Atténuation de l'usurpation du protocole Blast-RADIUS (CVE-2024-3596)

Table des matières

- Introduction
- Aperçu
- Fond
- Atténuation
  - Authentificateur De Message
  - Chiffrement avec TLS/IPSec
    - RADIUS sur DTLS
    - RADIUS sur TLS
    - IPSEC
- Atténuation partielle
  - Segmentation RADIUS
- État de vulnérabilité Identity Services Engine
  - ISE comme serveur RADIUS
  - ISE comme client RADIUS
- ISE en tant que client RADIUS Mises à jour
  - Boîtier
  - NAD a inclus Message Authenticator dans la demande
  - NAD n'a pas inclus Message Authenticator dans la demande
  - Serveur de jetons RADIUS
  - Serveur RADIUS externe
  - Changement d'autorisation (CoA)

Introduction

Ce document décrit comment atténuer l'usurpation du protocole Blast RADIUS.

Aperçu

Le 7 juillet 2024, des chercheurs en sécurité ont révélé cette vulnérabilité dans le protocole RADIUS : CVE-2024-3596 : Le protocole RADIUS dans le cadre de la RFC 2865 est susceptible d'être attaqué par un pirate sur le chemin qui peut modifier n'importe quelle réponse valide (Access-Accept, Access-Reject ou Access-Challenge) à n'importe quelle autre réponse en utilisant

une attaque de collision de préfixe choisi contre la signature de l'authentificateur de réponse MD5. Ils ont publié un document détaillant leurs conclusions dans ce livre blanc qui démontre une réponse réussie de falsification contre les flux qui n'utilisent pas l'attribut Message-Authenticator.

Pour obtenir une liste à jour des produits Cisco affectés par cette vulnérabilité et des versions contenant des correctifs, consultez le site : Vulnérabilité d'usurpation de protocole RADIUS (Blast-RADIUS) : Juillet 2024. Cet article décrit les techniques générales de réduction des risques ainsi que leur application à certains produits Cisco, mais pas à tous. La documentation de chaque produit doit être consultée pour obtenir des informations spécifiques. En tant que serveur RADIUS phare de Cisco, Cisco Identity Service Engine est traité plus en détail.

Fond

Cette attaque tire parti d'une attaque à préfixe choisi MD5 utilisant des collisions dans MD5, ce qui permet à un attaquant d'ajouter des données supplémentaires au paquet de réponse RADIUS tout en modifiant les attributs existants du paquet de réponse. Un exemple démontré a été la capacité de changer un RADIUS Access-Reject en un RADIUS Access-Accept. Cela est possible parce que RADIUS par défaut n'inclut pas de hachage de tous les attributs dans le paquet. Le document RFC 2869 ajoute l'attribut Message-Authenticator, mais il n'est actuellement requis que pour l'utilisation des protocoles EAP, ce qui signifie que l'attaque décrite dans CVE-2024-3596 est possible contre tout échange non-EAP où le client RADIUS (NAD) n'inclut pas l'attribut Message-Authenticator.

Atténuation

Authentificateur De Message

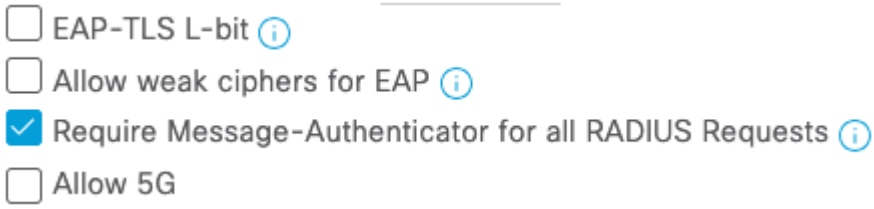
1.- Le client RADIUS doit inclure l'attribut Message-Authenticator.

Lorsque le périphérique d'accès réseau (NAD) inclut l'attribut Message-Authenticator dans la demande d'accès, Cisco Identity Services Engine inclut Message-Authenticator dans le paquet Access-Accept, Access-Challenge ou Access-Reject résultant dans toutes les versions.

2.- Le serveur RADIUS doit imposer la réception de l'attribut Message-Authenticator.

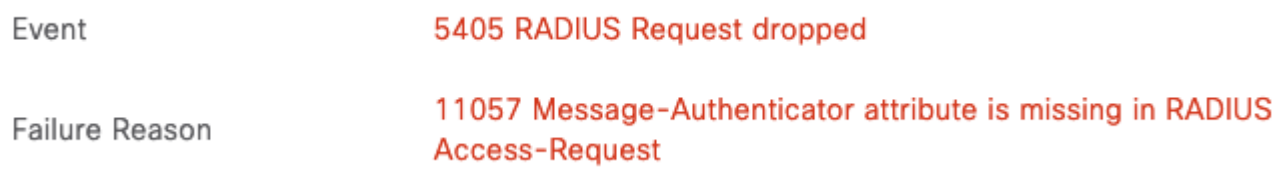
Il ne suffit pas d'inclure l'authentificateur de message dans la demande d'accès, car l'attaque permet de supprimer l'authentificateur de message de la demande d'accès avant qu'elle ne soit transférée au serveur RADIUS. Le serveur RADIUS doit également exiger que le NAD inclue Message-Authenticator dans la demande d'accès. Cette option n'est pas activée par défaut sur

Cisco Identity Services Engine, mais elle peut être activée au niveau des protocoles autorisés, qui s'applique au niveau du jeu de stratégies. L'option sous la configuration des protocoles autorisés est Require Message-Authenticator for all RADIUS Requests :



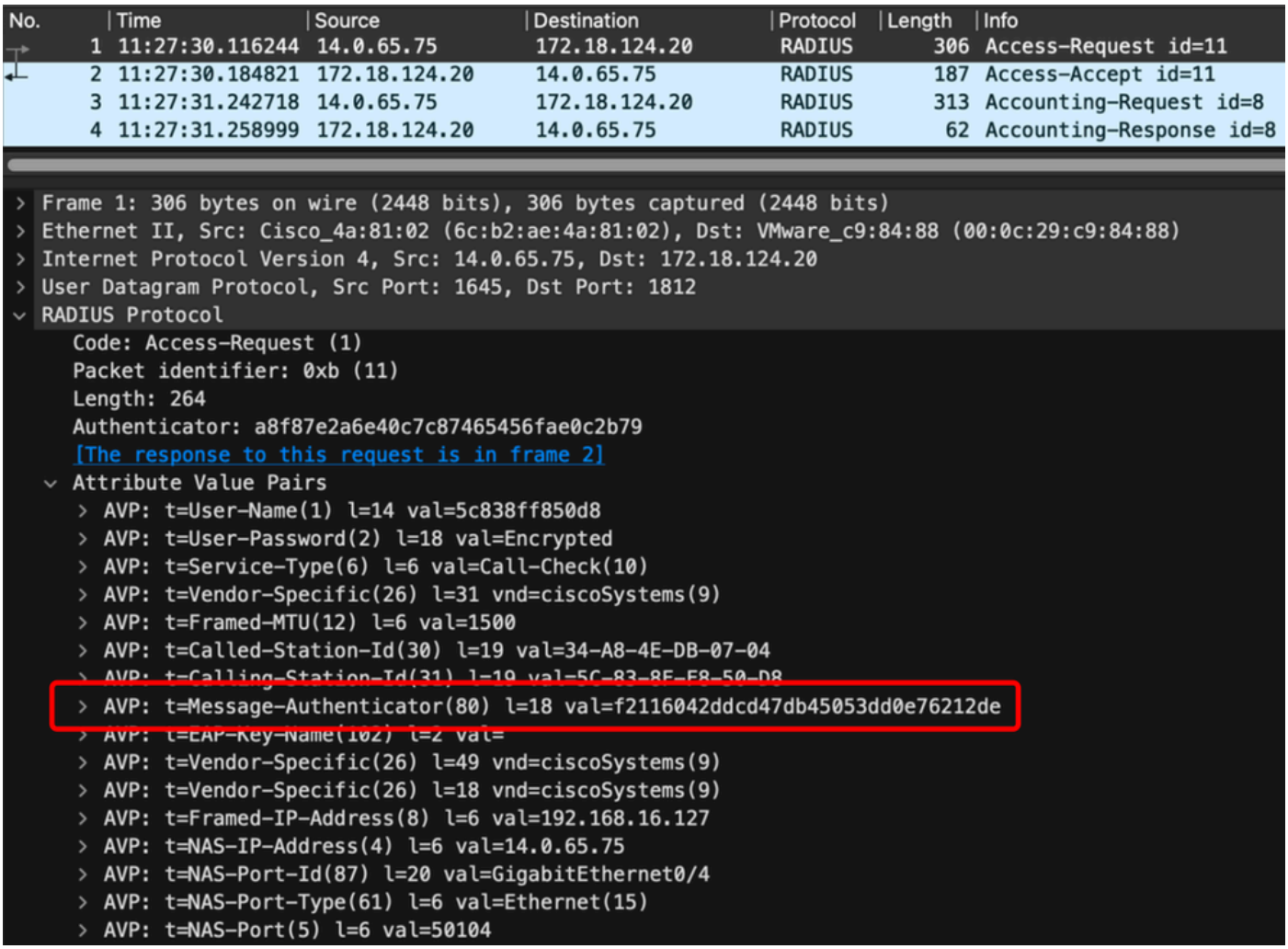
Option Protocoles autorisés dans Identity Services Engine

Les authentifications qui correspondent à un ensemble de stratégies où la configuration des protocoles autorisés nécessite Message-Authenticator, mais où la demande d'accès ne contient pas l'attribut Message-Authenticator sont abandonnées par ISE :



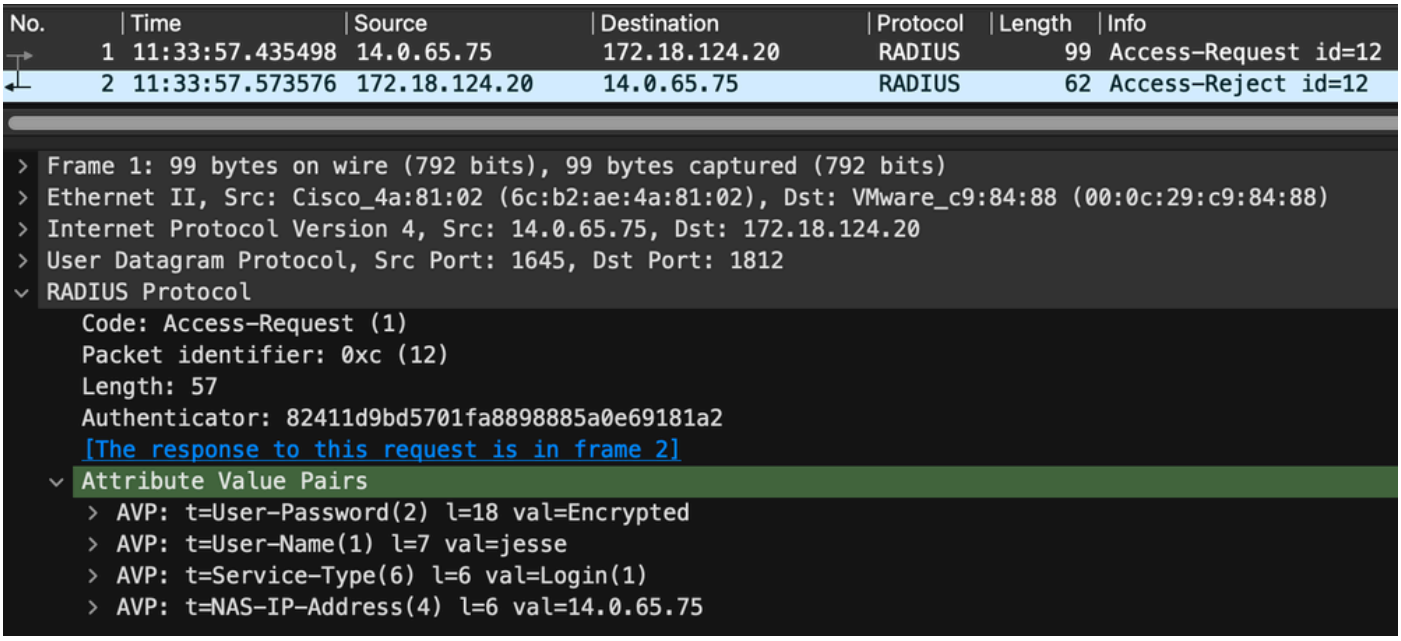
Il est important de vérifier si le NAD envoie Message-Authenticator avant d'être requis par le serveur RADIUS car il ne s'agit pas d'un attribut négocié, il appartient au NAD de l'envoyer par défaut ou d'être configuré pour l'envoyer. Message-Authenticator n'est pas l'un des attributs signalés par ISE, une capture de paquets est la meilleure façon de déterminer si un NAD/Cas d'utilisation inclut Message-Authenticator. ISE a intégré la fonctionnalité de capture de paquets sous Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump. Gardez à l'esprit que différents cas d'utilisation du même NAD peuvent inclure ou non Message-Authenticator.

Voici un exemple de capture d'une demande d'accès qui inclut l'attribut Message-Authenticator :



Attribut Message-authenticator dans la requête d'accès Radius

Voici un exemple de capture d'une demande d'accès qui n'inclut pas l'attribut Message-Authenticator :



Chiffrement avec TLS/IPSec

La solution à long terme la plus efficace pour sécuriser RADIUS consiste à chiffrer le trafic entre le serveur RADIUS et le NAD. Ceci ajoute à la fois la confidentialité et une intégrité cryptographique plus forte que le simple fait de se fier à l'authentificateur de message dérivé de MD5-HMAC. Si l'un de ces éléments peut être utilisé entre le serveur RADIUS et le NAD, cela dépend de la prise en charge de la méthode de cryptage par les deux parties.

Les termes généraux utilisés dans le secteur pour le chiffrement TLS de RADIUS sont les suivants :

- RadSec - fait référence à RFC 6614
- RadSec TLS - fait référence à RFC 6614
- RadSec DTLS - fait référence à RFC 7360

Il est important de déployer le cryptage de manière contrôlée, car le cryptage TLS est surchargé en termes de performances et de gestion des certificats. Les certificats doivent également être renouvelés sur une base régulière.

RADIUS sur DTLS

Le protocole DTLS (Datagram Transport Layer Security) en tant que couche de transport pour RADIUS est défini par la RFC 7360 qui utilise des certificats pour authentifier mutuellement le serveur RADIUS et le NAD chiffre ensuite le paquet RADIUS complet à l'aide d'un tunnel TLS. La méthode de transport reste UDP et nécessite le déploiement de certificats sur le serveur RADIUS et NAD. Gardez à l'esprit que lors du déploiement de RADIUS sur DTLS, il est impératif que l'expiration et le remplacement des certificats soient étroitement gérés pour empêcher les certificats expirés d'interrompre la communication RADIUS. ISE prend en charge DTLS pour les communications ISE à NAD, car à partir de la version ISE 3.4, Radius sur DTLS n'est pas pris en charge pour les serveurs proxy RADIUS ou les serveurs à jetons RADIUS. RADIUS sur DTLS est également pris en charge par de nombreux périphériques Cisco qui agissent en tant que NAD, tels que des commutateurs et des contrôleurs sans fil exécutant Cisco IOS-XE®.

RADIUS sur TLS

Le chiffrement TLS (Transport Layer Security) pour RADIUS est défini par la RFC 6614, modifie le transport en TCP et utilise TLS pour chiffrer entièrement les paquets RADIUS. C'est un exemple couramment utilisé par le service eduroam. Depuis ISE 3.4, RADIUS sur TLS n'est pas pris en charge, mais il est pris en charge par de nombreux périphériques Cisco qui agissent en tant que NAD, tels que des commutateurs et des contrôleurs sans fil exécutant Cisco IOS-XE.

IPSEC

Identity Services Engine prend en charge de manière native les tunnels IPSec entre ISE et NAD, qui prennent également en charge les tunnels IPSec de fin. Il s'agit d'une bonne option lorsque RADIUS sur DTLS ou RADIUS sur TLS n'est pas pris en charge, mais doit être utilisé avec parcimonie, car seuls 150 tunnels sont pris en charge par noeud de services de stratégie ISE. ISE 3.3 et versions ultérieures n'exige plus de licence pour IPSec ; elle est désormais disponible en mode natif.

Atténuation partielle

Segmentation RADIUS

Segmenter le trafic RADIUS vers les VLAN de gestion et les liaisons chiffrées sécurisées, telles que celles fournies via SD-WAN ou MACSec. Cette stratégie ne réduit pas le risque d'attaque à zéro, mais peut réduire considérablement la surface d'attaque de la vulnérabilité. Il peut s'agir d'une bonne mesure d'interruption pendant que les produits déploient la configuration requise pour Message-Authenticator ou la prise en charge DTLS/RadSec. L'attaque nécessite qu'un pirate réussisse à faire fonctionner la communication RADIUS avec le mode Man-in-the-Middle (MITM). Ainsi, si un pirate ne parvient pas à accéder à un segment de réseau avec ce trafic, l'attaque n'est pas possible. La raison pour laquelle ce problème n'est qu'une atténuation partielle est qu'une configuration incorrecte ou une compromission d'une partie du réseau peut exposer le trafic RADIUS.

Si le trafic RADIUS ne peut pas être segmenté ou chiffré, des fonctionnalités supplémentaires peuvent être implémentées pour empêcher la réussite de la MITM sur les segments à risque tels que : Protection de la source IP, inspection ARP dynamique et surveillance DHCP. Il est également possible d'utiliser d'autres méthodes d'authentification basées sur le type de flux d'authentification, telles que TACACS+, SAML, LDAPS, etc.

État de vulnérabilité Identity Services Engine

Ces tableaux décrivent ce qui est disponible dans Cisco ISE 3.4 pour protéger les flux d'authentification contre Blast-RADIUS.

Pour récapituler, ces trois éléments suivants doivent être en place pour un flux utilisant uniquement Message-Authenticator et non le chiffrement DTLS/RadSec/IPSec, pour que le flux ne soit pas vulnérable :

- Le périphérique d'accès réseau DOIT envoyer l'attribut Message-Authenticator dans la demande d'accès.
- Le serveur RADIUS DOIT exiger l'attribut Message-Authenticator dans la demande d'accès.
- Le serveur RADIUS DOIT répondre avec l'attribut Message-Authenticator dans Access-Challenge, Access-Accept et Access-Reject.

Veuillez vous reporter à l'ID de bogue Cisco CSCwk67747 qui suit les modifications pour fermer les vulnérabilités lorsque Cisco ISE agit en tant que client RADIUS.

ISE comme serveur RADIUS

AAA Scenario	ISE Config	NAD capabilities	Status	Alternative options
EAP Protocols	--	--	Protected	
MAB, PAP, CHAP, MSCHAPv1/v2, Authorize-Only	Have on the checkbox "Require Message-Authenticator for all protocols"	Supports Message-Authenticator for non-EAP protocols	Protected	
		Doesn't support Message-Authenticator for non-EAP protocols	Vulnerable (because of NAD)	Can use IPsec
	Use RADIUS DTLS for this NAD	Supports RADIUS DTLS	Protected	
		Doesn't support RADIUS DTLS	Vulnerable (because of NAD)	Can use IPsec

ISE comme client RADIUS

AAA Scenario	ISE Config	Peers' capabilities	Status	Alternative options
ISE as RADIUS Proxy	--	NAD supports Message-Authenticator **AND** RADIUS Server supports Message-Authenticator	Protected	
		NAD doesn't support Message-Authenticator **OR** RADIUS Server doesn't support Message-Authenticator	Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if both NAD and RADIUS Server use Message-Authenticator
ISE as RADIUS Token Client	--		Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if RADIUS Token Server uses Message-Authenticator
ISE as CoA Client	Configured to use Message-		Vulnerable (ISE must require	Can use IPsec Partial mitigation is achieved if Device Profiler checked option to use Message-Authenticator

ISE en tant que client RADIUS Mises à jour

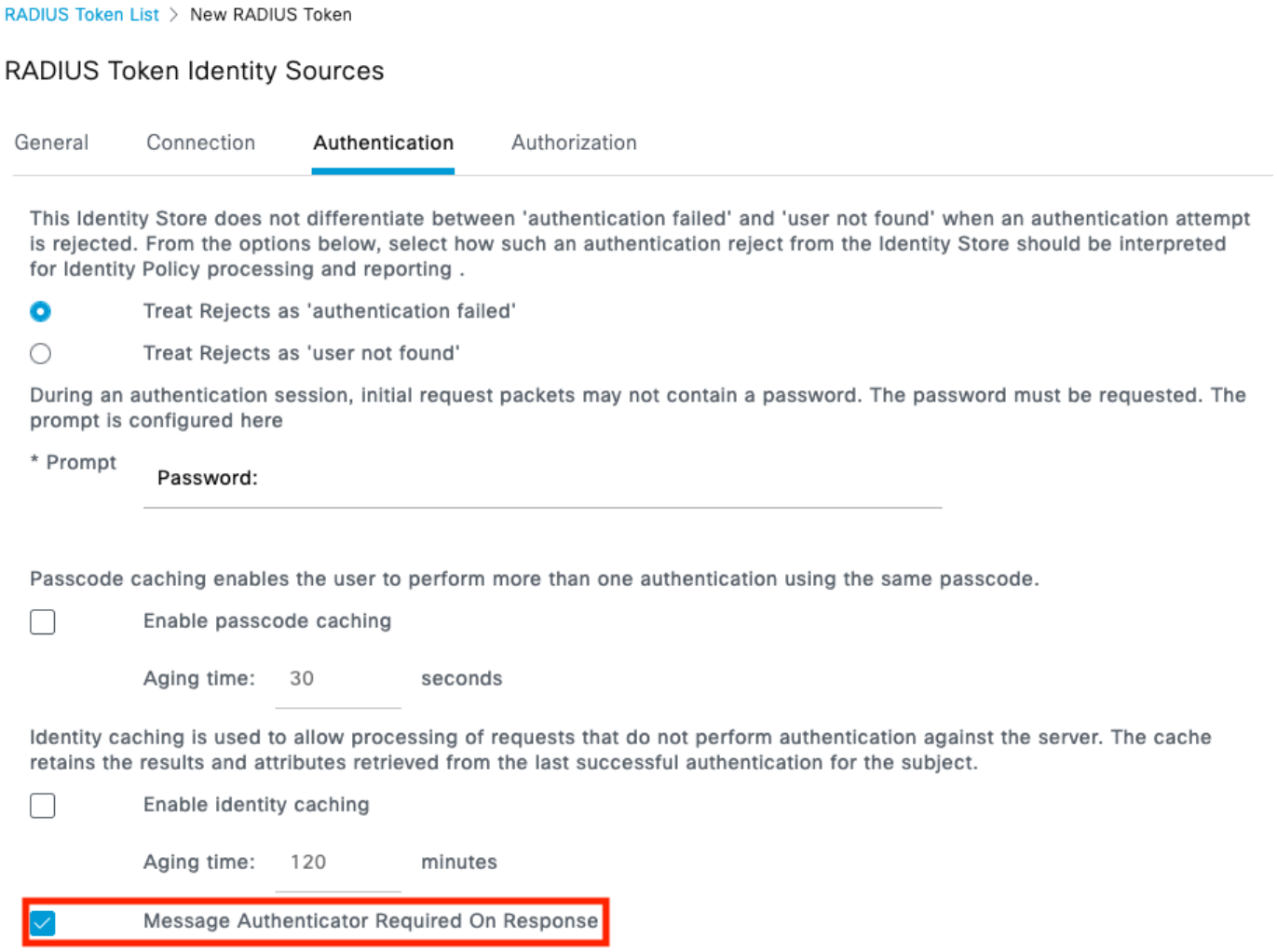
Les améliorations apportées à Cisco ISE en tant que client RADIUS sont incluses dans les versions suivantes : 3.1 patch 10, 3.2 patch 8, 3.3 patch 5, 3.4 patch 2, 3.5 et versions ultérieures via l'ID de bogue Cisco CSCwk67747. Après l'application du patch ou la mise à niveau, toute nouvelle ressource créée est définie par défaut sur la nouvelle configuration, plus sécurisée. Les ressources existantes doivent être modifiées pour utiliser le correctif ou la mise à niveau post-configuration plus sécurisée. Une nouvelle case à cocher a été ajoutée : "Message Authenticator Required On Response", si cette case est cochée, il a un double objectif : Cisco ISE envoie toujours l'authentificateur de message et il échoue l'authentification si une réponse est reçue sans authentificateur de message. Le comportement est le suivant :

Boîtier	NAD a inclus Message Authenticator dans la demande	NAD n'a pas inclus Message Authenticator dans la demande
Avant le correctif/la mise à niveau	ISE envoie l'authentificateur de message au jeton RADIUS, au serveur RADIUS externe ou à la	ISE n'envoie pas l'authentificateur de message au jeton RADIUS, au serveur

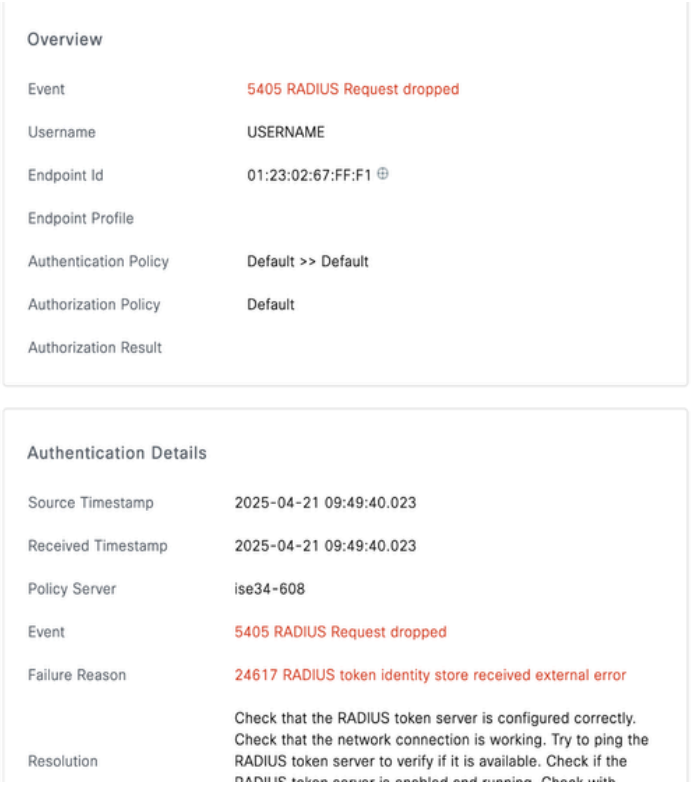
	CoA	RADIUS externe ou à la CoA
La case Après le correctif/la mise à niveau et Authentificateur de message requis en réponse est décochée.	ISE envoie l'authentificateur de message au jeton RADIUS, au serveur RADIUS externe ou à la CoA	ISE n'envoie pas l'authentificateur de message au jeton RADIUS, au serveur RADIUS externe ou à la CoA
La case Après le correctif/la mise à niveau et Authentificateur de message requis en réponse est cochée.	ISE envoie l'authentificateur de message au jeton RADIUS, au serveur RADIUS externe ou à la CoA	ISE envoie l'authentificateur de message au jeton RADIUS, au serveur RADIUS externe ou à la CoA

Serveur de jetons RADIUS

Une nouvelle case à cocher : Message Authenticator Required On Response a été ajoutée sous l'onglet Authentication pour la configuration du serveur de jetons RADIUS :



Lorsque cette case est cochée, si une réponse RADIUS est reçue sans l'authentificateur de message, un message d'échec est consigné dans le journal d'authentification détaillé, auquel vous pouvez accéder via les journaux en direct ou un rapport d'authentification RADIUS :

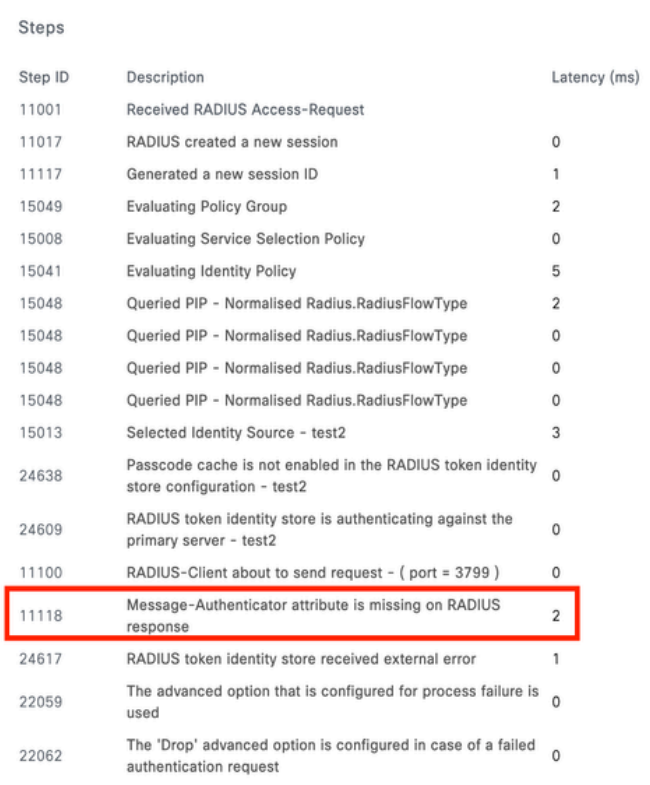


Overview

Event	5405 RADIUS Request dropped
Username	USERNAME
Endpoint Id	01:23:02:67:FF:F1
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default
Authorization Result	

Authentication Details

Source Timestamp	2025-04-21 09:49:40.023
Received Timestamp	2025-04-21 09:49:40.023
Policy Server	ise34-608
Event	5405 RADIUS Request dropped
Failure Reason	24617 RADIUS token identity store received external error
Resolution	Check that the RADIUS token server is configured correctly. Check that the network connection is working. Try to ping the RADIUS token server to verify if it is available. Check if the



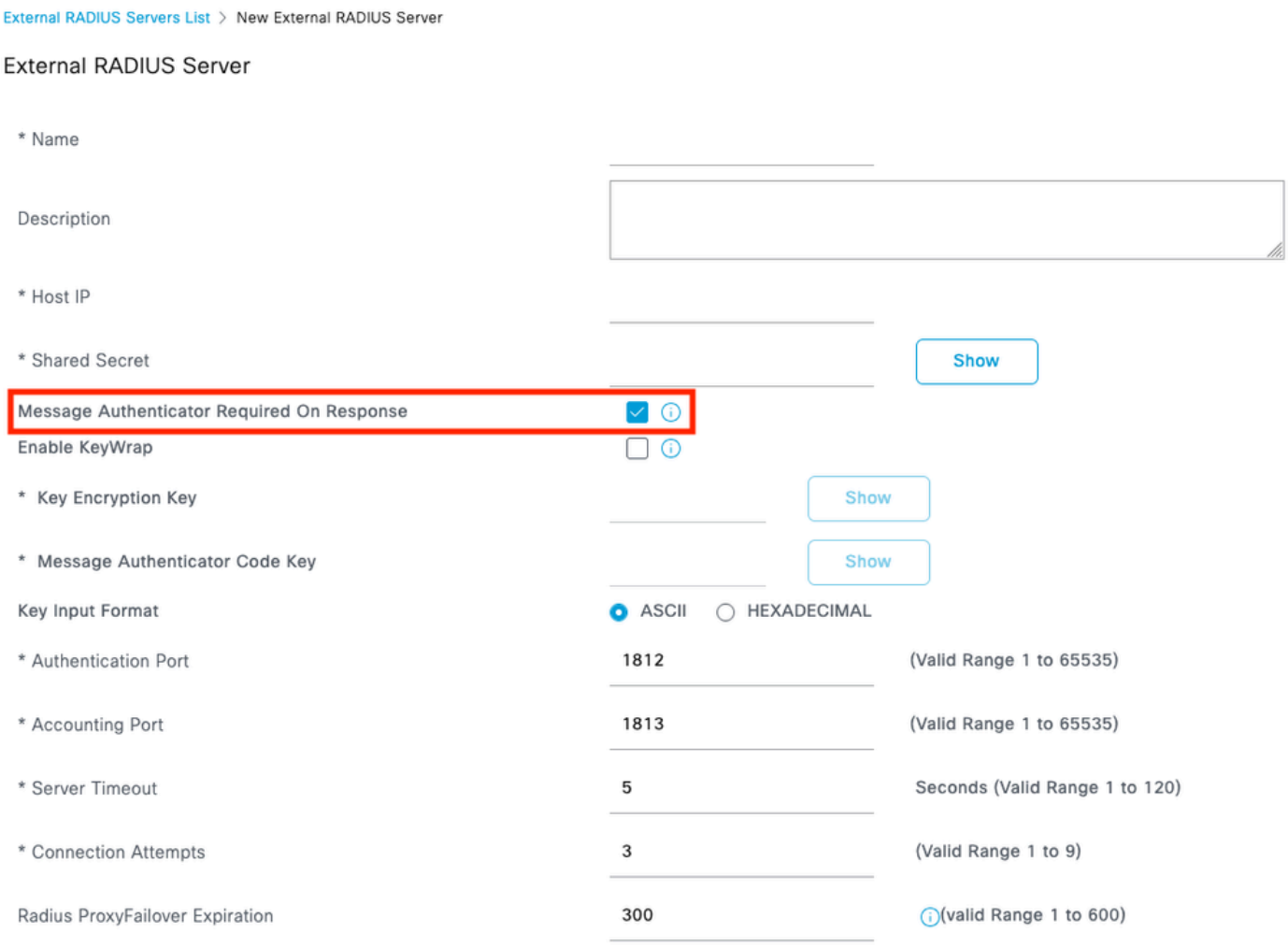
Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11117	Generated a new session ID	1
15049	Evaluating Policy Group	2
15008	Evaluating Service Selection Policy	0
15041	Evaluating Identity Policy	5
15048	Queried PIP - Normalised Radius.RadiusFlowType	2
15048	Queried PIP - Normalised Radius.RadiusFlowType	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	0
15013	Selected Identity Source - test2	3
24638	Passcode cache is not enabled in the RADIUS token identity store configuration - test2	0
24609	RADIUS token identity store is authenticating against the primary server - test2	0
11100	RADIUS-Client about to send request - (port = 3799)	0
11118	Message-Authenticator attribute is missing on RADIUS response	2
24617	RADIUS token identity store received external error	1
22059	The advanced option that is configured for process failure is used	0
22062	The 'Drop' advanced option is configured in case of a failed authentication request	0

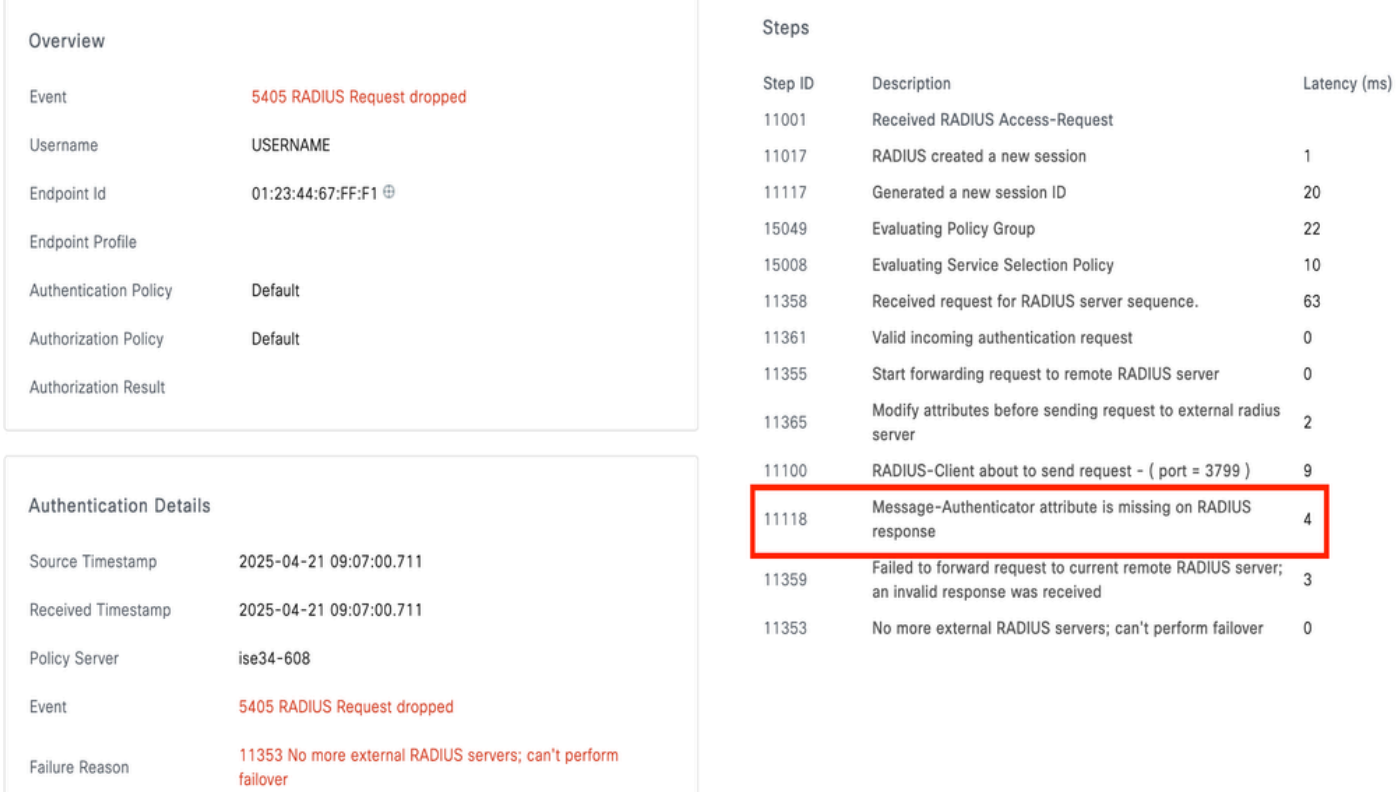
Remarque : L'authentification globale peut toujours passer en fonction de la configuration de la stratégie, par le biais de l'authentification peut correspondre à une stratégie inattendue.

Serveur RADIUS externe

Une nouvelle case à cocher : Message Authenticator Required On Response a été ajouté à la configuration du serveur RADIUS externe :



Lorsque cette case est cochée, si une réponse RADIUS est reçue sans l'authentificateur de message, un message d'échec est consigné dans le journal d'authentification détaillé, auquel vous pouvez accéder via les journaux en direct ou un rapport d'authentification RADIUS :



Overview

Event	5405 RADIUS Request dropped
Username	USERNAME
Endpoint Id	01:23:44:67:FF:F1
Endpoint Profile	
Authentication Policy	Default
Authorization Policy	Default
Authorization Result	

Authentication Details

Source Timestamp	2025-04-21 09:07:00.711
Received Timestamp	2025-04-21 09:07:00.711
Policy Server	ise34-608
Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover

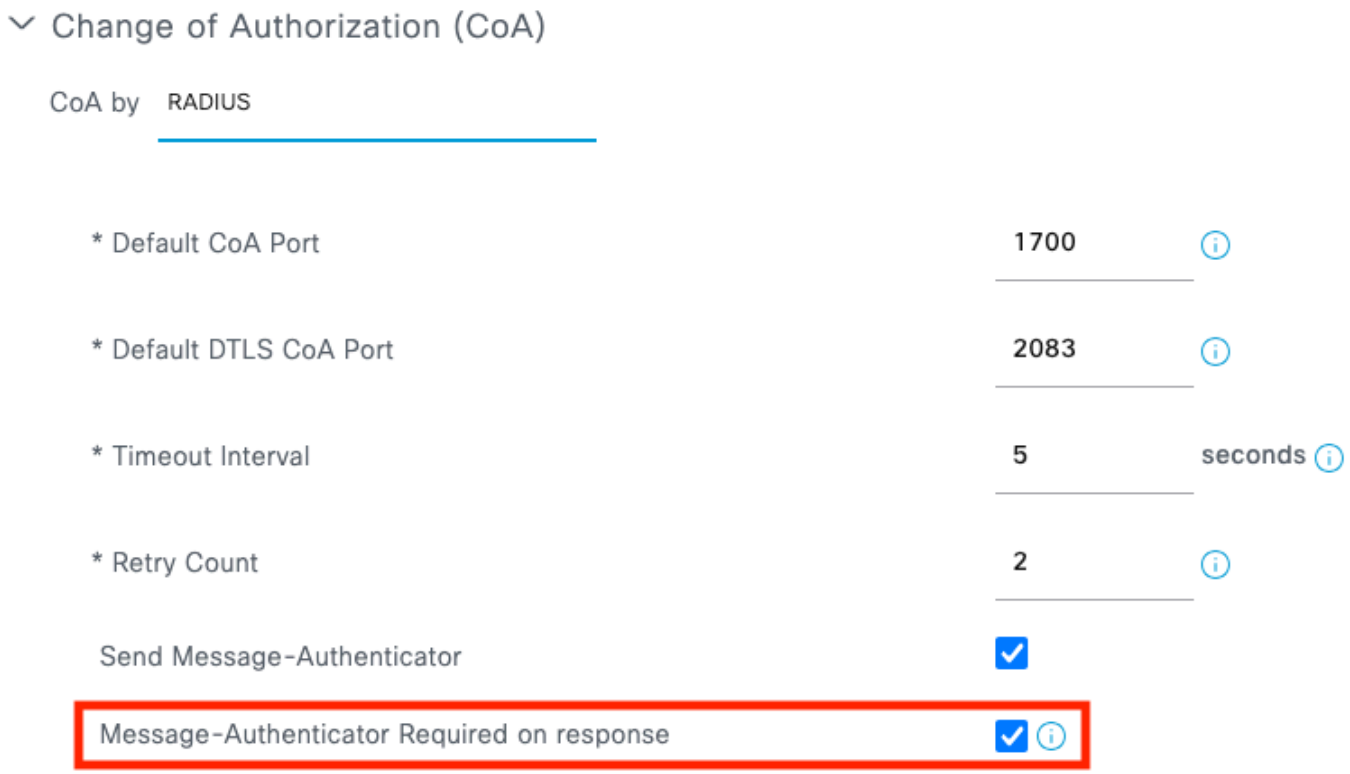
Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	1
11117	Generated a new session ID	20
15049	Evaluating Policy Group	22
15008	Evaluating Service Selection Policy	10
11358	Received request for RADIUS server sequence.	63
11361	Valid incoming authentication request	0
11355	Start forwarding request to remote RADIUS server	0
11365	Modify attributes before sending request to external radius server	2
11100	RADIUS-Client about to send request - (port = 3799)	9
11118	Message-Authenticator attribute is missing on RADIUS response	4
11359	Failed to forward request to current remote RADIUS server; an invalid response was received	3
11353	No more external RADIUS servers; can't perform failover	0

Remarque : L'authentification globale peut toujours passer en fonction de la configuration de la stratégie, par le biais de l'authentification peut correspondre à une stratégie inattendue.

Changement d'autorisation (CoA)

Les modifications CoA ont été apportées aux profils de périphériques réseau dans le tiroir Modification d'autorisation (CoA) :



L'option Send Message-Authenticator est une fonctionnalité précédente, la nouvelle option est Message-Authenticator Required on response. Cisco ISE envoie l'attribut Message Authenticator si la case Message-Authenticator Required on response est cochée, que la case Send Message-Authenticator soit cochée ou non. Send Message-Authenticator est conservé pour les configurations existantes. Si le NAD n'inclut pas l'authentificateur de message dans la réponse CoA, l'erreur suivante apparaît dans le rapport d'authentification détaillé disponible via Live Logs :

Event	5417 Dynamic Authorization failed
Failure Reason	11118 Message-Authenticator attribute is missing on RADIUS response
Resolution	The Message-Authenticator attribute is selected as required on RADIUS response. For authentications against external RADIUS server: Go to Administration->Network Resources->External RADIUS servers. Go to the specific External server and see that the checkbox "Message Authenticator Required On Response" is selected. For COA: Go to Administration->Network Resources->Network Devices. Go to the device, and see what is its Profile. Then go the to profile and see that the checkbox "Message Authenticator Required On Response" is selected. Either deselect the checkbox, or enforce the external resource to send valid Message-Authenticator on response.
Root cause	11118 Message-Authenticator attribute is missing on RADIUS response

Remarque : Le CoA peut réussir sur le NAD même si une défaillance est enregistrée sur Cisco ISE, car le NAD peut avoir traité le CoA mais n'a pas inclus Message Authenticator dans la réponse.

Les profils de périphérique réseau fournis par Cisco par défaut ne peuvent pas être modifiés. Pour utiliser la nouvelle option, le profil de périphérique réseau peut être dupliqué et le paramètre activé sur le profil dupliqué. Les périphériques réseau doivent ensuite se voir attribuer le profil de périphérique réseau nouvellement créé. Cela a été fait pour réduire le risque de provoquer une panne du réseau suite à un correctif ou une mise à niveau en introduisant une incompatibilité entre Cisco ISE et les NAD existants. Si un profil défini par l'utilisateur existant est en cours d'utilisation, il est recommandé de dupliquer ce profil et de tester au moins 1 de chaque type de périphérique sur le réseau à l'aide de ce profil avant d'apporter une modification au profil de périphérique réseau existant.

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.