Configuration de RADKit pour le dépannage à distance sur HyperFlex

Table des matières

Introduction

Ce document décrit comment démarrer et préparer un environnement RADKit pour le dépannage à distance d'un environnement Cisco HyperFlex.

Informations générales

L'objectif principal de ce document est d'expliquer comment préparer votre environnement pour une utilisation par le TAC afin d'exploiter RADKit pour le dépannage.

Qu'est-ce que RADKit ?

RADKit est un orchestrateur à l'échelle du réseau. Faites l'expérience d'une nouvelle façon radicale d'aborder votre équipement, d'augmenter vos services Cisco et d'élargir vos capacités.

Plus d'informations sur RADKit sont disponibles ici : https://radkit.cisco.com/

Pourquoi RADKit pour HX ?

Cisco HyperFlex se compose de plusieurs composants : Fabric Interconnects, UCS Servers, ESXi, vCenter et SCVM. Dans de nombreux cas, les informations provenant de différents périphériques doivent être collectées et corrélées. Lors du dépannage, de nouvelles informations peuvent s'avérer nécessaires au fil du temps et le faire au cours d'une (longue) session WebEx ou en récupérant (de grandes) offres d'assistance via Intersight n'est pas toujours le moyen le plus efficace. À l'aide de RADKit, un ingénieur du centre d'assistance technique peut demander les informations requises au cours du processus de dépannage, à partir des différents périphériques et services, de manière sécurisée et contrôlée.

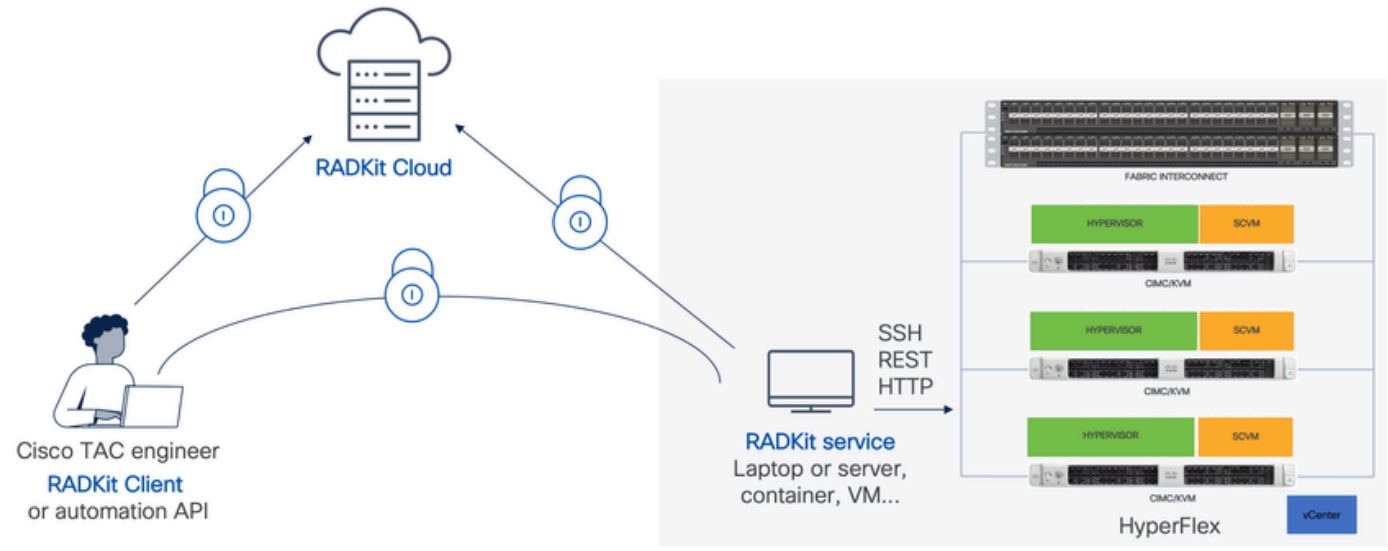
RADKit et Intersight

Intersight reste la principale méthode de connectivité pour les clusters HyperFlex, offrant de nombreux avantages tels que la collecte automatique des journaux, la télémétrie et la surveillance proactive de votre environnement pour le matériel et d'autres alertes connues.

Bien qu'un grand nombre de clusters HX soient connectés à Intersight, Intersight est actuellement principalement destiné au déploiement, à la maintenance et à la surveillance de vos clusters HyperFlex. Intersight permet de collecter des bundles d'assistance et des informations télémétriques, ce qui constitue généralement un bon point de départ pour le dépannage. Pour le dépannage en direct, où dans un scénario classique, un ingénieur TAC utiliserait une session WebEx, RADKit est mis en place. Il ne remplace pas Intersight, mais ajoute une approche différente du dépannage, soit en utilisant une session interactive, soit en exploitant des séquences de requête-réponse programmatiques.

Présentation de haut niveau

Diagramme de connectivité



Composants

- RADKit Service : composant de service RADkit sur site, utilisé comme passerelle sécurisée vers votre environnement HX. En tant que client, vous conservez le contrôle total sur les périphériques accessibles et sur les personnes autorisées à y accéder à tout moment. Ce service peut être hébergé sur n'importe quelle machine Linux, MacOS ou Windows.
- RADKit Client : solution frontale utilisée par l'ingénieur du centre d'assistance technique pour accéder à votre environnement à l'aide de fonctions de dépannage et de surveillance programmatiques, de récupération automatisée et d'analyse des sorties des périphériques à l'aide d'outils internes de Cisco ou d'une interaction directe avec les périphériques via l'interface de ligne de commande.
- RADKit Cloud : assure un transport sécurisé entre le client et le service.

Préparation

Présentation des étapes à suivre

Les étapes suivantes sont requises avant qu'un ingénieur TAC puisse utiliser RADKit pour connecter et dépanner votre environnement HX :

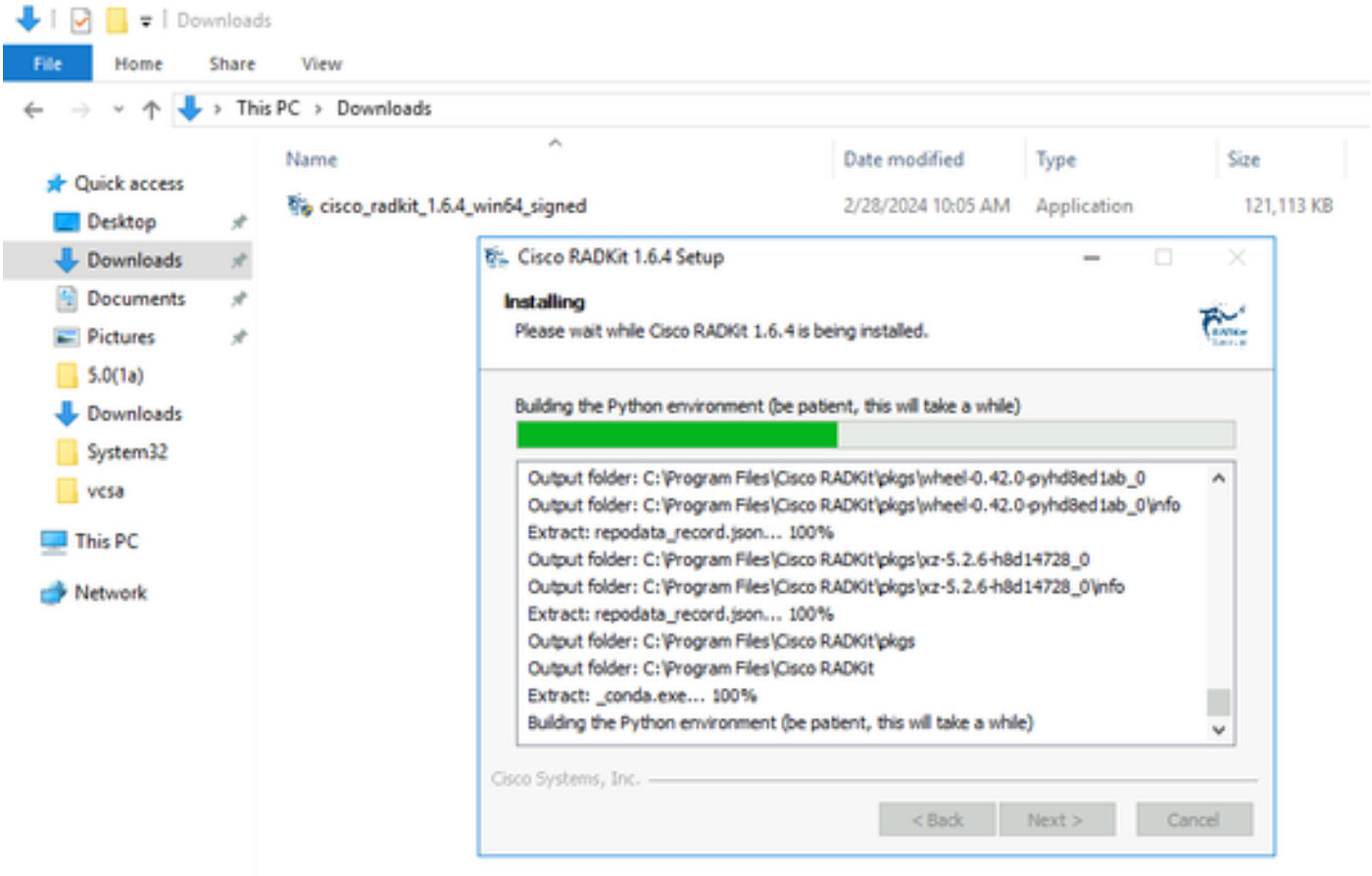
1. Téléchargez et installez le service RADkit. Il peut être installé sur n'importe quelle machine Linux, MacOS ou Windows.
2. Démarrez le service RADKit et effectuez la configuration initiale (bootstrap). Créez un compte super admin pour continuer à gérer le service RADKit via une interface Web.
3. Inscrivez votre service RADKit avec le cloud RADKit. Enregistrez votre service RADKit sur le cloud RADKit et générez un ID de service pour identifier votre environnement.
4. Ajoutez des périphériques et des terminaux. Fournissez une liste des périphériques et stockez les informations d'identification des périphériques qui peuvent être nécessaires.

Une explication plus détaillée/générique de ces étapes peut être trouvée ici : https://radkit.cisco.com/docs/pages/one_page_setup.html

Étape 1. Télécharger et installer le service RADKit

Les détails dans cette étape peuvent être un peu différents, selon le système d'exploitation que vous utilisez pour installer le service RADKit, mais en général, le processus est très similaire. Téléchargez la dernière version de votre système d'exploitation à l'adresse suivante : https://radkit.cisco.com/downloads/release/.

Exécutez le programme d'installation de votre système et suivez les instructions jusqu'à ce que l'installation soit terminée :



Une fois que tous les composants RADKit sont installés, vous pouvez passer à l'étape suivante de la configuration initiale.

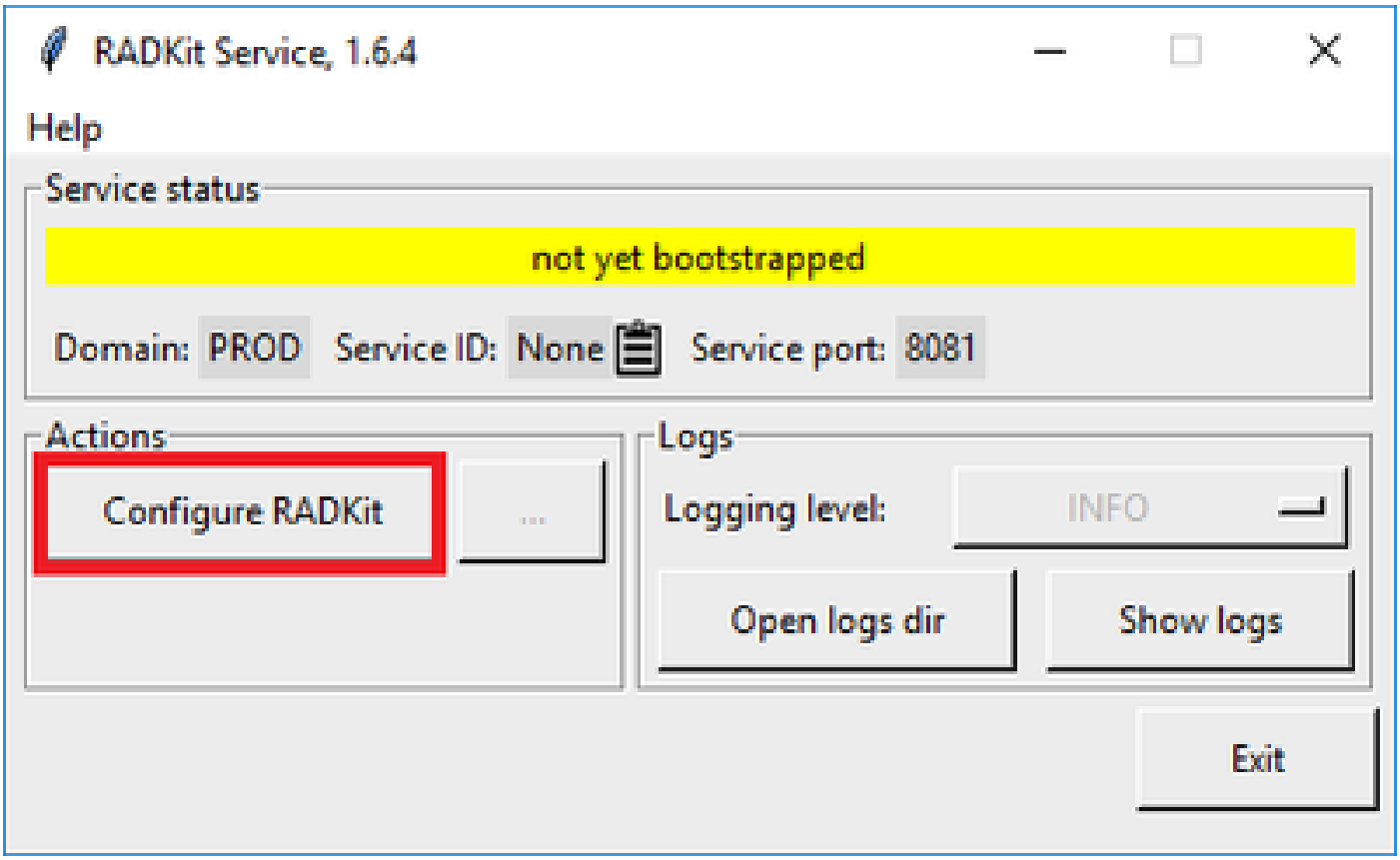
Étape 2. Démarrez le service RADKit et effectuez la configuration initiale (bootstrap)

Au cours de cette étape, créez un compte superadmin pour continuer à gérer le service RADKit via une interface Web.

Recherchez RADKit Service dans le menu Démarrer (sous Windows) ou le dossier Applications (sous macOS) et démarrez-le :

La toute première fois que vous le démarrez, le démarrage du service RADKit peut prendre un peu de temps (environ 10 à 30 secondes selon la vitesse de votre système). Les exécutions suivantes seront beaucoup plus rapides.

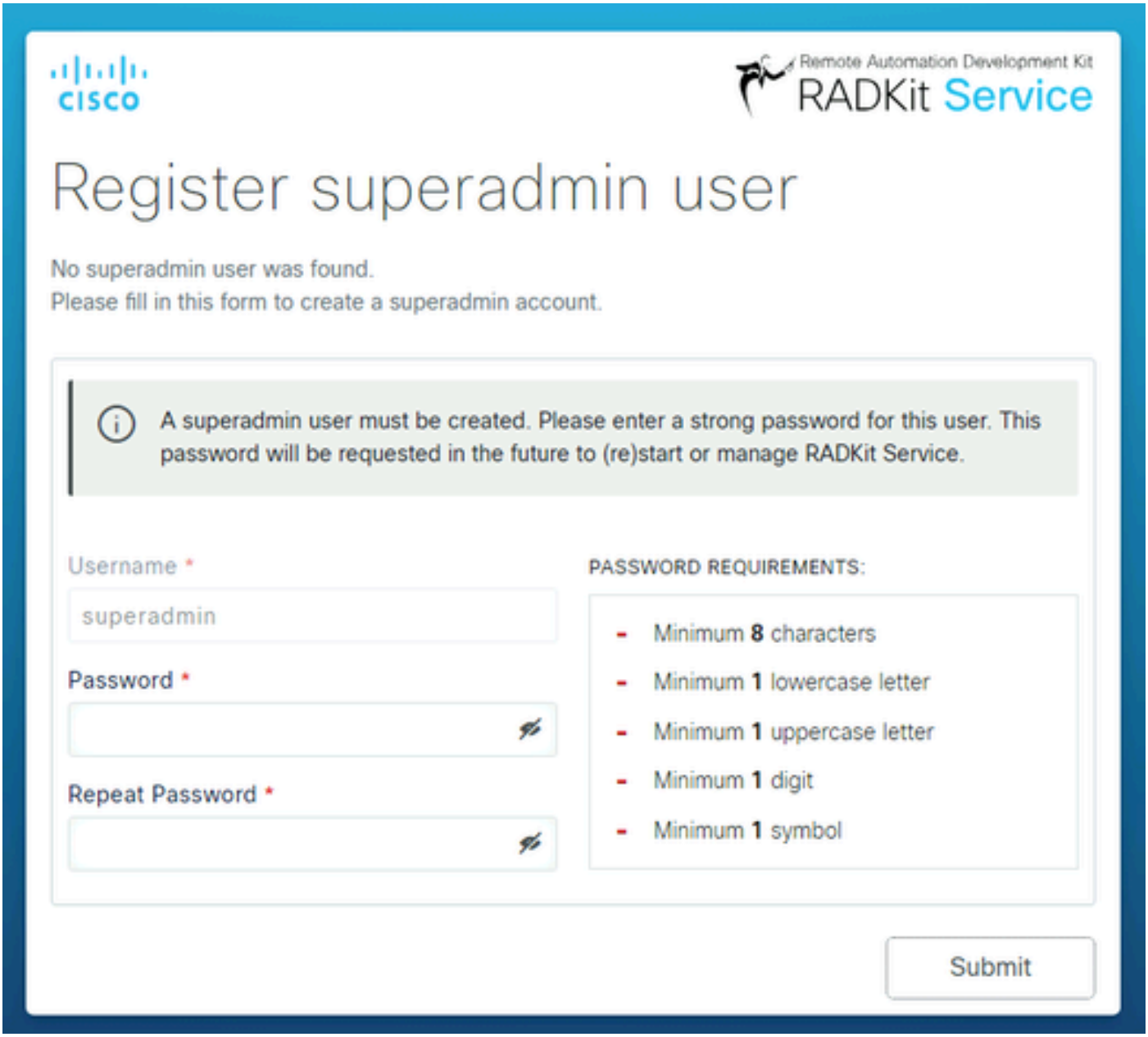
Une fois le démarrage terminé, dans la boîte de dialogue RADKit Service, une fois que l'état change pour not yet bootstrapped appuyer sur Configure RADKit :



Cela ouvre votre navigateur Web et vous amène à l'interface Web du service RADKit, une interface de gestion basée sur le Web qui vous permet de gérer le service RADKit.

Il est censé recevoir un avertissement de certificat, que vous pouvez ignorer, lors de la connexion à cette URL car il utilise un certificat auto-signé.

Étant donné qu'un utilisateur superadmin n'existe pas encore, l'interface utilisateur Web vous demandera de créer un mot de passe pour cet utilisateur :



Sélectionnez un mot de passe qui respecte les exigences de force de mot de passe affichées à droite.

Le mot de passe de ce compte sera utilisé pour protéger les secrets tels que les clés privées et les identifiants de périphérique. Si vous le perdez, tous les secrets seront perdus et le service RADKit devra être réinitialisé. Choisissez-le avec soin et notez-le dans un emplacement sécurisé. Il peut être modifié ultérieurement si nécessaire.

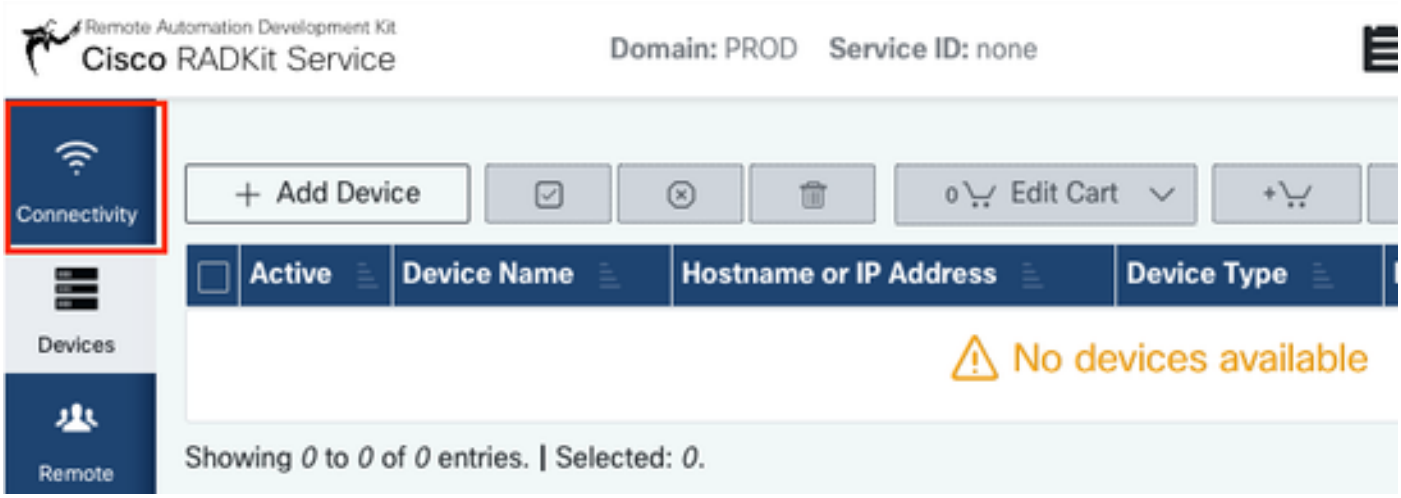
Après avoir créé le compte superadmin, utilisez-le pour vous connecter à WebUI :

Une fois que le compte superadmin a été créé et que vous vous êtes connecté avec succès à l'interface utilisateur Web, vous pouvez passer à l'étape suivante où votre service RADKit est enregistré avec le composant cloud RADKit.

Étape 3. Inscrivez votre service RADKit avec RADKit Cloud

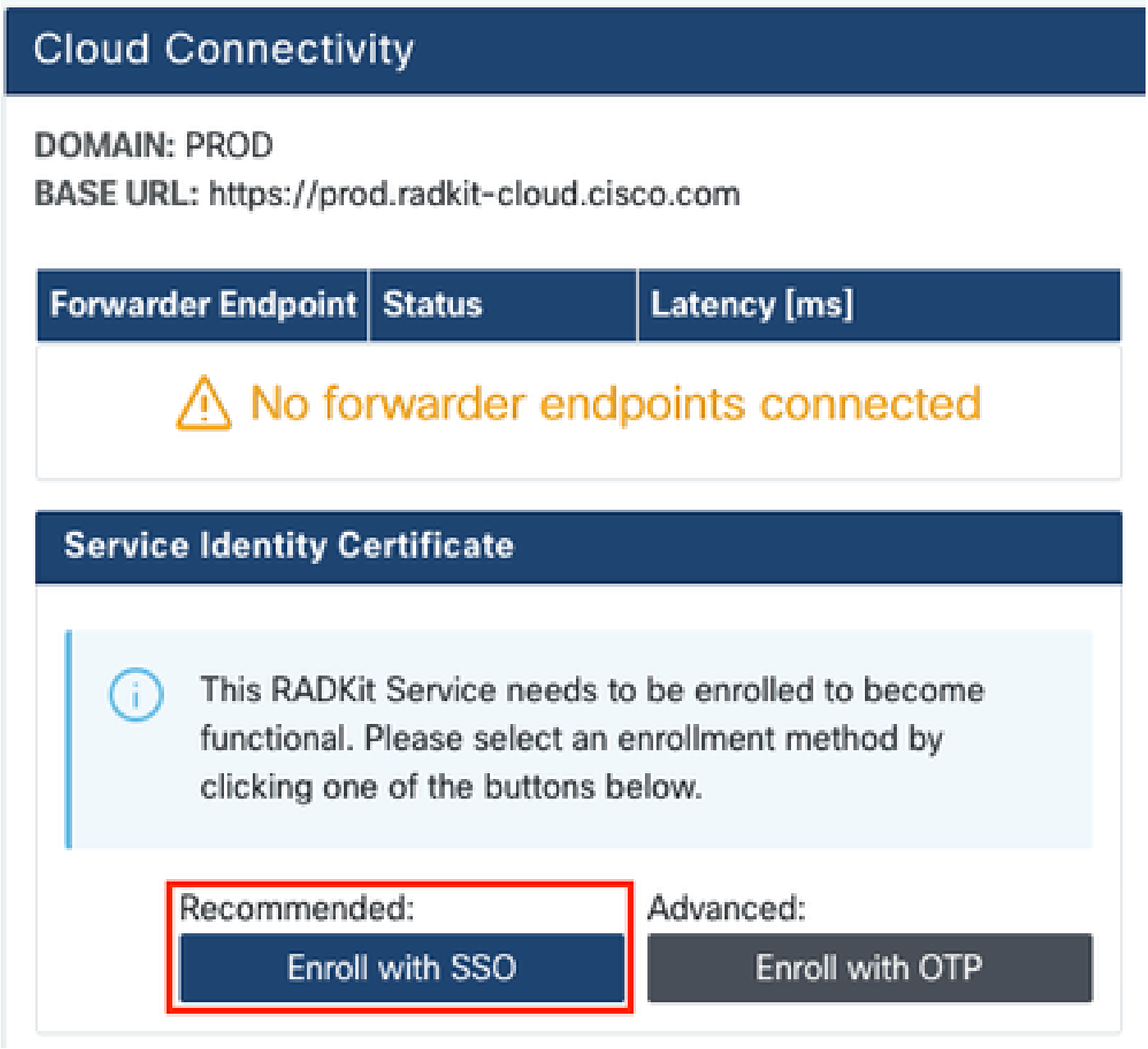
Dans cette étape, enregistrez votre service RADKit avec le cloud RADKit et générez un ID de service pour identifier votre environnement.

Après vous être connecté à WebUI avec l'utilisateur superadmin (voir l'étape 2), accédez à l'écran de connectivité :

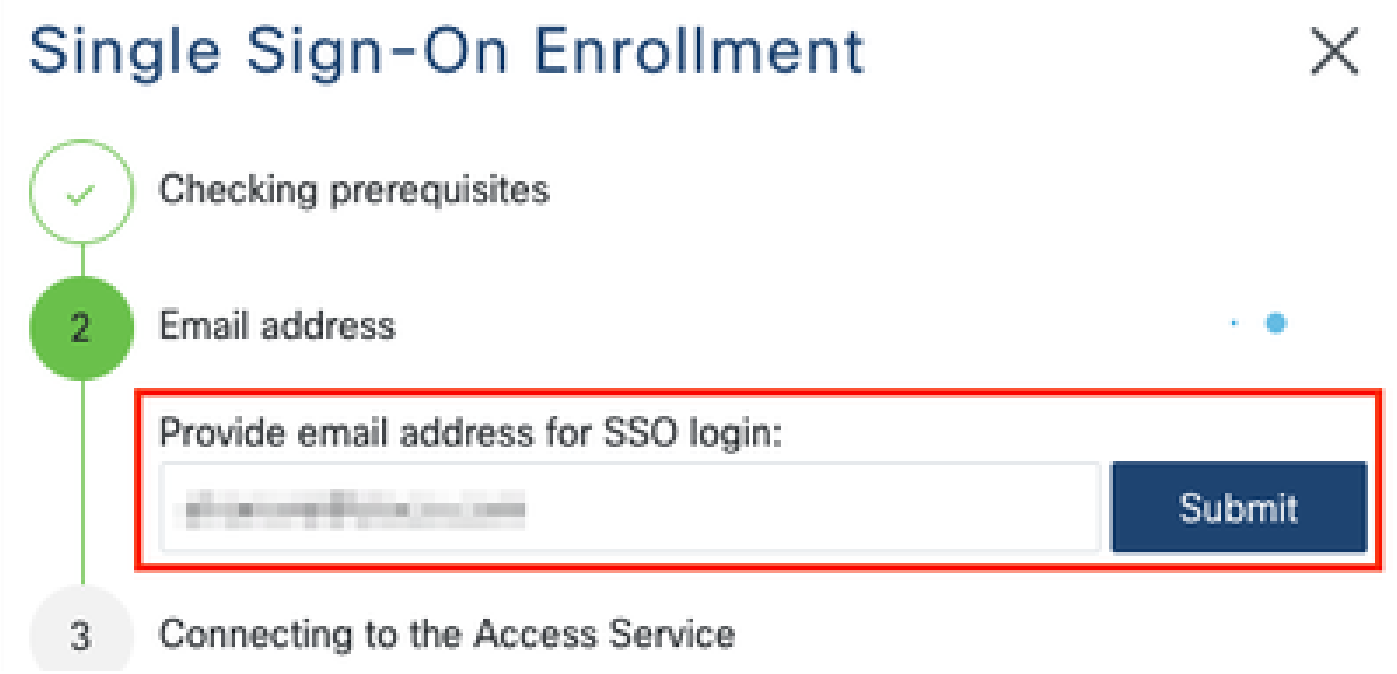


Si vous avez besoin d'un proxy pour vous connecter à Internet, reportez-vous aux instructions de configuration détaillées disponibles ici : https://radkit.cisco.com/docs/pages/one_page_setup.html

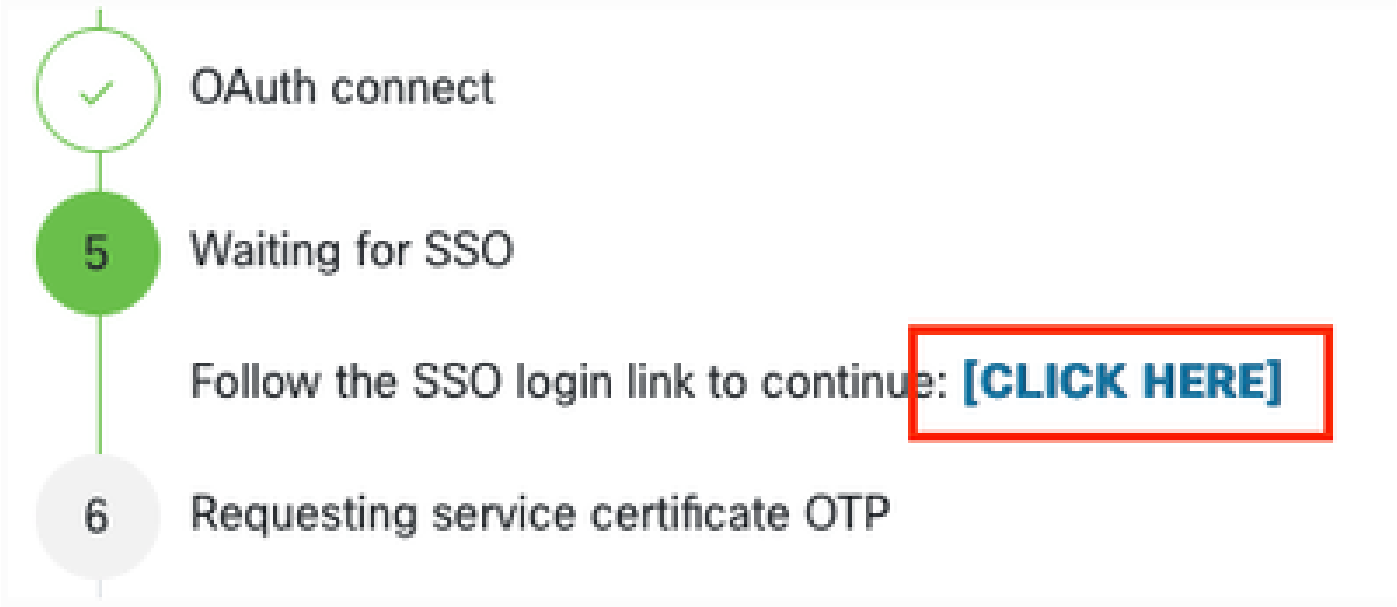
Vous devez à présent inscrire le service pour le connecter à RADKit Cloud. Pour ce faire, connectez-vous via l'interface utilisateur Web du service à l'aide de votre compte Cisco.com (CCO). Cliquez sur Enroll with SSO pour continuer :



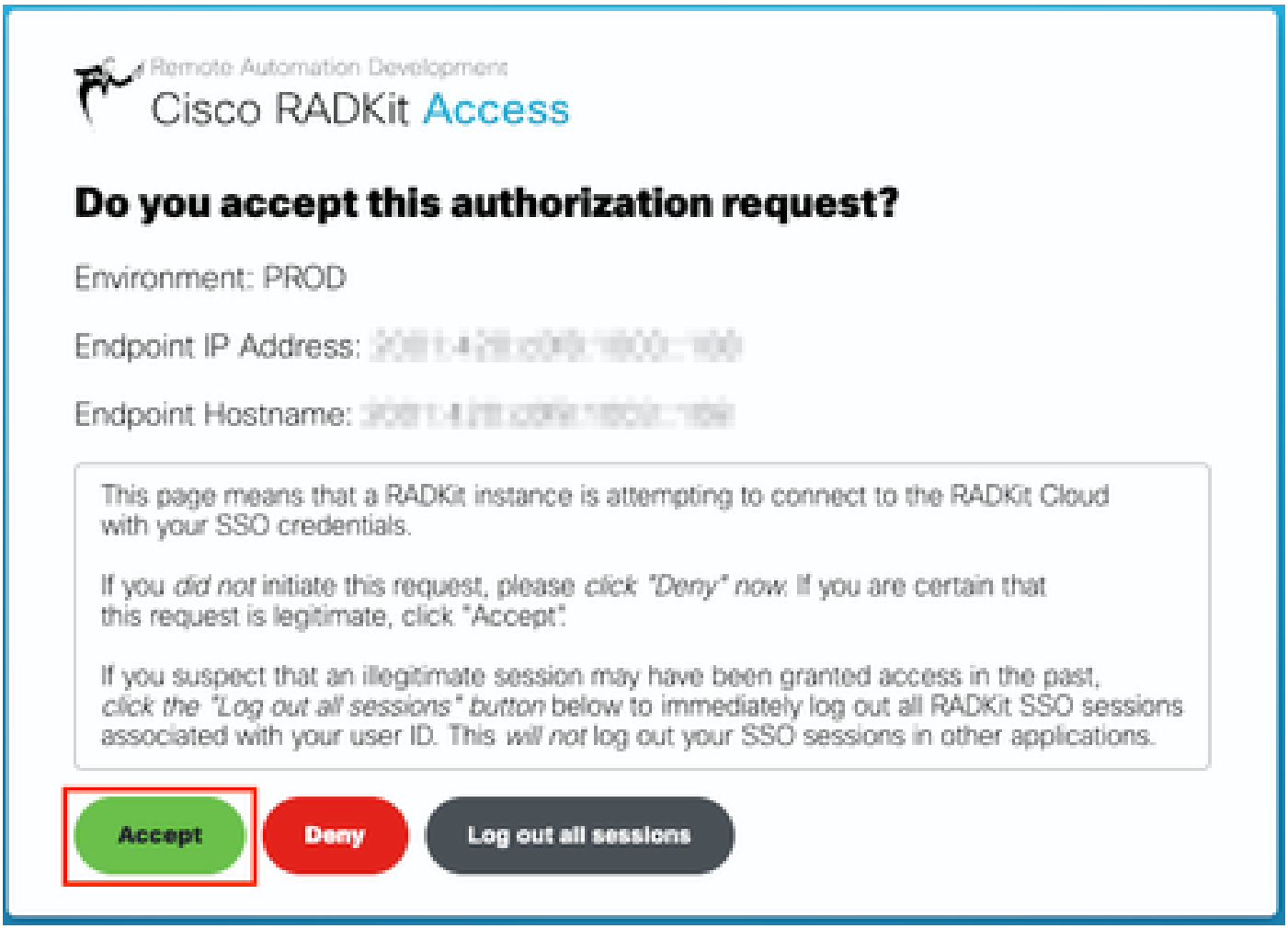
Saisissez l'adresse e-mail correspondant à votre compte Cisco.com (CCO) dans le champ d'adresse e-mail de l'étape 2. et cliquez sur Submit as shown in the image:



Une fois que le service RADKit se connecte à RADKit Cloud pour obtenir une autorisation, il affiche un lien qui vous mène vers le serveur Cisco[CLICK HERE] SSO pour l'authentification. Cliquez sur le lien pour continuer ; il s'ouvrira dans un nouvel onglet/une nouvelle fenêtre de navigateur. Assurez-vous d'utiliser la même adresse e-mail pour vous connecter à SSO, comme celle que vous avez entrée à l'étape mentionnée précédemment :



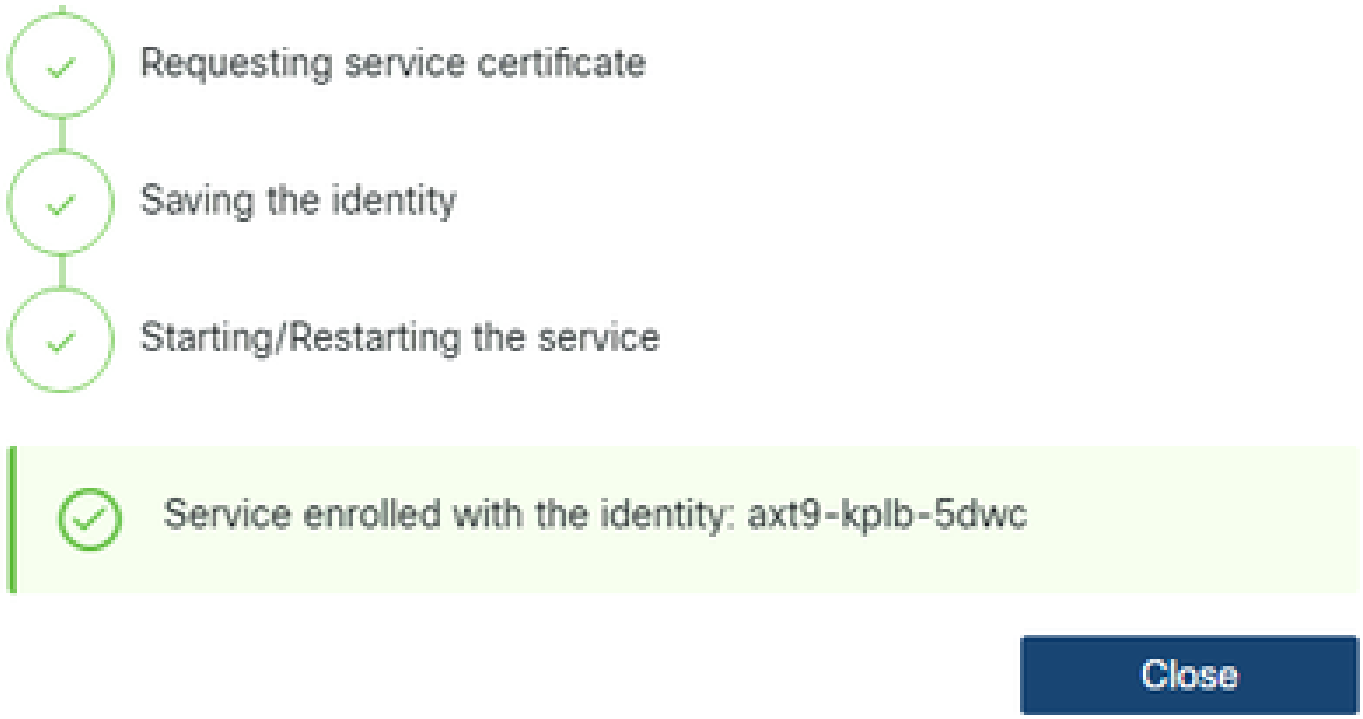
Une fois l'authentification SSO terminée (ou immédiatement si vous avez déjà été authentifié), vous êtes redirigé vers une page de confirmation d'accès RADKit. Lisez les informations de la page et cliquez sur Accept pour autoriser le service RADKit à s'inscrire avec votre compte CCO en tant que propriétaire.



Vous accédez ensuite à un écran qui indique Authentication result: Success .

Ne cliquez pas sur le boutonLog out all sessions ; fermez simplement l'onglet/la fenêtre SSO et revenez à l'interface Web du service RADKit.

Ceci montre Service enrolled with the identity: … . L'identifiant unique qui suit est votre ID de service RADKit, également appelé numéro de série du service. Dans l'exemple de capture d'écran, l'ID de service est axt9-kplb-5dwc le vôtre. Il sera différent.



Cliquez sur Close pour fermer la boîte de dialogue et revenir à l'Connectivity écran.

Après l'actualisation de l'interface WebUI, votre ID de service s'affiche en haut de l'interface utilisateur graphique de RADKit, ainsi que l'état de connectivité, comme indiqué ici :

Chaque fois qu'un ingénieur TAC a besoin d'accéder à l'un des périphériques de votre environnement, il a besoin de cet ID de service pour identifier votre service RADKit.

Maintenant qu'une connectivité est établie avec le composant cloud RADKit et qu'un ID de service est généré, ajoutez à l'étape suivante les périphériques accessibles via RADKit.

Étape 4. Ajout de périphériques et de terminaux

Au cours de cette étape, ajoutez les périphériques et leurs informations d'identification pour les périphériques accessibles via RADKit. Pour HyperFlex, cela signifie qu'idéalement, ces périphériques et leurs informations d'identification doivent être ajoutés :

Périphérique	Type de périphérique	Protocoles de gestion	Identifiants	Ports TCP transférés	Remarques
Hyperviseur (hôtes	Linux	Terminal (SSH)	racine		

ESXi)					
Contrôleur de stockage (SCVM)	HyperFlex	Terminal (SSH)Swagger	admin root (enable)	443	Entrez le mot de passe racine dans le champ enable password. Ce code sera utilisé lorsqu'un jeton de consentement est requis. Pour Swagger : décochez la case « Vérifier le certificat TLS » et laissez le champ URL de base vide
vCenter	Linux	Terminal (SSH)	racine		
UCSM	Générique	Terminal (SSH)	admin		
Installer (facultatif)	Linux	Terminal (SSH)	racine	443	
CIMC (uniquement pour les clusters de périphérie)	Générique	Terminal (SSH)	admin		
Témoin (uniquement pour les clusters étirés)	Linux	Terminal (SSH)	racine		
Intersight CVA/PCA (en option)	Linux	Terminal (SSH)	admin	443	

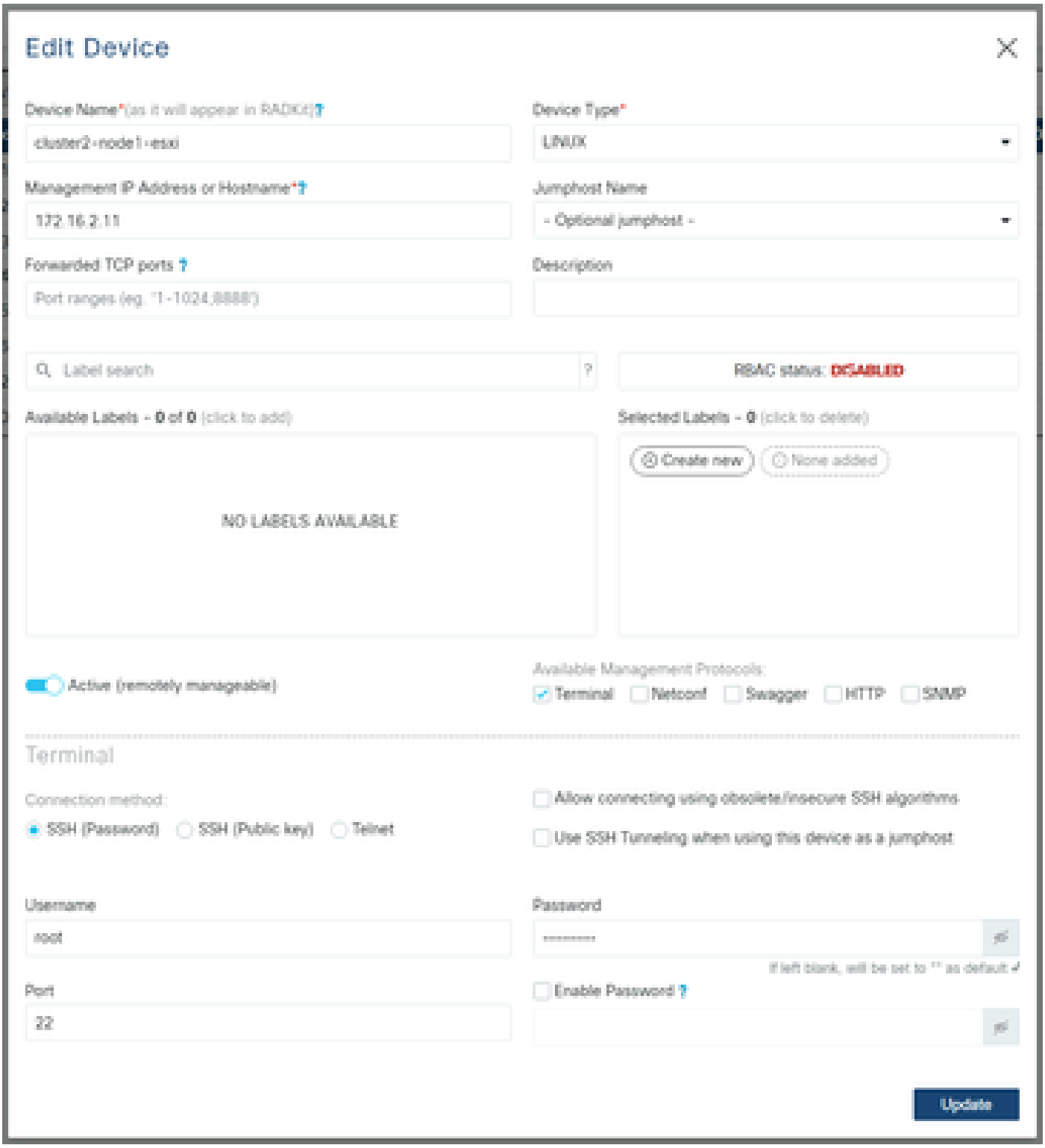
Il est important d'ajouter les périphériques uniquement en utilisant leur adresse IP et non leur nom d'hôte, car cela est nécessaire pour mettre en corrélation les périphériques qui appartiennent au même cluster.

Pour ajouter ces périphériques, dans l'interface utilisateur Web RADKit, accédez à l'écran Devices (Périphériques) :

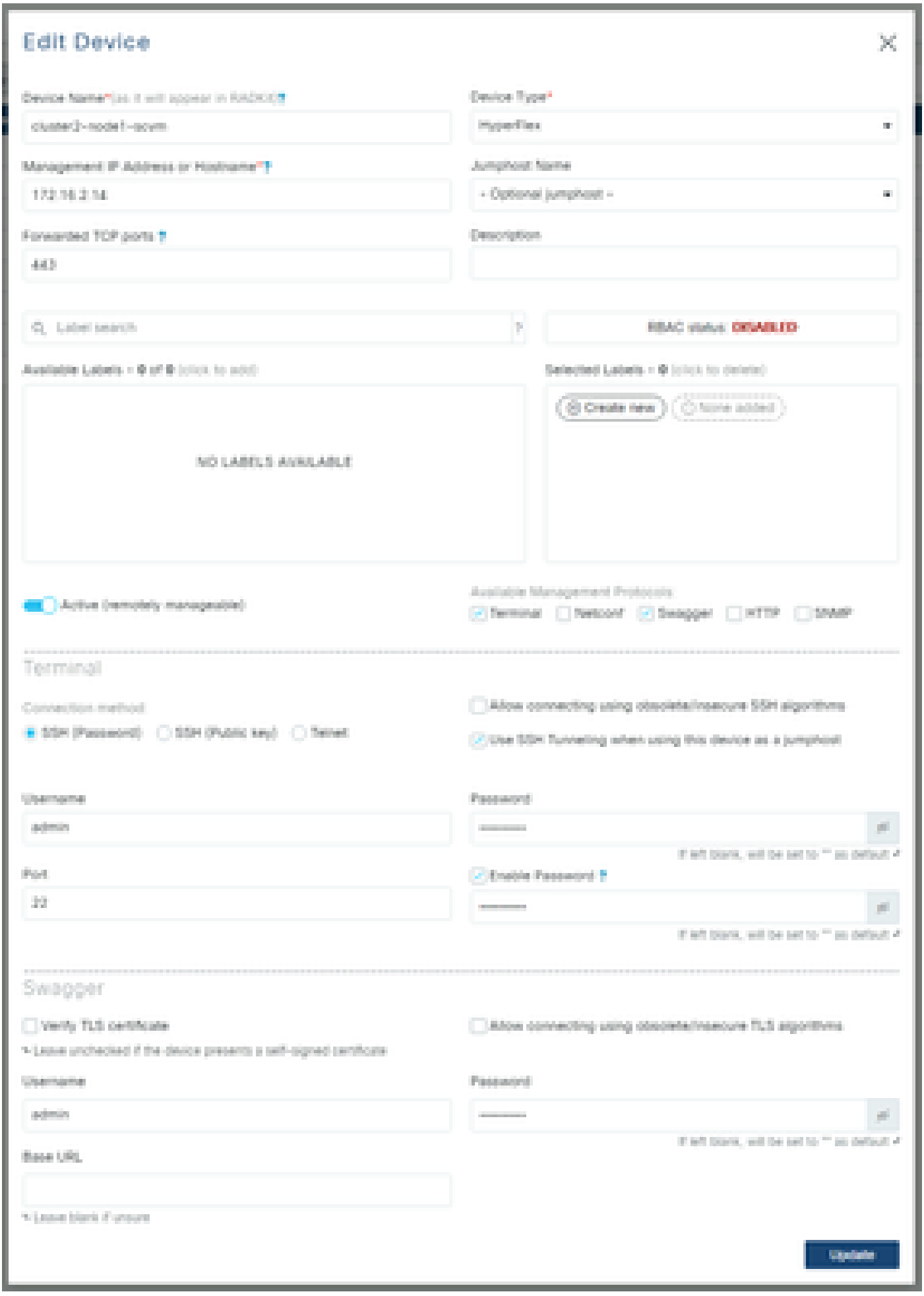
Pour chacun des périphériques répertoriés ci-dessus, créez une nouvelle entrée en cliquant sur Add Device . Saisissez l'adresse IP, sélectionnez le type de périphérique et fournissez des détails en fonction de chaque type de périphérique pour tous les noeuds de votre cluster. Lorsque vous avez terminé, cliquez sur Add & closepour revenir à l'écran Devices (Périphériques) ou Add & continue pour ajouter un autre périphérique.

Vous trouverez ici des exemples d'entrées et leur configuration pour chaque type de périphérique :

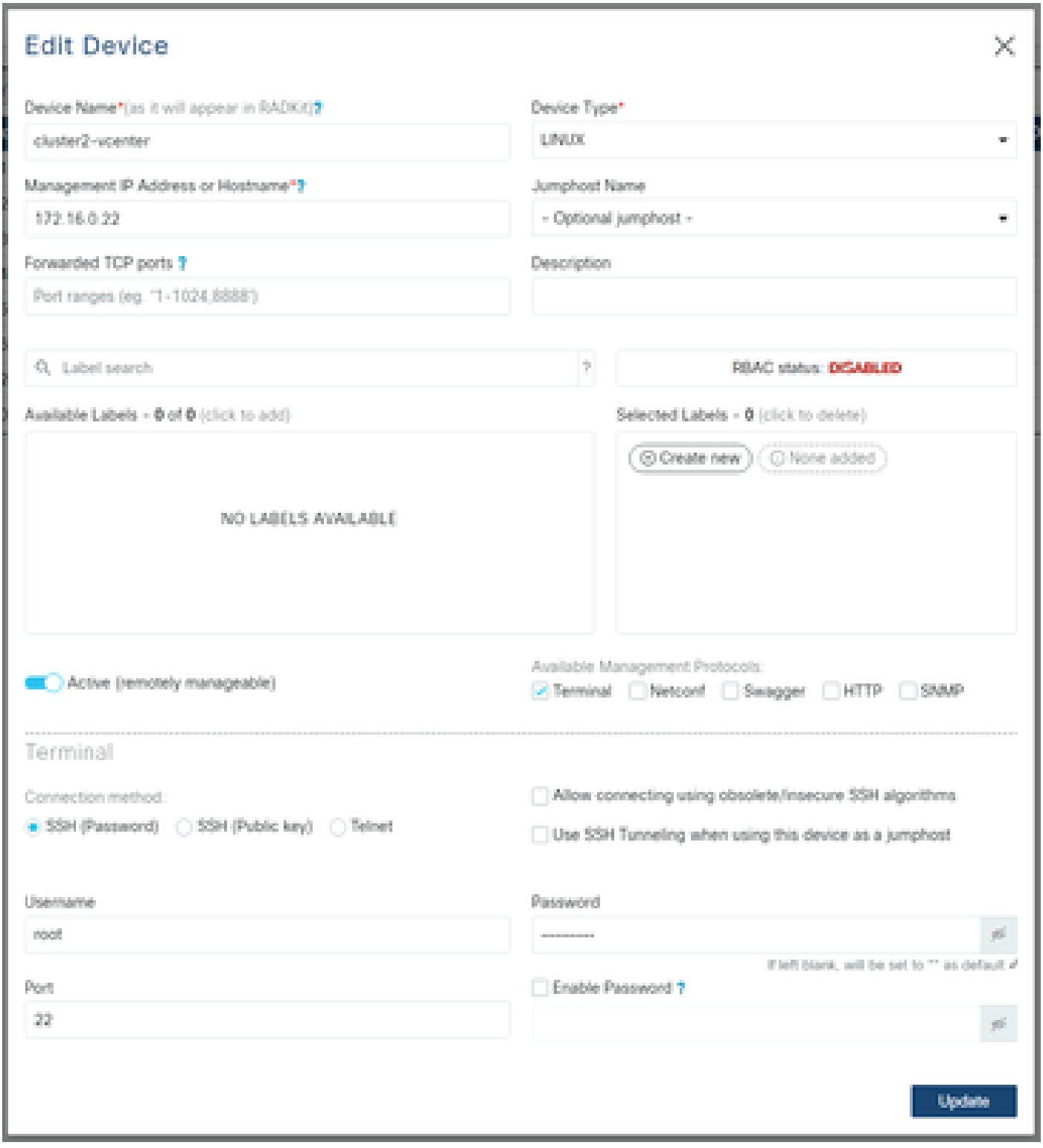
Exemple pour les hôtes ESXi :



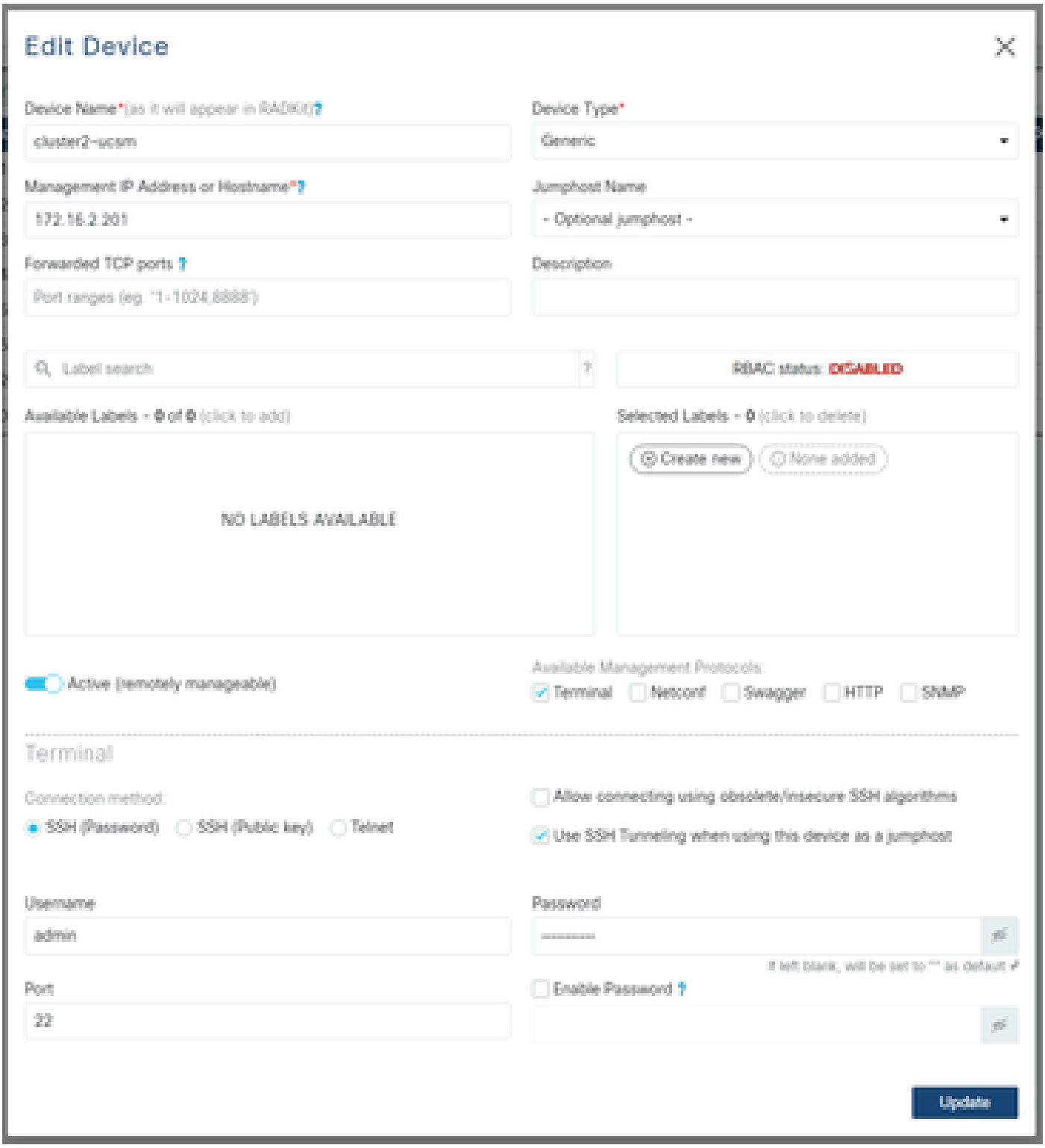
Exemple pour les contrôleurs de stockage :


Edit Device
Device Name*(as it will appear in RADKit)
cluster3-node1-acvm
Device Type*
HyperFlex
Management IP Address or Hostname*
172.16.2.14
Jumphost Name
- Optional jumphost -
Forwarded TCP ports
443
Description
Label search
RBAC status: DISABLED
Available Labels - 0 of 0 (click to add)
NO LABELS AVAILABLE
Selected Labels - 0 (click to delete)
Create new
None added
Active (remotely manageable)
Available Management Protocols
Terminal
Netconf
Swagger
HTTP
SNMP
Terminal
Connection method
SSH (Password)
SSH (Public key)
Telnet
Allow connecting using obsolete/insecure SSH algorithms
Use SSH Tunneling when using this device as a jumphost
Username
admin
Password
If left blank, will be set to "" as default
Port
22
Enable Password
If left blank, will be set to "" as default
Swagger
Verify TLS certificate
Allow connecting using obsolete/insecure TLS algorithms
* Leave unchecked if the device presents a self-signed certificate
Username
admin
Password
If left blank, will be set to "" as default
Base URL
* Leave blank if unsure
Update

Exemple pour vCenter :



Exemple pour UCSM :



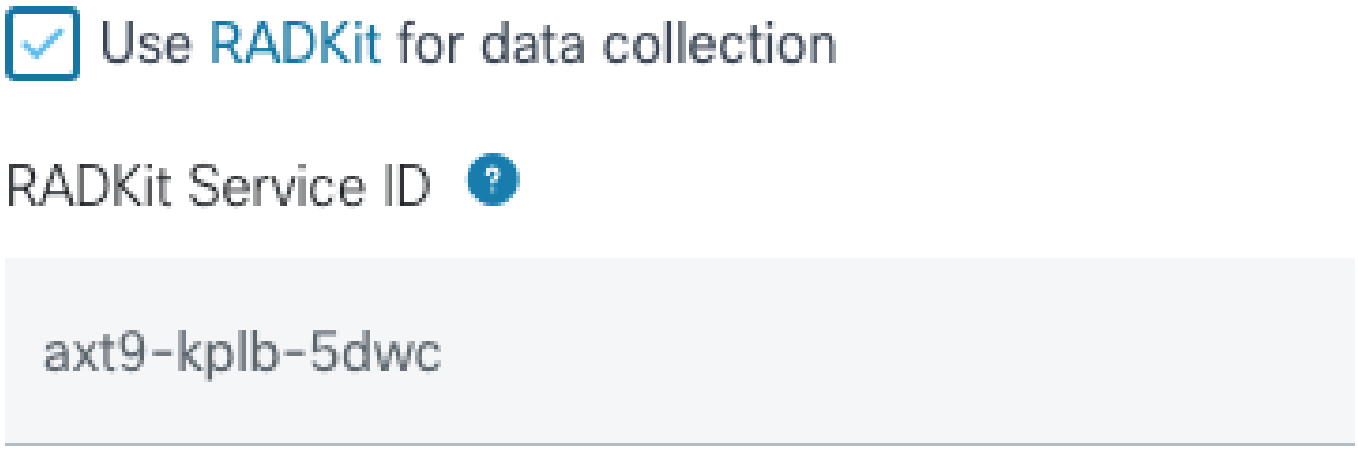
Utilisation de RADKit sur un TAC SR

Si toute la préparation est terminée et que vous souhaitez fournir l'accès à vos périphériques à un ingénieur du centre d'assistance technique, vous pouvez suivre ces étapes.

Un ingénieur a besoin de votre ID de service RADKit et d'un accès à votre environnement ou à des périphériques sélectionnés (lors de l'utilisation de RBAC) pendant le temps requis.

1. Fournir l'ID de service RADKit

Si vous n'avez pas encore ouvert de dossier TAC, vous avez la possibilité de le mentionner Use RADKit for data collection dans le gestionnaire de dossiers d'assistance sur Cisco.com :

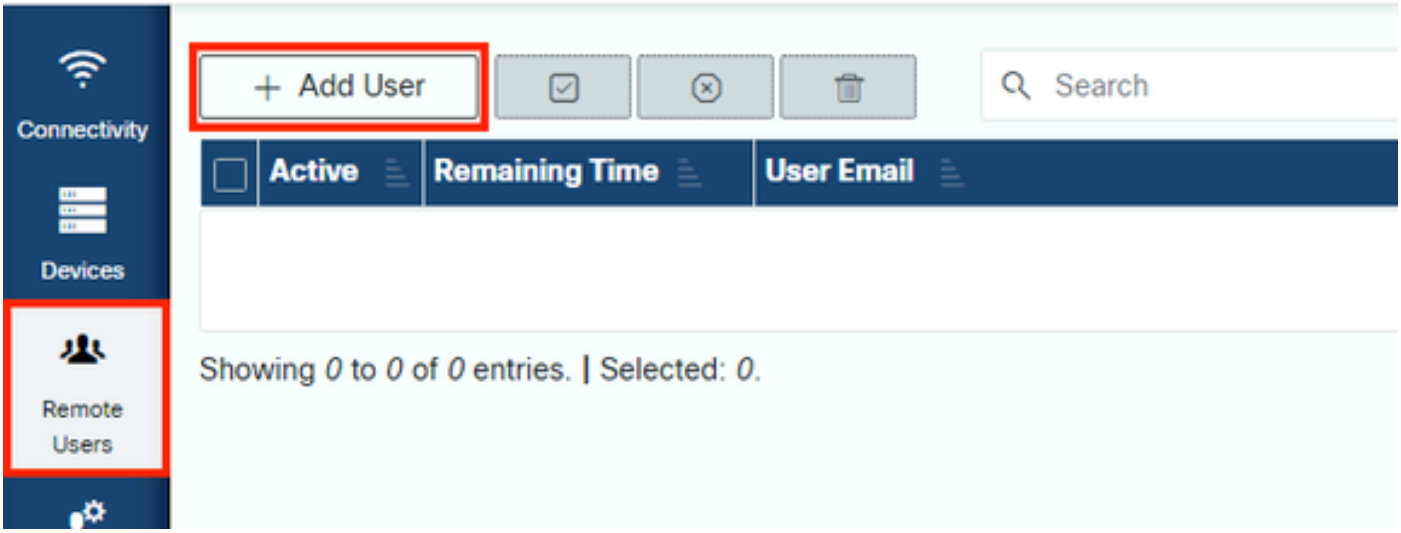


Si vous avez déjà une demande de service en cours, vous pouvez ajouter l'ID de service RADKit dans le Gestionnaire de cas d'assistance avec la section Coordonnées du client :

Vous pouvez également mentionner votre ID à l'ingénieur du centre d'assistance technique chargé de votre dossier.

2. Ajouter un utilisateur distant

Avant qu'un utilisateur puisse utiliser vos périphériques, vous devez fournir un accès explicite et configurer une période pendant laquelle cet accès reste valide. Pour ce faire, dans l'interface utilisateur Web RADKit, accédez à l'Remote Users écran et créez un nouvel utilisateur distant en cliquant sur Add User.



Saisissez l'adresse e-mail @cisco.com de l'ingénieur TAC (attention aux fautes de frappe). Assurez-vous de prêter attention à la caseActivate this user à cocher et aux Time slice ou Manual paramètres.

Pendant que l'utilisateur est actif, il a accès aux périphériques configurés via le service RADKit, à condition que ces périphériques soient activés et que la stratégie RBAC le lui permette.

La tranche de temps représente la durée après laquelle l'utilisateur sera automatiquement désactivé ; en d'autres termes, une tranche de temps représente une session de dépannage limitée dans le temps. La session de l'utilisateur peut être prolongée jusqu'à la durée de la tranche de temps de cet utilisateur. Si vous préférez activer/désactiver manuellement les utilisateurs, sélectionnez Manual plutôt.

Les utilisateurs peuvent toujours être activés/désactivés manuellement, qu'une tranche de temps soit configurée ou non. Lorsqu'un utilisateur est désactivé, toutes ses sessions via le service RADKit sont instantanément déconnectées.

Lorsque vous avez terminé, cliquez sur Add & close pour revenir à l'écran Utilisateurs distants.

Informations connexes

- Vous trouverez plus d'informations et des réponses aux questions les plus courantes sur le site Web de RADKit : https://radkit.cisco.com/
- **Assistance technique de Cisco et téléchargements**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.