26/08/2024

Atelier 00 – Activité 7 PT : Configurer les routeurs Cisco pour les opérations Syslog, NTP et SSH

**Document de l’atelier :**

[Bloc2\_sem3-4\_Atelier-00-activite-1\_Inter-VLAN\_Routing Challenge.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-1_Inter-VLAN_Routing%20Challenge.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-2\_Découverte-NAT-RIP-01.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-2_Découverte-NAT-RIP-01.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-5-Configure-and-Verify-NTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-5-Configure-and-Verify-NTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-6-reconstruction-reseau.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-6-reconstruction-reseau.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut .pka](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut%20.pka)

[Bloc2\_sem3-4\_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-10-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-10-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-11-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-11-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx)

Table des matières

[1. Tableau d'adressage 2](#_Toc176817863)

[2. Tâche 1 : Configurer les routeurs en tant que clients NTP. 2](#_Toc176817864)

[1.1 Étape 1. Tester la connectivité 2](#_Toc176817865)

[1.2 Étape 2. Configurer R1, R2 et R3 en tant que clients NTP. 3](#_Toc176817866)

[1.3 Étape 3. Configurer les routeurs pour mettre à jour l'horloge matérielle. 3](#_Toc176817867)

[1.4 Étape 4. Configurer les routeurs pour horodater les messages de journal. 4](#_Toc176817868)

[1.5 Étape 5. Configurer le service d'horodatage pour l'enregistrement sur les routeurs. 4](#_Toc176817869)

[3. Tâche 2 : Configurer les routeurs pour enregistrer des messages sur le serveur Syslog. 4](#_Toc176817870)

[1.1 Étape 1. Configurer les routeurs pour identifier l'hôte distant (serveur Syslog) qui recevra les messages de journalisation. 4](#_Toc176817871)

[1.2 Étape 2. Vérifier la configuration de l'enregistrement en utilisant la commande show logging. 4](#_Toc176817872)

[1.3 Étape 3. Examiner les journaux du serveur Syslog. 4](#_Toc176817873)

[4. Tâche 3 : Configurer R3 pour prendre en charge les connexions SSH. 5](#_Toc176817874)

[1.1 Étape 1. Configurer un nom de domaine. 5](#_Toc176817875)

[1.2 Étape 2. Configurer des utilisateurs pour la connexion depuis le client SSH sur R3. 5](#_Toc176817876)

[1.3 Étape 3. Configurer les lignes VTY entrantes sur R3. 5](#_Toc176817877)

[1.4 Étape 4. Effacer les paires de clés existantes sur R3. 5](#_Toc176817878)

[1.5 Étape 5. Générer la paire de clés de chiffrement RSA pour R3. 5](#_Toc176817879)

[1.6 Étape 6. Vérifier la configuration SSH. 6](#_Toc176817880)

[1.7 Étape 7. Configurer les délais d'expiration SSH et les paramètres d'authentification. 6](#_Toc176817881)

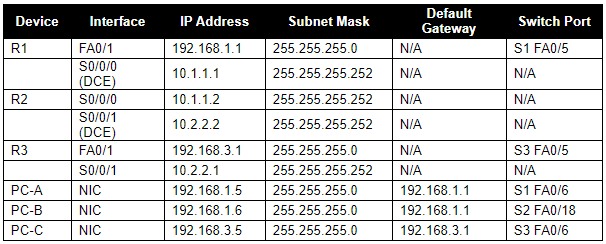
[1.8 Étape 8. Tenter de se connecter à R3 via Telnet depuis PC-C. 6](#_Toc176817882)

[1.9 Étape 9. Se connecter à R3 en utilisant SSH sur PC-C. 7](#_Toc176817883)

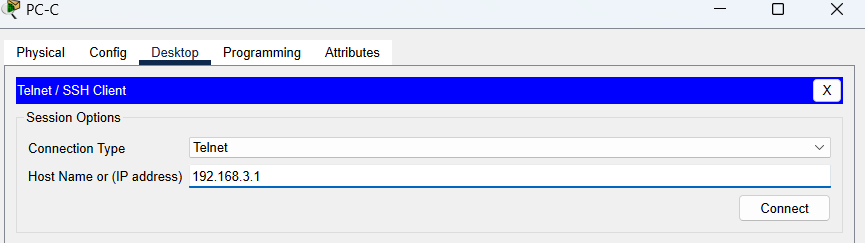
[1.10 Étape 10. Se connecter à R3 en utilisant SSH sur R2. 7](#_Toc176817884)

[1.11 Étape 11. Vérifier les résultats**.** 8](#_Toc176817885)

# Tableau d'adressage



Connection Telnet :



# Tâche 1 : Configurer les routeurs en tant que clients NTP.

## Étape 1. Tester la connectivité

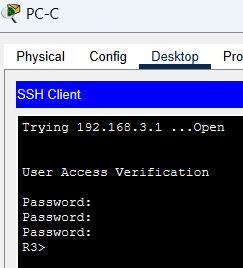
* Pinger depuis PC-C vers R3.



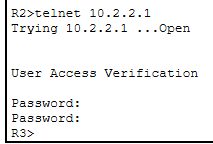
* Pinger depuis R2 vers R3.



* Telnet depuis PC-C vers R3.



* Telnet depuis R2 vers R3.



* Mot de passe d'activation : ciscoenpa55
* Mot de passe pour les lignes VTY : ciscovtypa55

## Étape 2. Configurer R1, R2 et R3 en tant que clients NTP.

Vérifiez la configuration du client en utilisant la commande show ntp status.



## Étape 3. Configurer les routeurs pour mettre à jour l'horloge matérielle.

Configurez R1, R2 et R3 pour mettre à jour périodiquement l'horloge matérielle avec le temps appris de NTP.



Vérifiez que l'horloge matérielle a été mise à jour en utilisant la commande show clock.







## Étape 4. Configurer les routeurs pour horodater les messages de journal.



## Étape 5. Configurer le service d'horodatage pour l'enregistrement sur les routeurs.

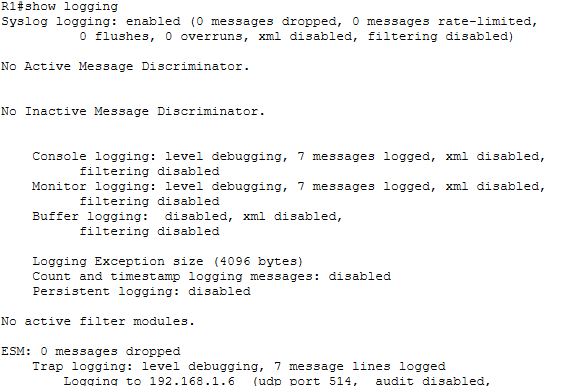
# Tâche 2 : Configurer les routeurs pour enregistrer des messages sur le serveur Syslog.

## Étape 1. Configurer les routeurs pour identifier l'hôte distant (serveur Syslog) qui recevra les messages de journalisation.

La console du routeur affichera un message indiquant que l'enregistrement a commencé.

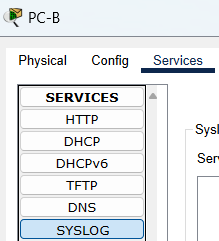


## Étape 2. Vérifier la configuration de l'enregistrement en utilisant la commande show logging.



## Étape 3. Examiner les journaux du serveur Syslog.

Depuis l'onglet Config du dialogue du serveur Syslog, sélectionnez le bouton des services Syslog. Observez les messages de journalisation reçus des routeurs.



**Remarque :** Des messages de journal peuvent être générés sur le serveur en exécutant des commandes sur le routeur. Par exemple, entrer et sortir du mode de configuration global générera un message de configuration informatif.

# T**âche 3 : Configurer R3 pour prendre en charge les connexions SSH.**

## Étape 1. Configurer un nom de domaine.

Configurez un nom de domaine de ccnasecurity.com sur R3.



## Étape 2. Configurer des utilisateurs pour la connexion depuis le client SSH sur R3.

Créez un identifiant utilisateur de SSHadmin avec le niveau de privilège le plus élevé possible et un mot de passe secret de ciscosshpa55.



## Étape 3. Configurer les lignes VTY entrantes sur R3.

Utilisez les comptes d'utilisateur locaux pour une connexion et une validation obligatoire. Acceptez uniquement les connexions SSH.



## Étape 4. Effacer les paires de clés existantes sur R3.

Toute paire de clés RSA existante doit être effacée sur le routeur.

**Remarque :** Si aucune clé n'existe, vous pourriez recevoir ce message : % No Signature RSA Keys found in configuration.



## Étape 5. Générer la paire de clés de chiffrement RSA pour R3.

Le routeur utilise la paire de clés RSA pour l'authentification et le chiffrement des données SSH transmises. Configurez les clés RSA avec un module de 1024. La valeur par défaut est 512, et la plage est de 360 à 2048.

R3(config)# crypto key generate rsa

Le nom des clés sera : R3.ccnasecurity.com

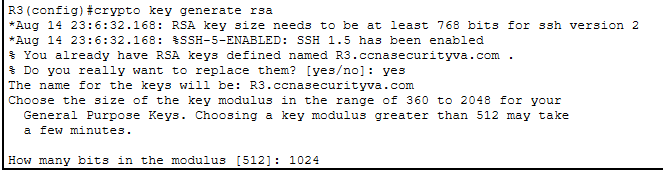
Choisissez la taille du module de clé dans la plage de 360 à 2048 pour vos clés à usage général. Choisir un module de clé supérieur à 512 peut prendre quelques minutes.

Code

Copier le code

Combien de bits dans le module [512] : 1024

% Génération de clés RSA de 1024 bits, les clés ne seront pas exportables...[OK]



**Remarque :** La commande pour générer des paires de clés de chiffrement RSA pour R3 dans Packet Tracer diffère de celles utilisées dans le laboratoire.

## Étape 6. Vérifier la configuration SSH.

Utilisez la commande show ip ssh pour voir les paramètres actuels. Vérifiez que le délai d'authentification et les tentatives sont à leurs valeurs par défaut de 120 et 3.



## Étape 7. Configurer les délais d'expiration SSH et les paramètres d'authentification.

Les délais d'expiration par défaut de SSH et les paramètres d'authentification peuvent être modifiés pour être plus restrictifs. Réglez le délai d'expiration à 90 secondes, le nombre de tentatives d'authentification à 2, et la version à 2.



Émettez à nouveau la commande show ip ssh pour confirmer que les valeurs ont été modifiées.

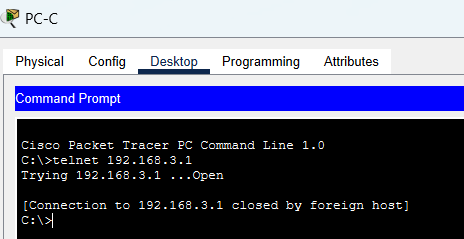


## Étape 8. Tenter de se connecter à R3 via Telnet depuis PC-C.

Ouvrez le bureau de PC-C. Sélectionnez l'icône de l'invite de commande. Depuis PC-C, entrez la commande pour vous connecter à R3 via Telnet.

PC> telnet 192.168.3.1

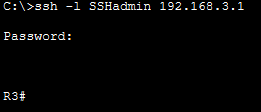
Cette connexion devrait échouer, puisque R3 a été configuré pour accepter uniquement les connexions SSH sur les lignes de terminal virtuel.



## Étape 9. Se connecter à R3 en utilisant SSH sur PC-C.

Ouvrez le bureau de PC-C. Sélectionnez l'icône de l'invite de commande. Depuis PC-C, entrez la commande pour vous connecter à R3 via SSH. Lorsque vous êtes invité à entrer le mot de passe, entrez le mot de passe configuré pour l'administrateur : ciscosshpa55.

PC> ssh -l SSHadmin 192.168.3.1



C:\>ssh -l SSHadmin 192.168.3.1

Password:

% Login invalid

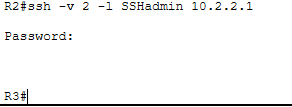
Password:

[Connection to 192.168.3.1 closed by foreign host]

## Étape 10. Se connecter à R3 en utilisant SSH sur R2.

Pour dépanner et maintenir le routeur R3, l'administrateur du FAI doit utiliser SSH pour accéder à l'interface de ligne de commande du routeur. Depuis l'interface de ligne de commande de R2, entrez la commande pour vous connecter à R3 via SSH version 2 en utilisant le compte utilisateur SSHadmin. Lorsque vous êtes invité à entrer le mot de passe, entrez le mot de passe configuré pour l'administrateur : ciscosshpa55.

R2# ssh -v 2 -l SSHadmin 10.2.2.1



## Étape 11. Vérifier les résultats**.**

Votre pourcentage d'achèvement devrait être de 100 %. Cliquez sur Vérifier les résultats pour voir les commentaires et la vérification des composants requis qui ont été complétés.

