Exemple enregistré par individu de configuration portaile d'invité de version 1.3 ISE

Contenu

Introduction

La version 1.3 du Logiciel Cisco Identity Services Engine (ISE) a un nouveau type de portail d'invité appelé le portail d'invité enregistré par individu, qui permet l'auto-registre d'utilisateurs d'invité quand ils accèdent aux ressources de réseau. Ce portail te permet pour configurer et personnaliser de plusieurs caractéristiques. Ce document décrit comment configurer et dépanner cette fonctionnalité.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez l'expérience avec la configuration ISE et la connaissance de base de ces thèmes :

- Déploiements ISE et écoulements d'invité
- Configuration des contrôleurs LAN Sans fil (WLC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Version 7.6 et ultérieures de Cisco WLC
- Logiciel ISE, version 3.1 et ultérieures

Topologie et écoulement

Ce scénario présente des nombreuses options disponibles pour des utilisateurs d'invité quand ils exécutent l'auto-enregistrement.

Voici le flux général :

Étape 1. Associés d'utilisateur d'invité à l'Identifiant SSID (Service Set Identifier) : Invité. C'est un réseau ouvert avec le filtrage MAC avec ISE pour l'authentification. Cette authentification apparie la deuxième règle d'autorisation sur l'ISE et les redirect to de profil d'autorisation le portail enregistré par individu d'invité. ISE renvoie un RAYON Access-reçoit avec deux Cisco-poids du commerce-paires :

- URL-réorienter-acl (que le trafic devrait être réorienté, et le nom de la liste de contrôle d'accès (ACL) défini localement sur le WLC)
- URL-réorientez (où réorienter ce trafic à ISE)

Étape 2. L'utilisateur d'invité est réorienté à ISE. Plutôt que fournissent les qualifications afin d'ouvrir une session, l'utilisateur que les clics « n'ont pas un compte ». L'utilisateur est réorienté à une page où ce compte peut être créé. Un code secret facultatif d'enregistrement pourrait être activé afin de limiter le privilège d'auto-enregistrement aux gens qui connaissent cette valeur secrète. Après que le compte soit créé, l'utilisateur est les qualifications fournies (nom d'utilisateur et mot de passe) et les logins avec ces qualifications.

Étape 3. ISE envoie une modification de RAYON de l'autorisation (CoA) authentifie à nouveau au WLC. Le WLC authentifie à nouveau l'utilisateur quand il envoie l'Access-demande de RAYON avec l'attribut réservé Autoriser. ISE répond avec ACL Access-reçoit et d'Airespace défini localement sur le WLC, qui fournit l'accès à Internet seulement (l'accès final pour l'utilisateur d'invité dépend de la stratégie d'autorisation).

Notez que pour des sessions de Protocole EAP (Extensible Authentication Protocol), ISE doit envoyer un CoA se termine afin de déclencher la ré-authentification parce que la session d'EAP est entre le suppliant et l'ISE. Mais pour le MAB (filtrage MAC), CoA Reauthenticate est assez ; il n'y a aucun besoin de-associate/de-authenticate le client sans fil.

Étape 4. L'utilisateur d'invité a désiré l'accès au réseau.

De plusieurs fonctionnalités supplémentaires comme la posture et le Bring Your Own Device (BYOD) peuvent être activées (discuté plus tard).

Configurez

WLC

1. Ajoutez le nouveau serveur de RAYON pour l'authentification et la comptabilité. Naviguez vers la **Sécurité > l'AAA > Radius > Authentication** afin d'activer CoA de RAYON (RFC 3576).

   Il y a une configuration semblable pour la comptabilité. On lui informe également configurer le WLC pour envoyer le SSID dans l'attribut d'ID de station appelée, qui permet à l'ISE pour configurer des règles flexibles basées sur le SSID :

2. Sous les WLAN tabulez, créez l'invité Sans fil du RÉSEAU LOCAL (WLAN) et configurez l'interface appropriée. Placez la Sécurité Layer2 à **aucun** avec le filtrage MAC. Dans des serveurs de Sécurité/Authentification, autorisation et comptabilité (AAA), sélectionnez l'adresse IP ISE pour l'authentification et la comptabilité. Sur l'onglet Avancé, le **dépassement d'AAA d'**enable et a placé l'état de Contrôle d'admission au réseau (NAC) au RAYON NAC (support CoA).

3. Naviguez vers la **Sécurité > les listes de contrôle d'accès > les listes de contrôle d'accès** et créez deux Listes d'accès :

   GuestRedirect, qui permet le trafic qui ne devrait pas être réorienté et réoriente tout autre traficInternet, qui est refusé pour des réseaux d'entreprise et permis pour tous les autres

   Voici un exemple pour l'ACL de GuestRedirect (le besoin d'exclure le trafic à/de ISE de la redirection) :

ISE

1. Naviguez vers l'**accès invité > configurent > des portails d'invité**, et créent un nouveau type portail, portail d'invité enregistré par individu :

2. Choisissez le nom portail qui sera mis en référence dans le profil d'autorisation. Placez toutes les autres configurations pour se transférer. Sous la personnalisation de page du portail, toutes les pages présentées peuvent être personnalisées.

3. Configurez les profils d'autorisation :

   Invité (avec la redirection à nom portail et à ACL GuestRedirect d'invité)

   PermitInternet (avec l'Internet égal d'ACL d'Airespace)

4. Afin de vérifier les règles d'autorisation, naviguez vers la **stratégie > l'autorisation**. Dans ISE la version 1.3 par défaut pour l'authentification défectueuse d'accès de dérivation d'authentification MAC (MAB) (adresse MAC non trouvée) est continuée (non rejeté). C'est très utile pour des portails d'invité parce qu'il n'y a aucun besoin de changer n'importe quoi dans des règles d'authentification par défaut.

   Les nouveaux utilisateurs qui s'associent à l'invité SSID ne sont pas encore une partie de tout groupe d'identité. C'est pourquoi ils apparient la deuxième règle, qui emploie le profil d'autorisation d'invité pour les réorienter au portail correct d'invité.

   Après qu'un utilisateur crée un compte et des logins avec succès, ISE envoie un CoA de RAYON et le WLC exécute la ré-authentification. Cette fois, la première règle est appariée avec le profil PermitInternet d'autorisation et renvoie le nom d'ACL qui est appliqué sur le WLC.

5. Ajoutez le WLC comme périphérique d'accès au réseau de la **gestion > des ressources de réseau > des périphériques de réseau**.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Après que vous vous associiez avec l'invité SSID et tapiez un URL, puis vous êtes réorienté à la page de connexion :

2. Puisque vous n'avez aucune qualification encore, devez-vous choisir **n'avez-vous pas un compte ?** option. Une nouvelle page qui permet la création de compte affiche. Si l'option de code d'enregistrement était activée sous la configuration portaile d'invité, cette valeur secrète est exigée (ceci s'assure que seulement aux gens avec des autorisations correctes sont permis l'auto-registre).

3. S'il y a des problèmes avec le mot de passe ou la stratégie d'utilisateur, naviguez vers l'**accès invité > les configurations > la politique de mot de passe d'invité ou l'accès invité > les configurations > la stratégie de nom d'utilisateur d'invité** afin de changer des configurations. Voici un exemple :

4. Après que réussi rendent compte la création, vous sont présentées avec des qualifications (mot de passe généré selon des politiques de mot de passe d'invité) :

5. Cliquez sur **se connectent** et fournissent des qualifications (le code de passage supplémentaire d'Access pourrait être exigé si configuré sous le portail d'invité ; c'est un autre mécanisme de sécurité qui permet seulement ceux qui connaissent le mot de passe pour ouvrir une session).

6. Si réussie, une Politique d'Utilisation Acceptable facultative (AUP) pourrait être présentée (si configuré sous le portail d'invité). La page d'Access de courrier (aussi portail de dessous configurable d'invité) pourrait également afficher.

   La dernière page confirme qu'on a accordé l'accès :

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Àce stade, ISE présente ces logs :

Voici l'écoulement :

- L'utilisateur d'invité rencontre la deuxième règle d'autorisation (Guest_Authenticate) et est réorienté à l'invité (« Auhentication a réussi »).
- L'invité est réorienté pour l'auto-enregistrement. Après qu'avec succès la procédure de connexion (avec le compte de création récente), ISE envoie le CoA authentifiez à nouveau, qui est confirmé par le WLC (« autorisation dynamique réussie »).
- Le WLC exécute la ré-authentification avec l'attribut réservé Autoriser et le nom d'ACL est retourné (« réservé Autoriser réussi »). L'invité est fourni l'accès de réseau approprié.

Les états (les **exécutions > signale > ISE signale > accès invité signale > état d'invité de maître**)

confirme également cela :

Un utilisateur de sponsor (avec des privilèges corrects) peut vérifier l'état actuel d'un utilisateur d'invité.

Cet exemple confirme que le compte est créé, mais l'utilisateur n'a jamais ouvert une session (« attendant la procédure de connexion initiale ») :

Configuration facultative

Pour chaque étape de cet écoulement, différentes options peuvent être configurées. Toute la ceci est configurée par portail d'invité à l'**accès invité > configure > des portails > PortalName d'invité > édite > les configurations portailes de comportement et d'écoulement**. Des configurations plus importantes incluent :

Configurations d'Auto-enregistrement

- Type d'invité - Décrit combien de temps le compte est en activité, échéance options de mot de passe, heures de connexion et options (c'est la combinaison de profil de temps et de rôle d'invité de version 1.2 ISE)
- Code d'enregistrement - Si activés, on permet seulement à des utilisateurs qui connaissent le code secret l'auto-registre (doit fournir le mot de passe quand le compte est créé)
- AUP - Recevez la stratégie d'utilisation pendant l'auto-enregistrement
- La condition requise pour que le sponsor approuve/lancent le compte d'invité

Configurations d'invité de procédure de connexion

- Code d'accès - Si activés, on permet seulement aux des utilisateurs d'invité qui connaissent le code secret pour ouvrir une session
- AUP - Recevez la stratégie d'utilisation pendant l'auto-enregistrement
- Option de modification de mot de passe

Configurations d'enregistrement de périphérique

- Par défaut, le périphérique est enregistré automatiquement

Configurations de conformité de périphérique d'invité

- Tient compte d'une posture dans l'écoulement

Configurations BYOD

- Permet les utilisateurs en entreprise qui emploient le portail comme invités pour enregistrer leurs périphériques personnels

Comptes Sponsor-approuvés

Si les **invités auto-enregistrés Require à être** option **approuvée** est sélectionnés, alors le compte créé par l'invité doit être approuvé par un sponsor. Cette caractéristique pourrait employer l'email afin de fournir la notification au sponsor (pour l'approbation de compte d'invité) :

Si le serveur ou le par défaut de Protocole SMTP (Simple Mail Transfer Protocol) de la notification de l'email n'est pas configuré, alors le compte ne sera pas créé :

Le log de guest.log confirme que le global de l'adresse utilisée pour la notification manque :

```
2014-08-01 22:35:24,271 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null.  A global default From address can be
configured in global settings for SMTP server.
```

Quand vous avez la configuration appropriée d'email, le compte est créé :

Après que vous permettiez aux **invités auto-enregistrés Require d'être** option **approuvée**, les champs de nom d'utilisateur et mot de passe sont automatiquement retirés de l'**inclure ces informations sur la** section de **page de succès d'Auto-enregistrement**. C'est pourquoi, quand l'approbation de sponsor est nécessaire, des qualifications pour des utilisateurs d'invité ne sont pas affichées par défaut sur la page Web qui présente les informations pour prouver que le compte a été créé. Au lieu de cela ils doivent être livrés par Short Message Services (SMS) ou email. Cette option doit être activée dans la **notification de créance d'envoi sur l'approbation utilisant la** section (marque email/SMS).

Un email de notification est fourni au sponsor :

Le sponsor se connecte dans le sponsor portail et approuve le compte :

Àpartir de là, on permet à l'l'utilisateur d'invité pour ouvrir une session (les qualifications étant reçu par l'email ou le SMS).

En résumé, il y a trois adresses e-mail utilisées dans cet écoulement :

- Notification « » d'adresse. Ceci est défini statiquement ou pris du compte de sponsor et utilisé en tant que de l'adresse pour chacun des deux : notification à commanditer (pour approbation) et détails de créance à l'invité. Ceci est configuré sous l'**accès invité > configurent > des configurations > des configurations d'email d'invité**.

- Notification « » à adresser. Ceci est utilisé afin d'informer le sponsor qu'il a reçu une approbation d'explication. Ceci est configuré dans le portail d'invité sous l'**accès invité > configurent > des portails d'invité > nom portail > invités auto-enregistrés Require à approuver > demande d'approbation d'email à**.

- Invité « » à adresser. Ceci est fourni par l'utilisateur d'invité pendant l'enregistrement. Si **envoyez la notification de créance sur l'approbation utilisant l'email** est sélectionnée, l'email avec les détails de créance (nom d'utilisateur et mot de passe) est livrée à l'invité.

Livrez les qualifications par l'intermédiaire du SMS

Des qualifications d'invité peuvent être également livrées par SMS. Ces options devraient être configurées :

1. Choisissez le fournisseur de service SMS :

2. Vérifiez la **notification de créance d'envoi sur l'approbation utilisant :** Case **SMS**.

3. Puis, l'utilisateur d'invité est invité à choisir le fournisseur disponible quand il crée un compte :

4. Un SMS est livré avec le fournisseur et le numéro de téléphone choisis :

5. Vous pouvez configurer des fournisseurs SMS sous la **gestion > le système > les configurations > la passerelle SMS**.

Enregistrement de périphérique

Si les **invités d'autoriser pour enregistrer l'**option de **périphériques** est sélectionnés après qu'un utilisateur d'invité ouvre une session et reçoive l'AUP, vous pouvez enregistrer des périphériques :

Notez que le périphérique déjà a été ajouté automatiquement (il est sur la liste de périphériques Manage). C'est parce qu'**automatiquement des périphériques d'invité de registre** ont été sélectionnés.

Posture

Si l'option de **conformité de périphérique d'invité d'exigence** est sélectionnée, alors des utilisateurs d'invité provisioned avec un agent qui exécute la posture (agent NAC/Web) après qu'ils ouvrent une session et reçoivent l'AUP (et exécutez sur option l'enregistrement de périphérique). ISE traite des règles de ravitaillement de client de décider quel agent devrait provisioned. Alors l'agent qui s'exécute sur la station exécute la posture (selon des règles de posture) et envoie des résultats à l'ISE, qui envoie le CoA authentifie à nouveau pour changer l'état d'autorisation si nécessaire.

Les règles possibles d'autorisation pourraient sembler semblables à ceci :

Les premiers nouveaux utilisateurs qui rencontrent le redirect to de règle de Guest_Authenticate le portail d'invité de registre d'individu. Après les auto-registres et les logins d'utilisateur, le CoA change l'état d'autorisation et l'utilisateur est équipé d'accès limité pour exécuter la posture et la correction. Seulement après que l'agent NAC provisioned et la station est conforme fait l'état d'autorisation de modification CoA de nouveau afin de fournir l'accès à Internet.

Les problèmes typiques avec la posture incluent le manque de règles correctes de ravitaillement

de client :

Ceci peut également être confirmé si vous examinez le fichier de guest.log (nouveau dans la version 1.3 ISE) :

```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

Si les **employés d'autoriser pour utiliser les périphériques personnels sur l'option Network** est sélectionnés, alors les utilisateurs en entreprise qui utilisent ce portail peuvent passer par BYOD circulent et enregistrent les périphériques personnels. Pour des utilisateurs d'invité, cette configuration ne change rien.

Que les « employés utilisant le portail comme invité » veut-ils dire ?

Par défaut, des portails d'invité sont configurés avec la mémoire d'identité de **Guest_Portal_Sequence** :

C'est l'ordre interne de mémoire qui juge les utilisateurs internes d'abord (avant des utilisateurs d'invité) :

Quand à ce stade sur le portail d'invité, l'utilisateur fournit les qualifications qui sont définies dans les utilisateurs internes enregistrent et la redirection BYOD se produit :

Les utilisateurs en entreprise de cette manière peuvent exécuter BYOD pour les périphériques personnels.

Quand au lieu des qualifications d'utilisateurs internes, invité des qualifications que d'utilisateurs sont fournis, écoulement normal est continué (aucun BYOD).

Modification VLAN

C'est une option semblable au changement VLAN configuré pour le portail d'invité de la version 1.2 ISE. Il te permet pour exécuter activeX ou un applet Java, qui déclenche le DHCP pour libérer et renouveler. C'est nécessaire quand le CoA déclenche la modification du VLAN pour le point final. Quand le MAB est utilisé, le point final ne se rend pas compte d'une modification de VLAN. Une solution possible est de changer le VLAN (la release DHCP/renouvellent) avec l'agent NAC. Une autre option est de demander une nouvelle adresse IP par l'intermédiaire de l'applet retourné sur la page Web. Un retard entre la release/CoA/renouvellent peut être configuré. Cette option n'est pas prise en charge pour des périphériques mobiles.

Informations connexes

- Services de posture sur le guide de configuration de Cisco ISE
- Radio BYOD avec le Cisco Identity Services Engine

- Soutien ISE SCEP d'exemple de configuration BYOD
- Guide d'administrateurs de Cisco ISE 1.3
- Authentification Web centrale exemple sur WLC et ISE configuration
- Authentification Web centrale avec FlexConnect aps sur un WLC avec l'exemple de configuration ISE
- Support et documentation techniques - Cisco Systems