont être envoyées (plutôt que de contacter directement les serveurs de noms externes, utile dans les scénarios avec pare-feu).

Toutes ces directives prennent comme liste de correspondance d'adresses des éléments séparés par point-virgule et entre accolades : par exemple, **`listen-on { any; };`** ou **`allow-query { 127.0.0.1; 10.0.0.0/8; };`**.

Démonstration de serveur de noms cache uniquement : Configuration

- Installez le package logiciel *bind* :

```
[root@serverX]# yum install bind
```

- Modifiez **/etc/named.conf** :

```
listen-on port 53 { any; };
listen-on-v6 port 53 { any; };
allow-query { 192.168.0.0/24; };
forwarders { 192.168.0.254; };
```

- Démarrez et activez le serveur DNS :

```
[root@serverX]# service named start
[root@serverX]# chkconfig named on
```



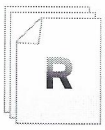
Note

La configuration par défaut de BIND dans Red Hat Enterprise Linux 6 intègre les paramètres que fournissait auparavant le *serveur de noms cache* dans Red Hat Enterprise Linux 5.



Important

Dans Red Hat Enterprise Linux 6, BIND 9.7 tente automatiquement de valider les réponses DNS avec, par défaut, DNSSEC. Comme la zone racine est signée, dans une salle de cours sans accès à Internet, il arrive que BIND refuse d'accepter des réponses DNS du serveur de la salle de cours par ce qu'il est impossible de contacter les vrais serveurs de noms racine, ce qui entraîne des erreurs de validation DNSSEC. Pour contourner cette difficulté, désactivez la validation automatique DNSSEC en définissant l'option **dnssec-validation** sur **no**.



Références

Red Hat Enterprise Linux Deployment Guide

- Unité 10 : Serveur de noms BIND

Administrateur BIND : Guide de référence
/usr/share/doc/bind-9.7.0/arm/



Test

Test de critère

Étude de cas

Serveur DNS cache uniquement

Avant de commencer...

Avant de commencer, exécutez le script **`lab-setup-cachingdns`** sur desktopX.

Pour sa florissante entreprise d'import-export, M. Hnath veut améliorer les performances de la résolution de noms par le déploiement d'un serveur de noms cache dans chacune de ses implantations commerciales.

Les requêtes récursives devront être envoyées au serveur de noms principal qui se trouve au siège de Hnath Import/Export.

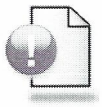
- Installez un serveur de noms cache sur serverX.
- Configurez le serveur de noms de manière que les requêtes récursives sont envoyées à instructor.example.com. De plus, configurez le serveur de noms pour qu'il accepte les requêtes provenant de quiconque sur le réseau de la classe.

Lorsque vous êtes prêt, exécutez le **`lab-grade-cachingdns`** sur desktopX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Vue d'ensemble de DNS

Dans cette section, vous avez appris à :

- Utilisez **dig** pour vérifier la fonctionnalité de votre serveur DNS.

Serveurs DNS cache uniquement

Dans cette section, vous avez appris à :

- Installer un serveur de noms cache.
- Faire suivre les requêtes DNS à instructor.example.com.



MODULE SEIZE

PARTAGE DE FICHIERS AVEC NFS

Introduction

Sujets couverts dans cette unité :

- Configuration du serveur NFS
- Considérations sur le client NFS

Concepts et configuration NFS

NFS, pour « Network File System », est un système de gestion de fichiers en réseau qu'utilisent couramment les systèmes Unix et les systèmes de stockage NAS pour permettre à plusieurs clients de partager l'accès à des fichiers sur le réseau. Il peut servir à fournir l'accès à des répertoires partagés de fichiers binaires ou à permettre aux utilisateurs d'accéder à leurs fichiers à partir de différents clients au sein d'un même groupe de travail.

Le protocole NFS a plusieurs versions : Linux prend en charge les versions 4, 3 et 2, et la plupart des administrateurs système connaissent NFSv3. Le protocole est non sécurisé par défaut, mais les versions les plus récentes comme NFSv4 prennent en charge une authentification mieux sécurisée voire le chiffrement avec Kerberos. Dans le tableau ci-dessous, indiquez les améliorations de NFSv4 abordées par l'instructeur :

NFSv2	NFSv3	NFSv4 = port 2049
Original public NFS protocol	Extended NFSv2 architecture	
Still in use	Added features: TCP support 64-bit file sizes and offsets Larger read/write sizes	
	Some implementations (including Red Hat Enterprise Linux) support Kerberos	
Requires support services: nfsd, rpc.mountd, rpc.statd, lockd	Also requires support services: nfsd, rpc.mountd, rpc.statd, lockd	
More difficult to secure behind a firewall	More difficult to secure behind a firewall	
Useful for backward compatibility	Useful for backward compatibility	

rpc fournit un port

Configuration du serveur NFS

Pour configurer un serveur NFS de base, assurez-vous que le groupe de packages **nfs-file-server**, qui comprend le package *nfs-utils*, est installé. Modifiez ensuite **/etc/exports** pour y lister les systèmes de fichiers que vous avez l'intention de partager sur le réseau avec les systèmes clients, et indiquez les clients qui ont accès à l'export ainsi que le type d'accès. Par exemple :

```
/var/ftp/pub      192.168.0.0/24(ro,sync)
```

exporte le répertoire **/var/ftp/pub** vers tous les hôtes sur le réseau 192.168.0.0/24 en lecture seule. De même,

```
/export/homes     *.example.com(rw,sync)
```

exporte le répertoire **/export/homes** en lecture-écriture vers tous les hôtes sur example.com. Chaque export est spécifié sur sa ligne propre dans le fichier **/etc/exports** du serveur.

Chaque fois que vous modifiez **/etc/exports** alors que le serveur NFS est en cours d'exécution, assurez-vous d'appliquer ces changements en exécutant **exportfs -r** après avoir enregistré vos modifications. Vous pouvez utiliser **exportfs -v** pour afficher tous les exports.

NFSv4 exporte également une *pseudo-racine*, la racine de tous les systèmes de fichiers exportés. Si un client monte *nfs-server*:/, ceci permet de monter automatiquement tous les systèmes de fichiers exportés selon leur position relative sous / sur le serveur NFS. C'est utile pour explorer tous les systèmes de fichiers exportés d'un serveur sur un client. Vous pouvez également monter des systèmes de fichiers séparément.



Note

L'option d'exportation **fsid=0** qui servait dans Red Hat Enterprise Linux 5 à exporter manuellement une pseudo-racine NFSv4 n'est plus nécessaire. Le nouveau serveur NFS exporte automatiquement une pseudo-racine sans configuration supplémentaire ni besoin de configurer de montages de liens. (Si pour quelque raison que ce soit vous spécifiez l'option, seul l'export où cette option est définie sera utilisé comme niveau racine de la pseudo-racine.)

Pour que la propriété des fichiers et les permissions fonctionnent correctement, les noms des groupes et des utilisateurs qui utilisent NFS doivent exister et être mappés avec cohérence vers les mêmes UID et GID sur les clients et sur le serveur NFS. Ces utilisateurs peuvent configurés manuellement dans **/etc/passwd** et **/etc/group** à l'aide des outils en local. Vous pouvez également les coordonner avec une authentification LDAP centrale et un répertoire des informations sur l'utilisateur.

Par défaut, un super utilisateur sur un client NFS est traité comme un utilisateur nfsnobody par le serveur NFS. Ainsi, si un super utilisateur tente d'accéder à un fichier dans un export monté, le serveur le traitera comme un accès de l'utilisateur nfsnobody. Cette mesure de sécurité peut s'avérer gênante dans des cas où l'export NFS sert de / à un client sans disque et où le super utilisateur doit vraiment être traité comme super utilisateur. Pour désactiver cette protection, le serveur doit ajouter **no_root_squash** à la liste des options définies pour l'export dans **/etc/exports**:

```
/exports/root-192.168.0.1     192.168.0.1(rw,no_root_squash)
```

Notez que cette configuration-là n'est pas sécurisée et qu'il vaudrait mieux l'utiliser conjointement à l'authentification et à la vérification d'intégrité de Kerberos, ce qui dépasse le cadre de cette formation.



Important

Si les noms d'utilisateurs ont des numéros d'UID différents sur les divers clients ou sur le serveur, vous rencontrerez des problèmes de propriété et d'autorisation.

Un des symptômes de ce type d'erreur est quand un fichier semble appartenir à et être utilisable par un utilisateur non privilégié donné et qu'une erreur d'autorisation de produit lorsque ledit utilisateur tente d'y accéder en lecture ou en écriture. L'utilisateur a probablement des UID différents sur le client et le serveur ; utilisez **`ls -ln`** sur le fichier pour afficher l'UID du propriétaire et **`id`** pour trouver l'UID d'utilisateur local pour vous aider dans votre diagnostic. Un autre symptôme des incohérences entre les noms d'utilisateurs et les UID que l'on rencontre avec les versions NFSv3 ou antérieures est lorsqu'un fichier créé par un utilisateur sur un système de fichiers NFS monté affiche un autre utilisateur comme propriétaire. Notez que le super utilisateur est délibérément mappé par défaut vers un utilisateur sans privilèges (nfsnobody).

Pour NFSv4, le port 2049/TCP (pour **`nfsd`**) doit être ouvert sur le serveur. Pour NFSv3 et les versions antérieures, des ports supplémentaires doivent être ouverts pour **`rpcbind`**, **`rpc.mountd`**, **`lockd`** et **`rpc.rquotad`**, ce qui est d'autant plus compliqué que beaucoup de ces services démarrent sur des ports sélectionnés de manière « aléatoire ». De plus, NFSv2 et NFSv3 prennent en charge le transport UDP, qui exige aussi que certains ports précis soient ouverts. Dans un souci de simplicité de configuration, nous allons nous concentrer ici sur NFSv4.



Note

Le service **`rpcbind`** remplace **`portmap`** de Red Hat Enterprise Linux 5.

Démonstration NFSv4

- Créez un utilisateur sur deux machines avec un UID commun.
- Créez un répertoire à partager avec NFS et définissez les autorisations adéquates.
- Modifiez **`/etc/exports`**. Par exemple :

```
/exports/read   192.168.0.0/24(ro,sync)
/exports/write  192.168.0.0/24(rw,sync) 127.0.0.1(rw,sync)
```

- Configurez le service **`nfs`**.

```
[root@serverX]# service nfs start
[root@serverX]# chkconfig nfs on
```

- Montez le partage de pseudo-racine NFS à partir d'un client :

```
[root@serverX]# mount -t nfs demo.example.com:/ /mnt
```



Références

Red Hat Enterprise Linux Storage Administration Guide

- Unité 10 : Network File System (NFS)

exports(5), **exportfs**(8) (pages du manuel)

Liens vers les Spécifications et ressources NFSv4

http://www.citi.umich.edu/projects/nfsv4/



Exercice de Questionnaire

Questionnaire sur les concepts de NFS

1. Dans quelles circonstances est-il conseillé d'utiliser NFSv2 ou NFSv3 ?

_____

2. Quelle est la syntaxe du fichier /etc/exports ?

_____

3. Quelles sont les étapes de publication d'un nouvel export sur un serveur NFSv4 existant ?

_____

_____

4. Quelle option demande au système NFS d'autoriser le super utilisateur des systèmes clients à avoir aussi les privilèges de super utilisateur sur le partage ?

_____

Utilisation de NFS

Avec NFSv4, vous pouvez monter l'export pseudo-racine du serveur NFS pour afficher les systèmes de fichiers dont l'exportation est en cours. Si le serveur prend en charge les versions NFSv3 et antérieures, utilisez **showmount -e *nfsserver*** pour parler à **rpc.mountd** et déterminer quels exports sont disponibles pour quelles machines.

Le type de système de fichiers **nfs** est utilisé lors du montage d'exports NFS sur un client. Dans Red Hat Enterprise Linux 6, le premier type essayé est NFSv4 s'il est pris en charge, puis NFSv3, et enfin NFSv2. Pour déterminer la version du système NFS utilisé sur un système de fichiers NFS monté, exécutez **mount** sans option ou argument et cherchez la valeur de l'option **vers=** dans la ligne du système de fichiers de la sortie.

Pour monter un système de fichiers NFS sur un client :

- Créez un répertoire vide pour le point de montage s'il n'existe pas encore.
- Pour un montage temporaire : **mount -t nfs *nfsserver*:*/export/mount-point***
- Pour un montage immédiatement au démarrage, ajoutez une ligne appropriée à **/etc/fstab** :

```
nfsserver:/exports    /mount-point    nfs    defaults    0 0
```



Note

Les entrées NFS dans **/etc/fstab** sont montées par le script de service **netfs** après le démarrage du réseau. Le montage des exports NFS à la demande est plus robuste avec l'automonteur qu'en utilisant les entrées de **/etc/fstab** pour éviter des problèmes possibles au démarrage du client quand le serveur NFS est hors ligne ou que le réseau n'est pas disponible.

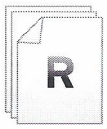
Options de montage NFS côté client

- `rw` : monte le système de fichiers en lecture-écriture.
- `ro` : monte le système de fichiers en lecture seule.
- `vers=4` : tente de monter le système uniquement avec la version NFS spécifiée. Si la version n'est pas prise en charge par le serveur, la demande de montage échoue.
- `soft` : en cas de temporisation de la demande NFS, renvoie une erreur après trois nouvelles tentatives. Arbitrage entre les problématiques d'intégrité des données et une meilleure réactivité du client en faveur de cette dernière. (Le comportement par défaut est **hard**, soit un nombre de tentative illimité).



Important

L'option de montage **intr** ne peut plus être utilisée dans Red Hat Enterprise Linux 6 (noyau Linux 2.6.25 et ultérieur). Seule **SIGKILL** (**kill -9**) peut interrompre une opération NFS en attente NFS sur les noyaux les plus récents.



Références

Red Hat Enterprise Linux Storage Administration Guide

- Section 10.2 : Configuration de client NFS

nfs(5) (page de manuel)



Test

Test de critère

Étude de cas

Partage de fichiers avec NFS

Avant de commencer...

Assurez-vous d'exécuter **`lab-setup-strickland`** à partir de votre système desktopX, qui prépare votre système serverX pour l'exercice pratique.

Strickland Pro Play est un magasin spécialisé en équipement et accessoires de loisir haut de gamme. Le nouveau logiciel de vente exige un serveur de fichiers avec deux partages montés sur chacune des stations de vente dans le magasin.

Pour le serveur de fichiers, déployez un service NFSv4 sur desktopX. Créez et partagez deux exports sur desktopX :

- Le premier export est pour la prise des commandes actuelles. Sur desktopX, exportez **`/share/current`** et rendez-le accessible en écriture. Sur le client, le super utilisateur doit pouvoir écrire vers **`/share/current`** après le montage. Le deuxième export sert à l'archivage des commandes.
- Le deuxième export sert à l'archivage des anciennes commandes. Toujours sur desktopX, exportez le chemin d'accès **`/share/archives`** et rendez-le accessible en lecture seule.
- Configurez les deux exports de manière qu'ils soient uniquement accessibles au réseau de la classe.

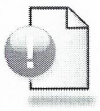
Configurez serverX pour monter **`desktopX:/share/current`** en tant que **`/sales/current`** et **`desktopX:/share/archives`** en tant que **`/sales/archives`**. Les montages doivent être disponibles après le redémarrage de serverX.

Lorsque vous êtes prêt, exécutez le script **`lab-grade-strickland`** sur le serverX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Concepts et configuration NFS

Dans cette section, vous avez appris à :

- Connaître les différences entre NFSv4 et les versions plus anciennes de NFS
- Configurer un serveur NFS

Utilisation de NFS

Dans cette section, vous avez appris à :

- Exporter des répertoires de plusieurs partitions avec NFSv4
- Monter des systèmes de fichiers NFS automatiquement au démarrage
- Déterminer les options de montage appropriées pour l'accès en lecture seule et en lecture-écriture lors du montage de systèmes de fichiers NFS au démarrage



MODULE DIX-SEPT

PARTAGE DE FICHIERS AVEC CIFS

Introduction

Sujets couverts dans cette unité :

- Notions fondamentales de la configuration de CIFS
- Clients CIFS
- Partages CIFS collaboratifs

Accès aux partages CIFS

Le protocole CIFS (Common Internet File System), aussi appelé SMB (Server Message Block), est le système de partage d'impression et de fichiers classique des serveurs et des clients Microsoft Windows. Red Hat Enterprise Linux peut agir aussi bien comme un client qu'un serveur pour les partages d'impression et de fichiers CIFS.

Dans cette section, nous allons examiner quatre méthodes de base pour connecter à un partage de fichiers CIFS :

1. Accès graphique à un partage CIFS

   Cette technique utilise Nautilus pour définir l'icône du partage qui permet ensuite d'accéder à son contenu par glisser-déplacer.

   Allez sur **Sites** → **Connexion au serveur**. Remplissez les champs ci-dessous (remplacez X par le numéro de votre station et laissez les autres champs vierges) :

```
Service type: Windows share
Server: serverX
Share: winuserX
User Name: winuserX
Domain Name: CLASSX
```

2. Accès de type ftp avec ligne de commande à un partage CIFS : **smbclient**

```
[root@serverX ~]# smbclient -L instructor.example.com
Enter root's password:  Enter
Anonymous login successful
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.5.4-68.el6]

        Sharename       Type      Comment
        ---------       ----      -------
        ftp             Disk      Instructor Public FTP
...
[root@serverX ~]# smbclient -L serverX -U winuserX
Enter winuserX's password: winpass
        Sharename       Type      Comment
        ---------       ----      -------
        winuser         Disk      Home Directories
...
[root@serverX ~]# smbclient //server1/homes -U winuserX
Enter winuserX's password: winpass
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.5.4-68.el6]
smb: \> ls
  .bash_profile                       H      176  Tue Jun 22 11:49:51 2010
```

3. Montage manuel d'un partage CIFS

   Cette technique traite le partage de fichiers CIFS comme un système de gestion de fichiers en réseau standard depuis une perspective Linux, exactement comme NFS.

```
mount -t cifs -o user=username //server/share /mntpoint
```

Exemple :

```
[root@serverX ~]# mount -t cifs -o user=winuserX //serverX/winuserX /mnt/
```

4. Montage durable d'un partage CIFS

   C'est une variante de l'exemple précédent qui monte automatiquement le partage de fichiers CIFS au démarrage. Notez qu'un fichier d'identification sert à fournir les nom d'utilisateur et mot de passe du partage.

   Ajoutez la ligne suivante dans **/etc/fstab**:

   ```
   //server/share /mntpoint cifs credentials=/etc/filename 0 0
   ```

   Exemple :

   /etc/fstab:

   ```
   //serverX/homes /mnt/serverX-share cifs credentials=/root/credentials 0 0
   ```

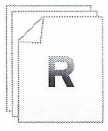
   /root/credentials:

   ```
   user=bob
   pass=password
   ```



Important

Le format UNC (Uniform Naming Convention) standard de Microsoft Windows de représentation d'une ressource réseau est ***ServerName**Share***. Toutefois, comme \ est un caractère d'échappement et non un séparateur de chemin d'accès dans les shells Linux standard comme **bash**, le caractère / est généralement utilisé en remplacement de \ pour écrire un UNC dans des systèmes Linux.



Références

mount.cifs(8) (page de manuel)



Exercice de Questionnaire

Questionnaire sur l'accès aux partages CIFS

1. Quelle ligne de commande donne un accès de type ftp à un partage CIFS nommé « common » sur un serveur appelé « nas2010 », en vous connectant en tant que l'utilisateur « winston » ?

_____

2. Qu'est-ce qui ne va pas avec la ligne suivante dans /etc/fstab ?

```
\\server\share /mnt/point cifs
user=ralph,pass=password 0 0
```

_____

3. Comment stocker les informations de connexion dans un fichier distinct pour les conserver en dehors de **`/etc/fstab`** ?

_____

4. Lors du montage d'un partage CIFS Windows, quelle option vous permet d'indiquer que tous les fichiers montés sont de propriété Linux ?

_____

Répertoires personnels fournis comme partages CIFS

Le service Samba peut servir à partager des systèmes de fichiers sous Linux comme partages de fichiers en réseau CIFS/SMB et des imprimantes sous Linux comme partages d'impression CIFS/SMB. Dans cette section, nous allons examiner la configuration de base d'un serveur Samba et plus particulièrement comment partager les répertoires personnels des utilisateurs à l'aide de Samba.

Packages CIFS

- **samba-common** - fichiers de prise en charge de Samba
- **samba-client** - applications clientes
- **samba** - applications serveur
- **samba-doc** - documentation (dans le canal RHN « Optional »)

Parties du service Samba

- Packages : *samba-common*, *samba-client*, *samba*, *samba-doc*
- Nom du script de service : **smb**
- Fichier de configuration principal : **/etc/samba/smb.conf**

Le fichier /etc/samba/smb.conf

Section /etc/samba/smb.conf: [global]

- `workgroup`

  workgroup sert à spécifier le groupe de travail ou le nom de domaine Windows du réseau.

- `hosts allow`

  hosts allow est un ensemble d'hôtes, séparés par des virgules, des espaces ou des tabulations, et qui ont l'autorisation d'accéder à un service. S'il est spécifié dans la section **[global]**, il s'applique à tous les services quelles que soient les paramètres spécifiés pour chaque service individuellement.

  Vous pouvez spécifier les hôtes par nom ou numéro IP. Par exemple, vous pouvez restreindre l'accès aux seuls hôtes d'un sous-réseau de classe C par exemple avec **allow hosts = 150.203.5.** (en utilisant la notation *point final*). Vous trouverez la syntaxe complète de la liste à la page du manuel **hosts_access(5)**.

- `security`

  Cette option affecte la façon de répondre à Samba des clients. C'est l'un des paramètres les plus importants du fichier **smb.conf**.

Si vos PC utilisent des noms d'utilisateurs identiques à ceux de la machine UNIX, vous privilégierez alors **security = user**. Si la plupart des noms d'utilisateurs que vous utilisez n'existent pas sur la machine UNIX, alors utilisez **security = share**.

Avec **security = share**, les clients n'ont pas besoin de se connecter au serveur avec un couple valide de nom d'utilisateur et de mot de passe avant de se connecter à une ressource partagée. À la place, les clients envoient les informations d'authentification pour chaque partage au moment où ils tentent de se connecter à ce partage.

Pour **security = user**, le client doit se connecter avec un couple valide de nom d'utilisateur et de mot de passe avant de recevoir les informations de partage ou de définir les paramètres comme **guest only**.

security = domain fonctionnera correctement uniquement si la machine a été ajoutée au domaine NT. Le paramètre attendu pour **encrypted passwords** est **yes**. Dans ce mode, Samba tente de valider le couple nom d'utilisateur/mot de passe en le transmettant au contrôleur de domaine principal ou de sauvegarde de Windows NT, exactement comme le ferait un serveur Windows NT. Notez qu'un utilisateur UNIX valide doit exister ainsi que le compte sur le contrôleur de domaine pour que Samba puisse avoir un compte UNIX valide vers lequel mapper l'accès au fichier. Vous devez définir le paramètre **password server** pour indiquer à Samba le serveur de validation des mots de passe.

Avec **security = server**, Samba tente de valider le coupler nom d'utilisateur/mot de passe en le transmettant à un autre server SMB. Vous devez définir le paramètre **password server** pour indiquer à Samba le serveur de validation des mots de passe.

Avec **security = ads**, Samba agit comme un membre du domaine dans le domaine ADS. Dans ce mode, Kerberos doit être installé et configuré sur la machine qui exécute Samba et Samba doit être rattaché au domaine ADS avec l'utilitaire **net**. Reportez-vous au chapitre sur **Domain Membership** dans la partie HOWTO pour toute information complémentaire (dans le package **samba-doc**). En plus de la commande **net**, la commande **netdomjoin-gui** fournie par le package **samba-domainjoin-gui** dans le Référentiel facultatif sert à rattacher une machine à ADS.

/etc/samba/smb.conf: Autres sections

- **[homes]**

  Ce partage, activé par défaut, est un partage spécial qui rend les répertoires personnels de l'utilisateur disponibles par CIFS. Il comprend **browseable = no** et n'est donc pas affiché comme partage disponible tant que l'utilisateur n'est pas authentifié. Le nom de partage peut soit spécifié comme **homes** (et dans ce cas, le serveur Samba le convertit en chemin d'accès du répertoire personnel de l'utilisateur), soit comme ***username*** .

- **[printers]**

  Également disponible par défaut, cette option partage les imprimantes actuellement disponibles.

- **[*share*]**

Si vous voulez créer d'autres partages, placez le nom de partage entre des crochets carrés comme indiqué ci-dessus. Ce partage exige au moins un paramètre **path**. Vous trouverez plusieurs exemples dans le fichier **smb.conf**.

Exemple a minima du fichier **/etc/samba/smb.conf**:

```
[global]
        workgroup = MYGROUP
        server string = Samba Server version %v
        log file = /var/log/samba/log.%m
        max log size = 50

        security = user
        passdb backend = tdbsam

        load printers = yes
        cups options = raw

[homes]
        comment = Home Directories
        browsable = no
        writable = yes

[printers]
        comment = All Printers
        path = /var/spool/samba
        browsable = no
        guest ok = no
        writable = no
        printable = yes
```

Autre configuration

Utilisateurs Samba uniquement

- **useradd**

  security = user nécessite des informations sur le compte UNIX et Samba. Vous pouvez soit ajouter un utilisateur (de préférence avec le même nom que le compte Samba), soit saisir une entrée dans **/etc/samba/smbusers** (qui contient quelques exemples). Si vous créez un utilisateur Samba uniquement, définissez le mot de passe UNIX sur **/sbin/nologin**.

```
[root@serverX ~]# useradd -s /sbin/nologin winuser
```

- **smbpasswd**

  Si vous n'avez pas de serveur de mots de passe Samba, vous devez créer des données d'authentification sur la machine locale. Utilisez **smbpasswd** pour créer les comptes et mots de passe Samba.

  Si **smbpasswd** reçoit un nom d'utilisateur sans aucune option, il tentera de *modifier* le mot de passe du compte. L'envoi de l'option **-a** ajoute le compte et définit le mot de passe.

```
[root@serverX ~]# smbpasswd -a winuser
New SMB password:  winpass
Retype new SMB password:  winpass
```

```
...
Added user winuser.
```

Sécurisation Samba

- Booléens SELinux `samba_enable_home_dirs` et `use_samba_home_dirs`

  Le booléen **`samba_enable_home_dirs`** permet l'exportation de répertoires personnels Linux locaux comme partages de fichiers CIFS vers d'autres systèmes. D'un autre côté, le booléen **`use_samba_home_dirs`** permet de monter des partages de fichiers distants et de les utiliser comme des répertoires personnels Linux locaux. Il arrive souvent de confondre ces deux options. Voir la page de manuel **`samba_selinux`**(8) pour obtenir de plus amples informations.

```
[root@serverX ~]# setsebool -P samba_enable_home_dirs on
```

- Ports de service

  Samba utilise normalement TCP/445 pour toutes les connexions et les ports UDP/137, UDP/138 et TCP/139 pour la compatibilité ascendante.



Références

`smb.conf`(5), **`smbd`**(8) et **`samba_selinux`**(8) (pages du manuel)

`samba-doc` Package RPM (dans le Référentiel facultatif, **`/usr/share/doc/samba-doc-*/`**)



Exercice de Liste de contrôle des performances

Exercice de configuration des répertoires personnels Samba

Modifiez la configuration et les éléments de sécurité Samba par défaut pour prendre en charge l'accès aux répertoires personnels des utilisateurs.

- ☐ Connectez-vous au serverX et étendez les privilèges au niveau super utilisateur.
- ☐ Installez le ou les packages nécessaires à un serveur Samba.
- ☐ Lancez et activez le service Samba.
- ☐ Configurez le système pour être dans le groupe de travail CLASSX (où X représente votre numéro de station) avec les définitions d'utilisateurs locaux.
- ☐ Ajoutez un utilisateur Samba uniquement nommé **`winuserX`** (où X représente votre numéro de station) avec pour mot de passe Samba **`winpass`**.
- ☐ Activez l'accès répertoires personnels des utilisateurs dans SELinux.
- ☐ Activez le pare-feu et ouvrez les ports nécessaires pour autoriser l'accès.
- ☐ Testez la configuration en accédant au répertoire personnel de l'utilisateur Samba uniquement à partir de desktopX.

Configuration des partages CIFS d'impression et de groupe

Configuration d'un partage de groupe en trois étapes :

La première étape est la création d'un répertoire collaboratif dans Linux comme suit :

```
[root@serverX ~]# mkdir -p /shared/dir
[root@serverX ~]# groupadd -r groupname
[root@serverX ~]# chgrp groupname /shared/dir
[root@serverX ~]# chmod 755 /shared
[root@serverX ~]# chmod 2770 /shared/dir
```

Définissons ensuite le contexte SELinux correct sur ce répertoire. Ces étapes sont nécessaires pour établir le partage durablement (en cas de ré-étiquetage).

```
[root@serverX ~]# semanage fcontext -a -t public_content_t '/shared(/.*)?'
[root@serverX ~]# semanage fcontext -a -t samba_share_t '/shared/dir(/.*)?'
[root@serverX ~]# restorecon -FRvv /shared
```



Note

/shared dans l'exemple ci-dessus est un répertoire de haut niveau partageable via CIFS, NFS, FTP, etc. **public_content_t** permet à chaque service d'accéder au répertoire de haut niveau. Le sous-répertoire **/shared/dir** est alors affecté du type **samba_share_t** auquel seul CIFS peut accéder.

Pour partager ce répertoire via Samba, ajoutez ce qui suit à la fin du fichier **/etc/samba/smb.conf** et redémarrez le service **smb**.

```
[dir]
  path = /shared/dir
  valid users = @groupname
  writeable = yes
  public = no
```

Le partage précédent autorise uniquement les utilisateurs du groupe **groupname** à accéder au partage. Si vous voulez autoriser les autres à accéder au partage en lecture seule, modifiez les permissions Linux du répertoire :

```
[root@serverX ~]# chmod 2775 /shared/dir
```

...et modifiez le partage dans **/etc/samba/smb.conf** comme suit :

```
[dir]
  path = /shared/dir
  writeable = no
  write list = @groupname
```

```
  public = no
```

Partage d'imprimante individuelle en deux étapes :

Pour éviter le partage automatique de toutes les imprimantes définies localement par Samba, supprimez ou commentez le partage **printers** dans **/etc/samba/smb.conf** :

```
#[printers]
#        comment = All Printers
#        path = /var/spool/samba
#        browseable = no
#        guest ok = no
#        writable = no
#        printable = yes
```

Vous pouvez également modifier **load printers** de **yes** en **no** (comme la valeur par défaut est **yes**, se contenter de commenter cette ligne ne suffit pas).

Pour partager une imprimante particulière, ajoutez ce qui suit à **/etc/samba/smb.conf** et redémarrez le service :

```
[myprinter]
  comment = My Printer Description
  path = /var/spool/samba
  read only = yes
  printable = yes
  printer name = cups_printer_name
```

Limiter l'accès du système client :

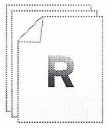
Pour limiter les systèmes clients qui peuvent accéder à un partage donné selon leur adresse IP, ajoutez une ligne comme celle-ci à la section de partage dans **/etc/samba/smb.conf** :

```
hosts allow = 192.168.0.1 10.2.12.
```



Note

iptables est une fonction qui n'appartient pas à Samba et qui permet de limiter selon leur adresse IP les systèmes clients ayant accès à un partage CIFS quel qu'il soit.



Références

Red Hat Enterprise Linux Deployment Guide

- Section 15.5.1 : Répertoires de groupe



Test

Test de critère

Étude de cas

Partage de fichiers avec CIFS

Avant de commencer...

Assurez-vous d'exécuter **lab-setup-samba** à partir de votre système desktopX, qui prépare votre système serverX pour l'exercice.

L'école School of Butler and Hacker a récemment déployé plusieurs serveurs CIFS pour permettre à leurs systèmes clients Windows d'accéder à des partages de fichiers.

La garde « Color Guard », constituée des verts « Green » et des rouges « Red », déploie un nouveau serveur et a besoin de partager des informations via CIFS. Ce partage doit être accessible en écriture par les membres de la garde mais toute autre personne peut y accéder uniquement en lecture seule.

Activez le pare-feu et laissez tous les clients sur le réseau local accéder au serveur CIFS.

Configurez votre serverX de manière qu'il fonctionne comme un serveur CIFS avec les informations suivantes :

- Groupe de travail : BUTLER
- Groupe Linux : greenred
- Nom de partage CIFS : school
- Répertoire : /shared/school
- Aucune imprimante en partage

Test de la configuration :

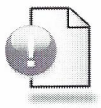
- Créez un utilisateur en tant que membre de **greenred** et assurez-vous qu'il a accès en écriture au partage CIFS **school**.
- instructor.example.com fournit plusieurs imprimantes que CUPS devrait automatiquement activer. Avant de satisfaire le critère des imprimantes, vérifiez que celles-ci sont disponibles, normalement sous le nom de « printerX ». Configurez Samba de manière qu'aucune imprimante ne soit partagée et vérifiez avec **smbclient** que l'utilisateur ne voit pas leur liste.
- Créez un deuxième utilisateur qui n'est pas membre de **greenred** et assurez-vous qu'il a accès au partage CIFS **school** uniquement en lecture seule.

Lorsque vous êtes prêt, exécutez le script **lab-grade-samba** sur le serverX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Accès aux partages CIFS

Dans cette section, vous avez appris à :

- Accès aux partages d'impression et de fichiers basés sur CIFS

Répertoires personnels fournis comme partages CIFS

Dans cette section, vous avez appris à :

- Configurez un serveur de répertoires personnels basé sur CIFS
- Ajoutez des utilisateurs Samba uniquement dans le système

Configuration des partages CIFS d'impression et de groupe

Dans cette section, vous avez appris à :

- Créez et configurez un partage CIFS utilisable pour la collaboration entre les groupes



MODULE DIX-HUIT

PARTAGE DE FICHIER AVEC FTP

Introduction

Sujets couverts dans cette unité :

- Implémentez en toute sécurité le partage de fichier anonyme avec FTP, à l'aide d'une « zone de dépôt » pour le téléchargement

Zone de dépôt FTP de téléchargement anonyme

FTP, le protocole de transfert de fichiers, constitue l'un des protocoles réseau les plus anciens toujours utilisés sur Internet. De nombreuses organisations utilisent toujours FTP pour les transferts de fichiers de base qui ne nécessitent pas une sécurité élevée.

La définition d'un serveur FTP qui autorise le téléchargement de contenu par des utilisateurs anonymes peut se révéler utile. Cependant, il est important de configurer le serveur de manière à *ne pas* autoriser le téléchargement de contenu depuis le répertoire de téléchargement par des utilisateurs anonymes. Si l'utilisateur FTP anonyme peut télécharger du contenu téléchargé par d'autres utilisateurs FTP anonymes depuis le site FTP, votre site FTP peut être utilisé par certaines personnes comme moyen de transfert de contenu illégal ou inapproprié à votre insu. Il convient de vous assurer que tout contenu proposé par votre site a été approuvé par un administrateur autorisé.

Dans cette section, nous allons étudier comment configurer un répertoire de téléchargement FTP afin qu'un utilisateur anonyme ne puisse télécharger son contenu, ni même le répertorier.

1. Créez un répertoire de téléchargement
   - Propriété du groupe : **ftp**
   - Autorisations : le groupe **ftp** dispose d'un accès en écriture et en exécution, mais pas en lecture ; l'« autre » ne dispose d'aucun accès
2. Modifiez SELinux pour un téléchargement anonyme
   - Contexte de type fichier/répertoire : **public_content_rw_t**
   - Booléen : **allow_ftp_anon_write** doit être activé
3. Modifiez **/etc/vsftpd/vsftpd.conf**
   - **anon_upload_enable = YES**
   - **chown_uploads = YES**
   - **chown_username = daemon**
   - **anon_umask = 077** (valeur par défaut)
4. Modifiez **iptables** pour prendre en charge les connexions FTP entrantes
   - Modification de **/etc/sysconfig/iptables_config** :

```
IPTABLES_MODULES="nf_conntrack_ftp nf_nat_ftp"
```

Ce module permet de garder les connexions avec les transfert sur le port 20 de ftp.

   - Ouvrez de nouvelles connexions sur le port TCP 21 et autorisez le trafic réseau ESTABLISHED et RELATED :

```
# iptables -A INPUT -p tcp --dport 21 -j ALLOW
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ALLOW
```



Références

Red Hat Enterprise Linux Security Guide
- Section 2.2.6 : sécurisation de FTP

Red Hat Enterprise Linux SELinux Guide
- Section 5.6 : Booléens

Red Hat Enterprise Linux Managing Confined Services
- Section 5.4.1 : Téléchargement sur un site FTP

Pages man **`ftpd_selinux`**(8) et **`vsftpd.conf`**(5)



Test

Test de critère

Étude de cas

Zone de dépôt FTP

Avant de commencer...

Assurez-vous d'exécuter **`lab-setup-dropbox`** à partir de votre système desktopX, qui prépare votre système serverX pour l'exercice.

L'entreprise Quiet Pleases, qui fabrique des cônes de silence et autres appareils antibruit, dispose d'un programme de collecte d'informations sur les niveaux sonores dans le monde. Des volontaires ont collecté des données concernant le bruit et ont besoin d'un moyen aisé pour transmettre leurs rapports.

L'entreprise a décidé d'utiliser un serveur FTP avec un répertoire de téléchargement anonyme pour récupérer les rapports.

Déployez vsftpd sur votre serverX et configurez un répertoire de téléchargement en lecture seule, accessible depuis: `ftp://serverX.example.com/dropbox`

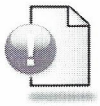
Comme ces volontaires sont disséminés dans le monde, le serveur FTP doit accepter les connexions depuis n'importe quel emplacement sur Internet.

Lorsque vous êtes prêt, exécutez le script **`lab-grade-dropbox`** sur desktopX pour vérifier votre travail.

Comment procéderiez-vous pour gérer l'étude de cas décrite ci-dessus ? Prenez des notes sur votre processus dans l'espace ci-dessous, puis procédez à la mise en œuvre.



Notes personnelles



Résumé du module

Zone de dépôt FTP de téléchargement anonyme

Dans cette section, vous avez appris à :

- Configurer le service de zone de dépôt FTP
- Gérer SELinux pour prendre en charge les téléchargements FTP
- Gérer le pare-feu pour prendre en charge les transferts FTP



MODULE DIX-NEUF

SERVICE CUPS

Introduction

Sujets couverts dans cette unité :

- Configuration des files d'attente d'impression sur une imprimante locale et une imprimante partagée avec un autre système
- Partage de l'une des files d'attente d'impression de votre système avec d'autres serveurs
- Définition de l'une des files d'attente d'impression comme file d'attente « par défaut »
- Activation ou désactivation d'une file d'attente pour qu'elle puisse recevoir des requêtes d'impression
- Envoi de tâches d'impression dans une file d'attente
- Liste des tâches en attente d'impression dans la file d'attente
- Suppression d'une tâche d'impression dans une file d'attente

Configurer des imprimantes

Le système d'impression de Red Hat Enterprise Linux est très flexible. Les imprimantes peuvent être installées en parallèle, en série ou en réseau. Les configurations d'impression prises en charge sont les CUPS IPP, lpd (sous-système d'impression commun Linux et Unix), les imprimantes Windows, Netware, et JetDirect distantes.

Une ou plusieurs files d'attente sont associées à chaque imprimante. Les tâches d'impression sont envoyées vers une file d'attente, pas vers une imprimante. Différentes files d'attente pour la même imprimante peuvent disposer d'options de priorité ou de sortie qui diffèrent. La configuration de files d'attente d'impression incombe à l'administrateur système ; les utilisateurs individuels ne créent pas de files d'attente d'impression.

Les impressions effectuées sur un système Red Hat Enterprise Linux sont gérées par le Common Unix Printing System, ou CUPS. La configuration CUPS par défaut prend en charge des milliers de modèles d'imprimantes, qui peuvent être reliés au système en local ou via le réseau. Les configurations d'imprimantes en réseau prises en charge incluent les autres serveurs CUPS, les serveurs d'impression Unix plus anciens, les imprimantes JetDirect et les imprimantes partagées sur les serveurs Microsoft Windows.

Un outil de configuration graphique est fourni pour simplifier l'ajout de nouvelles imprimantes à votre système. Pour exécuter cet outil, sélectionnez **Système → Administration → Impression** et suivez les instructions pour spécifier le nom de votre imprimante, le fabricant, le modèle et le type de connexion. Une fois l'imprimante ajoutée, elle peut être sélectionnée dans la liste des imprimantes à des fins de configuration. Cette interface peut également servir à imprimer des pages test et à paramétrer l'imprimante comme celle par défaut de votre système.

Configurer une démonstration d'imprimantes

- Créez une nouvelle imprimante « texte générique uniquement »
- Partagez la file d'attente d'impression.
- Créez une imprimante réseau qui correspond à une file d'attente d'impression de données brutes envoyée vers l'imprimante locale ci-dessus.
- Définissez une imprimante par défaut.
- Activez/désactivez l'imprimante.



Références

Pages man **cupsenable**(8), **cupsdisable**(8)

Exercice de Exercice de groupe

Gérer les files d'attente d'impression

1. Créez une file d'attente d'impression locale et partagez-la avec d'autres systèmes. Nommez la file d'attente d'impression **`local`** et faites-en une imprimante texte qui pointe vers le port série ou parallèle de votre système.



Note

Une imprimante texte seul n'accepte pas de fichiers PostScript, tels que ceux envoyés par la fonctionnalité **Test d'impression**. Ne vous inquiétez pas si la page de test ne s'imprime pas.

2. Créez une seconde file d'attente d'impression qui pointe vers la file d'attente d'impression locale d'un partenaire. Nommez la file d'attente d'impression **`remote`** et faites-en une file d'attente d'impression de données brutes qui transfère les tâches vers la file d'attente d'impression **`local`** de votre partenaire.

3. Une fois l'opération terminée, imprimez des fichiers texte sur **`local`** et **`remote`** pour vérifier.



Note

Si vous utilisez un port série, les tâches d'impression sont envoyées vers celui-ci presque immédiatement. Par conséquent, la vérification du fonctionnement correct de vos files d'attente d'impression peut se révéler difficile. Si tel est le cas, utilisez les fichiers avec « comptage » (par exemple, c00001, c00002, etc.) dans **`/var/spool/cups/`** pour vérifier. Un fichier numéroté est généré à chaque introduction d'une tâche d'impression dans la file d'attente.

Gérer les tâches d'impression

Un fichier envoyé vers une file d'attente d'impression est appelé une tâche. Les tâches peuvent être annulées lorsqu'elles se trouvent dans la file d'attente d'impression.

Gérer une démonstration de tâches d'impression

- *Désactivez la file d'impression* : dans l'interface graphique utilisateur, cliquez avec le bouton droit de la souris sur l'imprimante et désélectionnez la case à cocher **Activée**. À partir de l'interface de ligne de commande, exécutez **cupsdisable *PRINTER***, où *PRINTER* correspond au nom de l'imprimante.

- *Envoyez une tâche d'impression* : dans une application d'interface graphique utilisateur, utilisez **Ctrl**+**p** ou cliquez sur le bouton **Imprimer**. À partir de l'interface de ligne de commande, utilisez la commande **lpr** ou **lp**.

- *Affichez les tâches en attente* : dans l'interface utilisateur graphique, double-cliquez sur l'icône d'imprimante. À partir de l'interface de ligne de commande, utilisez la commande **lpq** ou **lpstat**.

- *Sélectionnez la tâche en attente et supprimez-la* : dans l'interface graphique utilisateur, ouvrez la file d'attente de l'imprimante, cliquez avec le bouton droit sur l'imprimante et choisissez **Annuler**. À partir de l'interface de commande, recherchez l'ID de travail dans la file d'attente et utilisez **lprm** ou **cancel** pour supprimer la tâche.

- *Activez la file d'impression* : dans l'interface graphique utilisateur, cliquez avec le bouton droit de la souris sur l'imprimante et sélectionnez la case à cocher **Activée**. À partir de l'interface de ligne de commande, exécutez **cupsenable *PRINTER***, où *PRINTER* correspond au nom de l'imprimante.



Références

Aide en ligne de CUPS : « Impression et options en ligne de commande »
http://localhost:631/help/options.html

Pages man **lpr**(1), **lpq**(1), **lprm**(1), **lp**(1), **lpstat**(1), **cancel**(1), **cupsenable**(8), **cupsdisable**(8)



Exercice de Liste de contrôle des performances

Gestion des tâches d'impression

- ☐ Désactivez la file d'attente par défaut de votre système.
- ☐ Ajoutez une tâche d'impression dans la file d'attente.
- ☐ Répertoriez les tâches d'impression de la file d'attente par défaut.
- ☐ Annulez la tâche d'impression que vous venez d'ajouter.
- ☐ Activez la file d'attente par défaut



Test

Test de critère

Exercice

Configurer et gérer une imprimante

Avant de commencer...

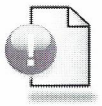
À partir de desktopX, exécutez **`lab-setup-cups`** pour réinitialiser votre serveur virtuel pour cet exercice.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Configurez une imprimante réseau de façon à envoyer des tâches d'impression vers une file d'attente IPP sur instructor.example.com appelée /printers/printer*X* où *X* est le numéro de votre poste de travail.
2. Votre file d'attente d'impression doit être nommée **`remote-test`** et être définie en tant que file d'attente d'impression par défaut.
3. Une fois que vous avez terminé, exécutez le script d'évaluation, **`lab-grade-cups`**.



Notes personnelles



Résumé du module

Configurer des imprimantes

Dans cette section, vous avez appris à :

- Configurer une imprimante
- Partager une imprimante

Gérer les tâches d'impression

Dans cette section, vous avez appris à :

- Gérer les tâches d'une file d'impression
- Activer et désactiver des files d'impression
- Annuler des tâches d'impression



MODULE VINGT

SERVICE SSH

Introduction

Sujets couverts dans cette unité :

- Utilisation de clés SSH pour l'authentification des connexions

Utilisation de clés SSH

Le protocole Secure Shell, **ssh**, vous permet de vous authentifier à l'aide d'un schéma de clé privée-publique. Autrement dit, vous devez générer deux clés, l'une appelée clé privée et l'autre clé publique. La clé privée doit, comme son nom l'indique, demeurer privée. La clé publique peut être fournie à n'importe qui. Un serveur ssh possédant votre clé publique peut poser une question à laquelle seul un système possédant votre clé privée peut répondre. Par conséquent, vous pouvez vous authentifier grâce à votre clé. Cela vous permet d'accéder à des systèmes d'une manière qui ne requiert aucune saisie de mot de passe à chaque connexion, mais qui demeure sûre.

La génération des clés s'effectue à l'aide de la commande **ssh-keygen**. Les clés peuvent être de type DSA ou RSA avec SSH version 2. La version 1 du protocole SSH est connue pour comporter un défaut de sécurité, par conséquent son utilisation n'est pas recommandée, sauf si vous devez vous connecter à d'anciens serveurs ssh.

Au cours de la génération des clés, vous avez la possibilité de spécifier une expession comme mot de passe, que vous devez fournir pour accéder à votre clé privée. De cette manière, même si cette clé est volée, il sera très difficile à une autre personne que vous de l'utiliser. Cela vous laisse le temps de générer une nouvelle paire de clés et de supprimer toutes les références aux anciennes avant que la clé privée puisse être utilisée par un pirate qui l'a décryptée.

Il est toujours judicieux de protéger par un mot de passe complexe votre clé privée, car elle vous permet d'accéder à d'autres machines. Cependant, cela signifie que vous devez taper l'expression de votre mot de passe dès qu'une clé est utilisée. Du coup, le processus d'authentification n'est plus sans mot de passe. Cela peut être évité en utilisant **ssh-agent**, auquel vous pouvez donner votre mot de passe une fois au début de votre session (à l'aide de **ssh-add**) afin qu'il le fournisse lorsque c'est nécessaire sans interrompre la connexion.

Une fois que vos clés SSH ont été générées, elles sont stockées par défaut dans le répertoire **.ssh/** de votre répertoire personnel. Les modes par défaut doivent correspondre à 600 sur votre clé privée et à 644 sur votre clé publique.

Avant de pouvoir utiliser l'authentification basée sur des clés, vous devez copier votre clé publique sur le système de destination. Pour ce faire, utilisez **ssh-copy-id**.

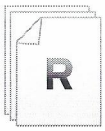
```
[student@desktopX ~]$ ssh-copy-id -i .ssh/id_rsa.pub root@desktopY
```

Lorsque vous copiez votre clé sur un autre système via **ssh-copy-id**, elle utilise le fichier **~/.ssh/id_rsa.pub** par défaut. Si vous utilisez une autre clé, ou si vous attribuez un nom différent à votre clé, vous devez le spécifier à l'aide de l'option **-i**, lors de l'utilisation de **ssh-copy-id**.

Démonstration pour les clés SSH

- Utilisez **ssh-keygen** pour créer une paire de clés publique-privée.
- Utilisez **ssh-copy-id** pour copier la clé publique à l'emplacement approprié sur un système distant. Par exemple :

```
[root@serverX]# ssh-copy-id root@serverY.example.com
```



Références

Red Hat Enterprise Linux Deployment Guide

- Section 9.2.4 : Utilisation d'une authentification basée sur des clés

Pages man **ssh-keygen**(1), **ssh-copy-id**(1), **ssh-agent**(1),**ssh-add**(1)



Exercice de Exercice

Utilisation de clés SSH

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Créez une paire de clés SSH en tant que **student** sur desktopX.
2. Installez la clé SSH publique pour le compte **student** sur serverX.
3. Connectez-vous à serverX à partir de desktopX à l'aide des clés SSH.



Test

Test de critère

Exercice

Sécurisation SSH

Avant de commencer...

Exécutez la commande **`lab-setup-server`** en tant que **`root`** (super utilisateur) sur votre système desktopX. Cela préparera votre système serverX pour l'exercice.

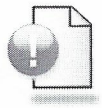
Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Copiez la clé publique SSH générée précédemment sur desktopX dans le compte **`student`** sur serverX.

2. Vérifiez que vous pouvez vous connecter par **`ssh`** à serverX en tant que **`student`** depuis desktopX à l'aide des clés SSH.



Notes personnelles



Résumé du module

Utilisation de clés SSH

Dans cette section, vous avez appris à :

- Créer et utiliser des clés SSH



MODULE VINGT-ET-UN

SERVICE VNC (VIRTUAL NETWORK COMPUTING)

Introduction

Sujets couverts dans cette unité :

- Configuration d'un bureau distant
- Connexion sécurisée à un serveur VNC

Configuration d'un serveur VNC

Bien que de nombreux centres de données auront recours par défaut à **ssh** pour l'administration à distance des systèmes Unix et Linux, certains utiliseront VNC (Virtual Network Computing) pour l'administration à distance des serveurs Windows. Red Hat Enterprise Linux 6 prend en charge l'implémentation d'un serveur VNC pouvant gérer un ou plusieurs bureaux graphiques distants.

Configurer un serveur VNC - Démonstration

1. Installez le package du serveur VNC

```
[root@demo ~]# yum install tigervnc-server
```

2. Modifiez **/etc/sysconfig/vncservers**:

```
VNCSERVERS="2:root"
VNCSERVERARGS[2]="-geometry 800x600 -nolisten tcp -localhost"
```

L'option **-localhost** empêche les clients VNC distants de se connecter sauf s'ils ont recours à un tunnel sécurisé, par exemple, s'ils utilisent **vncviewer** et son option **-via**:

```
vncviewer -via user@remotehost localhost:2
```

3. Définissez un mot de passe VNC.

```
[root@demo ~]# vncpasswd
Password: password
Verify: password
```

4. Lancez et activez le service:

```
[root@demo ~]# service vncserver start
[root@demo ~]# chkconfig vncserver on
```



Références

Red Hat Enterprise Linux Deployment Guide

- Section 18.1.23 - /etc/sysconfig/vncservers

Pages man **vncviewer**(1), **vncpasswd**(1)



Exercice de Exercice

Activation d'un serveur VNC

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Installez le package **tigervnc-server** sur serverX.
2. Configurez l'affichage VNC 1 pour student. Ajoutez ce qui suit à **/etc/sysconfig/vncservers**:

```
VNCSERVERS="1:student"
```

3. Définissez **redhat** comme mot de passe VNC pour student:

```
[student@serverX ~] vncpasswd
Password: redhat
Verify: redhat
```

4. Lancez et activez le service VNC.
5. Vous vérifierez la connexion dans la section suivante.

Sécuriser l'accès à un bureau GNOME distant

La commande **vncviewer** est un visionneur (client) utilisé pour établir une connexion à un serveur VNC exécuté sur un système distant.



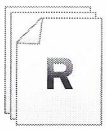
Avertissement

Utilisez l'option **-via** pour acheminer le trafic VNC sur un tunnel SSH à chaque fois que c'est possible. VNC est un protocole de transmission en texte clair, par conséquent vos mots de passe et vos sessions bureau seront exposés aux écoutes indiscrètes et aux interférences si vous n'utilisez pas une connexion sécurisée.

Se connecter à un serveur VCN de façon sécurisée - Démonstration

1. Connectez-vous à un serveur VNC avec SSH :

```
[root@instructor ~]# vncviewer -via visitor@demo localhost:1
```



Références

Page man **vncviewer**(1)



Exercice de Exercice

Se connecter à VCN de façon sécurisée

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Configurez le serveur VNC sur serverX pour autoriser uniquement les connexions locales. Modifiez **/etc/sysconfig/vncservers** et ajoutez ce qui suit :

```
VNCSERVERARGS[1]="-localhost"
```

2. Connectez-vous au serveur VNC sur serverX de manière sécurisée à partir de desktopX à l'aide d'un tunnel SSH :

```
[student@desktopX ~] vncviewer -via serverX localhost:1
```

3. Vérifiez que tout est correct.



Test

Test de critère

Exercice

Configurer plusieurs bureaux avec VNC

Avant de commencer...

Exécutez la commande **`lab-setup-server`** en tant que **`root`** (super utilisateur) sur votre système desktopX. Cela préparera votre système serverX pour l'exercice.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

1. Installez le package du serveur VNC sur serverX.
2. Configurez l'affichage 1 pour **`student`** et l'affichage 2 pour **`visitor`**.
3. Autorisez les connexions uniquement à partir de l'hôte local.
4. Définissez **`redhat`** comme mot de passe VNC pour **`student`** et **`visitor`**.
5. Lancez et activez le service VNC.
6. Vérifiez que tout est correct, puis contrôlez votre travail en utilisant une connexion sécurisée.

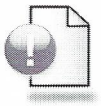


Note

Le paramètre après **`-via`** sert pour les connexions avec **`ssh`**. Il n'est pas nécessaire d'utiliser le nom d'utilisateur de la session VNC à laquelle vous vous connectez. N'importe quel nom d'utilisateur fonctionnera si vous connaissez le mot de passe.



Notes personnelles



Résumé du module

Configuration d'un serveur VNC

Dans cette section, vous avez appris à :

- Configurer un serveur VNC

Sécuriser l'accès à un bureau GNOME distant

Dans cette section, vous avez appris à :

- Établir une connexion sécurisée à un serveur VNC



MODULE VINGT-DEUX

EXAMEN EXHAUSTIF



Test

Test d'examen exhaustif

Exercice

Examen exhaustif

Avant de commencer...

Exécutez la commande **`lab-setup-server`** en tant que **`root`** sur desktopX.

Effectuez attentivement les étapes suivantes. Adressez-vous à votre formateur si vous rencontrez un problème ou si vous avez des questions.

Configurez serverX afin qu'il réponde aux exigences suivantes. Pour tous les services, autorisez les connexions depuis le sous-réseau 192.168.0.0/24 local, mais n'autorisez pas les connexions depuis le sous-réseau 192.168.1.0/255.255.255.0.

1. Configurez SELinux avec le mode Enforcing.
2. Autorisez les connexions SSH depuis le sous-réseau local.
3. Configurez un serveur SMTP qui autorise les connexions depuis le sous-réseau local.
4. Connectez-vous au serveur LDAP, instructor.example.com, à l'aide du nom distinctif de **`dc=example,dc=com`** pour les informations de compte. Le serveur LDAP nécessite des connexions sécurisées à l'aide du certificat qui se trouve sur *ftp://instructor.example.com/pub/EXAMPLE-CA-CERT*. Le serveur LDAP fournit un compte nommé **`ldapuserX`**.

   Utilisez des mots de passe Kerberos avec un domaine **`EXAMPLE.COM`** pour l'authentification. Utilisez instructor.example.com pour définir les serveurs KDC et Admin. Les comptes possèdent le mot de passe **`kerberos`**.
5. Configurez un répertoire personnel monté automatiquement pour le compte **`ldapuserX`**. Le répertoire personnel est partagé via NFS depuis instructor.example.com.
6. Connectez-vous au **`rdisks.serverX`** cible iSCSI fourni par instructor.example.com.
7. Supprimez l'ensemble des partitions actuelles sur le disque iSCSI. Configurez une nouvelle partition physique de 30 Mo, à l'aide de la cible iSCSI avec un système de fichiers ext4 et une étiquette **`test`** montés sur **`/test/`**. Le répertoire **`/test/`** doit appartenir à l'utilisateur **`root`** et au groupe **`root`**. En outre, il doit disposer d'une autorisation de 755.
8. Configurez un nouveau volume logique de 1 Go nommé **`mylv`** dans le groupe de volumes **`vgsrv`**, avec un système de fichiers ext4 monté sur **`/mylv/`**.
9. Configurez NFS pour partager le répertoire **`/test/`**. Mettez-le en lecture seule sur le sous-réseau local. Autorisez **`root`** à disposer de privilèges de super utilisateur (root) lors de l'accès au partage NFS.
10. Créez un compte utilisateur appelé **`matt`** à l'aide du mot de passe **`matt`**.
11. Créez un compte utilisateur appelé **`cindy`** à l'aide du mot de passe **`cindy`**.

12. Créez un groupe nommé **admins** incluant **matt** et **cindy**.

13. Configurez Samba pour partager le répertoire **/test/** à l'aide du nom de partage **test**. Faites en sorte qu'il soit accessible en lecture pour **cindy** (utilisez le mot de passe Samba **password**) et accessible en écriture pour **matt** (utilisez le mot de passe Samba **password**). Assurez-vous que les autorisations Linux permettent la lecture/écriture tel que cela est répertorié ici, et qu'elles respectent les conditions requises ci-dessus pour les utilisateurs, les groupes et les autorisations. .

14. Configurez un serveur Web sécurisé à l'aide du certificat et de la clé se trouvant sur *http://instructor/pub/materials/tls/certs/serverX.crt* et sur *http://instructor/pub/materials/tls/private/serverX.key*. Configurez le serveur Web afin qu'il utilise **/mylv/index.html** comme page Web par défaut. Configurez le fichier **index.html** afin que l'accès au site Web sécurisé présente ce qui suit :

```
Hello World!
```

15. Autorisez **cindy** et **matt** à écrire le fichier **/mylv/index.html**.



Notes personnelles

Annexe A. Solutions

Gestion des logiciels



Exercice de Questionnaire

Enregistrement Red Hat Network

1. L'élément de menu qui lance l'enregistrement auprès de Red Hat Network est **Système → Administration → Enregistrement RHN**
2. Le premier choix d'enregistrement détermine si un système est enregistré avec RHN hébergé ou Satellite RHN.
3. Un serveur de proxy Web supplémentaire peut être requis en option et des informations d'authentification peuvent être demandées
4. Un nom d'utilisateur RHN ou un compte RHN ainsi que le mot de passe correspondant doivent être fournis pour un enregistrement Red Hat Network correct.
5. Les dernières questions auxquelles vous devez répondre lors du processus d'enregistrement sont le nom du système et s'il faut télécharger les informations de profil relatives au matériel et aux logiciels ou packages.



Exercice de Exercice

Utilisation de référentiels YUM

Vous allez configurer votre serveur pour utiliser un référentiel YUM distinct afin d'obtenir des mises à jour et de mettre à jour votre machine.

1. Créer le fichier **/etc/yum.repos.d/errata.repo**, pour activer le référentiel « Mises à jour » qui se trouve sur la machine de l'instructeur. Il devrait accéder au contenu trouvé à l'adresse URL suivante : ftp://instructor.example.com/pub/rhel6/Errata

   Créez le fichier **/etc/yum.repos.d/updates.repo** avec le contenu suivant :

   ```
   [updates]
   name=Red Hat Updates
   baseurl=ftp://instructor.example.com/pub/rhel6/Errata
   enabled=1
   gpgcheck=1
   ```

2. Mettez à jour tous les logiciels appropriés fournis par le référentiel à l'aide de **yum update**.

   yum update



Exercice de Exercice

Recherche et installation de packages

Connectez-vous en tant que **root** sur le serverX et effectuez les tâches suivantes :

1. Essayez d'exécuter la commande **gnuplot**. Vous devez trouver qu'elle n'est pas installée.
2. Recherchez les packages de tracés.

   ```
   yum search plot
   ```

3. Recherchez des informations supplémentaires sur le package **gnuplot**.

   ```
   yum info gnuplot
   ```

4. Installez le paquetage de **gnuplot**.

   ```
   yum install gnuplot
   ```

5. Tentez de supprimer le package **gnuplot**, mais sélectionnez non.

   ```
   yum remove gnuplot
   ```

   Combien de packages seraient supprimés ? 1

6. Tentez de supprimer le package **gnuplot-common**, mais sélectionnez non.

   ```
   yum remove gnuplot-common
   ```

   Combien de packages seraient supprimés ? 2



Exercice de Exercice

Traitement de logiciels tiers

Dans cet exercice, vous allez collecter des informations sur un package tiers, en extraire des fichiers et l'installer en entier sur le système desktopX.

1. Téléchargez *wonderwidgets-1.0-4.x86_64.rpm* à partir de *http://instructor/pub/materials*.
2. Quels fichiers contient-il ?

   ```
   rpm -qlp wonderwidgets-1.0-4.x86_64.rpm
   ```

3. Quels scripts contient-t-il ?

   ```
   rpm -qp --scripts wonderwidgets-1.0-4.x86_64.rpm
   ```

4. Quelle quantité d'espace disque utilise-t-il une fois installé ?

   ```
   rpm -qip wonderwidgets-1.0-4.x86_64.rpm
   ```

5. Utilisez **yum localinstall** pour installer le package

```
yum localinstall wonderwidgets-1.0-4.x86_64.rpm
```



Exercice de Questionnaire

Fichier spec RPM

1. Le package **Version** est en général dérivé du projet open source tandis que le package **Release** est la version du créateur.
2. La directive **Group** indique la catégorie à laquelle appartient le type du package créé.
3. Le nom du tarball contenant les fichiers utilisés pour créer le package est spécifié avec la directive **Source**.
4. La directive **BuildArch** spécifie l'architecture cible pour laquelle le package est créé. **noarch** sera sa valeur lorsque le package peut être installé sur n'importe quelle architecture.
5. La directive **Summary** spécifie la description sur une ligne d'un package tandis que la section **%description** fournit une explication plus complète de l'objectif du package.
6. La section **%install** contient le code utilisé pour placer les fichiers dans la structure du répertoire chroot **$RPM_BUILD_ROOT**.
7. La section **%files** définit quels fichiers et répertoires devront être intégrés au RPM.
8. Les sections **%prep**, **%build** et **%clean** contiennent le code shell utilisé pour assembler un package et le nettoyer après sa création.



Exercice de Questionnaire

Créer un référentiel Yum -Questionnaire

1. Installez le package **createrepo** si nécessaire.
2. Créez un répertoire pouvant être partagé (via FTP ou HTTP).
3. Créez un sous-répertoire appelé Packages.
4. Copiez tous les packages RPM à publier dans Packages.
5. Exécutez createrepo sur le répertoire de premier niveau.



Test

Test de critère

Liste de contrôle des performances

Créer un RPM

- ☐ Téléchargez le fichier *ftp://instructor.example.com/pub/materials/hello.sh*.

```
[student@serverX ~]$ mkdir ~/hello-1.0
[student@serverX ~]$ cd ~/hello-1.0
[student@serverX hello-1.0]$ wget ftp://instructor.example.com/pub/materials/
hello.sh
```

- ☐ Créez un RPM simple qui installe **hello.sh** dans **/root/bin**. Veillez à ce que **hello.sh** soit installé avec le mode 755.

```
[student@serverX hello-1.0]$ cd
[student@serverX ~]$ mkdir -p ~/rpmbuild/SOURCES
[student@serverX ~]$ mkdir -p ~/rpmbuild/SPECS
[student@serverX ~]$ tar -cvzf ~/rpmbuild/SOURCES/hello-1.0-1.tar.gz hello-1.0
```

~/rpmbuild/SPECS/hello.spec doit ressembler à ceci:

```
Name:       hello
Version:    1.0
Release:    1
Summary:    Hello
Group:      RHCE
License:    GPL
URL:        http://www.redhat.com
Source0:    %{name}-%{version}-%{release}.tar.gz
BuildRoot:  /var/tmp/%{name}-buildroot

%description
Installs /root/bin/hello.sh

%prep
%setup -q -n %{name}-%{version}

%build

%install
rm -rf $RPM_BUILD_ROOT
mkdir -p $RPM_BUILD_ROOT/root/bin
install -m 755 hello.sh $RPM_BUILD_ROOT/root/bin/hello.sh

%clean
rm -rf $RPM_BUILD_ROOT

%files
%defattr(-,root,root,-)
/root/bin/hello.sh

%changelog
```

```
[student@serverX ~]$ su -
Password: redhat
[root@serverX ~]# yum install -y rpm-build
[root@serverX ~]# exit
[student@serverX ~]$ rpmbuild -ba ~/rpmbuild/SPECS/hello.spec
```

- ☐ Créez une clé GPG et signez le package avec la clé. Exportez la clé GPG publique.



Note

Vous devez avoir une session graphique ouverte pour générer une clé GPG. **gpg** utilise maintenant une application graphique pour entrer et valider la clé.

```
[student@serverX ~]$ gpg --gen-key
gpg (GnuPG) 2.0.14; Copyright (C) 2009 Free Software Foundation, Inc. This is free
 software: you are free to change and redistribute it. There is NO WARRANTY, to
 the extent permitted by law. Please select what kind of key you want: (1) RSA and
 RSA (default) (2) DSA and Elgamal (3) DSA (sign only) (4) RSA (sign only) Your
 selection?   Enter
RSA keys may be between 1024 and 4096 bits long. What keysize do you want?
 (2048)  Enter
Requested keysize is 2048 bits Please specify how long the key should be valid. 0
 = key does not expire <n> = key expires in n days <n>w = key expires in n weeks
 <n>m = key expires in n months <n>y = key expires in n years Key is valid for?
 (0)  Enter
Key does not expire at all Is this correct? (y/N) y
GnuPG needs to construct a user ID to identify your key. Real name: My Name
Email address: student@serverX.example.com
Comment:  Enter
You selected this USER-ID: "My Name <student@serverX.example.com>" Change (N)ame,
 (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key. Enter passphrase
 Passphrase: testing123
Please re-enter this passpassphrase. Passphrase: testing123
We need to generate a lot of random bytes. It is a good idea to perform some other
 action (type on the keyboard, move the mouse, utilize the disks) during the prime
 generation; this gives the random number generator a better chance to gain enough
 entropy.

gpg: /home/student/.gnupg/trustdb.gpg: trustdb created
gpg: key 54AF5285 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/54AF5285 2010-12-09
   Key fingerprint = 315F E90B 1745 2288 EBAE 4E7B 4BC6 4568 54AF 5285
uid    My Name <student@serverX.example.com>
sub    2048R/D08B2951 2010-12-09
```

Pour exporter la clé, recherchez l'ID de la clé dans les résultats ci-dessus. Il se trouve après **pub 2048R/** ci-dessus. Dans cet exemple, l'ID de la clé est **54AF5285**. Les exemples suivants montreront les commandes utilisant cet ID. L'ID de votre clé sera différent, aussi remplacez l'ID de clé de l'exemple par l'ID de votre clé.

```
[student@serverX ~]$ gpg -a -o ~/RPM-GPG-KEY-student --export 54AF5285
```

Créez le fichier **~/.rpmmacros** et ajoutez le contenu suivant :

```
%_gpg_name 54AF5285
```

Signez le package RPM

```
[student@serverX ~]$ rpm --resign ~/rpmbuild/RPMS/x86_64/hello-1.0-1.x86_64.rpm
Enter pass phrase: testing123
Pass phrase is good. /home/instructor/rpmbuild/RPMS/x86_64/hello-1.0-1.x86_64.rpm:
```

- ☐ Déployez un serveur Web et créez un référentiel yum dans **/var/www/html/Packages/**. Créez un fichier de référentiel qui référence *http://serverX/Packages*. Servez la clé GPG à partir du serveur Web et incluez-la dans le fichier de référentiel.

```
[root@serverX ~]# mkdir /var/www/html/Packages
[root@serverX ~]# cp ~student/rpmbuild/RPMS/x86_64/hello-1.0*.rpm /var/www/html/
Packages/
[root@serverX ~]# cp ~student/RPM-GPG-KEY-student /var/www/html/Packages/
[root@serverX ~]# createrepo -v /var/www/html/Packages/
[root@serverX ~]# service httpd start
```

Créez le fichier **/etc/yum.repos.d/hello.repo** avec le contenu suivant :

```
[hello]
name=hello
description=ServerX Yum Repo
baseurl=http://serverX.example.com/Packages
enabled=1
gpgcheck=1
gpgkey=http://serverX.example.com/Packages/RPM-GPG-KEY-student
```

- ☐ Installez votre rpm en utilisant le référentiel yum ci-dessus et exécutez **/root/bin/hello.sh**.

```
[root@serverX ~]# yum -y install hello
[root@serverX ~]# hello.sh
```

Gestion réseau



Exercice de Questionnaire

Configuration avancée de l'interface réseau - Questionnaire

1. Quel mode de liaison Linux Ethernet utilise principalement une interface esclave et change d'interface en cas d'échec ?

   (sélectionnez une des réponses suivantes...)

   a. Mode 0 (balance-rr)
   b. Mode 1 (active-backup)
   c. Mode 3 (broadcast)

2. Quelle liaison Linux Ethernet utilise toutes les interfaces à tour de rôle pour obtenir plus de capacité ?

   (sélectionnez une des réponses suivantes...)

   a. Mode 0 (balance-rr)
   b. Mode 1 (active-backup)
   c. Mode 3 (broadcast)

3. Lors de la création d'une interface réseau liée, quel fichier de configuration contient les définitions d'adresse IP et de masque de réseau pour l'interface ?

   (sélectionnez une des réponses suivantes...)

   a. **`/etc/sysconfig/network`**
   b. **`/etc/sysconfig/network-scripts/ifcfg-bond0`**
   c. **`/etc/sysconfig/network-scripts/ifcfg-`*`iface`***
   d. Aucune des propositions ci-dessus

4. Lors de la création d'une interface réseau liée, quel fichier de configuration définit le type de la liaison ?

   (sélectionnez une des réponses suivantes...)

   a. **`/etc/sysconfig/network`**
   b. **`/etc/sysconfig/network-scripts/ifcfg-bond0`**
   c. **`/etc/sysconfig/network-scripts/ifcfg-`*`iface`***
   d. Aucune des propositions ci-dessus

5. Lors de la création d'une interface réseau liée, quelles définitions de variable doivent être spécifiées dans le fichier de configuration **`/etc/sysconfig/network-scripts/ifcfg-`*`iface`*** ?

   (sélectionnez une des réponses suivantes...)

   a. **`GATEWAY`**
   b. **`IPADDR`**
   c. **`MASTER`**

d. Aucune des propositions ci-dessus



Test

Test de critère 1

Étude de cas

Routage du trafic réseau : OSHU (Operation Strategic Holistic Unusual)

Avant de commencer...

Exécutez le script **lab-setup-oshu** sur desktopX.

Operation Strategic Holistic Unusual (ou OSHU) est un système de discussion en ligne pour les fans d'énigmes à résoudre. Deux conditions sont requises pour rejoindre le site, elles sont indiquées ci-dessous.

1. Pour remplir la première condition, vous devez prouver que vous êtes capable de faire « disparaître » un serveur. Pour cela, vous devez modifier la configuration sur serverX pour qu'il ne réponde pas aux requêtes ping. Rendez cette modification permanente pour qu'elle soit toujours effective après chaque redémarrage.

2. La seconde condition est de rejoindre le réseau OSHU « secret ». Pour rejoindre le réseau, ajoutez une adresse IP supplémentaire à serverX, X correspondant au numéro de votre bureau/serveur :

   10.42.10.X/24

Lorsque vous remplissez les conditions, exécutez **lab-grade-oshu** sur desktopX pour vérifier votre travail.

1. Ajoutez ce qui suit à **/etc/sysctl.conf**

```
net.ipv4.icmp_echo_ignore_all = 1
```

2. Activez le paramètre

```
[root@serverX ~] sysctl -p
```

3. Configurez les paramètres réseau statiques

```
[root@serverX ~] service NetworkManager stop
[root@serverX ~] chkconfig NetworkManager off
```

4. Créez le fichier **/etc/sysconfig/network-scripts/ifcfg-eth0:0** et ajoutez le contenu suivant :

```
DEVICE=eth0:0
```

```
IPADDR=10.42.10.X
NETMASK=255.255.255.0
ONPARENT=yes
```

5. Activez les nouveaux paramètres réseau

```
[root@serverX ~] ifup eth0:0
```



Test

Test de critère 2

Exercice

Résolution des problèmes de configuration réseau à partir de la ligne de commande

Toutes les opérations suivantes doivent être effectuées sur votre serveur virtuel, serverX. Vous commencez par exécuter un script qui « casse » la configuration réseau. Vous avez cinq minutes pour résoudre chacun des deux problèmes. Veillez à documenter vos découvertes, car nous effectuerons une analyse à la fin de l'exercice.

Les paramètres réseau pour serverX sont indiqués ci-dessous :

```
IP Address: 192.168.0.X+100
Netmask:  255.255.255.0  (/24)
DNS Server: 192.168.0.254
Default Gateway: 192.168.0.254
```

1. Exécutez le premier script pour effectuer une mauvaise configuration de votre mise en réseau :

   `lab-break-net 1`

2. Symptôme : un navigateur Web ne peut pas accéder à la page Web de l'adresse `http://instructor.remote.test`

3. Appliquez les étapes : TESTER, VÉRIFIER, CORRIGER pour identifier et résoudre le problème.

4. Documentez vos découvertes

   Dans ce premier problème, le nom d'hôte instructor.remote.test n'était pas résolu en adresse IP. **`/etc/resolv.conf`** pointait vers le mauvais serveur DNS. Corrigez le problème en modifiant **`/etc/sysconfig/network-scripts/ifcfg-eth0`** pour obtenir **`DNS1=192.168.0.254`**

5. Exécutez le deuxième script pour effectuer une mauvaise configuration de votre mise en réseau

lab-break-net 2

6. Symptôme: un navigateur Web ne peut pas accéder à la page Web de l'adresse `http://instructor.remote.test`
7. Appliquez les étapes: TESTER, VÉRIFIER, CORRIGER pour identifier et résoudre le problème.
8. Documentez vos découvertes

Dans ce deuxième problème, l'hôte instructor.remote.test se trouve sur un réseau distinct et ne peut pas être atteint. **`ip route`** indiquait que la passerelle par défaut pointait vers le mauvais routeur. Corrigez le problème en modifiant **`/etc/sysconfig/network-scripts/ifcfg-eth0`** pour obtenir **`GATEWAY=192.168.0.254`**

Gestion du stockage



Exercice de Questionnaire

Ajouter un nouveau système de fichiers

1. Identifiez un disque qui comporte de l'espace libre fdisk -cul
2. Créez une nouvelle partition sur ce disque fdisk -cu /dev/***device***
3. Mettez à jour la table de partition du noyau reboot
4. Créez un système de fichiers sur la partition mkfs -t ext4 /dev/***device***
5. Ajoutez une entrée au fichier de la table du système de fichiers Ajoutez une entrée à /etc/fstab comme suit : UUID=cb79b7d0-dc14-4402-8465-6857346c9a53 /directory ext4 defaults 1 2
6. Créez un point de montage mkdir /***directory***
7. Montez le système de fichiers mount -a



Exercice de Exercice de reclassement

Création d'un système de fichiers chiffré

Pour chaque nom de fichier ou répertoire ci-dessous, écrivez le numéro de sa définition dans la liste du bas.

1 Créez une nouvelle partition
4 Créer un système de fichiers **ext4**
2 Formater la nouvelle partition pour le chiffrement
6 Monter le système de fichiers sur le périphérique déverrouillé
8 Créer une entrée dans **/etc/fstab**
5 Créer un répertoire à utiliser comme point de montage
3 Déverrouiller la partition chiffrée
7 Créer une entrée dans **/etc/crypttab**
9 Informer LUKS de la présence du fichier de mot de passe

1. 1. **fdisk**
2. 2. **cryptsetup luksFormat /dev/vda*N***
3. 3. **cryptsetup luksOpen /dev/vda*N* *secret***
4. 4. **mkfs -t ext4 /dev/mapper/*secret***
5. 5. **mkdir /secret**
6. 6. **mount /dev/mapper/*secret* /secret**
7. 7. ***secret* /dev/vda*N* */password/file***

8. 8. **/dev/mapper/*secret* /secret ext4 defaults 1 2**
9. 9. **cryptsetup luksAddKey /dev/vda*N* */password/file***



Exercice de Exercice

Créer et utiliser une nouvelle partition swap.

Créer et utiliser une nouvelle partition swap de 256 Mo sur votre serveur virtuel serverX.

1. Démarrez **fdisk** et créez une nouvelle partition



Important

Veillez à créer une partition étendue au préalable afin d'avoir de l'espace pour créer des partitions supplémentaires ultérieurement.

2. Changez le type de partition sur **swap**.

   Saisissez **t** pour modifier le type de partition sur « 0x82 Linux Swap ».

3. Préparez la nouvelle partition pour l'utilisation comme swap

   mkswap /dev/vda*N*

   (où *N* est le numéro de partition)

4. Déterminez l'UUID

   blkid /dev/vda*N*

5. Ajoutez la nouvelle partition à **/etc/fstab**

   UUID=*uuid* swap swap defaults 0 0

6. Déterminez la quantité actuelle de swap

   swapon -s

7. Activez le nouveau swap

   swapon -a

8. Vérifiez le nouveau swap activé

   swapon -s



Test

Test de critère

Exercice

Partitions et systèmes de fichiers - Exercice

Avant de commencer...

Réinitialisez serverX en exécutant **`lab-setup-server`** depuis desktopX.

1. Sur serverX, connectez-vous à la cible iSCSI **`iqn.2010-09.com.example:rdisks.serverX`** à partir de 192.168.0.254 et assurez-vous qu'elle est activée lors du démarrage.

```
[root@serverX ~]# service iscsid start
[root@serverX ~]# chkconfig iscsid on
[root@serverX ~]# iscsiadm -m discovery -t st -p 192.168.0.254
[root@serverX ~]# iscsiadm -m node -T iqn.2010-09.com.example:rdisks.serverX -p
 192.168.0.254 -l
```

2. Créez deux nouvelles partitions physiques de 10 Mo chacune sur le disque iSCSI.

```
[root@serverX ~]# fdisk -cu /dev/sda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0x14d0f83d.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (2048-65535, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-65535, default 65535): +10M

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): Partition number (1-4): 2
First sector (22528-65535, default 22528):  Enter
Using default value 22528
Last sector, +sectors or +size{K,M,G} (22528-65535, default 65535): +10M
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

3. Avec la première partition, créez un système de fichiers ext4 monté de manière permanente sur **/test**.

```
[root@serverX ~]# mkfs -t ext4 /dev/sda1
[root@serverX ~]# blkid /dev/sda1
/dev/sda1: UUID="14ec9746-b443-4f89-af7b-d827adfd3de1" TYPE="ext4"
```

Copiez la ligne « UUID=*XXXXXXXX* » dans la sortie et ajoutez une entrée à **/etc/fstab**:

```
UUID=XXXXXXXX  swap swap defaults 0 0
```

Pour l'exemple ci-dessus, ce devrait être:

```
UUID=14ec9746-b443-4f89-af7b-d827adfd3de1  /test ext4 defaults 1 2
```

```
[root@serverX ~]# mkdir /test[root@serverX ~]# mount -a
```

4. Avec la seconde, créez un système de fichiers ext4 monté de manière permanente sur **/opt** avec **acl** en tant qu'option de montage par défaut.

```
[root@serverX ~]# mkfs -t ext4 /dev/sda2
[root@serverX ~]# blkid /dev/sda2
/dev/sda2: UUID="c261f7fb-b2e9-4678-b7e4-61293c87d095" TYPE="ext4"
```

Copiez l'UUID de la sortie et utilisez cette information pour ajouter une entrée à **/etc/fstab**

```
UUID=XXXXXXX /opt ext4 acl 1 2
```

Pour l'exemple ci-dessus, ce devrait être:

```
UUID=c261f7fb-b2e9-4678-b7e4-61293c87d095 /opt ext4 acl 1 2
```

```
[root@serverX ~]# mount -a
[root@serverX ~]# df -h /opt
Filesystem Size Used Avail Use% Mounted on
/dev/sda2            9.7M  1.1M  8.1M  12% /opt
```

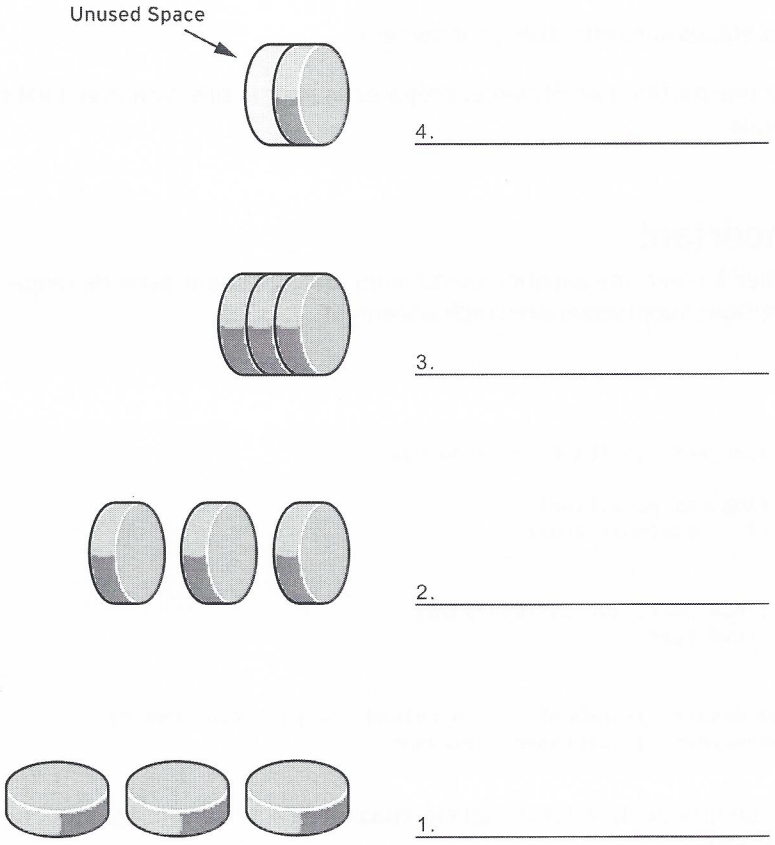
Gestion de volumes logiques



Exercice de Questionnaire

Composants de LVM

1. Renseignez les deux graphiques suivants avec les noms des composants.



1. Stockage physique
2. Volume(s) physique(s)
3. Groupe de volumes
4. Volume(s) logique(s)

2. Quelles sont les plus petites pièces (morceaux ou blocs) du volume physique ?
   Extensions physiques

3. Quelle est la plus petite taille à laquelle vous pouvez réduire le volume logique ?
   La taille d'une extension physique.

4. Qu'est-ce qui fait référence aux extensions physiques d'un volume logique ?
   Les extensions logiques



Exercice de Exercice

Implémenter LVM et créer un volume logique

Toutes ces étapes sont effectuées sur serverX.

1. Créez une partition de 512 Mo et préparez-la pour l'utilisation avec LVM en tant que volume physique.



Important

Veillez à créer une partition étendue au préalable pour avoir de l'espace pour créer des partitions supplémentaires ultérieurement.

```
[root@serverX ~]# fdisk -cu /dev/vda
n
l    (logical partition)
[enter]    (default start)
+512M
t
8    (this partition is /dev/vda8)
8e    (LVM type)
w

[root@serverX ~]# reboot    (to reload the partition table)
[root@serverX ~]# pvcreate /dev/vda8
```

2. Créez un groupe de volumes appelé **shazam** à l'aide du volume physique créé à l'étape précédente.

```
[root@serverX ~]# vgcreate shazam /dev/vda8
```

3. Créez et formatez avec **ext4** un nouveau volume logique de 256 Mo appelé **/dev/shazam/storage**.

```
[root@serverX ~]# lvcreate -n storage -L 256MB shazam
[root@serverX ~]# mkfs -t ext4 /dev/shazam/storage
```

4. Modifiez votre système pour que **/dev/shazam/storage** soit monté au moment du démarrage en tant que **/storage**.

```
[root@serverX ~]# mkdir /storage
```

Mettez à jour /etc/fstab avec l'entrée suivante :

```
/dev/shazam/storage     /storage    ext4   defaults  1 2
```

```
[root@serverX ~]# mount -a
[root@serverX ~]# df
[root@serverX ~]# reboot    (to confirm persistence)
```



Exercice de Exercice

Etendre un volume logique

Toutes ces étapes sont effectuées sur serverX.

1. Déterminez la quantité d'espace libre dans le groupe de volumes **shazam**.

   ```
   [root@serverX ~]# vgdisplay shazam
   ```

2. Étendez le volume logique **/dev/shazam/storage** avec *la moitié* des extensions disponibles dans le groupe de volume, à l'aide d'outils en ligne de commande.

   Si 100 extensions étaient disponibles, la commande suivante étendrait le volume logique en utilisant la moitié d'entre elles :

   ```
   [root@serverX ~]# lvextend -l +50 /dev/shazam/storage
   ```

3. Étendez le système de fichiers monté sur **/storage** à l'aide d'outils en ligne de commande.

   ```
   [root@serverX ~]# resize2fs /dev/shazam/storage
   ```



Exercice de Exercice

Étendre un groupe de volumes

Toutes ces étapes sont effectuées sur serverX.

1. Créez une partition de 512 Mo et préparez-la pour l'utilisation avec LVM en tant que volume physique.



Important

Veillez à créer une partition étendue au préalable pour avoir de l'espace pour créer des partitions supplémentaires ultérieurement.

Utilisez **fdisk** et **pvcreate** pour préparer le volume physique.

```
[root@serverX ~]# fdisk -cu /dev/vda
n
l    (logical partition)
[enter]    (default start)
+512M
t
9    (this partition is /dev/vda9)
8e    (LVM type)
w

[root@serverX ~]# reboot    (to reload the partition table)
[root@serverX ~]# pvcreate /dev/vda9
```

2. Étendez le groupe de volumes **shazam** en ajoutant le volume physique créé à l'étape précédente.

   Utilisez **vgextend** pour étendre le groupe de volumes:

```
[root@serverX ~]# vgextend shazam /dev/vda9
[root@serverX ~]# vgdisplay shazam   (check size and free space)
```



Exercice de Exercice

Création d'un instantané LVM

Comparez le contenu de notre volume logique existant, **/dev/shazam/storage**, avec un nouveau volume d'instantané, **/dev/shazam/storagesnap**, tout en apportant des modifications au volume initial.

Toutes ces étapes sont effectuées sur serverX.

1. Copiez le fichier **/usr/share/dict/linux.words** dans **/storage** pour avoir des données à comparer.

```
[root@serverX ~]# cp /usr/share/dict/linux.words /storage
```

2. Créez un volume logique d'instantané de 20 Mo de **/dev/shazam/storage**, appelé **storagesnap**.

```
[root@serverX ~]# lvcreate -n snapstore -L20M -s /dev/shazam/storage
```

3. Montez manuellement **/dev/shazam/storagesnap** en lecture seule sur **/storagesnap**

```
[root@serverX ~]# mkdir /storagesnap
[root@serverX ~]# mount -o ro /dev/shazam/storagesnap /storagesnap
```

4. Répertoriez le contenu de **/storagesnap** et notez qu'il est identique à **/storage**.

```
[root@serverX ~]# ls /storagesnap ; ls /storage
```

5. Supprimez le fichier **/storage/linux.words** et notez qu'il existe encore dans **/storagesnap**.

```
[root@serverX ~]# rm /storage/linux.words
[root@serverX ~]# ls /storagesnap
```

6. Nettoyage : démontez **/storagesnap**, supprimez le répertoire et supprimez le volume logique **storagesnap**.

```
[root@serverX ~]# umount /storagesnap
[root@serverX ~]# rmdir /storagesnap
[root@serverX ~]# lvremove /dev/shazam/storagesnap
```



Test

Test de critère

Étude de cas

Étude de cas LVM

Avant de commencer...

Assurez-vous d'exécuter **lab-setup-lvm** depuis votre système desktopX afin de préparer votre système serverX pour l'exercice.

Allison doit stocker des données pour son entreprise. La taille actuelle de sa base de données de clients est de 256 Mo. Les données qu'elle contient changent à un taux d'environ 10 Mo par heure au cours d'une journée normale. Le logiciel de sauvegarde prend 10 minutes pour terminer une exécution complète.

Créez un nouveau groupe de volumes appelé **allison** avec assez d'espace pour un volume de 512 Mo et un instantané de ce volume pour le logiciel de sauvegarde. Créez un volume logique de 512 Mo pour la base de données de clients d'Allison, appelée **custdb**. Créez un volume d'instantané de la base de données de clients d'Allison, appelé **custdbsnap** pour son logiciel de sauvegarde.

Lorsque vous êtes prêt, exécutez le script **lab-grade-lvm** sur le serverX pour vérifier votre travail.

1. Créez une nouvelle partition d'1 Go à l'aide de **fdisk** et préparez-la pour l'utilisation avec LVM.

```
[root@serverX ~]# fdisk -cu /dev/vda

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First sector (9914368-12582911, default 9914368):  Enter
Using default value 9914368
```

```
Last sector, +sectors or +size{K,M,G} ((9914368-12582911, default 12582911): +1G
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@serverX ~]# reboot
```

```
[root@serverX ~]# pvcreate /dev/vda3
  Physical volume "/dev/vda3" successfully created
```

2. Créez un groupe de volumes appelé **allison** à l'aide de la nouvelle partition.

```
[root@serverX ~]# vgcreate allison /dev/vda3
  Volume group "allison" successfully created
```

3. Créez un volume logique de 512 Mo pour la base de données de clients d'Allison.

```
[root@serverX ~]# lvcreate -n custdb -L512M allison
  Logical volume "custdb" created
```

4. Créez un volume d'instantané de 10 Mo pour la base de données de clients d'Allison

```
[root@serverX ~]# lvcreate -n custdbsnap -L10M -s /dev/allison/custdb
  Rounding up size to full physical extent 12.00 MiB
  Logical volume "custdbsnap" created
```

Gestion de comptes



Exercice de Liste de contrôle des performances

Gestion des stratégies de durée de vie des mots de passe

Votre instructeur va vous répartir en petits groupes Dans chaque groupe, discutez pour déterminer les stratégies de durée de vie du mot de passe appropriées pour les *professeurs* (qui utilisent la machine pendant longtemps), les *étudiants diplômés* (qui utilisent la machine pendant quelques années) et les *internes d'été* (qui utilisent uniquement la machine pendant l'été).

- **`Professors`**: faraday, juliet
- **`Graduate Students`**: jack, kate, james
- **`Summer Interns`**: walt, ben, clair, hugo

☐ Si les utilisateurs et les groupes ne sont pas définis, exécutez **`lab-add-users`** sur serverX.

```
[root@serverX ~]# lab-add-users
```

☐ Pour chaque groupe d'utilisateurs, déterminez une stratégie de durée de vie du mot de passe appropriée, qui inclut

- Les dates d'expiration du compte (le cas échéant).
- Le délai avant la modification du mot de passe.
- Le délai avant que les mots de passe inchangés forcent l'inactivité d'un compte.

Les comptes des professeurs n'expireront pas. Les professeurs doivent changer leur mot de passe chaque trimestre (tous les 90 jours). Lorsque leur mot de passe a expiré, leur compte sera inactif après 30 jours.

Les comptes des étudiants diplômés n'expireront pas. Les étudiants diplômés doivent changer leur mot de passe chaque mois (tous les 30 jours). Lorsque leur mot de passe a expiré, leur compte sera inactif après 30 jours.

Les comptes des stagiaires saisonniers pendant l'été expirent à la fin de l'été (notre exemple porte sur l'été 2011). Les stagiaires saisonniers doivent changer leur mot de passe chaque mois (tous les 30 jours). Lorsque leur mot de passe a expiré, leur compte sera inactif après 7 jours.

☐ Une fois déterminée, utilisez la commande **chage** pour implémenter votre règle pour les utilisateurs ajoutés dans la section précédente, en fonction de leur rôle.

De plus, obligez tous les utilisateurs à modifier leur mot de passe lors de la première connexion.

Voici ci-dessous les ajustements apportés au compte de faraday (un professeur).

```
[root@serverX ~]# chage -M 90 -I 30 faraday
```

Voici ci-dessous les ajustements apportés au compte de kate (une étudiante diplômée).

```
[root@serverX ~]# chage -M 30 -I 30 kate
```

Voici ci-dessous les ajustements apportés au compte d'hugo (un stagiaire saisonnier).

```
[root@serverX ~]# chage -M 90 -I 30 -E 2011-09-30 hugo
```



Exercice de Questionnaire

Autorisations sur un répertoire collaboratif

1. Quelle commande permet de changer les autorisations d'un répertoire pour qu'il devienne un répertoire collaboratif de groupe unique privé ?
   `chmod 2770 /directory`

2. Quelle commande permet d'accorder l'accès au répertoire à un second groupe ?
   `setfacl -m g:group:rwx /directory`

3. Quelle commande permet d'accorder à ce deuxième groupe un accès en lecture-écriture à tout fichier créé dans ce répertoire ?
   `setfacl -m d:g:group:rw /directory`



Test

Test de critère

Exercice

Utilisation d'ACL pour accorder et limiter l'accès

Utilisation d'utilisateurs et de groupes créés précédemment sur serverX...

Si les utilisateurs et les groupes ne sont pas définis, exécutez **`lab-add-users`** sur serverX.

Les étudiants diplômés ont besoin d'un répertoire /opt/recherche où ils pourront stocker les résultats de recherche générés. Les propriétés suivantes doivent être définies sur les fichiers créés dans le répertoire :

1. Le groupe des étudiants diplômés doit être propriétaire des fichiers.
2. Les professeurs (membres du groupe Professeurs) doivent avoir un accès en lecture/écriture au répertoire.
3. Les stagiaires saisonniers (membre du groupe Stagiaires) doivent avoir accès au répertoire en lecture seule.

4. En outre, les autres utilisateurs (non-membres des groupes Professeurs, Étudiants ou Stagiaires) ne doivent pas pouvoir accéder au répertoire.

```
mkdir /opt/research
chgrp grads /opt/research/
chmod g=rwxs /opt/research/
setfacl -m g:profs:rwx /opt/research/
setfacl -m g:interns:rx /opt/research/
setfacl -m d:g:profs:rwx /opt/research/
setfacl -m d:g:interns:rx /opt/research/
setfacl -m d:g:grads:rwx /opt/research/
```

Gestion de l'authentification



Exercice de Questionnaire

Configuration du client LDAP

1. Quelles sont les sept informations généralement fournies par les services d'*information sur les comptes d'utilisateur* ?

```
username:password:UID:GID:GECOS:/home/dir:shell
```

2. Quel « autre » type d'information peut être fourni par un *service d'annuaire réseau* ?
   Méthode d'authentification

3. Quelles sont les trois informations devant être configurées pour une machine client afin d'obtenir les informations sur l'utilisateur à partir d'un service d'annuaire LDAP ?
   Nom d'hôte qualifié complet du serveur, DN de base et certificat CA

4. Que fait la commande **`getent passwd ldapuser1`** ? Pourquoi est-ce utile ?
   La commande **`getent`** recherche les informations de l'utilisateur ldapuser1 dans la base de données des fichiers de mot de passe. Cela confirme qu'un système est correctement configuré en tant que client LDAP.



Exercice de Liste de contrôle des performances

Exercice de configuration Kerberos

Vous allez modifier votre configuration LDAP précédente pour utiliser désormais uniquement Kerberos pour l'authentification. LDAP continuera à être utilisé pour fournir les informations des comptes.

- ☐ Connectez-vous à serverX et passez au niveau de privilèges du super utilisateur

```
[student@serverX ~]$ su -
Password:
[root@serverX ~]#
```

- ☐ Vérifiez que les packages nécessaires sont installés

```
[root@serverX ~]# rpm -q krb5-workstation
krb5-workstation-1.8.2-3.el6.x86_64
```

Si **`krb5-workstation`** n'est pas installé, utilisez **`yum`** pour l'installer :

```
[root@serverX ~]# yum install -y krb5-workstation
```

- ☐ Configurez le système afin qu'il utilise les paramètres LDAP et Kerberos suivants :
  - Serveur LDAP : instructor.example.com (utilise TLS)
  - Certificat LDAP : `ftp://instructor.example.com/pub/EXAMPLE-CA-CERT`

- DN de base LDAP : dc=example,dc=com
- Domaine Kerberos : EXAMPLE.COM
- KDC Kerberos : instructor.example.com
- Serveur d'administration Kerberos : instructor.example.com
- Assurez-vous que le service **sssd** est activé

Lancez **system-config-authentication**. Sélectionnez LDAP pour la base de données des comptes d'utilisateur et le mot de passe Kerberos pour la méthode d'authentification. Fournissez les informations ci-dessus pour chacun des deux services. Une fois que vous avez fourni les informations et appliqué les modifications, vous devez lancer le service sssd. Pour confirmer que le service est exécuté, effectuez ce qui suit :

```
[root@serverX ~]# service sssd status
sssd (pid 2634) is running...
```

☐ Testez les modifications en vous connectant à serverX avec ssh :

- Nom d'utilisateur : **ldapuserX** (où X est le numéro de votre station de travail)
- Mot de passe : **kerberos**

Le test peut être effectué via ssh ou en vous connectant à une autre console virtuelle sur le gestionnaire virt-manager. Notez que le répertoire personnel de l'utilisateur ne sera disponible que lorsque le service de montage automatique sera configuré plus tard dans cette unité.



Exercice de Questionnaire

Résolutions des problèmes d'authentification - Questionnaire

1. Comment configure-t-on normalement SSSD ? À l'aide de l'outil de configuration de l'authentification **authconfig** ou en modifiant **/etc/sssd/sssd.conf**

2. Quel répertoire contient les messages de journal de sssd ? **/var/log/sssd/**

3. Comment peut-on augmenter les détails du journal qui est généré ? Il suffit de changer **/etc/sssd/sssd.conf** et de définir **debug_level=[0-10]** en augmentant la valeur pour obtenir plus de détails. Cette valeur est définie dans chaque zone « service » du fichier, ce qui permet des niveaux de détails propres à chacune de ces zones.

4. Quand vous ne pouvez pas vous connecter pour corriger une configuration d'authentification incorrecte, quelles approches adoptez-vous ? Mode utilisateur unique ou niveau d'exécution1



Exercice de Liste de contrôle des performances

Utiliser un serveur de répertoires personnels NFS pour fournir des répertoires personnels montés automatiquement.

L'université fournit également un serveur de répertoires personnels NFS pour ses étudiants de licence. Utilisez le serveur des répertoires personnels NFS pour monter automatiquement les répertoires personnels des utilisateurs définis précédemment.

Voici les informations relatives au serveur de répertoires personnels.

- Nom d'hôte : *instructor.example.com*
- Répertoire exporté : **/home/guests/**

☐ Étendez la configuration du service de montage automatique pour monter les répertoires dans le répertoire **/home/guests**.

Ajoutez la ligne suivante dans **/etc/auto.master** :

```
/home/guests   /etc/auto.guests
```

☐ Indiquez au service de montage automatique de se mapper à un répertoire cible spécifique en tant que répertoire analogue à partir du serveur de répertoires personnels.

Par exemple, une requête pour accéder au répertoire local **/home/guests/ldapuser1** tentera de monter le répertoire **/home/guests/ldapuser1** depuis instructor.example.com.

Créez un fichier appelé **/etc/auto.guests**, qui contiendra ce qui suit :

```
*     instructor.example.com:/home/guests/&
```

☐ Indiquez au service de montage automatique de recharger ses fichiers de configuration.

```
[root@serverX ~]# service autofs reload
```

☐ À partir d'un autre terminal, émettez une commande shell sur le serveur distant en tant qu'utilisateur **ldapuserX** avec le mot de passe **password**. Le répertoire personnel de l'utilisateur doit être monté automatiquement.

☐ Lorsque vous avez terminé, exécutez le script **lab-grade-autofshomes** pour vérifier votre travail.

```
[root@serverX ~]# lab-grade-autofshomes
```



Test

Test de critère

Étude de cas

Augmenter la sécurité des utilisateurs

Avant de commencer...

Assurez-vous d'exécuter **`lab-setup-taylorlocke`** depuis votre système desktopX afin de préparer votre système serverX pour l'exercice.

Taylor and Locke, un prestigieux cabinet d'avocats, a engagé récemment un consultant de sécurité pour le conseiller concernant la configuration de ses serveurs. Étant donné que les serveurs du cabinet contiennent des informations sensibles concernant les comptes client, la sécurité est une priorité !

Le consultant de sécurité a recommandé que tous les serveurs utilisent LDAP pour les comptes centralisés et Kerberos pour l'authentification. Globalement, le déploiement LDAP/Kerberos s'est bien passé. Cependant, l'un des serveurs que vous gérez semble être incorrectement configuré.

Corrigez la configuration sur serverX pour que les utilisateurs LDAP puissent se connecter avec l'authentification Kerberos (voir ci-dessous pour plus de détails).

- Serveur LDAP : instructor.example.com (utilise TLS)
- Certificat LDAP : ftp://instructor.example.com/pub/EXAMPLE-CA-CERT
- DN de base LDAP : dc=example,dc=com
- Domaine Kerberos : EXAMPLE.COM
- KDC Kerberos : instructor.example.com
- Serveur d'administration Kerberos : instructor.example.com

Testez les modifications en vous connectant à serverX avec ssh :

- Nom d'utilisateur : ldapuserX (où *X* est le numéro de votre station de travail)
- Mot de passe : kerberos

Une fois que les utilisateurs LDAP peuvent se connecter, configurez autofs pour qu'il fournisse les répertoires personnels montés automatiquement. Les répertoires personnels sont partagés sur instructor.example.com.

Lorsque vous êtes prêt, exécutez le script **`lab-grade-taylorlocke`** sur le serverX pour vérifier votre travail.

1. Activez le mode utilisateur unique sur serverX.
2. Configurez l'authentification LDAP/Kerberos :

```
# authconfig --enableldap --ldapserver=instructor.example.com --enableldaptls
--ldaploadcacert=ftp://instructor.example.com/pub/EXAMPLE-CA-CERT
```

```
--ldapbasedn="dc=example,dc=com" --disableldapauth --enablekrb5
--krb5kdc=instructor.example.com --krb5adminserver=instructor.example.com
--krb5realm=EXAMPLE.COM --enablesssd --enablesssdauth --update
```

3. Activez le mode multiutilisateur sur serverX avec le niveau d'exécution 3 ou 5.

4. Ajoutez la ligne suivante dans **/etc/auto.master**:

```
/home/guests    /etc/auto.home
```

Créez **/etc/auto.home** et ajoutez-lui ce qui suit:

```
*   -rw,hard,intr   instructor.example.com:/home/guests/&
```

Indiquez au service de montage automatique de recharger sa configuration:

```
[root@serverX ~]# service autofs reload
```

Installation, Kickstart et virtualisation



Exercice de Liste de contrôle des performances

Modification d'un fichier Kickstart sans system-config-kickstart

À la fin de cet exercice, vous aurez effectué toutes les étapes nécessaires pour lancer un nouveau système avec l'utilitaire Kickstart (sans installation). Vous effectuerez une installation Kickstart plus loin dans cette unité. Effectuez la procédure suivante sur desktopX :

- ☐ Créez une copie de **`/root/anaconda-ks.cfg`** appelée **`~/projman.cfg`**. À l'aide d'un éditeur de texte uniquement, modifiez ce fichier pour qu'il remplisse les critères suivants : L'installation doit être entièrement automatisée et identique à celle du poste de travail de base, sauf...

  - Effectuez le partitionnement de disque suivant :
    - Initialisez le schéma de partitionnement MBR si nécessaire
    - Supprimez toutes les partitions existantes
    - /boot (ext4) - 200 Mo
    - swap - 512 Mo
    - / (ext4) - tout l'espace restant (5 Go minimum)

    Les directives de partitionnement seront similaires à ce qui suit dans la section de lancement du fichier Kickstart :

    ```
    # Partitioning according to lab specifications:
    zerombr
    clearpart --all
    part /boot --fstype=ext4 --size=200
    part swap --size=512
    part / --fstype=ext4 --size=5000 --grow
    ```

  - Le groupe de packages **`E-mail server`** doit être installé.

    La section **`%packages`** doit contenir la ligne suivante :

    ```
    @E-mail server
    ```

  - Le package **`fetchmail`**, non inclus avec le groupe **`E-mail server`** par défaut, doit être installé

    La section **`%packages`** doit également contenir la ligne suivante :

    ```
    fetchmail
    ```

  - Assurez-vous de supprimer les scripts existants de **`%pre`** et de **`%post`**

- Utilisez **echo** pour ajouter le texte suivant à la fin de **/etc/issue**:

```
PROJECT MANAGEMENT
```

La section **%post** doit ressembler à ce qui suit:

```
%post
echo 'PROJECT MANAGEMENT' >> /etc/issue
%end
```

☐ **ksvalidator** doit être en mesure de valider le fichier.

Aucun résultat ne doit s'afficher lorsque la commande suivante est exécutée:

```
[root@desktopX ~]# ksvalidator projman.cfg
```

☐ Une fois toutes ces étapes effectuées, publiez le fichier pour qu'il puisse servir à une installation. Déployez un serveur Web sur desktopX et copiez **projman.cfg** sur **/var/www/html/**.

Effectuez la procédure nécessaire pour déployer un serveur Web. Installez le package **httpd** si nécessaire, puis démarrez le service et configurez-le pour qu'il soit lancé à chaque démarrage:

```
[root@desktopX ~]# yum install -y httpd
[root@desktopX ~]# service httpd start
[root@desktopX ~]# chkconfig httpd on
```

Assurez-vous que le fichier Kickstart est lisible, puis publiez-le:

```
[root@desktopX ~]# chmod 644 projman.cfg
[root@desktopX ~]# cp projman.cfg /var/www/html/
```

☐ Utilisez un navigateur Web pour vérifier que le fichier Kickstart est lisible. L'URL que vous utilisez pour afficher le fichier est celle que vous transmettriez au programme d'installation avec l'argument **ks=*URL***.

Lancez Firefox et entrez l'adresse **http://desktopX.example.com/projman.cfg**. Le fichier Kickstart doit normalement s'afficher si l'avez publié correctement.

Points importants concernant la virtualisation KVM

- KVM = Kernel-based Virtual Machine (machine virtuelle basée sur le noyau)
- Exigences en matière de KVM:
- Prise en charge VirtIO = pilotes paravirtualisés utilisés par les invités KVM (améliorent les performances E/S)
- Les avantages de KVM comprennent:

- Implémenté sous forme de modules du noyau
- Permet à un noyau Linux standard de fonctionner en tant qu'hyperviseur
- Processeurs 64 bits AMD ou Intel
- Extensions de virtualisation assistées par le matériel
- Système d'exploitation 64 bits
- Des performances élevées
- Un concept simple
- Une adoption par les développeurs de noyau en amont
- **`grep flags /proc/cpuinfo`**
- Les indicateurs pertinents comprennent :
- **`lm`** = mode long (64-bit x86)
- **`svm`** = machine virtuelle sécurisée (AMD)
- **`vmx`** = extensions de machines virtuelles (Intel)



Exercice de Questionnaire

Introduction à la virtualisation KVM

1. La virtualisation matérielle nécessite qu'un processeur spécial doté de capacités de virtualisation soit activé dans le BIOS.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

2. KVM est une technologie de virtualisation basée sur le noyau qui permet d'installer à la fois Linux et Windows en tant que machine virtuelle sans avoir à utiliser de noyau spécial.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

3. KVM est très prisé en raison de ses performances élevées et de sa conception complexe.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

   La conception de KVM est vraiment simple.

4. Les indicateurs de processeur **lm** et **svm** ou **vmx** sont requis pour la virtualisation basée sur le noyau.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

5. KVM fonctionne à la fois sur des machines 32 et 64 bits.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

   KVM doit s'exécuter sur un hôte avec un système d'exploitation 64 bits fonctionnant sur du matériel 64 bits (c'est ce que l'indicateur de processeur représente). Les machines virtuelles doivent être de type x86 32 bits.

6. Les développeurs de logiciels amont ont intégrés KVM dans le code source du noyau Linux.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux



Exercice de Liste de contrôle des performances

Installation d'invités virtuels

Dans cet exercice, vous allez installer une nouvelle machine virtuelle avec Red Hat Enterprise Linux en utilisant **virt-manager** et le programme d'installation graphique. Lorsque vous avez terminé l'exercice, vous devez supprimer la machine virtuelle et son volume logique afin de restaurer les ressources système requises pour d'autres exercices.

Effectuez la procédure suivante sur desktopX :

- ☐ Arrêtez normalement votre machine virtuelle serverX pour récupérer les ressources système du processeur et de la mémoire.

  Démarrez **virt-manager** en choisissant **Applications** → **Outils système** → **Gestionnaire des machines virtuelles**. Cliquez avec le bouton droit de la souris sur l'icône représentant la machine virtuelle **vserver**, puis sélectionnez **Arrêter** → **Arrêter**.

- ☐ Créez un volume logique de 10 Go à partir du groupe de volumes **vol0** et appelez-le **guest**.

```
[root@desktopX ~]# lvcreate -n guest -L 10G vol0
```

- ☐ Créez une machine virtuelle Red Hat Enterprise Linux 6 avec les caractéristiques suivantes :

- Nom = invité
- Support d'installation = installation réseau à partir de http://instructor.example.com/pub/rhel6/dvd
- Mémoire (RAM) = 768 Mo
- CPU = 1
- Périphérique de stockage = le volume logique créé lors de l'étape précédente
- Réseau - utiliser DHCP pour obtenir une adresse IP

Dans **virt-manager**, cliquez avec le bouton droit de la souris sur **localhost (QEMU)** et sélectionnez **Nouveau**. Lorsque la boîte de dialogue « Nouvelle machine virtuelle » s'affiche, tapez **guest** pour le nom et sélectionnez le bouton radio **Installation réseau (HTTP, FTP ou NFS)** pour la méthode d'installation. Cliquez sur le bouton **Suivant** pour continuer.

Tapez **http://instructor.example.com/pub/rhel6/dvd** dans le champ **URL**. Cliquez sur le bouton **Suivant** pour continuer. Si une boîte de dialogue d'avertissement s'affiche vous demandant si vous disposez des autorisations pour **/home/student/.virtinst/boot**, cliquez sur **Oui** et continuez.

Dans la boîte de dialogue suivante, sélectionnez **768 MB** pour **Mémoire (RAM)** et conservez la valeur 1 pour **Processeurs**. Cliquez sur le bouton **Suivant** pour continuer.

Pour le stockage, sélectionnez le bouton radio **Sélectionner le stockage géré ou existant**, puis spécifiez le nom de chemin **/dev/vol0/guest**. Cliquez sur le bouton **Suivant** pour continuer.

Après avoir vérifié les informations de la dernière boîte de dialogue, cliquez sur **Terminer** pour terminer la création de la machine virtuelle et commencer à utiliser le programme d'installation Red Hat, Anaconda.

Lorsque les menus texte s'affichent, sélectionnez la langue et le clavier appropriés pour vos paramètres régionaux. À chaque fois, cliquez sur **OK** pour passer au menu suivant. Une fois que les paramètres réseau ont été spécifiés, le programme d'installation graphique s'affiche. Sélectionnez **Afficher → Redimensionner selon la machine virtuelle** dans les menus de **virt-manager**.

☐ Une fois **Anaconda** lancé, structurez votre système invité en tenant compte des spécifications suivantes :

- Utilisez la totalité de l'unité périphérique avec un schéma de partitionnement du disque par défaut
- Affectez **redhat** comme mot de passe root
- Installez le groupe de packages Desktop

Cliquez sur le bouton **Suivant** pour quitter l'écran d'introduction.

Sur l'écran de stockage, assurez-vous que le bouton radio **Périphériques de stockage de base** est sélectionné et cliquez sur **Suivant**. Si une boîte de dialogue d'**avertissement**

s'affiche vous indiquant que le stockage doit être réinitialisé, cliquez sur le bouton **Réinitialiser tout** pour réinitialiser le lecteur de la machine virtuelle.

Lorsque l'écran de configuration réseau s'affiche, conservez le nom d'hôte par défaut choisi. Le réseau sera configuré, car une installation réseau est effectuée. Cliquez sur le bouton **Suivant** pour continuer.

Choisissez un fuseau horaire approprié et vérifiez que la case à cocher **L'horloge système utilise UTC** est activée. Cliquez sur **Suivant** pour continuer.

Spécifiez le mot de passe root de **redhat** deux fois, puis cliquez sur le bouton **Suivant**. Lorsque la boîte de dialogue **Mot de passe faible** s'affiche, ignorez l'avertissement et cliquez sur le bouton **Utiliser quand même** pour continuer.

Étant donné que l'exercice de résolution du problème vous a indiqué d'utiliser le schéma de partitionnement par défaut, cliquez sur le bouton **Suivant** pour quitter l'écran de partitionnement du disque et passer à l'écran suivant. Cliquez sur le bouton **Enregistrer les modifications sur le disque** lorsque la boîte de dialogue d'avertissement s'affiche. Vous verrez que le disque est alors partitionné et formaté.

L'écran de sélection du logiciel s'affiche ensuite. Sélectionnez le bouton radio pour le groupe de packages **Bureau** au lieu de **Serveur de base** qui est sélectionné par défaut. Cliquez sur le bouton **Suivant** pour continuer. Une fois la vérification des dépendances logicielles terminée, l'installation commence.

- ☐ Récupérez les ressources système utilisées par cet exercice pratique. Supprimez la machine virtuelle que vous avez créée et le stockage qu'elle utilise.

  Utilisez **virt-manager** pour forcer l'arrêt de l'invité virtuel. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Supprimer** pour supprimer le profil système. Enfin, exécutez la commande suivante pour récupérer les ressources disque utilisées par l'invité virtuel :

```
[root@desktopX ~]# lvremove /dev/vol0/guest
Do you really want to remove active logical volume guest? [y/n]: y[enter]
```

Commandes utilisées pour gérer les machines virtuelles

Jusqu'à présent **virt-manager** était utilisé pour gérer les machines virtuelles. Mais il existe un outil en ligne de commande, **virsh**, qui a les mêmes fonctions que **virt-manager** sans recourir à une interface graphique utilisateur. Ces deux utilitaires ont recours à la bibliothèque **libvirt**, ce qui permet de les utiliser indifféremment pour gérer les machines virtuelles.

1. Activer une machine virtuelle : **virsh start *name***
2. Arrêter normalement une machine virtuelle : **virsh shutdown *name***
3. Désactiver une machine virtuelle : **virsh destroy *name***
4. Connexion à la console d'une machine virtuelle : **virsh console *name***
5. Déconnexion de la console d'une machine virtuelle : **Ctrl+]**

6. Démarrer une machine virtuelle au démarrage du système: **virshautostart *name***



Exercice de Liste de contrôle des performances

Commandes de virtualisation

Effectuez toutes les tâches suivantes à partir de la ligne de commande sur desktopX. N'utilisez ni **virt-manager** ni **virt-viewer** au cours de cet exercice pratique.

- ☐ Utilisez **virsh list --all** pour déterminer l'ID (ou le nom) du domaine virtuel de serverX. Vous aurez besoin du nom du domaine pour effectuer la procédure suivante.

```
[root@desktopX ~]# virsh list --all
 Id Name                 State
----------------------------------
  - vserver              shut off
```

- ☐ Si serverX n'est pas en cours de fonctionnement, activez-le.

```
[root@desktopX ~]# virsh start vserver
Domain vserver started
```

- ☐ Fermez normalement serverX.

```
[root@desktopX ~]# virsh shutdown vserver
Domain vserver is being shutdown
```

- ☐ Activez serverX.

```
[root@desktopX ~]# virsh start vserver
Domain vserver started
```

- ☐ Connectez-vous à la console de serverX.

```
[root@desktopX ~]# virsh console vserver
Connected to domain vserver
Escape character is ^]
```

- ☐ Si la machine virtuelle n'est pas configurée pour présenter une console sur la console virtuelle, déconnectez-vous de la console.

  Saisissez **Ctrl+]** pour quitter la console virtuelle.

- ☐ Désactivez serverX.

```
[root@desktopX ~]# virsh destroy vserver
Domain vserver destroyed
```

- ☐ Vérifiez que serverX démarre au démarrage du système.

```
[root@desktopX ~]# virsh autostart vserver
```

```
Domain vserver marked as autostarted
```



Test

Test de critère

Liste de contrôle des performances

Lancer une machine virtuelle avec Kickstart

- ☐ Copiez le fichier **/root/anaconda-ks.cfg** de serverX à desktopX et appelez-le **~/test.cfg**. Arrêtez serverX après avoir copié le fichier pour récupérer les ressources système pour le reste de l'exercice pratique.
- ☐ Modifiez **test.cfg** selon les critères suivants :
  - Partitionnez le stockage en tenant compte de ce qui suit :
    - /boot (ext4) 200 Mo
    - swap 512 Mo
    - / (ext4) 8 Go
  - Ajoutez le package **gimp**
  - Créez un fichier **/root/install-date** avec la date et l'heure.

  Ajoutez ce qui suit au fichier Kickstart

```
clearpart --all
part /boot --fstype=ext4 --size=200
part swap --size=512
part / --fstype=ext4 --size=8192
....
[after %packages]
gimp
...

%post
date > /root/install-date
%end
```

- ☐ Copiez **test.cfg** dans **/var/www/html/** sur desktopX. Assurez-vous que le fichier est lisible par Apache. Démarrez le démon **httpd** s'il n'est pas déjà activé.

```
[root@desktopX ~]# cp ~/test.cfg /var/www/html/
[root@desktopX ~]# chmod 644 /var/www/html/test.cfg
[root@desktopX ~]# service httpd restart
```

- ☐ Créez un volume logique dans le groupe de volume **vol0** nommé **test** qui a suffisamment d'espace pour servir de disque à votre machine virtuelle.

```
[root@desktopX ~]# lvcreate -n test -L 10G vol0
```

- ☐ Lancez l'installation d'une machine virtuelle à l'aide du fichier Kickstart **test.cfg**. Nommez la machine virtuelle **test**. Utilisez le support d'installation de http://instructor/pub/rhel6/dvd et allouez à la machine virtuelle 768 Mo de RAM et 1 processeur. Utilisez le volume logique que vous avez créé à l'étape précédente comme stockage pour votre machine virtuelle.

- ☐ Redémarrez la machine virtuelle lorsque son installation est terminée et vérifiez que celle-ci est correcte.

- ☐ *IMPORTANT :* supprimez votre machine virtuelle et le volume logique qu'elle utilise pour le stockage afin de récupérer les ressources nécessaires pour les futurs exercices.

```
[root@desktopX ~]# virsh destroy test
[root@desktopX ~]# virsh undefine test
[root@desktopX ~]# lvremove -f /dev/vol0/test
```

Gestion du démarrage



Exercice de Liste de contrôle des performances

Résoudre les problèmes liés à GRUB

- ☐ Exécutez le script **lab-setup-bootbreak** sur desktopX, afin de préparer votre serveur virtuel pour les problèmes de démarrage.

```
[root@desktopX ]# lab-setup-bootbreak
```

- ☐ Une fois serverX démarré, exécutez le script **lab-setup-bootbreak-5** sur celui-ci pour générer un problème de séquence de démarrage.

```
[root@serverX ]# lab-setup-bootbreak-5
```

- ☐ Redémarrez serverX et modifiez temporairement le chargeur de démarrage, afin que le système puisse démarrer et que vous puissiez vous connecter.

  1. Arrêtez le compte à rebours GRUB : touche **Esc**
  2. Utilisez "e" pour éditer la configuration actuelle.
  3. Sélectionnez la ligne **initrd** à corriger à l'aide des touches fléchées.
  4. Tapez à nouveau « e » pour modifier la ligne actuelle, en supprimant la phrase « **-BROKEN** ».
  5. Tapez « b » pour démarrer avec les modifications actuelles.
  6. Vérifiez que vous pouvez à nouveau ouvrir une session.



Exercice de Liste de contrôle des performances

Résoudre définitivement les problèmes liés à GRUB

- ☐ Redémarrez et assurez-vous que le problème précédemment traité persiste. Comme précédemment, vous devrez appliquer le correctif pour démarrer le système.

  Interrompez le compte à rebours GRUB (touche Échap.) Utilisez « e » pour éditer la configuration actuelle. Sélectionnez la ligne **initrd** à corriger à l'aide des touches fléchées. Tapez à nouveau « e » pour modifier la ligne actuelle, en supprimant la phrase « **-BROKEN** ». Tapez « b » pour démarrer avec les modifications actuelles.

- ☐ Modifiez le fichier de configuration pour résoudre définitivement le problème.

  Modifiez **/boot/grub/grub.conf** et supprimez définitivement « **-BROKEN** » de la ligne **initrd**.

- ☐ Installez un nouveau noyau à partir du référentiel **Errata**.

```
[root@serverX ~]# yum update kernel
```

- ☐ Rétablissez l'ancien noyau. En d'autres termes, le nouveau noyau étant toujours disponible, assurez-vous que, lors du redémarrage, le noyau plus ancien est celui par défaut.

  Modifiez **/boot/grub/grub.conf** et définissez **default=1** pour que l'ancien noyau démarre par défaut.

- ☐ Redémarrez le système pour vérifier que l'ancien noyau démarre correctement et que vous pouvez vous connecter.

```
[root@serverX ~]# reboot
```



Exercice de Liste de contrôle des performances

Modifier le niveau d'exécution par défaut

Vous configurez un nouveau système auquel vous accèderez à distance. Le système démarre actuellement au niveau d'exécution 5 par défaut, mais cette machine sera hébergée dans un centre de données auquel vous ne vous connecterez qu'à distance. Vous souhaitez modifier le système serverX pour qu'il démarre par défaut au niveau d'exécution 3.

- ☐ Configurez le système pour qu'il démarre par défaut au niveau d'exécution 3.

  Modifiez la ligne de **/etc/inittab** comme suit :

```
id:3:initdefault:
```

- ☐ Redémarrez, puis vérifiez le niveau d'exécution actuel.

```
[root@serverX ~]# reboot
...
[root@serverX ~]# who -r
         run-level 3  2010-12-13 10:26
```



Exercice de Liste de contrôle des performances

Modification du mot de passe root

Cet exercice est destiné à vous apprendre à modifier le mot de passe root dans un système avec mot de passe root inconnu.

- ☐ Commencez par exécuter le script **lab-setup-bootbreak-4** sur serverX. Cela modifiera le mot de passe en un élément inconnu et indiquera l'heure du jour.

```
[root@serverX ~]# lab-setup-bootbreak-4
```

- ☐ Entrez dans le système et réinitialisez le mot de passe root en **redhat**.



Note

Lors de la parution de Red Hat Enterprise Linux 6, un bogue provenant de SELinux bloquait la commande **passwd** en mode utilisateur unique (#644820). Si le package *selinux-policy* d'origine est installé, vous devez exécuter la commande **setenforce 0** au niveau d'exécution1 avant la commande **passwd** pour que cela fonctionne. Après avoir modifié le mot de passe, vous devez exécuter **setenforce 1** à nouveau pour remettre SELinux en mode enforcing.

Interrompez le compte à rebours GRUB (touche Échap.) Utilisez « e » pour éditer la configuration actuelle. Sélectionnez la ligne **kernel** à corriger à l'aide des touches fléchées. Tapez « e » à nouveau pour modifier la ligne actuelle, en ajoutant un « espace » et « **single** ». Tapez « b » pour démarrer avec les modifications actuelles.

```
# setenforce 0
# passwd
Changing password for user root.
New password: redhat
BAD PASSWORD: it is based on a dictionary word
BAD PASSWORD: is too simple
Retype new password: redhat
passwd: all authentication tokens updated successfully.
# setenforce 1
```

- ☐ Lorsque le mot de passe est réinitialisé, basculez le système vers le niveau d'exécution 5 et exécutez le script **lab-grade-bootbreak-4** sur serverX.

```
# init 5
...
[root@serverX ~]# lab-grade-bootbreak-4
```

- ☐ Consultez le retour d'information du script pour vous assurer que vous avez correctement mené à bien la tâche. Le script de notation affiche une heure, notez-la.
- ☐ Répétez au moins cinq fois ce processus.
- ☐ Entourez votre meilleur temps.



Exercice de Exercice

Utilisation du mode de secours

Avant de commencer...

Exécutez **lab-setup-bootbreak** sur desktopX.

Cette exploration automatique a été conçue de manière à vous exercer à accéder au mode de secours. Le chemin d'installation est *http://instructor.example.com/pub/rhel6/dvd*. Le chemin pour les packages individuels est *http://instructor.example.com/pub/rhel6/dvd/Packages/*

1. Une fois que serverX a démarré, exécutez le script **lab-setup-bootbreak-0**. Ce script modifiera votre système et entraînera des problèmes d'initialisation.

   Essayez de démarrer le système sans les arguments noyau de **rhgb quiet**. Notez les messages d'erreur suivants (vous pouvez utiliser la combinaison de touches Maj.-Page précédente pour faire défiler l'écran vers le haut):

```
/etc/rc.d/rc.sysinit/: line 26: mount: command not found
readahead: starting
               Welcome to Red Hat Enterprise Linux Server
...
Remounting root filesystem in read-write mode:  /etc/init.d/functions: line 536:
 mount: command not found
...
```

2. Démarrez en mode de secours pour diagnostiquer et résoudre le problème.

   - Démarrez en mode de secours.

     Au lieu de démarrer notre machine virtuelle depuis un DVD d'installation, démarrez-la depuis le réseau, en appuyant sur <Ctrl-B> lors de l'affichage de la boîte de dialogue gPXE.

```
gPXE> autoboot
```

     Choisissez « Rescue installed system » (Dépanner le système installé).

     Choisissez la langue et le type de clavier qui conviennent

     Choisissez l'« URL » pour le dépannage

     Utilisez DHCP pour IPv4 uniquement

     Choisissez *http://instructor.example.com/pub/rhel6/dvd* comme URL d'installation

     « Continuez » pour monter votre disque dur sous **/mnt/sysimage**

     Enfin, ouvrez un « shell »

   - Vérifiez le problème d'après un message d'erreur précédent:

```
bash-4.1# chroot /mnt/sysimage
sh-4.1# mount
sh: mount: command not found
sh-4.1# yum provides /bin/mount
... output omitted ...
sh-4.1# yum reinstall util-linux-ng
... output omitted ...
sh-4.1# mount
... output omitted ...
```

3. Vérifiez que celui-ci a été résolu en redémarrant le système.

```
sh-4.1# exit
exit
bash-4.1# exit
```

Choisissez « redémarrer »

4. Répétez ce processus aussi souvent que possible au cours de la période allouée.



Exercice de Questionnaire

Résolution des problèmes - Questionnaire

1. En mode maintenance, exécutez mount -o remount,rw / pour marquer la partition / comme accessible en écriture.

2. Si vous ne disposez que d'un seul disque dur et que la première partition contient /boot, en cas de problème mineur d'altération du schéma de partitionnement MBR, résolvez ce problème en démarrant en mode de secours, puis exécutez la commande grub. Tapez root (hd0,0), suivi de setup (hd0), puis quittez.

3. Si vous rencontrez des problèmes de corruption du système de fichiers, la machine démarrera en mode de maintenance.

4. En mode de maintenance, exécutez fsck pour résoudre les problèmes d'altération du système de fichiers.



Test

Test de critère

Exercice

Dépannage de la séquence de démarrage

Avant de commencer...

Exécutez la commande **lab-setup-bootbreak** sur desktopX pour configurer l'exercice.

Cet exercice pratique comprend trois problèmes à résoudre. Pour chacun d'eux, votre machine virtuelle serverX sera modifiée de manière à l'empêcher de démarrer correctement et vous devrez diagnostiquer et résoudre le problème.

1. Exécutez **lab-setup-bootbreak-1** sur serverX. Après avoir exécuté le script, serverX ne doit normalement plus démarrer correctement. Diagnostiquez et résolvez le problème. Vous saurez que vous avez trouvé la solution lorsque serverX démarre de nouveau normalement.

lab-setup-bootbreak-1 remplace **UUID** par **UID** dans **/etc/fstab**. Notez que **vim** marquera cette erreur en rouge. Pour résoudre le problème, rendez le système de fichiers **/** accessible en écriture, puis remplacez **UID** par **UUID** dans **/etc/fstab**.

2. Lorsque vous avez résolu le premier scénario, répétez la procédure avec **lab-setup-bootbreak-2** et **lab-setup-bootbreak-3**.

   lab-setup-bootbreak-2 définit le niveau d'exécution par défaut sur 9. Pour résoudre ce problème, démarrez avec le niveau d'exécution standard (en ajoutant **3** à la ligne du noyau, par exemple), puis modifiez **/etc/inittab** et remplacez **id:9:initdefault:** par **id:3:initdefault:**

   lab-setup-bootbreak-3 introduit une erreur de frappe dans **/boot/grub/grub.conf**. Pour résoudre ce problème, modifiez la ligne du noyau à partir de l'invite grub et remplacez **rot=** par **root=**. Lorsque le système démarre, effectuez la même correction dans **/boot/grub/grub.conf**.

Gestion de SELinux



Exercice de Questionnaire

Concepts SELinux de base

1. Parmi les éléments suivants SELinux, auxquels applique-t-il des contextes de sécurité (sélectionnez toutes les réponses correctes) ?

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. Ports
   b. Processus
   c. Fichiers
   d. Répertoires
   e. Systèmes de fichiers distants

2. SELinux peut être utilisé pour :

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. Empêcher un service de s'exécuter sur d'autres ports.
   b. Protéger les données de l'utilisateur d'applications telles que le serveur Web.
   c. Bloquer les systèmes distants afin qu'ils n'accèdent pas à des ports locaux.

      Ceci décrit un pare-feu.

   d. Garder le système à jour.

      Ceci peut décrire Red Hat Network.

   e. Accéder à un serveur Web.

      Ceci décrit un navigateur Web tel que Firefox.

3. Parmi les éléments suivants, lesquels sont des types de contextes SELinux standard ?

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. selinux_type

      Cet élément n'existe pas.

   b. object_r

      Ceci correspond à un rôle SELinux.

   c. httpd_sys_content_t
   d. tmp_t
   e. user_u

      Il s'agit d'un utilisateur de contexte SELinux.



Exercice de Questionnaire

Modes SELinux

1. Le mode permissif de SELinux permet la connexion, mais pas la protection.
2. Le mode enforcing de SELinux protège le système.
3. Parmi les éléments suivants, lesquels sont des modes SELinux valides ?

   (sélectionnez une ou plusieurs des réponses suivantes...)

   a. enforcing
   b. testing
   c. permissive
   d. disabled
   e. logging



Exercice de Exercice

Correction de contextes de fichiers SELinux

Vous avez été invité à régler la configuration DNS de votre machine distante pour qu'elle corresponde exactement à la configuration de votre machine de bureau. Vous déterminez la manière la plus facile de copier le fichier **/etc/resolv.conf** de votre machine locale vers la machine distante.

1. Transférez le fichier **/etc/resolv.conf** depuis votre machine de bureau vers le répertoire principal de *root* sur serverX.

   ```
   scp /etc/resolv.conf root@serverX:
   ```

2. Émettez une commande shell sur serverX en tant que **root**. Toutes les étapes suivantes doivent être effectuées sur votre serveur.
3. Observez le contexte SELinux du fichier **/etc/resolv.conf** initial.

   ```
   ls -Z /etc/resolv.conf
   ```

   Contexte **/etc/resolv.conf** initial: **system_u:object_r:net_conf_t:s0**

4. Déplacez **resolv.conf** du répertoire personnel du *root* vers **/etc/resolv.conf**.

   ```
   mv /root/resolv.conf /etc
   ```

5. Observez le contexte SELinux du fichier **/etc/resolv.conf** récemment copié.

   ```
   ls -Z /etc/resolv.conf
   ```

   Nouveau contexte **/etc/resolv.conf**: **unconfined_u:object_r:admin_home_t:s0**

6. Restaurez le contexte SELinux de votre fichier **/etc/resolv.conf** récemment positionné.

   ```
   restorecon /etc/resolv.conf
   ```

7. Observez le contexte SELinux du fichier **/etc/resolv.conf** restauré.

   ls -Z /etc/resolv.conf

   Contexte **/etc/resolv.conf** restauré: **system_u:object_r:net_conf_t:s0**



Exercice de Questionnaire

Contrôle des violations SELinux

1. Quel fichier contient les entrées de journal qui fournissent les identificateurs uniques des violations SELinux ? **/var/log/audit/audit.log**.

2. Avec l'UUID d'une violation SELinux, quelle commande génère un rapport texte sur le problème ? **sealert -l UUID**



Test

Test de critère

Exercice

Gestion de SELinux

Avant de commencer...

Avant de commencer, exécutez la commande **lab-setup-selinux** sur desktopX

1. Connectez-vous à serverX en tant que **student**. Ouvrez un terminal et basculez vers l'utilisateur **root**.

2. Copiez l'archive *web_content.tgz* de *instructor:/var/ftp/pub/materials* vers **/tmp**.

```
[root@serverX ~]# cp /net/instructor/var/ftp/pub/materials/web_content.tgz /tmp
```

3. Extrayez l'archive dans **/tmp**.

```
[root@serverX ~]# cd /tmp
[root@serverX tmp]# tar -xvf web_content.tgz
```

4. Déplacez le répertoire extrait vers **/var/www/html**.

```
[root@serverX tmp]# mv web_content /var/www/html/
[root@serverX tmp]# cd
```

5. Démarrez le service Web.

```
[root@serverX ~]# service httpd start
```

6. Essayez d'observer le nouveau répertoire avec votre navigateur Web en accédant à l'adresse URL *http://serverX/web_content*.

```
[root@serverX ~]# elinks -dump http://serverX/web_content
```

7. Recherchez dans votre système les UUID de toute violation SELinux que votre tentative de parcours du nouveau contenu installé peut avoir générée.

```
[root@serverX ~]# cat /var/log/messages | grep 'sealert -l'
```

8. Générez les rapports texte des violations.

```
[root@serverX ~]# sealert -l UUID > ~/httpd_selinux.log
```

Où *UUID* est l'UUID donné dans **/var/log/messages**

9. Suivez le conseil dans le rapport et restaurez les contextes SELinux du nouveau contenu installé.

Recherchez la section **Fix Command** dans **~/httpd_selinux.log**

```
[root@serverX ~]# restorecon -Rv /var/www/html/web_content/
```

10. Vérifiez que vous pouvez afficher le contenu dans votre navigateur Web en accédant à l'adresse URL *http://serverX/web_content*.

```
[root@serverX ~]# elinks -dump http://serverX/web_content
```

Gestion du pare-feu

- Rule (Règle) - critères déterminant quels paquets détecter et une cible, ou une action, à effectuer concernant ces paquets.
- Chain (Chaîne) - liste de *règles* qui seront vérifiées dans l'ordre, la première prenant effet.
- Policy (Stratégie) - l'action par défaut, **ACCEPT** ou **DROP**, effectuée si aucune *règle* ne correspond dans une *chaîne* intégrée.
- Table (Table) - un ensemble de *chaînes* utilisé pour un but particulier: **`filter`** pour bloquer le trafic, **`nat`** pour modifier la destination ou la source apparente d'un paquet.
- INPUT (ENTRÉE) - paquets adressés au pare-feu
- OUTPUT (SORTIE) - paquets provenant d'un service sur le pare-feu (non transmis)
- FORWARD (TRANSFÉRER) - paquets provenant d'une autre machine, qui ne sont pas adressés au pare-feu mais sont transférés (routés) ailleurs (quand **`net.ipv4.ip_forward=1`**)
- ACCEPT - le paquet est accepté par la chaîne
- DROP - le paquet est ignoré comme s'il n'existait pas
- REJECT - le paquet est rejeté et le pare-feu émet un message d'erreur (un message indiquant que le port ICMP est inaccessible par défaut)
- LOG - les informations sur le paquet sont consignées dans syslog; nous passons à la règle suivante dans la chaîne



Exercice de Exercice

Implémenter un pare-feu

Dans cet exercice vous allez implémenter un pare-feu sur serverX qui rejette tous les paquets mais autorise le trafic ICMP pour example.com et autorise SSH pour tous sauf remote.test.

1. Connectez-vous à serverX en tant que **`root`** (super utilisateur) à l'aide de **`virt-viewer`** ou **`virt-manager`**.
2. Créez un pare-feu « deny all » (refuser tout) (sauf 'loopback') en créant **`/root/bin/resetfw.sh`** qui
    1. définit la stratégie par défaut de la chaîne **`INPUT`** sur **`DROP`**,
    2. vide la table de filtre de toutes ses règles et

3. **ACCEPT** (accepte) tout les paquets depuis l'interface loopback.

```
[root@serverX ~]# cat /root/bin/resetfw.sh
#!/bin/bash
# Set INPUT chain default policy to DROP
iptables -P INPUT DROP
# Flushes all rule in the filter table
iptables -F
# Will ACCEPT all packets from loopback interface
iptables -A INPUT -i lo -j ACCEPT
```

3. Exécutez le script et notez les résultats de ce qui suit :

   - Envoyez une requête **ping** et une requête **ssh** à serverX depuis desktopX et remoteX.remote.test

   Les deux requêtes doivent échouer, car seul le trafic depuis l'interface loopback de serverX est accepté.

4. Que se passe-t-il lorsque vous envoyez maintenant une requête **ping** à desktopX et 192.168.0.X depuis serverX ? Pour quelle raison ?

   Les deux requêtes doivent normalement échouer, car les réponses de desktopX et 192.168.0.X sont ignorées.

5. Activez le pare-feu avec état en ajoutant au script une règle qui

   - **ACCEPT**ERA tous les paquets **ESTABLISHED, RELATED** (établis, associés).

```
[root@serverX ~]# tail -n 2 /root/bin/resetfw.sh
# ACCEPT all ESTABLISHED, RELATED packets
iptables -A INPUT -m state --state ESTABLISHED,RELATED
```

6. Exécutez le script et notez les résultats de ce qui suit :

   - Envoyez une requête **ping** à desktopX et 192.168.0.X depuis serverX.

   Cette requête doit maintenant aboutir, car les réponses font partie d'une connexion ÉTABLIE. Notez que l'inverse n'est toujours pas possible, car la connexion n'a pas été établie.

7. Rejetez tous les paquets provenant de remote.test en ajoutant au script une règle qui

   - **REJECT** (rejettera) tous les paquets depuis le réseau 192.168.1.0/24

```
[root@serverX ~]# tail -n 2 /root/bin/resetfw.sh
# REJECT all packets from 192.168.1.0/24 network
iptables -A INPUT -s 192.168.1.0/24 -j REJECT
```

8. Exécutez le script et notez les résultats de ce qui suit :

   - Envoyez une requête **ping** et une requête **ssh** à serverX depuis desktopX et remoteX.remote.test

Ces requêtes ne fonctionneront toujours pas depuis desktopX (elles sont ignorées), car il n'y a aucune règle applicable pour le paquet entrant d'origine. Les tentatives depuis remoteX.remote.test sont explicitement rejetées et elles ne fonctionneront pas non plus.

9. Autorisez le trafic ICMP pour example.com en ajoutant au script une règle qui

   - **ACCEPT**ERA tout le trafic **icmp** depuis 192.168.0.0/24.

```
[root@serverX ~]# tail -n 2 /root/bin/resetfw.sh
# ACCEPT all icmp traffic from 192.168.0.0/24
iptables -A INPUT -p icmp -s 192.168.0.0/24 -j ACCEPT
```

10. Exécutez le script et notez les résultats de ce qui suit :

    - Envoyez une requête **ping** et une requête **ssh** à serverX depuis desktopX.

    La requête **ping** doit normalement fonctionner, car le protocole **icmp** entrant est désormais ACCEPTÉ. Cependant, la requête **ssh** ne fonctionnera toujours pas.

11. Autorisez le trafic SSH pour tous les hôtes en définissant le script sur

    - **ACCEPT**ER toutes les nouvelles connexions (**NEW**) sur le port **tcp22**.

    Notez que l'instruction n'a pas indiqué d'ajouter la nouvelle règle. Pour que toutes les nouvelles connexions soient acceptées, nous devons indiquer d'insérer la règle dans le script *au-dessus* de REJECT 192.168.1.0/24.

```
[root@serverX ~]# cat /root/bin/resetfw.sh
#!/bin/bash
# Set INPUT chain default policy to DROP
iptables -P INPUT DROP
# Flushes all rule in the filter table
iptables -F
# Will ACCEPT all packets from loopback interface
iptables -A INPUT -i lo -j ACCEPT
# ACCEPT all ESTABLISHED, RELATED packets
iptables -A INPUT -m state --state ESTABLISHED,RELATED
# ACCEPT all NEW connections to tcp port 22
iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
# REJECT all packets from 192.168.1.0/24 network
iptables -A INPUT -s 192.168.1.0/24 -j REJECT
# ACCEPT all icmp traffic from 192.168.0.0/24
iptables -A INPUT -p icmp -s 192.168.0.0/24 -j ACCEPT
```

12. Exécutez le script et notez les résultats de ce qui suit :

    - Envoyez une requête **ssh** serverX depuis desktopX et remoteX.remote.test.

    Cela doit maintenant fonctionner, car les « requêtes » sont une NOUVELLE connexion sur le port 22. Si seule la requête envoyée depuis desktopX fonctionne et pas celle envoyée depuis remoteX.remote.test, vérifiez l'ordre des règles à l'étape précédente.

13. Rejetez par défaut les paquets au lieu de les ignorer en ajoutant au script une règle qui

    - rejettera (**REJECT**) tout autre trafic.

```
[root@serverX ~]# tail -n 2 /root/bin/resetfw.sh
# REJECT all other traffic
iptables -A INPUT -j REJECT
```

14. Exécutez le script et notez les résultats de ce qui suit :

    - Envoyez une requête **ping** et une requête **ssh** à serverX depuis desktopX et remoteX.remote.test

    Les requêtes **ping** et **ssh** fonctionneront depuis desktopX, mais seule la requête **ssh** fonctionnera depuis remoteX.remote.test.



Exercice de Questionnaire

Traduction d'adresses réseau - Questionnaire

1. Les chaînes disponibles dans la table **filter** sont **INPUT**, **FORWARD** et **OUTPUT**
2. Les chaînes disponibles dans la table **nat** sont **PREROUTING**, **POSTROUTING** et **OUTPUT**
3. **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**
4. **iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.0.1**
5. **iptables -t nat -A PREROUTING -i eth0 -m tcp -p tcp --dport 80 -j DNAT --to-destination 192.168.0.100:8080**
6. La cible **DNAT** peut uniquement être utilisée dans la chaîne **PREROUTING** et la chaîne **OUTPUT** de la table **nat**.
7. Pour activer le transfert permanent d'un redémarrage à l'autre, ajoutez **net.ipv4.ip_forward=1** à **/etc/sysctl.conf** et exécutez **sysctl -p**.



Test

Test de critère

Étude de cas

L'entreprise de fournitures de pêche Morris Worm and Fish Supply

Avant de commencer...

Important : n'oubliez pas d'exécuter le script **lab-setup-morrisworm** sur desktopX avant de commencer ! Le script **lab-setup-morrisworm** configurera serverX pour qu'il s'exécute sur un réseau privé.

L'entreprise Morris Worm and Fish Supply a enfin décidé de moderniser son activité en ouvrant un site Web. Le serveur Web fonctionnera sur un réseau privé derrière un pare-feu. Le pare-

feu transférera tout le trafic sur le port TCP 80 au serveur Web et il effectuera une traduction d'adresses réseau (NAT) pour que le serveur Web puisse atteindre les hôtes externes.

- desktopX.example.com sera le pare-feu et serverX.example.com sera le serveur Web.
- Configurez Apache pour qu'il s'exécute sur serverX.example.com. Placez du contenu personnalisé dans **/var/www/html/index.html** pour identifier de façon exclusive le serveur.
- Configurez le pare-feu sur desktopX pour qu'il effectue une traduction d'adresses réseau, ce qui permettra au serveur Web d'accéder au réseau extérieur. Vous pourrez envoyer une requête **ping** à instructor.example.com depuis serverX pour vérifier que cela fonctionne.
- Configurez enfin le pare-feu pour qu'il transfère tout le trafic sur le port TCP 80 qui lui est envoyé au serveur Web fonctionnant sur serverX. Vous devrez identifier l'adresse IP de serverX pour effectuer cette étape. Vérifiez que cela fonctionne en utilisant un navigateur Web depuis une machine externe, et NON depuis desktopX, pour accéder à http://desktopX.example.com.

Une fois que vous avez réussi l'exercice, exécutez **lab-cleanup-morrisworm** sur desktopX pour rétablir l'état d'origine de votre réseau.

1. Déterminez l'adresse IP de serverX

```
[root@serverX ~]# ip a show eth0
```

2. Déployez un server Web sur serverX

```
[root@serverX ~]# yum install httpd
[root@serverX ~]# service httpd start ; chkconfig httpd on
[root@serverX ~]# echo serverX > /var/www/html/index.html
```

3. Sur desktopX, définissez **net.ipv4.ip_forward=1**.

```
[root@desktopX ~]# sysctl -w net.ipv4.ip_forward=1
```

4. Sur desktopX ajoutez ces règles au pare-feu (remplacez 192.168.122.Z par l'adresse IP trouvée à la première étape.

```
[root@desktopX ~]# NewServerIP=192.168.122.Z
[root@desktopX ~]# iptables -t nat -A POSTROUTING -s ${NewServerIP} -j MASQUERADE
[root@desktopX ~]# iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-
destination ${NewServerIP}
```

Configuration du serveur NTP



Exercice de Questionnaire

Configuration NTP - Questionnaire

Répondez aux questions ci-dessous en vous basant sur le fichier de configuration NTP suivant:

```
#/etc/ntp.conf

restrict default kod nomodify notrap nopeer noquery
restrict -6 default ignore

restrict 192.168.0.0 mask 255.255.255.0 nomodify notrap nopeer
restrict 192.168.0.101 kod nomodify notrap
restrict 192.168.0.200

server 192.168.0.2
server 192.168.0.3
peer 192.168.0.101
```

1. L'heure du client NTP est décalée de 15 minutes, elle se synchronisera plus tard avec les serveurs.

   (sélectionnez une des réponses suivantes...)

   a. Vrai
   b. Faux

2. Le client NTP utilisera le RTC (BIOS) de l'ordinateur comme source horaire.

   (sélectionnez une des réponses suivantes...)

   a. Vrai
   b. Faux

3. 192.168.0.200 pourra modifier l'heure sur ce serveur NTP.

   (sélectionnez une des réponses suivantes...)

   a. Vrai
   b. Faux

4. 192.168.0.4 pourra interroger ce serveur NTP.

   (sélectionnez une des réponses suivantes...)

   a. Vrai
   b. Faux

5. 192.168.0.3 pourra utiliser ce serveur NTP en tant que pair.

   (sélectionnez une des réponses suivantes...)

   a. Vrai
   b. Faux

6. Quiconque avec une adresse IPv4 pourra utiliser ce serveur NTP comme source horaire.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux

7. Quiconque avec une adresse IPv6 pourra utiliser ce serveur NTP comme source horaire.

   (sélectionnez une des réponses suivantes...)
   a. Vrai
   b. Faux



Test
Test de critère

Étude de cas
Configuration du serveur NTP

Avant de commencer...

Exécutez **`lab-setup-howsonclock`** sur desktopX.

Howson Heavy Machine and Clock Manufacture, un fabricant de pièces et d'accessoires pour horloges de clocher, a récemment effectué un audit de tous ses systèmes informatiques. L'audit a révélé que les horloges de plusieurs systèmes n'étaient pas synchronisées, y compris celle de la machine serverX.example.com.

Configurez NTP sur serverX pour que celui-ci soit un client du service NTP exécuté sur instructor.example.com.

Pour disposer de sources horaires supplémentaires, travaillez avec vos voisins pour que tous les systèmes serverX soient configurés pour se synchroniser comme pairs NTP.

Lorsque vous avez terminé, exécutez **`lab-grade-howsonclock`** sur desktopX pour vérifier votre travail.

1. Identifiez deux ou trois machines paires. Dans la classe, vous êtes encouragé à choisir un voisin comme pair, bien que ces instructions utiliseront à la place les 3 machines assignées comme pairs : desktop1 (192.168.1) et host1 (192.168.0.201) pour le serveur fonctionnant sur server1 (192.168.0.101).

   Créez le fichier de configuration **`/etc/ntp.conf`** suivant et distribuez-le aux 3 machines.

```
driftfile /var/lib/ntp/drift

restrict default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict 192.168.0.0 mask 255.255.255.0

server 192.168.0.254
peer 192.168.0.1
```

```
peer 192.168.0.101
peer 192.168.0.201
```

Sur chacune des machines, modifiez le fichier pour omettre la machine de la liste des pairs. Par exemple, sur desktop1, supprimez la ligne pour 192.168.0.1.

2. Sur chacune des machines, activez et démarrez le service ntp.

```
[root@server1 ~]# service ntpd restart
[root@server1 ~]# ssh desktop1 service ntpd restart
[root@server1 ~]# ssh host1 service ntpd restart
[root@server1 ~]# chkconfig ntpd on
[root@server1 ~]# ssh dekstop1 chkconfig ntpd on
[root@server1 ~]# ssh host1 chkconfig ntpd on
```

3. Pour chacune des machines, utilisez la commande **ntpq -p** pour contrôler les interactions du service NTP avec ses pairs. Pendant les 5-10 premières minutes, vous devriez normalement voir une sortie similaire à ce qui suit.

```
[root@server1 ~]# ntpq -p
remote           refid           st t when poll reach   delay   offset  jitter
==============================================================================
*instructor.exam LOCAL(0)        11 u   64   64   17    0.533   -0.096   0.223
 desktop1.exampl .INIT.          16 u   19   64    0    0.000    0.000   0.000
 server101.examp .INIT.          16 u   48   64    0    0.000    0.000   0.000
```

Conseil : la commande **watch** peut être utile pour contrôler le processus d'association de pairs. Dans chacun des trois terminaux, exécutez une commande shell vers chacune des trois machines et exécutez la commande **watch -d ntpq -p**. Utilisez **CTRL-C** pour annuler la commande **watch** lorsqu'elle a terminé.

4. Après 5-10 minutes, les services NTP doivent se reconnaître comme pairs, comme l'indique la sortie de la commande **ntpq -p**.

```
[root@server1 ~]# ntpq -p
remote           refid           st t when poll reach   delay   offset  jitter
==============================================================================
*instructor.exam LOCAL(0)        11 u   61   64   77    0.327    0.083   0.028
+desktop1.exampl 192.168.0.254   12 u    6   64   77    0.392    0.034   0.011
 server101.examp 192.168.0.254   12 u   36   64    2    0.420   -0.057   0.000
```

Notez que la colonne « st », signifiant « strate », ne considère plus les pairs comme totalement non fiables (strate 16) elle les considère désormais comme étant d'une strate au-dessus de la meilleure source horaire (strate 12), soit instructor.example.com.

Service de journalisation système



Exercice de Étude de cas

Rapports d'utilisation

Utilisez l'outil que vous avez examiné pour créer un rapport simple qui consigne les informations dans un fichier.

Une fois que vous avez utilisé l'outil pour générer un rapport, l'instructeur vous demandera de présenter la commande que vous avez utilisée et le résultat que vous avez obtenu au reste de la classe.

-
```
[root@serverX] ~]# df -h
[root@serverX] ~]# iostat -dNk 2 10
[root@serverX] ~]# vmstat 2 10
```



Exercice de Exercice

Journalisation distante

1. Configurez serverX pour qu'il accepte les messages de journaux distants à l'aide de TCP.

   Annulez les commentaires des lignes suivantes de la section MODULES de **/etc/rsyslog.conf**:

   ```
   $ModLoad imtcp.so
   $InputTCPServerRun 514
   ```

   Redémarrez **rsyslog**.

   ```
   [root@serverX ~]# service rsyslog restart
   ```

2. Configurez desktopX pour qu'il envoie tous les événements de priorité **info** et supérieure à serverX avec TCP.

   Ajoutez la ligne suivante à la section RULES de **/etc/rsyslog.conf**:

   ```
   *.info     @@192.168.0.X+100
   ```

   Redémarrez **rsyslog**.

   ```
   [root@serverX ~]# service rsyslog restart
   ```

3. Testez votre configuration.

   ```
   [root@desktopX ~]# logger Test from desktopX
   [root@desktopX ~]# tail /var/log/messages
   ```

```
Dec 25 00:00:01 desktopX root: Test from desktopX
[root@serverX ~]# tail /var/log/messages
Dec 25 00:00:01 desktopX root: Test from desktopX
```



Test

Test de critère

Étude de cas

Contrôle du système et journaux

Avant de commencer...

Avant de commencer, exécutez le script **lab-setup-blossoms** sur desktopX.

Blossoms, Inc. est une coopérative de floriculteurs aux États-Unis. La coopérative assure notamment des services informatiques pour tous ses membres. Son responsable informatique a décidé de renforcer la sécurité en exigeant la mise en œuvre de la journalisation distante sur tous les serveurs, y compris le vôtre (serverX).

Configurez rsyslog sur desktopX pour accepter les messages de journaux distants provenant de serverX via UDP. Puis configurez **rsyslog** sur serverX pour envoyer tous les messages de journaux ***.info** à desktopX via UDP.

Avant de vérifier votre travail, exécutez **lab-grade-blossoms** sur serverX, puis exécutez **lab-grade-blossoms** sur desktopX.

1. Sur desktopX, modifiez **/etc/rsyslog.conf** en supprimant le commentaire des lignes 13 et 14.

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514
```

2. Sur desktopX, redémarrez le service rsyslog.

```
[root@desktopX ~]# service rsyslog restart
```

3. Sur desktopX, confirmez que **rsyslogd** est lié au port externe UDP 514.

```
[root@desktopX ~]# lsof -i -n -P | grep rsyslogd
rsyslogd  2253    root    3u  IPv4  16673      0t0  UDP *:514
rsyslogd  2253    root    4u  IPv6  16674      0t0  UDP *:514
```

4. Sur serverX, modifiez le fichier **/etc/rsyslog.conf**. Insérez la ligne suivante en remplaçant « X » par le numéro de votre station de travail. Bien que l'emplacement ait peu d'importance, il est judicieux d'insérer la ligne autour de la ligne 39, près de la configuration « info » existante.

```
*.info                                  @desktopX.example.com
```

Sur serverX, redémarrez le service rsyslogd.

```
[root@serverX ~]# service rsyslog restart
```

5. Sur desktopX, examinez le champ du nom d'hôte (juste après la date) dans les messages de journaux distants récents pour vérifier que les messages de journaux relatifs à l'initialisation de rsyslog ont été reçus de serverX.

```
[root@desktopX ~]# tail -n 4 /var/log/messages
Dec  9 13:43:39 desktop1 ntpd[1547]: kernel time sync status change 2001
Dec  9 13:50:07 desktop1 ntpd[1547]: synchronized to 192.168.0.254, stratum 3
Dec  9 06:55:25 server1 kernel: imklog 4.6.2, log source = /proc/kmsg started.
Dec  9 06:55:25 server1 rsyslogd: [origin software="rsyslogd" swVersion="4.6.2" x-
pid="24482" x-info="http://www.rsyslog.com"] (re)start
```

Service Web



Exercice de Liste de contrôle des performances

Principes de base Apache avec mod_ssl

Déployez un serveur Web Apache encapsulé avec SSL sur serverX. Il doit utiliser le certificat SSL auto-signé par défaut.

- ☐ Connectez-vous à serverX en tant que super utilisateur.

- ☐ Installez le package (**httpd**) du serveur Web Apache, si nécessaire.

```
[root@serverX ~]# yum install -y httpd
```

- ☐ Installez le package **mod_ssl**.

```
[root@serverX ~]# yum install -y mod_ssl
```

- ☐ Examinez le fichier de configuration **/etc/httpd/conf.d/ssl.conf** fourni par le package **mod_ssl**.

  - Quelle directive Apache pointe vers le certificat SSL ?

  - Quelle est sa valeur ?

```
[root@serverX ~]# less /etc/httpd/conf.d/ssl.conf
...
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/localhost.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
...
```

- ☐ Relancez le service **httpd**.

```
[root@serverX ~]# service httpd restart
```

- ☐ Lancez Firefox et accédez à https://serverX.example.com. Lorsque Firefox affiche un avertissement, effectuez les opérations suivantes pour examiner le certificat avec ce navigateur.

- Cliquez sur le lien « Je comprends les risques ».
- Cliquez sur le bouton « Ajouter des exceptions... », puis cliquez sur « Afficher... » lorsque l'option devient active.
- Consultez les informations présentées dans les onglets « Général » et « Détails ».
- Cliquez sur « Fermer » lorsque vous avez fini d'examiner les informations relatives au certificat.



Exercice de Liste de contrôle des performances

Configurer des hôtes virtuels basés sur le nom

Pour cet exercice, wwwX.example.com est déjà configuré en tant qu'alias **CNAME** de serverX.example.com.

Au terme de la liste de contrôle, vous exécuterez un script de notation, par conséquent assurez-vous que votre serveur Web sert le contenu exactement comme il est décrit dans la procédure.

- ☐ Créez **/var/www/html/index.html** contenant le texte « **this is serverX** ».

```
[root@serverX ~]# echo this is serverX. > /var/www/html/index.html
```

- ☐ Depuis desktopX, utilisez Firefox pour vérifier que les sites Web wwwX, wwwX.example.com, serverX et serverX.example.com affichent tous votre **index.html** personnalisé.
- ☐ Créez **/wwwX/html/index.html** contenant le texte « **this is wwwX** ».

```
[root@serverX ~]# mkdir -p /wwwX/html
[root@serverX ~]# echo this is wwwX. > /wwwX/html/index.html
```

- ☐ Modifiez la configuration d'Apache pour activer l'hébergement virtuel basé sur le nom. serverX et serverX.example.com doivent servir **/var/www/html/index.html** comme page principale. wwwX et wwwX.example.com doivent servir **/wwwX/html/index.html** comme page principale.

  Ajoutez le contenu suivant à la fin de **/etc/httpd/conf/httpd.conf**:

```
# Enable name-based virtual hosting:
NameVirtualHost *:80

# serverX virtual host configuration
<VirtualHost *:80>
    ServerName serverX.example.com
    ServerAlias serverX
    ServerAdmin webmaster@serverX.example.com
    DocumentRoot /var/www/html
    ErrorLog logs/serverX.example.com-error_log
    CustomLog logs/serverX.example.com-access_log common
</VirtualHost>
```

```
# wwwX virtual host configuration
<VirtualHost *:80>
    ServerName wwwX.example.com
    ServerAlias wwwX
    ServerAdmin webmaster@wwwX.example.com
    DocumentRoot /wwwX/html
    ErrorLog logs/wwwX.example.com-error_log
    CustomLog logs/wwwX.example.com-access_log common
</VirtualHost>
```

Indiquez au serveur Apache de recharger sa configuration :

```
[root@serverX ~]# service httpd reload
```

- ☐ Ne désactivez pas SELinux (conseil : il peut être nécessaire de modifier la base de données des contextes de fichiers SELinux ou de changer le type SELinux de certains fichiers).

```
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/wwwX(/.*)?'
[root@serverX ~]# restorecon -vFR /wwwX
```

- ☐ Lorsque vous avez terminé, exécutez le script d'évaluation **`lab-grade-virthost`** à partir de serverX pour vous assurer que tout est correct.

```
[root@serverX ~]# lab-grade-virthost
Good, www1 works
Good, www1.example.com works
Good, server1 works
Good, server1.example.com works
Grading PASSED!
```



Exercice de Questionnaire

Questionnaire CGI Apache

1. CGI signifie

   (sélectionnez une des réponses suivantes...)

   a. Content Generated Interface
   b. Command Gateway Interface
   c. Common Generated Interface
   d. Common Gateway Interface

2. Le dernier argument dans **`ScriptAlias /cgi-bin/ /my/private/cgi-bin/`** est

   (sélectionnez une des réponses suivantes...)

   a. relatif à **`DocumentRoot`**
   b. relatif à **`/var/www/`**
   c. relatif à **`ServerRoot`**
   d. un chemin absolu sur le système de fichiers

3. Le **ScriptAlias** par défaut dans **/etc/httpd/conf/httpd.conf** pointe sur ...

(sélectionnez une des réponses suivantes...)

a. /var/www/cgi-bin
b. /var/html/cgi-bin
c. /cgi-bin
d. /var/www/html/cgi-bin

4. L'un des types de contexte SELinux intégré pour un programme CGI générique est

(sélectionnez une des réponses suivantes...)

a. **httpd_t**
b. **httpd_sys_script_exec_t**
c. **script_t**
d. **httpd_content_t**

5. Le processus Apache nécessite que les autorisations du système de fichiers suivantes soient sur les programmes CGI

(sélectionnez une des réponses suivantes...)

a. **---**
b. **r--**
c. **r-x**
d. **rwx**



Exercice de Liste de contrôle des performances

Configurer l'authentification LDAP

Vous allez configurer le serveur Web sur serverX avec une URL **/private** à laquelle les utilisateurs dans l'annuaire LDAP sur instructor.example.com peuvent accéder.

- ☐ Configurez l'authentification LDAP sur serverX en utilisant instructor.example.com comme serveur LDAP et **dc=example,dc=com** comme nom distinctif de base, et utilisez le certificat trouvé dans *ftp://instructor/pub/example-ca.crt*. Choisissez des mots de passe LDAP.

  Exécutez **system-config-authentication** sur serverX. Choisissez **LDAP** dans le menu déroulant **Base de données des comptes d'utilisateur**. Entrez **ldap://instructor.example.com/** comme serveur LDAP. Téléchargez le certificat depuis *ftp://instructor/pub/example-ca.crt*. Choisissez le mot de passe LDAP comme **méthode d'authentification**.

- ☐ Connectez-vous en tant que **root** (super utilisateur) sur serverX. Créez un nouveau répertoire **/var/www/html/private**.

```
[root@serverX ~]# mkdir /var/www/html/private
```

- ☐ Dans le répertoire **private**, créez un **index.html** contenant le texte **Private Data**.

```
[root@serverX ~]# echo "Private Data" > /var/www/html/private/index.html
```

- ☐ Téléchargez **ftp://instructor/pub/example-ca.crt** et placez-le dans **/etc/httpd**.

```
[root@serverX ~]# wget ftp://instructor/pub/example-ca.crt -O /etc/httpd/example-ca.crt
```

- ☐ Modifiez **/etc/httpd/conf/httpd.conf** et ajoutez l'authentification LDAP pour le répertoire **private**.

```
LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/example-ca.crt

<Directory /var/www/html/private>
    AuthName "Secret Stuff"
    AuthType  basic
    AuthBasicProvider ldap
    AuthLDAPUrl "ldap://instructor.example.com/dc=example,dc=com" TLS
    Require valid-user
</Directory>
```

Ajoutez la strophe ci-dessus au bas du fichier **/etc/httpd/conf/httpd.conf**.

- ☐ Redémarrez Apache.

```
[root@serverX ~]# service httpd restart
```

- ☐ Accédez à http://serverX.example.com/private. Une boîte de dialogue d'authentification doit normalement s'afficher. Si ce n'est pas le cas, fermez toutes les fenêtres du navigateur, vérifiez votre configuration et réessayez.

```
[root@serverX ~]# elinks http://serverX.example.com/private
```

- ☐ Connectez-vous en tant qu'utilisateur **ldapuserX** avec le mot de passe **password**.

Dans la boîte de dialogue qui s'affiche, entrez le nom d'utilisateur et le mot de passe ci-dessus.



Exercice de Questionnaire

Résolution des problèmes liés à Apache - Questionnaire

1. Complétez la commande suivante pour répertorier tous les contextes de port : **semanage** port **-l**.

2. Complétez la commande suivante pour qu'Apache utilise le port TCP 8001 : **semanage** port -a **-t httpd_port_t** -p tcp **8001**.

3. Les deux directives du fichier de configuration Apache pour spécifier la gravité (détails) des messages d'erreur et le fichier dans lequel consigner les erreurs sont LogLevel et ErrorLog.

4. La directive du fichier de configuration Apache pour spécifier le format et l'emplacement du contenu auquel les clients peuvent accéder est CustomLog.

5. Les messages AVC complets (bruts) SELinux sont transmis à **/var/log**/audit/audit.log.

6. Pour que SELinux fournisse plus de détails, vous pouvez exécuter **semanage** dontaudit **off**.

7. Les commandes pour obtenir et définir les booléens SELinux sont getsebool et setsebool.

8. **man** httpd_selinux présente une page man SELinux spécifique à Apache.

9. **man -k** _selinux répertorie toutes les pages man SELinux spécifiques aux services.

10. L'option **-F** de la commande **restorecon** réinitialise les types personnalisables.



Test

Test de critère 1

Étude de cas

Services Web encapsulés dans SSL

Avant de commencer...

Exécutez le script **lab-setup-hacker** sur desktopX.

Marcelo Hacker est un détective privé réputé. En fait, cela marche tellement bien pour lui qu'il lui est difficile de trouver le temps de rencontrer des clients potentiels. M. Hacker a décidé de créer un site Web sur lequel ses clients potentiels pourront lui envoyer des messages. La confidentialité étant un élément essentiel dans le secteur de l'enquête privée, le site Web doit utiliser un certificat SSL signé.

- Configurez Apache sur serverX pour qu'il chiffre le site Web de Marcelo Hacker avec SSL.
- Vous trouverez un certificat SSL signé pour le serveur et la clé correspondante à l'emplacement suivant: **/net/instructor/var/ftp/pub/materials/tls**. Sous ce répertoire, **certs/serverX.crt** contient le certificat signé pour le serveur et **private/serverX.key** contient la clé privée correspondante.

  Déployez le certificat signé pour Apache sur serverX. Laissez le site Web par défaut réservé pour le contenu. M. Hacker téléchargera ce contenu personnalisé ultérieurement.

Une fois toutes ces opérations effectuées, exécutez le script **lab-grade-hacker** sur desktopX pour vérifier votre travail.

1. Assurez-vous que le package mod_ssl est installé.

```
[root@serverX ~]# yum install mod_ssl
```

2. Copiez le certificat signé et la clé correspondante se trouvant dans le répertoire « pub » de l'instructeur et déployez-les dans les emplacements appropriés au sein du répertoire **/etc/pki/tls**. Vérifiez qu'ils sont lisibles par l'utilisateur Apache et que le contexte SELinux approprié leur est affecté.

```
[root@serverX ~]# cd /net/instructor/var/ftp/pub/materials/tls/
[root@serverX tls]# cp certs/serverX.crt /etc/pki/tls/certs/
[root@serverX tls]# cp private/serverX.key /etc/pki/tls/private/
[root@serverX tls]# cd /etc/pki/tls/
[root@serverX tls]# ls -lZ certs/serverX.crt private/serverX.key
-rw-r--r--. root root unconfined_u:object_r:cert_t:s0  certs/serverX.crt
-rw-r--r--. root root unconfined_u:object_r:cert_t:s0  private/serverX.key
```

3. Vérifiez que le nom courant du certificat convient pour le serveur.

```
[root@serverX tls]# openssl x509 -text < certs/serverX.crt | grep Subject:
    Subject: C=US, ST=North Carolina, O=Example, Inc., CN=serverX.example.com
```

4. Mettez à jour le fichier de configuration **/etc/httpd/conf.d/ssl.conf** du serveur, autour de la ligne 100, en définissant SSLCertificateFile et SSLCertifcateKeyFile de sorte qu'ils fassent référence au certificat et à la clé nouvellement installés.

```
...
#SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateFile /etc/pki/tls/certs/serverX.crt
...
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
SSLCertificateKeyFile /etc/pki/tls/private/serverX.key
...
```

5. Redémarrez le service Web. Notez qu'un arrêt FAILED indique simplement un service qui n'a probablement jamais démarré.

```
[root@serverX tls]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

6. (Facultatif) Utilisez la commande **curl** pour vous assurer que les clients peuvent vérifier les connexions chiffrées avec votre serveur. Ce qui vous intéresse ce n'est pas le contenu mais que **curl** peut télécharger et vérifier le certificat sans problème.

```
[root@serverX tls]# CACERT=/net/instructor/var/ftp/pub/example-ca.crt
[root@serverX tls]# curl --cacert $CACERT https://serverX.example.com > /dev/null
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
102  3985  102  3985    0     0  62741      0 --:--:-- --:--:-- --:--:-- 1297k
```

7. Afin de vérifier que le navigateur Web Firefox peut authentifier les connexions chiffrées avec votre serveur, installez d'abord le certificat de l'autorité de certification locale en utilisant Firefox pour ouvrir *http://instructor/pub/example-ca.crt*.

   Dans la boîte de dialogue qui s'affiche, acceptez l'autorité de certification qui identifiera (au moins) les sites Web.

   Accédez à *https://serverX.example.com*. Firefox doit vérifier le site en utilisant « Example, Inc. ». Vous pouvez le vérifier en plaçant le curseur sur le préfixe example.com dans la barre d'adresse.



Test

Test de critère 2

Étude de cas

Configuration supplémentaire du serveur Web

Avant de commencer...

Exécutez le script **`lab-setup-website`** sur desktopX.

Example Industries, une entreprise performante, a besoin d'un nouveau site Web. En fait, elle en a besoin de deux ! L'un sera le site Web de l'entreprise et l'autre servira au test du contenu. En outre, le site Web de l'entreprise devra comporter une zone protégée par mot de passe et une application CGI spéciale devra y être installée.

Sur la machine serverX, déployez un serveur Web avec deux hôtes virtuels.

Hôte virtuel1 : *http://serverX.example.com*

- Créez une page simple réservée à l'URL de base

Hôte virtuel2 : *http://wwwX.example.com*

- Créez une page simple réservée à l'URL de base différente de celle utilisée sur l'hôte virtuel1.
- Protégez la zone *http://wwwX.example.com/private* par un mot de passe
- Ajoutez l'utilisateur **`forrest`** avec le mot de passe **`trees`** à **`/private`**
- Téléchargez le fichier CGI ftp://instructor.example.com/pub/gls/special.cgi et installez-le en tant que *http://wwwX.example.com/cgi-bin/special.cgi*

Avant de vérifier votre travail, exécutez le script de notation **`lab-grade-website`** sur desktopX.

1. Créez un répertoire qui servira de DocumentRoot pour le site Web virtuel.

```
[root@serverX ~]# mkdir -p /var/www/virtual/wwwX/html
```

2. Créez des « pages personnelles » réservées pour chacun des sites en créant un fichier **`index.html`** distinct dans leurs DocumentRoot respectifs.

```
[root@serverX ~]# echo server > /var/www/html/index.html
[root@serverX ~]# echo www > /var/www/virtual/wwwX/html/index.html
```

3. Créez le fichier de configuration minimale **/etc/httpd/conf.d/virtual.conf** suivant, qui contient les définitions des hôtes virtuels. Le nom du fichier n'a aucune importance tant qu'il correspond à **/etc/httpd/conf.d/*.conf**.

```
NameVirtualHost 192.168.0.101

<VirtualHost 192.168.0.101>
        ServerName serverX.example.com
        ServerAlias serverX s1
</VirtualHost>

<VirtualHost 192.168.0.101>
        ServerName wwwX.example.com
        ServerAlias wwwX
        DocumentRoot /var/www/virtual/wwwX/html
</VirtualHost>
```

4. Redémarrez le serveur et vérifiez que les deux hôtes virtuels servent le contenu attendu.

```
[root@serverX ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@serverX ~]# curl http://serverX.example.com
server
[root@serverX ~]# curl http://wwwX.example.com
www
```

5. Créez une zone privée pour votre site virtuel et créez du contenu test pour cette zone.

```
[root@serverX ~]# mkdir -p /var/www/virtual/wwwX/html/private
[root@serverX ~]# echo "sssshhhhh" > /var/www/virtual/wwwX/html/private/secret
```

6. Ajoutez la strophe de contexte suivante au fichier de configuration **virtual.conf**.

```
<Directory /var/www/virtual/wwwX/html/private>

        AuthName "Secret Hideout"
        AuthType basic

        AuthUserFile /etc/httpd/users
        require valid-user

        Options +Indexes

</Directory>
```

Notez qu'il n'est pas demandé ici d'activer l'accès aux répertoires mais de simuler le comportement par défaut du « serveur réel ». Surtout, cela facilitera la tâche du script de notation.

7. Redémarrez le serveur et vérifiez que la strophe de contexte produit l'effet voulu.

```
[root@serverX ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@serverX ~]# curl http://wwwX.example.com/private/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Authorization Required</title>
</head><body>
...
```

8. Créez l'utilisateur Web spécifié et le mot de passe.

```
[root@serverX ~]# htpasswd -cm /etc/httpd/users forrest
New password: trees
Re-type new password: trees
Adding password for user forrest
```

9. Vérifiez que l'utilisateur spécifié peut accéder à la zone privée.

```
[root@serverX ~]# curl http://forrest:trees@wwwX.example.com/private/secret
sssshhhhh
```

10. Étirez-vous et respirez à fond.

11. Dans **/etc/httpd/conf.d/virtual.conf**, ajoutez la directive ScriptAlias suivante dans la strophe relative à wwwX VirtualHost.

```
<VirtualHost 192.168.0.101>
        ServerName wwwX.example.com
        ServerAlias wwwX
        DocumentRoot /var/www/virtual/wwwX/html
        ScriptAlias /cgi-bin/  "/var/www/virtual/wwwX/cgi-bin/"
</VirtualHost>
```

12. Redémarrez le serveur pour que la nouvelle configuration prenne effet.

```
[root@serverX ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

13. Créez le répertoire **cgi-bin** spécifié. Téléchargez l'exécutable CGI spécifié, installez-le dans le nouveau répertoire et rendez-le exécutable.

```
[root@serverX ~]# mkdir -p /var/www/virtual/wwwX/cgi-bin
[root@serverX ~]# curl http://instructor/pub/gls/special.cgi > /var/www/virtual/wwwX/
cgi-bin/special.cgi
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0    77    0    77    0     0  17416      0 --:--:-- --:--:-- --:--:-- 77000
[root@serverX ~]# chmod 755 /var/www/virtual/wwwX/cgi-bin/special.cgi
```

14. Vérifiez que vous pouvez exécuter en local l'exécutable CGI.

```
[root@serverX ~]# /var/www/virtual/wwwX/cgi-bin/special.cgi
Content-Type: text-html

<h1>Hello world</h1>
```

15. Vérifiez que l'exécutable CGI est accessible à l'URL spécifiée.

```
[root@serverX ~]# curl http://wwwX/cgi-bin/special.cgi
<h1>Hello world</h1>
```

16. Remarque : étant donné que nous avons choisi de nous conformer aux emplacements de répertoires enregistrés dans la stratégie SELinux pour le contenu des hôtes virtuels, les nouveaux fichiers obtiennent automatiquement le contexte SELinux correct. Si nous avions choisi d'autres emplacements, nous aurions été obligés d'ajuster en conséquence les types SELinux. L'approche la plus simple serait de copier les types SELinux à partir des emplacements de serveur de base « approuvés ».

```
[root@serverX ~]# cd /var/www/virtual/wwwX/
[root@serverX wwwX]# chcon -R --reference /var/www/html html/
[root@serverX wwwX]# chcon -R --reference /var/www/cgi-bin cgi-bin/
[root@serverX wwwX]# ls -lZ
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
```

Configuration SMTP de base



Exercice de Étude de cas

Configuration Intranet

Avant de commencer...

DNS a déjà été configuré pour que vos hôtes soient membres du domaine **`domainX.example.com`**.

nom d'hôte	adresse IP	également connu comme
mail.domainX.example.com	192.168.0.X+100	(serverX.example.com)
smtp.domainX.example.com	192.168.0.X+200	(hostX.example.com)
desktop.domainX.example.com	192.168.0.X	(desktopX.example.com)

Tableau A.1. domainX.example.com

En outre, l'hôte mail.domainX.example.com est le destinataire **`MX`** du domaine domainX.example.com entier.

Complétez le tableau suivant avec les directives appropriées pour configurer ces hôtes afin qu'ils servent de serveurs de boîtes aux lettres intranet, d'hôte smtp et de station cliente, respectivement.

Essayez de n'utiliser que les fichiers **`BASIC_CONFIGURATION_README`**, **`STANDARD_CONFIGURATION_README`** et **`main.cf`** comme référence.

Une fois que vous avez terminé, demandez à un autre étudiant de vérifier votre travail.

DNS externe

```
domainX.example.com.      IN MX 10    mail.domainX.example.com.
```

Concept	Directive	*mail.domainX*	*desktop.domainX*	*smtp.domainX*
Interface de liaison	*inet_interfaces*			
Masquage en tant que	*myorigin*			
Remise indirecte	*relayhost*			
Recevoir le courrier pour ...	*mydestination*			
Remise locale	*local_transport*			
Relais depuis ...	*mynetworks*			

Tableau A.2. Configuration de la messagerie Intranet pour domainX.example.com

•



Test

Test de critère

Étude de cas

Configuration de la messagerie Intranet

Avant de commencer...

Avant de commencer, exécutez le script **`lab-setup-email`** sur desktopX.

L'entreprise Hoffman Hair Supply, un fabricant de produits de soins capillaires, veut centraliser la gestion de sa messagerie interne.

DNS a déjà été configuré pour que vos machines soient membres du domaine DNS **`domainX.example.com`** avec les adresses suivantes :

```
192.168.0.X      desktop.domainX.example.com   (a.k.a.  desktopX.example.com)
192.168.0.X+100     mail.domainX.example.com   (a.k.a.   serverX.example.com)
192.168.0.X+200     smtp.domainX.example.com   (a.k.a. hostX.example.com)
```

En outre, le serveur **`mail.domainX.example.com`** est le destinataire **`MX`** du domaine **`domainX.example.com`** entier.

Configurez l'hôte **`mail.domainX.example.com`** pour qu'il se comporte comme un serveur de courrier entrant uniquement. Ainsi, tout le courrier remis au domaine **`@domainX.example.com`** est stocké sur ce serveur.

Configurez le serveur **`smtp.domainX.example.com`** pour qu'il se comporte comme un serveur SMTP de courrier sortant et dont la mission est de transmettre le courrier des membres du domaine **`domainX.example.com`** aux réseaux extérieurs.

Configurez l'hôte **`desktop.domainX.example.com`** pour qu'il se comporte comme un « client null ». Il ne peut pas recevoir le courrier du réseau, la remise du courrier local est désactivée et tout le courrier sortant est envoyé indirectement via **`smtp.domainX.example.com`**.

Pour les trois hôtes, assurez-vous que le courrier entrant masque le domaine de l'expéditeur en tant que **`domainX.example.com`**.

Lorsque vous avez terminé, exécutez le script **`lab-grade-email`** pour vérifier votre travail.

1. Ces instructions feront référence à vos trois machines dans le contexte de l'exercice, *desktop.domainX.example.com*, *mail.domainX.domainX.eample.com* et *smtp.domainX.example.com*, bien que les noms d'hôte *desktopX*, *serverX* et *hostX*, respectivement, puissent continuer à être utilisés.

   Le nom de ces machines sera en général abrégé en *desktop*, *mail* et *smtp*, *domainX.example.com* étant sous-entendu.

   Sur *desktop.domainX.example.com* (*desktopX*), confirmez que DNS a été correctement préconfiguré pour votre domaine, en demandant un « extrait » du domaine

domainX.example.com. (Remarque : dans la réalité la plupart des serveurs DNS ne permettent pas aux clients d'extraire un domaine entier.)

```
[root@desktop1 ~]# host -al domainX.example.com
...
;; QUESTION SECTION:
;domainX.example.com.           IN      AXFR

;; ANSWER SECTION:
domainX.example.com.    86400   IN      SOA     instructor.example.com.
 root.instructor.example.com. 2009062000 3600 300 604800 60
domainX.example.com.    86400   IN      NS      instructor.example.com.
domainX.example.com.    86400   IN      MX      10 mail.domainX.example.com.
desktop.domainX.example.com. 86400 IN   A       192.168.0.X
mail.domainX.example.com. 86400 IN      A       192.168.0.X+100
smtp.domainX.example.com. 86400 IN      A       192.168.0.X+200
domainX.example.com.    86400   IN      SOA     instructor.example.com.
 root.instructor.example.com. 2009062000 3600 300 604800 60
...
```

Vérifiez surtout les enregistrements A de *desktop*, *mail* et *smtp* qui effectuent le mappage vers les adresses IP *domainX*, *serverX* et *hostX* et l'enregistrement MX qui établit *mail.domainX.example.com* comme « destinataire MX » pour le domaine domainX.example.com entier. Les autres entrées DNS peuvent être ignorées sans aucun risque.

2. Afin de contrôler votre progression, il est utile de consulter le **/var/log/maillog** sur chacune des trois machines. À cet égard, nous vous suggérons d'ouvrir 3 terminaux sur la machine *desktop*. Conservez un shell local sur un terminal et ouvrez un shell distant vers *mail* et *smtp* dans les deux autres. Dans chacun des terminaux, exécutez **less -F /var/log/messages**. (Cela place **less** dans le comportement « tail -f », ce qui permet d'utiliser **CTRL-C** pour rétablir le comportement **less** « normal », et **F** pour reprendre la suite du fichier.)

3. Premièrement, configurez *mail* pour qu'il soit le destinataire MX du domaine *domainX.example.com*. Toutes les étapes suivantes doivent être exécutées sur *mail.domainX.example.com*.

   a. Assurez-vous que le « postfix » est installé, qu'il a démarré et qu'il est activé.

   ```
   [root@serverX ~]# yum -y install postfix
   [root@serverX ~]# service postfix restart
   [root@serverX ~]# chkconfig postfix on
   ```

   b. Après avoir sauvegardé le fichier de configuration principal, émettez les commandes de configuration du postfix suivante et redémarrez le serveur. (Vous pouvez bien entendu modifier la configuration. Il suffit pour cela de modifier le fichier de configuration **/etc/postfix/main.cf** directement, qui bénéficie des commentaires utiles que vous pouvez apporter.)

   ```
   [root@serverX ~]# cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
   [root@serverX ~]# postconf -e inet_interfaces=all
   [root@serverX ~]# postconf -e myorigin=domainX.example.com
   [root@serverX ~]# postconf -e 'relayhost=[smtp.domainX.example.com]'
   ```

```
[root@serverX ~]# postconf -e mydestination=domainX.example.com
[root@serverX ~]# service postfix restart
```

c. Confirmez que le courrier envoyé localement à student@domainX.example.com est reçu par l'hôte *mail*, qui est sa destination finale.

```
[root@serverX ~]# date | mail -s test student@domainX.example.com
```

Examinez la fin de **/var/log/maillog** sur *mail* pour les lignes similaires à ce qui suit. Ce qui est compte est « to=<student@domain1.example.com> ... (delivered to mailbox) » est présente.

```
...
Dec 10 05:39:48 serverX postfix/qmgr[28222]: 53948105A0:
 from=<root@serverX.example.com>, size=470, nrcpt=1 (queue active)
Dec 10 05:39:48 serverX postfix/local[28260]: 53948105A0:
 to=<student@domainX.example.com>, relay=local, delay=0.1,
 delays=0.07/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)
...
```

4. Deuxièmement, configurez *smtp* en tant que relais du courrier sortant. Toutes les étapes suivantes doivent être exécutées sur *smtp.domainX.example.com*.

a. Assurez-vous que le « postfix » est installé, qu'il a démarré et qu'il est activé.

```
[root@hostX ~]# yum -y install postfix
[root@hostX ~]# service postfix restart
[root@hostX ~]# chkconfig postfix on
```

b. Après avoir sauvegardé le fichier de configuration principal, émettez les commandes de configuration du postfix suivante et redémarrez le serveur.

```
[root@hostX ~]# cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
[root@hostX ~]# postconf -e inet_interfaces=all
[root@hostX ~]# postconf -e myorigin=domainX.example.com
[root@hostX ~]# postconf -e local_transport="error:local delivery disabled"
[root@hostX ~]# postconf -e mynetworks="127.0.0.0/8 192.168.0.0/24"
[root@hostX ~]# service postfix restart
```

c. Malheureusement, à ce stade, vous ne pouvez confirmer que peu d'éléments, sauf le fait que la remise locale du courrier est désactivée.

```
[root@hostX ~]# date | mail -s test student
```

Examinez la fin de **/var/log/maillog** sur *smtp* pour les lignes similaires à ce qui suit. Ce qui compte est « status=bounced (local delivery disabled) ».

```
...
Dec 10 05:57:44 hostX postfix/bounce[27732]: 49BCD10591: sender non-delivery
 notification: 657C210594
Dec 10 05:57:44 hostX postfix/qmgr[27724]: 49BCD10591: removed
```

```
Dec 10 05:57:44 hostX postfix/error[27731]: 657C210594:
 to=<root@hostX.example.com>, relay=none, delay=0.02, delays=0.01/0/0/0,
 dsn=5.0.0, status=bounced (local delivery disabled)
...
```

5. Troisièmement, configurez *desktop* en tant que « client null ». Toutes les commandes suivantes doivent être exécutées sur *desktop.domainX.example.com*.

   a. Assurez-vous que le « postfix » est installé, qu'il a démarré et qu'il est activé.

```
[root@desktopX ~]# yum install postfix
[root@desktopX ~]# service postfix restart
[root@desktopX ~]# chkconfig postfix on
```

   b. Après avoir sauvegardé le fichier de configuration principal, émettez les commandes de configuration du postfix suivante et redémarrez le serveur.

```
[root@desktopX ~]# cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
[root@desktopX ~]# postconf -e myorigin=domainX.example.com
[root@desktopX ~]# postconf -e 'relayhost=[smtp.domainX.example.com]'
[root@desktopX ~]# postconf -e local_transport="error:local delivery disabled"
[root@desktopX ~]# service postfix restart
```

6. Comme confirmation finale de votre travail, depuis *desktop*, envoyez un message test à student@domainX.example.com. Dans les divers fichiers **/var/log/message**, suivez le cheminement du courrier en vérifiant qu'il provient de *desktop*, qu'il passe par *smtp* comme relais sortant et qu'il est reçu par *mail* comme destination finale.

```
[root@desktopX ~]# date | mail -s final_test student@domainX.example.com
```

   a. Sur *desktop*, examinez la fin de **/var/log/maillog** pour les lignes similaires à ce qui suit. Ce qui compte est 'relay="smtp.domainX.example.com[192.168.0.X+200]:25"' and 'status=sent'.

```
Dec 10 14:32:04 desktopX postfix/qmgr[8860]: 7D35D247D7:
 from=<root@desktopX.example.com>, size=473, nrcpt=1 (queue active)
Dec 10 14:32:04 desktopX postfix/smtp[8905]: 7D35D247D7:
 to=<student@domainX.example.com>, relay=smtp.domainX.example.com[192.168.0.X
+200]:25, delay=0.18, delays=0.06/0.02/0.06/0.04, dsn=2.0.0, status=sent (250
 2.0.0 Ok: queued as 606C510594)
Dec 10 14:32:04 desktopX postfix/qmgr[8860]: 7D35D247D7: removed
```

   b. Sur *smtp*, examinez la fin de **/var/log/maillog** pour les lignes similaires à ce qui suit, où la réception ("client=desktopX.example.com[192.168.0.X] ... from=<root@desktopX.example.com>") et la transmission ("to=<student@domainX.example.com> ... relay=mail.domainX.example.com[192.168.0.X +100]:25, ... status=sent") de l'email doivent être évidentes.

```
...
Dec 10 06:20:02 hostX postfix/smtpd[27799]: connect from
 desktopX.example.com[192.168.0.X]
Dec 10 06:20:02 hostX postfix/smtpd[27799]: 606C510594:
 client=desktopX.example.com[192.168.0.X]
```

```
Dec 10 06:20:02 hostX postfix/cleanup[27802]: 606C510594: message-
id=<20101210193204.7D35D247D7@desktopX.example.com>
Dec 10 06:20:02 hostX postfix/qmgr[27724]: 606C510594:
 from=<root@desktopX.example.com>, size=684, nrcpt=1 (queue active)
Dec 10 06:20:02 hostX postfix/smtpd[27799]: disconnect from
 desktopX.example.com[192.168.0.X]
Dec 10 06:20:02 hostX postfix/smtp[27803]: 606C510594:
 to=<student@domainX.example.com>, relay=mail.domainX.example.com[192.168.0.X
+100]:25, delay=0.13, delays=0.02/0.02/0.05/0.04, dsn=2.0.0, status=sent (250
 2.0.0 Ok: queued as 7EA04105A0)
...
```

c. Sur *mail*, examinez la fin de **/var/log/maillog** pour les lignes similaires à ce qui suit, où la réception (client=hostX.example.com[192.168.0.X+200] ... from=<root@desktopX.example.com>) et la remise finale du courrier ("to=<student@domainX.example.com> ... status=sent (delivered to mailbox)") doivent être évidentes.

```
...
Dec 10 06:20:02 serverX postfix/cleanup[28475]: 7EA04105A0: message-
id=<20101210193204.7D35D247D7@desktopX.example.com>
Dec 10 06:20:02 serverX postfix/qmgr[28457]: 7EA04105A0:
 from=<root@desktopX.example.com>, size=897, nrcpt=1 (queue active)
Dec 10 06:20:02 serverX postfix/smtpd[28472]: disconnect from
 hostX.example.com[192.168.0.X+200]
Dec 10 06:20:02 serverX postfix/local[28476]: 7EA04105A0:
 to=<student@domainX.example.com>, relay=local, delay=0.05,
 delays=0.02/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)
Dec 10 06:20:02 server1 postfix/qmgr[28457]: 7EA04105A0: removed
...
```

d. Enfin, en tant qu'utilisateur *student* sur *mail*, vérifiez votre messagerie en utilisant pour cela votre client de messagerie favori tel que **mutt**.

```
[root@serverX ~]# yum install -y mutt
[root@serverX ~]# su - student
[student@serverX ~]# mutt
```

En répertoriant *tous* les en-têtes (dans **mutt** vous devez taper **h** lorsque vous voyez le message), vous devez être en mesure de suivre le cheminement du courrier dans l'ordre inverse.

```
...
Received: from hostX.example.com (hostX.example.com [192.168.0.X+200])
        by serverX.example.com (Postfix) with ESMTP id 7EA04105A0
        for <student@domainX.example.com>; Fri, 10 Dec 2010 06:20:02 -0500
        (EST)
Received: from desktopX.example.com (desktopX.example.com [192.168.0.X])
        by hostX.example.com (Postfix) with ESMTP id 606C510594
        for <student@domainX.example.com>; Fri, 10 Dec 2010 06:20:02 -0500
        (EST)
Received: by desktopX.example.com (Postfix, from userid 0)
        id 7D35D247D7; Fri, 10 Dec 2010 14:32:04 -0500 (EST)
...
```

7. Enfin, depuis *desktop*, faites participer l'instructeur en envoyant un message à *instructor.example.com*.

```
[root@desktopX ~]# echo whew | mail -s done instructor@instructor.example.com
```

Serveur DNS de mise en cache uniquement



Test

Test de critère

Étude de cas

Serveur DNS de mise en cache uniquement

Avant de commencer...

Avant de commencer, exécutez le script **lab-setup-cachingdns** sur desktopX.

Pour son entreprise d'import/export en pleine croissance, M. Hnath voudrait améliorer les performances de la résolution de nom en déployant un serveur de mise en cache sur chacun de ses sites.

Les requêtes récursives doivent être transmises au serveur de noms principal du siège de l'entreprise de M. Hnath.

- Installez un serveur de mise en cache sur serverX.
- Configurez le serveur de noms pour que les requêtes récursives soient envoyées à instructor.example.com. Configurez également le serveur de noms pour qu'il accepte les requêtes provenant de toutes les personnes ayant accès au réseau de la salle de classe.

Lorsque vous êtes prêt, exécutez **lab-grade-cachingdns** sur desktopX pour vérifier votre travail.

1. Assurez-vous que le package bind est installé.

```
[root@serverX ~]# yum install bind
```

2. Modifiez la configuration nommée (**/etc/named.conf**) pour prendre en charge les connexions depuis le réseau. Pour cela, modifiez les lignes **listen-on** comme suit.

```
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
```

3. Modifiez la configuration nommée (**/etc/named.conf**) pour ignorer DNSSec. Pour cela, modifiez la ligne **dnssec-validation** comme suit.

```
        dnssec-validation no;
```

4. Modifiez la configuration nommée (**/etc/named.conf**) pour accepter les requêtes provenant de toutes les personnes ayant accès au réseau de la salle de classe. Pour cela, modifiez la ligne **allow-query** comme suit. Modifiez également la configuration pour que les requêtes récursives soient envoyées à **instructor.example.com**. Pour cela, insérez une ligne **forwarders** sous la ligne **allow-query** comme suit.

```
        allow-query     { localhost; 192.168.0.0/24; };
```

```
        forwarders { 192.168.0.254; };
```

5. Redémarrez le service nommé. Notez qu'un arrêt FAILED indique simplement un service qui n'a probablement jamais démarré.

```
[root@server1 ~]# service named restart
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]
```

6. Faites un test depuis le système desktopX.

```
[root@desktop1 ~]# host server1.example.com 192.168.0.101
Using domain server:
Name: 192.168.0.101
Address: 192.168.0.101#53
Aliases:

server1.example.com has address 192.168.0.101
```

Partage de fichiers avec NFS



Exercice de Questionnaire

Concepts NFS - Questionnaire

1. Dans quelles circonstances faut-il utiliser NFSv2 ou NFSv3 ? Les installations héritées et certains clients réseau ne prennent pas en charge NFSv4

2. Quelle est la syntaxe du fichier /etc/exports ? **`/directory/share host(options) host(options)`**

3. Quelle est la procédure à suivre pour publier un nouvel export sur un serveur NFSv4 existant ?

   Créez une entrée **`/etc/exports`** qui définit l'accès au partage

   Exécutez **`exportfs -r`** en tant que super utilisateur sur le serveur

4. Quelle option indique au NFS d'autoriser le super utilisateur à disposer également des privilèges de super utilisateur sur le partage ?

   `no_root_squash`



Test

Test de critère

Étude de cas

Partage de fichiers avec NFS

Avant de commencer...

Veillez à exécuter **`lab-setup-strickland`** depuis votre système desktopX afin de préparer votre système serverX pour l'exercice.

Strickland Pro Play est un magasin spécialisé dans les accessoires et équipements de pointe pour les loisirs. Le nouveau logiciel de vente requiert un serveur de fichiers avec deux partages montés sur chaque terminal dans le magasin.

Pour le serveur de fichiers, déployez un service NFSv4 sur desktopX. Créez et partagez deux exports sur desktopX :

- Le premier export est destiné à la prise des commandes. Sur desktopX, exportez **`/share/current`** et rendez-le accessible en écriture. Le super utilisateur sur le client doit pouvoir accéder en écriture à **`/share/current`** lorsque ce partage est monté. Le second export est destiné à l'archivage des commandes.

- Le second export est destiné à l'archivage des anciennes commandes. Sur desktopX toujours, exportez le chemin **`/share/archives`** et rendez-le accessible en lecture seulement.

- Configurez les deux exports pour qu'ils soient disponibles uniquement sur le réseau local de la salle de classe.

Configurez serverX pour monter **desktopX:/share/current** en tant que **/sales/current** et **desktopX:/share/archives** en tant que **/sales/archives**. Les partages montés doivent être disponibles après le redémarrage de serverX.

Lorsque vous êtes prêt, exécutez le script **lab-grade-strickland** sur le serverX pour vérifier votre travail.

1. Créez d'abord les deux répertoires à partager sur le serveur NFS, desktopX. Rendez le répertoire **current** accessible en écriture.

```
[root@desktopX ~]# mkdir -p /share/archives /share/current
[root@desktopX ~]# chmod 777 /share/current
```

   (Une autre option acceptable consiste à exporter **/share/current** avec l'option **no_root_squash** définie, à l'étape suivante.)

2. Définissez comment les deux répertoires seront partagés en créant **/etc/exports**.

```
[root@desktopX ~]# vi /etc/exports
[root@desktopX ~]# cat /etc/exports
/share/current 192.168.0.0/24(rw,sync)
/share/archives 192.168.0.0/24(ro,async)
```

3. Démarrez le service NFS et configurez-le pour qu'il démarre à chaque démarrage du serveur.

```
[root@desktopX ~]# service nfs start
Starting NFS services:                     [  OK  ]
Starting NFS quotas:                       [  OK  ]
Starting NFS daemon:                       [  OK  ]
Starting NFS mountd:                       [  OK  ]
[root@desktopX ~]# chkconfig nfs on
```

4. Une fois que le serveur NFS est configuré et qu'il fonctionne, connectez-vous en tant que super utilisateur sur serverX et configurez le client NFS. Créez d'abord les points de montage.

```
[root@serverX ~]# mkdir -p /sales/archives /sales/current
```

5. Confirmez que serverX peut voir les partages NFS exportés par desktopX.example.com et créez les entrées **/etc/fstab** à leur suite pour les monter.

```
[root@serverX ~]# showmount -e desktopX.example.com
Export list for desktopX.example.com:
/share/archives 192.168.0.0/24
/share/current  192.168.0.0/24
[root@serverX ~]# vi /etc/fstab
[root@serverX ~]# tail -n 2 /etc/fstab
desktopX.example.com:/share/current   /sales/current   nfs  rw  0 0
desktopX.example.com:/share/archives  /sales/archives  nfs  ro  0 0
```

6. Montez les partages NFS et confirmez qu'ils sont montés correctement. Si tout s'est bien passé, redémarrez serverX et exécutez le script de notation lab-grade-strickland.

```
[root@serverX ~]# mount -a
[root@serverX ~]# mount | grep desktop
desktopX.example.com:/share/current on /sales/current type nfs
 (rw,vers=4,addr=192.168.0.1,clientaddr=192.168.0.101)
desktopX.example.com:/share/archives on /sales/archives type nfs
 (ro,vers=4,addr=192.168.0.1,clientaddr=192.168.0.101)
[root@serverX ~]# reboot
```

Partage de fichiers avec CIFS



Exercice de Questionnaire

Accès à un partage CIFS - Questionnaire

1. Quelle ligne de commande vous donne un accès de type ftp à un partage CIFS nommé « common » sur un serveur nommé « nas2010 », lorsque vous vous connectez en tant qu'utilisateur nommé « winston » ?

   smbclient //nas2010/common -U winston

2. Qu'est-ce qui ne convient pas dans la ligne suivante de /etc/fstab ?

   \\server\share /mnt/point cifs user=ralph,pass=password 0 0

   Question piège : il n'y aucune erreur dans cette ligne. Vous pouvez utiliser des barres obliques inverses ou non dans **/etc/fstab**. Cependant, sur la ligne de commande, vous devez doubler les barres obliques inverses si vous avez choisi de les utiliser : **smbclient \\\\serverX\\share**

3. Comment stockez-vous les informations de connexion dans un fichier séparé pour qu'elles ne soient pas incluses dans **/etc/fstab** ?

   dans **fstab** (colonne 4) : **credentials=filename** et **filename** contiennent sur trois lignes : **username=value**, **password=value** et **domain=value**

4. Lorsque vous montez un partage CIFS sous Windows, quelle option vous permet de spécifier la propriété Linux de tous les fichiers montés ?

   uid=value, gid=value où la valeur peut être l'UID/GID Linux ou le nom d'utilisateur/nom du groupe



Exercice de Liste de contrôle des performances

Configuration des répertoires personnels Samba - Exercice

Modifiez la configuration par défaut Samba et les éléments de sécurité pour permettre l'accès aux répertoires personnels de l'utilisateur.

- ☐ Connectez-vous à serverX et passez au niveau de privilèges du super utilisateur

```
[student@serverX ~]# su -
```

- ☐ Installez les packages nécessaires pour un serveur Samba

```
[root@serverX ~]# yum install -y samba
```

- ☐ Lancez et activez le service Samba

```
[root@serverX ~]# service smb start
[root@serverX ~]# chkconfig smb on
```

- ☐ Configurez le système pour qu'il soit dans le groupe de travail CLASSX (X étant le numéro de votre station de travail) avec les définitions de l'utilisateur local.

  Modifiez **/etc/samba/smb.conf** et définissez les champs suivants.

```
workgroup = CLASSX  # X is your desktop number
security = user             # default
passdb backend = tdbsam     # default
```

- ☐ Ajoutez un utilisateur Samba uniquement nommé **winuserX** (X étant le numéro de votre station de travail) avec le mot de passe Samba **winpass**.

```
[root@serverX ~]# useradd -s /sbin/nologin winuserX
[root@serverX ~]# smbpasswd -a winuserX
New SMB password:  winpass
Retype new SMB password:  winpass
...
Added user winuserX.
```

- ☐ Activez l'accès au répertoire personnel de l'utilisateur dans SELinux.

```
[root@serverX ~]# setsebool -P samba_enable_home_dirs on
```

- ☐ Activez le pare-feu et ouvrez les ports nécessaires pour accorder l'accès.

```
[root@serverX ~]# iptables -I INPUT -p udp --dport 137:138 -j ACCEPT
[root@serverX ~]# iptables -I INPUT -p tcp --dport 139 -j ACCEPT
[root@serverX ~]# iptables -I INPUT -p tcp --dport 445 -j ACCEPT
[root@serverX ~]# service iptables save
```

- ☐ Testez la configuration en accédant au répertoire personnel de l'utilisateur Samba depuis desktopX.

```
[root@serverX ~]# smbclient //serverX/winuserX -U winuserX%winpass
```

  Pour tester la configuration à l'aide de l'interface utilisateur graphique, accédez à **Emplacement → Connecter au serveur**. Renseignez les champs suivants (laissez les autres vides et n'oubliez pas de remplacer X par le numéro de votre ordinateur) :

```
Service type: Windows share
Server: serverX
Share: winuserX
User Name: winuserX
Domain Name: CLASSX
```

Lorsqu'un message vous y invite, saisissez **winpass** comme mot de passe



Test

Test de critère

Étude de cas

Partage de fichiers avec CIFS

Avant de commencer...

Assurez-vous d'exécuter **lab-setup-samba** depuis votre système desktopX afin de préparer votre système serverX pour l'exercice.

L'école de Butler et Hacker a récemment déployé plusieurs serveurs CIFS pour permettre à ses systèmes clients Windows d'accéder aux partages de fichiers.

Le groupe chargé de représenter les couleurs de l'école (Color Guard), appelé Green et Red (Vert et Rouge) déploie un nouveau serveur et doit partager des informations à l'aide de CIFS. Ce partage doit être accessible en écriture par les membres du Color Guard mais les autres personnes ne peuvent y accéder qu'en lecture uniquement.

Activez le pare-feu et permettez à tous les clients sur le réseau local d'accéder au serveur CIFS.

Configurez serverX pour qu'il fonctionne en tant que serveur CIFS avec les informations suivantes :

- Groupe de travail : BUTLER
- Groupe Linux : greenred
- Nom du partage CIFS : school
- Répertoire : /shared/school
- Aucune imprimante n'est partagée

Testez la configuration en :

- Créant un utilisateur membre de **greenred** et vous assurant qu'il peut accéder en écriture au partage CIFS, **school**
- instructor.example.com fournit plusieurs imprimantes que CUPS doit automatiquement activer. Avant de fournir les informations relatives aux imprimantes, vérifiez qu'elles sont disponibles (elles doivent être nommées printerX). Configurez Samba pour qu'aucune imprimante ne soit partagée et vérifiez que l'utilisateur NE PEUT PAS les répertorier avec **smbclient**
- Créant un second utilisateur non membre de **greenred** et en vous assurant qu'il peut uniquement accéder en lecture au partage CIFS, **school**

Lorsque vous êtes prêt, exécutez le script **lab-grade-samba** sur le serverX pour vérifier votre travail.

1. Installez, démarrez et activez les packages requis.

```
[root@server1 ~]# yum install samba samba-doc
[root@server1 ~]# service smb start
[root@server1 ~]# chkconfig smb on
```

2. Activez le pare-feu et ajoutez les règles suivantes.

```
[root@server1 ~]# iptables -A INPUT -p udp --dport 137:138 -j ACCEPT
[root@server1 ~]# iptables -A INPUT -p tcp --dport 139 -j ACCEPT
[root@server1 ~]# iptables -A INPUT -p tcp --dport 445 -j ACCEPT
[root@server1 ~]# service iptables save
```

3. Créez le groupe et le répertoire Linux et configurez le support SELinux.

```
[root@server1 ~]# groupadd -r greenred
[root@server1 ~]# mkdir -p /shared/school
[root@server1 ~]# chgrp greenred /shared/school
[root@server1 ~]# chmod 2775 /shared/school
[root@server1 ~]# semanage fcontext -a -t public_content_t '/shared(/.*)?'
[root@server1 ~]# semanage fcontext -a -t samba_share_t '/shared/school(/.*)?'
[root@server1 ~]# restorecon -vvFR /shared
restorecon reset /shared context unconfined_u:object_r:default_t:s0-
>system_u:object_r:public_content_t:s0
restorecon reset /shared/school context unconfined_u:object_r:default_t:s0-
>system_u:object_r:samba_share_t:s0
```

4. Modifiez **`/etc/samba/samba.conf`**.

   Modifiez ou confirmez ce qui suit :

```
[global]
...
 workgroup = BUTLER
...
 security = user
 passdb backend = tdbsam
```

   Ajoutez une section (à la fin du fichier) comme suit.

```
[school]
 path = /shared/school
 write list = @greenred
 read only = yes
 guest ok = no
```

   Commentez ou supprimez les lignes suivantes pour les imprimantes.

```
[global]
...
load printers = no
-OR-
#[printers]
#       comment = All Printers
#       path = /var/spool/samba
```

```
#       browseable = no
#       guest ok = no
#       writable = no
#       printable = yes
```

5. Redémarrez samba.

```
[root@serverX]# service smb restart
```

6. Faites un test comme précédemment.

```
[root@server1 ~]# useradd -s /sbin/nologin -G greenred red
[root@server1 ~]# smbpasswd -a red
New SMB password:  red
Retype new SMB password:  red
Added user red.
[root@server1 ~]# useradd -s /sbin/nologin bernice
[root@server1 ~]# smbpasswd -a bernice
New SMB password:  bernice
Retype new SMB password:  bernice
Added user bernice.
[root@server1 ~]# smbclient -L serverX -U red%red | grep printer
Domain=[BUTLER] OS=[Unix] Server=[Samba 3.5.4-68.el6]
Domain=[BUTLER] OS=[Unix] Server=[Samba 3.5.4-68.el6]
[root@server1 ~]# smbclient //serverX/school -U red%red
smb: \> put /etc/hosts hosts
smb: \> ls
  hosts                               A      177  Tue Dec 21 10:10:03 2010
smb: \> exit
[root@server1 ~]# smbclient //serverX/school -U bernice%bernice
smb: \> mkdir test
NT_STATUS_MEDIA_WRITE_PROTECTED making remote directory \test
smb: \> get hosts
getting file \hosts of size 177 as hosts (57.6 KiloBytes/sec) (average 57.6 KiloBytes/
sec)
```

Partage de fichier avec FTP



Test

Test de critère

Étude de cas

Zone de dépôt FTP

Avant de commencer...

Assurez-vous d'exécuter **`lab-setup-dropbox`** depuis votre système desktopX afin de préparer votre système serverX pour l'exercice.

L'entreprise Quiet Pleases, qui fabrique des cônes de silence et autres appareils antibruit, dispose d'un programme de collecte d'informations sur les niveaux sonores partout dans le monde. Des volontaires ont collecté des données concernant le bruit et nécessitent un moyen aisé pour transmettre leurs rapports.

L'entreprise a décidé d'utiliser un serveur FTP avec un répertoire de téléchargement anonyme pour récupérer les rapports.

Déployez vsftpd sur votre serverX et configurez un répertoire de téléchargement en écriture seule, accessible depuis: `ftp://serverX.example.com/dropbox`

Comme ces volontaires sont disséminés aux quatre coins du monde, le serveur FTP doit accepter les connexions depuis n'importe quel emplacement sur Internet.

Lorsque vous êtes prêt, exécutez le script **`lab-grade-dropbox`** sur desktopX pour vérifier votre travail.

1. Installez, démarrez et activez les packages requis.

```
[root@server1 ~]# yum install vsftpd
[root@server1 ~]# service vsftpd start
[root@server1 ~]# chkconfig vsftpd on
```

2. Créez un répertoire de téléchargement.

```
[root@server1 ~]# mkdir /var/ftp/dropbox
[root@server1 ~]# chgrp ftp /var/ftp/dropbox
[root@server1 ~]# chmod 730 /var/ftp/dropbox
```

3. Configurez le support SELinux.

```
[root@server1 ~]# semanage fcontext -a -t public_content_rw_t '/var/ftp/dropbox(/.*)'
[root@server1 ~]# restorecon -vvFR /var/ftp/dropbox
restorecon reset /var/ftp/dropbox context unconfined_u:object_r:public_content_t:s0-
>system_u:object_r:public_content_rw_t:s0
[root@server1 ~]# setsebool -P allow_ftpd_anon_write on
```

4. Modifiez **`/etc/vsftpd/vsftpd.conf`**.

Modifiez, annulez le commentaire ou confirmez ce qui suit :

```
anon_upload_enable=yes
chown_uploads=yes
chown_username=daemon
anon_umask=077
```

Redémarrez **vsftpd**.

```
[root@server1 ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

5. Configurez iptables (s'il est activé).

Modifiez **/etc/sysconfig/iptables-config** :

```
IPTABLES_MODULES="nf_conntrack_ftp nf_nat_ftp"
```

Modifiez **/etc/sysconfig/iptables** :

```
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p tcp --dport 21 -j ACCEPT
```

Redémarrez **iptables**.

```
[root@server1 ~]# service iptables restart
```

Service CUPS



Exercice de Exercice de groupe

Gérer les files d'attente d'impression

1. Créez une file d'attente d'impression locale et partagez-la avec d'autres systèmes. Nommez la file d'attente d'impression **`local`** et faites-en une imprimante texte qui pointe vers le port série ou parallèle de votre système.



Note

Une imprimante texte seul n'accepte pas de fichiers PostScript, tels que ceux envoyés par la fonctionnalité **Test d'impression**. Ne vous inquiétez pas si la page de test ne s'imprime pas.

2. Créez une seconde file d'attente d'impression qui pointe vers la file d'attente d'impression locale d'un partenaire. Nommez la file d'attente d'impression **`remote`** et faites-en une file d'attente d'impression de données brutes qui transfère les tâches vers la file d'attente d'impression **`local`** de votre partenaire.

3. Une fois l'opération terminée, imprimez des fichiers texte sur **`local`** et **`remote`** pour vérifier que tout s'est bien déroulé.



Note

Si vous utilisez un port série, les tâches d'impression sont envoyées vers celui-ci presque immédiatement. Par conséquent, la vérification du fonctionnement correct de vos files d'attente d'impression peut se révéler difficile. Si tel est le cas, utilisez les fichiers avec « comptage » (c00001, c00002, etc., par exemple) dans **`/var/spool/cups/`** pour vérifier que tout est correct. Un fichier numéroté est généré à chaque introduction d'une tâche d'impression dans la file d'attente.



Test

Test de critère

Exercice

Configurer et gérer une imprimante

Avant de commencer...

À partir de desktopX, exécutez **`lab-setup-cups`** pour réinitialiser votre serveur virtuel pour cet exercice.

1. Configurez une imprimante réseau de façon à envoyer des tâches d'impression vers une file d'attente IPP sur instructor.example.com appelée /printers/printer*X* où *X* est le numéro de votre poste de travail.

```
[root@desktopX ~]# system-config-printer
```

Cliquez sur **Nouveau**. Développez **Imprimante réseau**. Sélectionnez **Internet Printing Protocol (ipp)** et entrez **`instructor.example.com`** comme **Hôte** et **`/printers/printerX`** en tant que **File d'attente**. Vous pouvez également sélectionner **Rechercher une imprimante réseau** et entrez **`instructor.example.com`** en tant que nom d'hôte, puis cliquez sur **Rechercher**. Assurez-vous que **`/printers/printerX`** se trouve dans la **file d'attente**, puis cliquez sur **Vérifier**.



Note

Vous devez entrer un nom de domaine complet lors de la recherche d'une imprimante réseau, sinon, CUPS risque de ne pas la trouver.

Une fois que vous avez entré et vérifié l'imprimante, cliquez sur **Suivant**.

2. Votre file d'attente d'impression doit être nommée **`remote-test`** et être définie en tant que file d'attente d'impression par défaut.

Choisissez **`Generic`** en tant qu'imprimante, puis cliquez sur **Suivant**. Choisissez **`text-only printer`** comme modèle et cliquez sur **Suivant**. Entrez **`remote-test`** comme **Nom de l'imprimante**, puis cliquez sur **Suivant**.

Si **`remote-printer`** n'est pas le paramètre par défaut, cliquez avec le bouton droit sur **`remote-test`** et choisissez **Définir par défaut**.

3. Lorsque vous avez terminé, exécutez le script d'évaluation, **`lab-grade-cups`**.

```
[root@serverX ~]# lab-grade-cups
```

Service SSH



Exercice de Exercice

Utilisation de clés SSH

1. Créez une paire de clés SSH en tant que **student** sur desktopX.

```
[student@desktopX ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):  Enter
Enter passphrase (empty for no passphrase): redhat
Enter same passphrase again: redhat
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
dc:cb:9b:30:98:b4:99:19:fc:fe:ba:97:2b:95:4d:29 student@desktop1.example.com
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|             .   |
|     . . .E o    |
|      + S .=     |
|     . X .o..    |
|      B +.o.     |
|       ..ooo     |
|        +*=.     |
+-----------------+
```

2. Installez la clé SSH publique pour le compte **student** sur serverX.

```
[student@desktopX ~]$ ssh-copy-id serverX
student@serverX's password: student
Now try logging into the machine, with "ssh 'serverX'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

3. Connectez-vous à serverX à partir de desktopX à l'aide des clés SSH.

```
[student@desktopX ~]$ ssh serverX
Enter passphrase for key '/home/student/.ssh/id_rsa': redhat
[student@serverX ~]$
```



Test

Test de critère

Exercice

Sécurisation SSH

Avant de commencer...

Exécutez la commande **lab-setup-server** en tant que **root** sur votre système desktopX. Cela préparera votre système serverX pour l'exercice.

1. Copiez la clé SSH publique précédemment générée sur desktopX dans le compte **student** sur serverX.

```
[student@desktopX ~]$ ssh-copy-id -i .ssh/id_rsa.pub student@serverX
```

2. Confirmez que vous pouvez vous connecter par **ssh** à serverX en tant que **student** depuis desktopX à l'aide des clés SSH.

```
[student@desktopX ~]$ ssh student@serverX
[student@serverX ~]$
```

Service VNC (Virtual Network Computing)



Exercice de Exercice

Activation d'un serveur VNC

1. Installez le package **tigervnc-server** sur serverX.

```
[root@serverX ~]# yum install tigervnc-server
```

2. Configurez l'affichage VNC 1 pour student. Ajoutez ce qui suit à **/etc/sysconfig/vncservers**:

```
VNCSERVERS="1:student"
```

3. Définissez **redhat** comme mot de passe VNC pour student:

```
[student@serverX ~] vncpasswd
Password: redhat
Verify: redhat
```

4. Lancez et activez le service VNC.

```
[root@serverX ~]# service tigervnc start
[root@serverX ~]# chkconfig tigervnc on
```

5. Vous vérifierez la connexion dans la section suivante.



Exercice de Exercice

Se connecter à VCN de façon sécurisée

1. Configurez le serveur VNC sur serverX pour autoriser uniquement les connexions locales. Modifiez **/etc/sysconfig/vncservers** et ajoutez ce qui suit:

```
VNCSERVERARGS[1]="-localhost"
```

2. Connectez-vous au serveur VNC sur serverX de manière sécurisée à partir de desktopX à l'aide d'un tunnel SSH:

```
[student@desktopX ~] vncviewer -via serverX localhost:1
```

3. Vérifiez que tout est correct.



Test

Test de critère

Exercice

Configurer plusieurs bureaux avec VNC

Avant de commencer...

Exécutez la commande **lab-setup-server** en tant que **root** sur votre système desktopX. Cela préparera votre système serverX pour l'exercice.

1. Installez le package du serveur VNC sur serverX.

```
[root@serverX ~]# yum -y install tigervnc-server
```

2. Configurez l'affichage1 pour **student** et l'affichage2 pour **visitor**.

   Ajoutez ce qui suit à **/etc/sysconfig/vncservers**

```
VNCSERVERS="1:student 2:visitor"
```

3. Autorisez les connexions uniquement à partir de l'hôte local.

   Ajoutez ce qui suit à **/etc/sysconfig/vncservers**

```
VNCSERVERARGS[1]="-localhost"
VNCSERVERARGS[2]="-localhost"
```

4. Définissez **redhat** comme mot de passe VNC pour **student** et **visitor**.

```
[root@iserverX ~]# su - student
[student@serverX ~]$ vncpasswd
Password: redhat
Verify: redhat
[student@serverX ~]$ exit
[root@serverX ~]# su - visitor
[visitor@serverX ~]$ vncpasswd
Password: redhat
Verify: redhat
[visitor@serverX ~]$ exit
```

5. Lancez et activez le service VNC.

```
[root@serverX ~]# service vncserver start
[root@serverX ~]# chkconfig vncserver on
```



Note

Vous devez définir le mot de passe VNC pour chaque utilisateur avant de lancer le service. Sinon, le service **vncserver** ne démarrera pas correctement.

6. Vérifiez que tout est correct, puis contrôlez votre travail en utilisant une connexion sécurisée.

```
[root@desktopX ~]# vncviewer -via student@serverX localhost:1
TigerVNC Viewer for X version 1.0.90 - built Jun 30 2010 11:30:49
Copyright (C) 2002-2005 RealVNC Ltd.
Copyright (C) 2000-2006 TightVNC Group
Copyright (C) 2004-2009 Peter Astrand for Cendio AB
See http://www.tigervnc.org for information on TigerVNC.
The authenticity of host 'serverX (192.168.0.X+100)' can't be established.
RSA key fingerprint is 5c:77:a4:e3:23:9e:72:cf:ac:d4:cd:a7:6b:c4:94:ba.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'serverX' (RSA) to the list of known hosts.
student@serverX's password: student

VNC authentication
Password:  redhat

[root@desktopX ~]# vncviewer -via visitor@serverX localhost:2
TigerVNC Viewer for X version 1.0.90 - built Jun 30 2010 11:30:49
Copyright (C) 2002-2005 RealVNC Ltd.
Copyright (C) 2000-2006 TightVNC Group
Copyright (C) 2004-2009 Peter Astrand for Cendio AB
See http://www.tigervnc.org for information on TigerVNC.
visitor@serverX's password: password

VNC authentication
Password:  redhat
```



Note

Le paramètre après **-via** sert pour les connexions avec **ssh**. Il n'est pas nécessaire d'utiliser le nom d'utilisateur de la session VNC à laquelle vous vous connectez. N'importe quel nom d'utilisateur fonctionnera si vous connaissez le mot de passe.

Examen exhaustif



Test

Test d'examen exhaustif

Exercice

Examen exhaustif

Avant de commencer...

Exécutez la commande **lab-setup-server** en tant que **root** sur desktopX.

Configurez serverX afin qu'il réponde aux exigences suivantes. Pour tous les services, autorisez les connexions depuis le sous-réseau 192.168.0.0/24 local, mais n'autorisez pas les connexions depuis le sous-réseau 192.168.1.0/255.255.255.0.

1. Configurez SELinux avec le mode enforcing.

   Assurez-vous que **/etc/sysconfig/selinux** contienne :

   ```
   SELINUX=enforcing
   ```

2. Autorisez les connexions SSH depuis le sous-réseau local.

   ```
   [root@serverX ~]# iptables -I INPUT -m state --state NEW -s 192.168.0.0/24 -p tcp --
   dport 22 -j ACCEPT
   [root@serverX ~]# iptables -I INPUT -i lo -j ACCEPT
   [root@serverX ~]# iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
   [root@serverX ~]# iptables -A INPUT -m state --state NEW -j REJECT
   [root@serverX ~]# service iptables save
   ```

3. Configurez un serveur SMTP qui autorise les connexions depuis le sous-réseau local.

   Modifiez **/etc/postfix/main.cf** et changez :

   ```
   inet_interfaces = localhost
   ```

   comme suit :

   ```
   inet_interfaces = all
   ```

   ```
   [root@serverX ~]# service postfix restart
   [root@serverX ~]# iptables -I INPUT 3 -m state --state NEW -s 192.168.0.0/24 -p tcp --
   dport 25 -j ACCEPT
   [root@serverX ~]# service iptables save
   ```



Note

Nous souhaitons définir les règles **ESTABLISHED,RELATED** et loopback (**-i lo**) en tant que premières règles. Nous ne souhaitons pas placer cette nouvelle règle à la fin (**-A**), car elle viendrait après la règle **REJECT**, par conséquent, **-I INPUT 3** place cette règle en troisième position.

4. Connectez-vous au serveur LDAP, instructor.example.com, à l'aide du nom distinctif **dc=example,dc=com** pour les informations de compte. Le serveur LDAP nécessite des connexions sécurisées à l'aide du certificat qui se trouve sur *ftp://instructor.example.com/pub/EXAMPLE-CA-CERT*. Le serveur LDAP fournit un compte nommé **ldapuserX**.

   Utilisez des mots de passe Kerberos avec un domaine **EXAMPLE.COM** pour l'authentification. Définissez les serveurs KDC et Admin sur instructor.example.com. Les comptes possèdent le mot de passe **kerberos**.

   Pour l'interface graphique **system-config-authentication**, choisissez **LDAP** dans le menu déroulant **Base de données de comptes utilisateur**. Définissez le **serveur LDAP** sur **ldap://instructor.example.com**. Sélectionnez **Utiliser TLS pour chiffrer des connexions**. Cliquez sur le bouton Télécharger un certificat AC... et entrez ftp://instructor/pub/EXAMPLE-CA-CERT. Définissez les **serveurs KDC** et **Admin** sur **instructor.example.com**. Conservez les autres paramètres tels quels et cliquez sur **Appliquer**.

   Pour utiliser l'outil en ligne de commande **authconfig**, utilisez la commande suivante :

```
authconfig --enableldap --ldapserver=instructor.example.com --enableldaptls \
   --ldaploadcacert=ftp://instructor.example.com/pub/EXAMPLE-CA-CERT \
   --ldapbasedn="dc=example,dc=com" --disableldapauth --enablekrb5 \
   --krb5kdc=instructor.example.com --krb5adminserver=instructor.example.com \
   --krb5realm=EXAMPLE.COM --enablesssd --enablesssdauth --update
```

5. Configurez un répertoire personnel monté automatiquement pour le compte **ldapuserX**. Le répertoire personnel est partagé via NFS depuis instructor.example.com.

   Ajoutez ce qui suit au fichier **/etc/auto.master** :

```
/home/guests /etc/auto.guests
```

   Créez **/etc/auto.guests** et ajoutez le contenu suivant :

```
*       instructor.example.com:/home/guests/&
```

```
[root@serverX ~]# service autofs reload
```

6. Connectez-vous à la cible iSCSI **rdisks.serverX** fournie par instructor.example.com.

```
[root@serverX ~]# iscsiadm -m discovery -t st -p 192.168.0.254
[root@serverX ~]# iscsiadm -m node -T iqn.2010-09.com.example:rdisks.serverX -p
 192.168.0.254 -l
```

7. Supprimez l'ensemble des partitions actuelles sur le disque iSCSI. Configurez une nouvelle partition physique de 30 Mo à l'aide de la cible iSCSI avec un système de fichiers ext4 et une étiquette **test** montés sur **/test/**. Le répertoire **/test/** doit appartenir à l'utilisateur **root** et au groupe **root**. En outre, il doit disposer de l'autorisation 755.

```
[root@serverX ~]# dd if=/dev/zero of=/dev/sda count=1
[root@serverX ~]# fdisk -cu /dev/sda
Command (m for help): n
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (2048-65535, default 2048):  Enter
Last sector, +sectors or +size{K,M,G} (2048-65535, default 65535): +30MB
Command (m for help): w
[root@serverX ~]# mkfs -t ext4 -L test /dev/sda1
[root@serverX ~]# mkdir /test
```

Ajoutez une ligne au fichier **/etc/fstab**:

```
LABEL=test      /test   ext4    _netdev 1 2
```

```
[root@serverX ~]# mount -a
[root@serverX ~]# chown root:root /test
[root@serverX ~]# chmod 755 /test
```

8. Configurez un nouveau volume logique de 1 Go nommé **mylv** dans le groupe de volumes **vgsrv**, avec un système de fichiers ext4 monté sur **/mylv/**.



Note

vgs nous indique que l'espace est insuffisant pour créer un volume logique de 1 Go, nous devons donc d'abord ajouter de l'espace disque au groupe de volumes.

```
[root@serverX ~]# fdisk -cu /dev/vda
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First sector (9914368-12582911, default 9914368):  Enter
Using default value 9914368
Last sector, +sectors or +size{K,M,G} (9914368-12582911, default 12582911): +1G

Command (m for help): t
```

```
Partition number (1-4): 3
Hex code (type L to list codes): 8e
Changed system type of partition 3 to 8e (Linux LVM)

Command (m for help): w
[root@serverX ~]# reboot
[root@serverX ~]# pvcreate /dev/vda3
[root@serverX ~]# vgextend vgsrv /dev/vda3
[root@serverX ~]# lvcreate -L 1G -n mylv vgsrv
[root@serverX ~]# mkfs -t ext4 /dev/vgsrv/mylv
[root@serverX ~]# mkdir /mylv
```

Ajoutez la ligne suivante au fichier **/etc/fstab**:

```
/dev/mapper/vgsrv-mylv  /mylv   ext4    defaults 1 2
```

```
[root@serverX ~]# mount -a
```

9. Configurez NFS pour partager le répertoire **/test/**. Rendez-le accessible en lecture seule sur le sous-réseau local. Autorisez **root** à disposer des privilèges de super utilisateur lors de l'accès au partage NFS.

   Ajoutez la ligne suivante au fichier **/etc/exports**:

```
/test 192.168.0.0/24(ro,no_root_squash)
```

```
[root@serverX ~]# service nfs restart
[root@serverX ~]# chkconfig nfs on
[root@serverX ~]# iptables -I INPUT 3 -m state --state NEW -s 192.168.0.0/24 -p tcp --
dport 2049 -j ACCEPT
[root@serverX ~]# service iptables save
```

10. Créez un compte d'utilisateur appelé **matt** à l'aide du mot de passe **matt**.

```
[root@serverX ~]# useradd matt
[root@serverX ~]# passwd matt
Changing password for user matt.
New password: matt
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password: matt
passwd: all authentication tokens updated successfully.
```

11. Créez un compte d'utilisateur appelé **cindy** à l'aide du mot de passe **cindy**.

```
[root@serverX ~]# useradd cindy
[root@serverX ~]# echo cindy | passwd --stdin cindy
Changing password for user cindy.
passwd: all authentication tokens updated successfully.
```

12. Créez un groupe nommé **admins** incluant **matt** et **cindy**.

```
[root@serverX ~]# groupadd -r admins
```

```
[root@serverX ~]# usermod -aG admins matt
[root@serverX ~]# usermod -aG admins cindy
```

13. Configurez Samba pour partager le répertoire **/test/** à l'aide du nom de partage **test**. Rendez-le accessible en lecture pour **cindy** (utilisez le mot de passe Samba **password**) et accessible en écriture pour **matt** (utilisez le mot de passe Samba **password**). Assurez-vous que les autorisations Linux permettent la lecture/écriture, tel que cela est répertorié ici, et qu'elles respectent les conditions requises ci-dessus pour les utilisateurs, les groupes et les autorisations.

```
[root@serverX ~]# yum -y install samba
```

Ajoutez ce qui suit au bas du fichier **/etc/samba/smb.conf**:

```
[test]
path = /test
writable = no
write list = matt
```

```
[root@serverX ~]# smbpasswd -a matt
New SMB password: password
Retype new SMB password: password
[root@serverX ~]# smbpasswd -a cindy
New SMB password: password
Retype new SMB password: password
[root@serverX ~]# service smb start
[root@serverX ~]# chkconfig smb on
```

Modifiez la ligne **/test** dans **/etc/fstab**, afin qu'elle contienne l'option **acl**, et rendez l'option ACL disponible pour le système de fichiers monté.

```
LABEL=test      /test   ext4    _netdev,acl 1 2
```

```
[root@serverX ~]# mount -o remount /test
[root@serverX ~]# setfacl -m u:matt:rwx /test
[root@serverX ~]# setfacl -m u:cindy:rx /test
[root@serverX ~]# semanage fcontext -a -t public_content_rw_t '/test(/.*)?'
[root@serverX ~]# restorecon -RFvv /test
[root@serverX ~]# setsebool -P allow_smbd_anon_write=1
[root@serverX ~]# iptables -I INPUT 3 -m state --state NEW -s 192.168.0.0/24 -p tcp --
dport 445 -j ACCEPT
[root@serverX ~]# service iptables save
```

14. Configurez un serveur Web sécurisé à l'aide du certificat et de la clé se trouvant sur *http://instructor/pub/materials/tls/certs/serverX.crt* et sur *http://instructor/pub/materials/tls/private/serverX.key*. Configurez le serveur Web afin qu'il utilise **/mylv/index.html** comme page Web par défaut. Configurez le fichier **index.html** afin que l'accès au site Web sécurisé présente ce qui suit:

```
Hello World!
```

```
[root@serverX ~]# yum install -y mod_ssl
```

```
[root@serverX ~]# wget http://instructor/pub/materials/tls/private/serverX.key -O /
etc/pki/tls/private/serverX.key
[root@serverX ~]# chmod 600 /etc/pki/tls/private/serverX.key
[root@serverX ~]# wget http://instructor/pub/materials/tls/certs/serverX.crt -O /etc/
pki/tls/certs/serverX.crt
```

Modifiez les emplacements de fichier de certificat dans **/etc/httpd/conf.d/ssl.conf** qui pointent vers l'hôte local :

```
SSLCertificateFile /etc/pki/tls/certs/serverX.crt

SSLCertificateKeyFile /etc/pki/tls/private/serverX.key
```

Modifiez **/etc/httpd/conf/httpd.conf** pour changer l'emplacement par défaut :

```
DocumentRoot "/mylv"
```

```
[root@serverX ~]# service httpd start
[root@serverX ~]# chkconfig httpd on
[root@serverX ~]# iptables -I INPUT 3 -m state --state NEW -s 192.168.0.0/24 -p tcp --
dport 443 -j ACCEPT
[root@serverX ~]# iptables -I INPUT 3 -m state --state NEW -s 192.168.0.0/24 -p tcp --
dport 80 -j ACCEPT
[root@serverX ~]# service iptables save
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/mylv(/.*)?'
[root@serverX ~]# restorecon -RFvv /mylv/
```

15. Autorisez **cindy** et **matt** à écrire le fichier **/mylv/index.html**.

```
[root@serverX ~]# chgrp admins /mylv/index.html
[root@serverX ~]# chmod 664 /mylv/index.html
```

Liste de contrôle d'examen supplémentaire

- ☐ Créez une nouvelle partition de 100 Mo avec un système de fichiers ext4 pouvant être monté sur **/encrypted**. Chiffrez le système de fichiers à l'aide du mot de passe **encrypted**. Placez une entrée dans **/etc/fstab**, mais n'autorisez pas son montage automatique au démarrage.
- ☐ Étendez le volume logique **mylv** et son système de fichiers jusqu'à 2 Go.
- ☐ Configurez un serveur VNC pour **student** avec le mot de passe VNC **test123**.
- ☐ Configurez un serveur de journalisation afin que toute personne disposant d'un accès au sous-réseau local puisse envoyer des journaux vers **TCP/514**.

- ☐ Créez un package RPM nommé **`test-1.0-1.el6.noarch.rpm`**. Incluez le fichier **`/root/bin/test.sh`** dans le package RPM. Le script **`test.sh`** doit simplement exécuter la commande **`ls`**.
- ☐ Configurez un accès sudo complet pour **`matt`** et **`cindy`**.
- ☐ Configurez un serveur de mise en cache uniquement.