Modèle de liste verte Cisco ISE TrustSec (IP par défaut refusée) avec SDA

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Configuration Diagramme du réseau Configuration Étape 1. Modifiez la SGT des commutateurs inconnus en périphériques TrustSec. Étape 2. Désactivez l'application basée sur les rôles CTS. Étape 3. Mappage IP-SGT sur les commutateurs en périphérie et en périphérie avec modèle DNAC. Étape 4. Basculement SGACL avec modèle DNAC. Étape 5. Activer le modèle Allow-List (Refus par défaut) dans la matrice TrustSec. Étape 6. Créer SGT pour les terminaux/utilisateurs. Étape 7. Créer une SGACL pour les terminaux/utilisateurs (pour le trafic de superposition de production). Vérification SGT de périphérique réseau Application sur les ports de liaison ascendante Mappage IP-SGT local SGACL FALLBACK local Activation Allow-List (Deny par défaut) sur les commutateurs de fabric SGACL pour les terminaux connectés au fabric Vérifier le contrat créé par DNAC Compteur SGACL sous-jacent sur les commutateurs de fabric Dépannage Problème 1. Si les deux noeuds ISE sont hors service. Problème 2. Voix unidirectionnelle sur téléphone IP ou pas de voix. Problème 3. Le point de terminaison VLAN critique n'a pas d'accès au réseau. Problème 4. VLAN critique de la liste déroulante de paquets. Additional Information

Introduction

Ce document décrit comment activer le modèle allow-list (Default Deny IP) de TrustSec dans SDA (Software Defined Access). Ce document fait appel à plusieurs technologies et composants, notamment Identity Services Engine (ISE), Digital Network Architecture Center (DNAC) et Switches (Border and Edge).

Deux modèles Trustsec sont disponibles :

- Modèle de liste de refus (IP d'autorisation par défaut) : Dans ce modèle, l'action par défaut est Permit IP et toute restriction doit être explicitement configurée avec l'utilisation de listes d'accès de groupe de sécurité (SGACL). Ceci est généralement utilisé lorsque vous ne comprenez pas parfaitement les flux de trafic au sein de leur réseau. Ce modèle est assez facile à mettre en oeuvre.
- Modèle de liste verte (IP de refus par défaut) : Dans ce modèle, l'action par défaut est Deny IP et, par conséquent, le trafic requis doit être explicitement autorisé avec l'utilisation des SGACL. Ceci est généralement utilisé lorsque le client comprend bien le type de flux de trafic dans son réseau. Ce modèle nécessite une étude détaillée du trafic du plan de contrôle, ainsi qu'il peut bloquer TOUT le trafic, dès qu'il est activé.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification Dot1x/MAB
- Cisco TrustSec (CTS)
- Protocole d'échange de sécurité (SXP)
- Proxy Web
- Concepts de pare-feu
- DNAC

Components Used

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

- Noeuds de périphérie 9300 et 9500 avec IOS 16.9.3
- DNAC 1.3.0.5
- ISE 2.6 patch 3 (deux noeuds Déploiement redondant)
- DNAC et ISE sont intégrés
- Les noeuds de périphérie et de périphérie sont provisionnés par DNAC
- Le tunnel SXP est établi de ISE (haut-parleur) aux deux noeuds de périphérie (écouteur)
- Les pools d'adresses IP sont ajoutés à l'intégration de l'hôte

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Diagramme du réseau



Configuration

Voici les étapes à suivre pour activer le modèle Allow-List (IP par défaut refusée) :

- 1. Modifiez la SGT des commutateurs inconnus en périphériques TrustSec.
- 2. Désactivez l'application basée sur les rôles CTS.
- 3. Mappage IP-SGT sur les commutateurs en périphérie et en périphérie à l'aide du modèle DNAC.
- 4. Basculement SGACL à l'aide du modèle DNAC.
- 5. Enable Allow-List (Default Deny IP) dans la matrice trustsec.
- 6. Créer SGT pour les terminaux/utilisateurs.
- 7. Créer une SGACL pour les terminaux/utilisateurs (pour le trafic de superposition de production).

Étape 1. Modifiez la SGT des commutateurs inconnus en périphériques TrustSec.

Par défaut, le Security Group Tag (SGT) inconnu est configuré pour l'autorisation des périphériques réseau. Le passage à TrustSec Device SGT offre plus de visibilité et aide à créer des SGACL spécifiques au trafic initié par le commutateur.

Naviguez jusqu'à **Centres de travail > TrustSec > Stratégie Trustsec > Autorisation de périphérique réseau**, puis changez-le en Trustsec_Devices from Unknown

Network Device Authorization Define the Network Device Authorization Policy by as	signing SGTs to network devices. Drag and drop rules to change the o	order.		٦
🖌 🖸 🔹 Defailt	If no rules defined or no match	ther	TrustSec_Devices	

Étape 2. Désactivez l'application basée sur les rôles CTS.

 Une fois le modèle Allow-List (Deny par défaut) en place, tout le trafic est bloqué dans le fabric, y compris le trafic de diffusion et de multidiffusion sous-jacent, tel que le trafic IS-IS (Intermediate System-to-Intermediate System), BFD (Bidirectional Forwarding Detection), Secure Shell (SSH).

• Tous les ports TenGig se connectant à la périphérie du fabric ainsi qu'à la bordure doivent être configurés avec la commande ici. Une fois que ceci est en place, le trafic initié à partir de cette interface et qui vient à cette interface ne sont pas soumis à l'application.

Interface tengigabitethernet 1/0/1

no cts role-based enforcement

Note: Cela peut être fait avec l'utilisation d'un modèle de plage dans DNAC pour plus de simplicité. Sinon, pour chaque commutateur, il est nécessaire de le faire manuellement lors du provisionnement. L'extrait ci-dessous montre comment le faire via un modèle DNAC.

interface range \$uplink1

no cts role-based enforcement

Pour plus d'informations sur les modèles DNAC, reportez-vous à cette URL pour le document.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-andmanagement/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_010000.html

Étape 3. Mappage IP-SGT sur les commutateurs en périphérie et en périphérie avec modèle DNAC.

L'idée est que le mappage IP-SGT local soit disponible sur les commutateurs même si tout ISE tombe en panne. Cela garantit que la sous-couche est opérationnelle et que la connectivité aux ressources critiques est intacte

La première étape consiste à lier les services critiques à une SGT (ex - Basic_Network_Services/1000). Certains de ces services incluent :

- Sous-réseau/ISIS
- ISE/DNAC
- Outil de surveillance
- · Sous-réseau du point d'accès en cas d'OTT
- Serveur Terminal Server
- · Services critiques Ex : Téléphone IP

Exemple :

cts role-based sgt-map <ISE/DNAC Subnet> sgt 1000 cts role-based sgt-map sgt 2 cts role-based sgt-map <Wireless OTT Infra> sgt 1000 cts role-based sgt-map <Underlay OTT AP Subnet> sgt 2 cts role-based sgt-map <Monitoring Tool IP> sgt 1000 cts role-based sgt-map vrf CORP_VN <Voice Gateway and CUCM Subnet> sgt 1000

Étape 4. Basculement SGACL avec modèle DNAC.

Un mappage SGT n'est d'aucune utilité tant qu'une SGACL appropriée n'est pas créée à l'aide de la SGT. Par conséquent, notre prochaine étape consisterait à créer une SGACL qui agit en tant que secours local en cas de panne des noeuds ISE (lorsque les services ISE sont hors service, que le tunnel SXP est hors service et donc que les SGACL et le mappage IP SGT ne sont pas téléchargés dynamiquement).

Cette configuration est transmise à tous les noeuds Edge et border.

Liste de contrôle d'accès/contrat basé sur les rôles de secours :

ip access-list role-based FALLBACK

permit ip Périphériques TrustSec à Périphériques TrustSec :

cts role-based permissions from 2 to 2 FALLBACK

Au-dessus de la SGACL Garantir la communication au sein des commutateurs de fabric et des adresses IP de sous-couche

Périphériques TrustSec à SGT 1000 :

cts role-based permissions from 2 to 1000 FALLBACK

Au-dessus de SGACL Assurez la communication des commutateurs et des points d'accès à ISE, DNAC, WLC et outils de surveillance

SGT 1000 vers périphériques TrustSec :

cts role-based permissions from 1000 to 2 FALLBACK

Au-dessus de SGACL Assurez la communication des points d'accès à ISE, DNAC, WLC et outils de surveillance aux commutateurs

Étape 5. Activer le modèle Allow-List (Refus par défaut) dans la matrice TrustSec.

La condition est de refuser la plupart du trafic sur le réseau et d'autoriser une moindre mesure. Ensuite, moins de stratégies sont nécessaires si vous utilisez le refus par défaut avec des règles d'autorisation explicites.

Accédez à Centres de travail > Trustsec > Stratégie TrustSec > Matrice > Par défaut et changezle en Refuser tout dans la règle de capture finale.



Note: Cette image représente (toutes les colonnes sont en rouge par défaut), le refus par défaut a été activé et seul le trafic sélectif peut être autorisé après la création de la SGACL.

Étape 6. Créer SGT pour les terminaux/utilisateurs.

Dans l'environnement SDA, de nouvelles balises SGT ne doivent être créées qu'à partir de l'interface graphique DNAC, car il existe de nombreux cas de corruption de base de données en

raison d'une non-correspondance de la base de données SGT dans ISE/DNAC.

Afin de créer SGT, connectez-vous à DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups, a Page Redirige vers ISE Scalable Group, cliquez sur Add, saisissez le nom SGT et enregistrez-le.



La même SGT se reflète dans DNAC via l'intégration PxGrid. Il s'agit de la même procédure pour toute création future de balises de groupe de sécurité.

Étape 7. Créer une SGACL pour les terminaux/utilisateurs (pour le trafic de superposition de production).

Dans l'environnement SDA, la nouvelle SGT doit être créée uniquement à partir de l'interface utilisateur DNAC.

Policy Name: Domain_Users_Access Contract : Permit Enable Policy : Enable Bi-Directional : Source SGT : Domain Users (Drag from Available Security Group) Destination SGT: Domain_Users, Basic_Network_Services, DC_Subnet, Unknown (Drag from Available Security Group) Policy Name: RFC_Access Contract : RFC_Access (This Contract contains limited ports) Enable Policy : Enable Bi-Directional : Source SGT : Domain Users (Drag from Available Security Group) Afin de créer un **contrat**, connectez-vous à **DNAC** et naviguez jusqu'à **Policy > Contracts > Add Contracts > Add Required protocol** et cliquez sur **Save**.

RFC_Access							
Name" RFC_Access		Implicit Action Deny	~				
Description (Optic	snal)						
Rows : 6	Buthesed						
Rows : 6 Action	Part/Protocol drs (TCP/LCP 53,5353)	Add 1 Edi	t Delete *				
Rows : 6 Action PERMIT PERMIT	PersProtecel dns (TCP/UDP 53,5353) dnop (JDP 67,68)	Add Edi Add Edi	t Delete *				
Rows : 6 Action PERMIT PERMIT PERMIT	Port/Protocol dns (TCP/UDP 53,5353) dhop (UDP 67,68) http-alt (TCP/UDP 591,8008,8080)	Add Edi Add Edi Add Edi	t Delete * t Delete t Delete				
Rows : 6 Action PERMIT PERMIT PERMIT	PersPreseel dns (TCP/UOP 53,5353) dhop (JDP 67,68) http-ait (TCP/UOP 591,8008,8080) ntp (JDP 123)	Add Edi Add Edi Add Edi Add Edi Add Edi	t i Delete t i Delete t i Delete t i Delete				
Rows : 6 Action PCRMIT PCRMIT PCRMIT PCRMIT PCRMIT	Part/Protectel dns (TCP/UDP 53,5353) dnop (UDP 67,68) http://utl? 531,8008,8080 ntp (UDP 123) echo (TCP/UDP 7)	Add Edi Add Edi Add Edi Add Edi Add Edi	t Delete t Delete t Delete t Delete t Delete				

Afin de créer un contrat, connectez-vous à DNAC et naviguez jusqu'à Policy > Group-Based Access Control > Group-Based Access-Policies > Add Policies > Create policy (avec les informations fournies) maintenant cliquez sur Save et ensuite sur Deploy.

0500	na i	NUMBER	POLICY	PROVISION A	SURANTE .	- *	0 1
Deshboard	Vitual N	lamoork.	Poles Admi	iatration Con	rects Registry		
Dro.g-Base	d Access Co	est Fabric)	12-0es	ed Access Control (Inn-Patric) Application Policies Traffic Copy Policies		
Create Pol	icy by noise	ting Source	e, Deetinati	on, and applying	a Contract		
Policy Name	e	Descrip	ation (Option	*0	Dontraut*	Cencel	Ser.
 Enable Pro Available Tex 	Ally O En	rate 81-direct	ional 😐		Source Science Science	_	
$\{Q_{i}:i\in I\}$							
AG	*0	AD	**	~	Dieg groups here		
AD, Ser vice, Ap	40,3m (,Am,	AG, My b, Sate -	Ageta	Authors			
	CA	00	00	00	Evelouine Scaleby Groups		
8400	Gamaro	General, G	General	Density:			
DS	00	80			Dag gragit tem		
Develop ment_R	Dector	006	Crophyse	duers			
н		-	۲	u			

Une fois que

SGACL/Contract est configuré à partir de DNAC, il se reflète automatiquement dans ISE. voici un exemple de vue matrx unidirectionnelle pour un sgt.

Journe/Destination	Operate Opera	Rosata Nation	P-Physics	Wes- destroyer	minutes	Rests, Harlands, Januaris	IK, Johnst	000, heter	2010	1000, Manualas A	8933468	Transient Dentities	University	
Demain (Jacob											WC_Asses			La matrice SGA

comme l'illustre l'image ci-dessous, est un exemple de vue pour le modèle Allow-list (Default Deny).

here, Destation	Donale Joan	Ounate Modelines	P.Pear	Tabo- tanhanas	-	Rate, Meaners, Services	DC, hallman	007,944r	NUK	CEC, Romana 1	#10AM	Tradium Dealers	Unineers
Burnals Burn											WC, Asses		
Durate Waltons											91,Acces		
P Para											Value_Research		
View Conference											Veter_Access		
ad-users.											WT, Acces		
Ball, Network, Bordon													
DC,balant													
BOD, Holes													
OC,Acortec													
HOUR .													
#1200	WC, Asses	WC/60000	Taken, Assess	Taux, Assess	WC, Asses								
Testine (testine													
internet .													
to be							Care P						

Color	Contract
	Deny IP
	Permit IP
	T CHINC II
	SGACL

Vérification

SGT de périphérique réseau

Afin de vérifier les commutateurs SGT reçus par ISE, exécutez cette commande : **show cts environment-data**



Application sur les ports de liaison ascendante

Afin de vérifier l'application sur l'interface de liaison ascendante, exécutez les commandes suivantes :

show run interface <liaison montante>

• show cts interface <interface de liaison ascendante>



Mappage IP-SGT local

Afin de vérifier les mappages IP-SGT configurés localement, exécutez cette commande : sh cts role-based sgt-map all

SDAFabricEdge#sh cts r Active IPv4-SGT Bindin	ole-based gs Inform	i sgt-map all mation
IP Address	SGT	Source
10. DNACIP	1102	CLI
10. ISE IP	1102	CLI
1 C . OTT Wireless Infra IP Range	1102	CLI
10 . Monitoring Server IP	1102	CLI
10. Critical Services IP	1102	CLI
10. OTT AP Subnet Range	2	CLI
10. Self IP	2	INTERNAL
10. Underlay IP subnet Range	2	CLI
10. Self IP	2	INTERNAL
10. Self IP	2	INTERNAL
10. Set IP	2	INTERNAL
IP-SGT Active Bindings	Summary	
Total number of CLI	bindi	ngs = 7
fotal number of INTERN	AL bindi	ngs = 4
Total number of active	bindi	ngs = 11

SGACL FALLBACK local

Afin de vérifier FALLBACK SGACL, exécutez cette commande : sh cts role-based permission

-	Test‡sh cts role-based permissions	
IPv4	Role-based permissions from group 3999 to group Unknown (configured)	
	FALLBACK	
CPv4	Role-based permissions from group 2 to group 2 (configured):	
	FALLBACK	
EPv4	Role-based permissions from group 1102 to group 2 (configured):	
	FALLBACK	
CPv4	Role-based permissions from group 2 to group 1102 (configured):	
	FALLBACK	
IPv4	Role-based permissions from group Unknown to group 3999 (configured)	
	FALLBACK	
RBACI	L Monitor All for Dynamic Policies : FALSE	
RBACI	Monitor All for Configured Policies : FALSE	

Note: La SGACL poussée par ISE a une priorité sur la SGACL locale.

Activation Allow-List (Deny par défaut) sur les commutateurs de fabric

Afin de vérifier le modèle Allow-list (Default Deny), exécutez cette commande : **sh cts role-based permission**



SGACL pour les terminaux connectés au fabric

Afin de vérifier la SGACL téléchargée depuis ISE, exécutez cette commande : **sh cts role-based permission**

SDAF	sbricEdge≸sh cts role-ba	ased pe	cmi se	ions to 101
IPv4	Role-based permissions	from g	roup	Unknown to group 101: Domain_Domain_Users:
	Permit IP-00			
IPvi	Role-based permissions	from q	anoup-	2:TrustSec_Devices to group 101: Domain_Decrs:
	Permit IP-00			
I Ev 4	Role-based permissions	reom q	troup	19:RPC1918 to group 101: Domain Deers:
	RFC_Access-00			
IFv4	Role-based permissions	from q	roup	101: Domain Users to group 101: Domain Users:
	Permit IP-00			
IEv4	Role-based permissions	from q	1 poup	1101:00 Same Commiss Revealed to group 101:000 The Domain Deers:
	Permit IP-00			
IP74	Role-based permissions	from q	an outp	1101: Desc,Newer, Series to group 101:50T TechN Domain Users:
	Permit TP+00			

Vérifier le contrat créé par DNAC

Afin de vérifier la SGACL téléchargée depuis ISE, exécutez cette commande : **show access-list <ACL/Contract Name>**

Role-based	IP acce	ss list	RFC_Access-00	(downloaded)
10 pers	mit udp	dst eq	domain	
20 perm	mit udp	dst eq	5353	
30 perm	mit tcp	dst eq	domain	
40 pers	mit tcp	dst eq	5353	
50 perm	mit udp	dst eq	bootps	
60 perm	mit udp	dst eq	bootpc	
70 perm	mit tcp	dst eq	591	
80 perm	mit tcp	dst eq	8008	
90 perm	mit tcp	dst eq	8080	
100 pe	rmit udp	dst eq	I 591	
110 per	rmit udp	dst eq	8008	
120 per	rmit udp	dst eq	1 8080	
130 per	rmit udp	dst eq	[ntp	
140 per	rmit udp	dst eq	[echo	
150 pe	rmit top	dst eq	(echo	
160 per	rmit top	dst eq	I 443	
170 per	rmit udp	dst eq	1 443	
180 der	ny ip			

Security Groups ACLs List > RFG Security Group ACLs	_Access		
* Name	RFC_Access		
Description	APIC_EM Created Sgacl		
IP Version	○ IPv4 ○ IPv6		
* Security Group ACL content	permit udp dst eq 53 permit udp dst eq 5353 permit tcp dst eq 5353 permit tcp dst eq 53 permit udp dst eq 67 permit udp dst eq 68 permit tcp dst eq 591 permit tcp dst eq 8008 permit udp dst eq 8008 permit udp dst eq 8008 permit udp dst eq 8080 permit udp dst eq 8080 permit udp dst eq 123 permit udp dst eq 7 permit tcp dst eq 443 permit udp dst eq 443	I	

Compteur SGACL sous-jacent sur les commutateurs de fabric

Afin de vérifier les accès aux stratégies SGACL, exécutez cette commande : **Show cts role-based** counter

Role-bas	ied IPv4	counters					
From	То	SW-Denied	HW-Denied	SW-Permitt	HW-Permitt	SW-Monitor	HW-Monitor
*							0
2	2			1644843			0
1101	2						0
1102							0
101	101						0
1101	101				57647		0
1102	101				12541		0
1103	101				25		0

Dépannage

Problème 1. Si les deux noeuds ISE sont hors service.

Si les deux noeuds ISE sont désactivés, le mappage IP/SGT reçu par ISE est supprimé et tous les DGT sont marqués comme inconnus, et toutes les sessions utilisateur qui existent s'arrêtent après 5 à 6 minutes.

Note: Ce problème ne s'applique que si sgt (xxxx) -> inconnu (0) l'accès SGACL est limité au port DHCP, DNS et proxy Web.

Solution :

- 1. Création d'une SGT (ex. RFC1918).
- 2. Poussez la plage d'adresses IP privées RFC sur les deux bords.
- 3. Limiter l'accès au serveur DHCP, DNS et proxy Web à partir de sgt (xxxx) -> RFC1918
- 4. Créer/modifier sgacl sgt (xxxx) -> inconnu avec le contrat Permit IP.

Maintenant, si les deux noeuds ise tombent en panne, sgt—>accès inconnu SGACL et la session qui existe sont intacts.

Problème 2. Voix unidirectionnelle sur téléphone IP ou pas de voix.

L'extension à la conversion IP s'est produite sur SIP et la communication vocale réelle s'est produite sur RTP entre IP et IP. CUCM et la passerelle vocale ont été ajoutés à **DGT_Voice**.

Solution :

- 1. Le même emplacement ou la communication vocale est-ouest peut être activé en autorisant le trafic à partir d'IP_Phone —> IP_Phone.
- 2. Le reste de l'emplacement peut être autorisé par la plage de protocoles Permitting RTP dans DGT RFC1918. La même plage peut être autorisée pour IP_Phone —> Inconnu.

Problème 3. Le point de terminaison VLAN critique n'a pas d'accès au réseau.

DNAC provisionne le commutateur avec le VLAN critique pour les données et, selon la configuration, toutes les nouvelles connexions pendant la panne ISE obtiennent le VLAN critique et SGT 3999. La stratégie Refuser par défaut dans trustsec limite la nouvelle connexion à accéder à toutes les ressources réseau.

Solution :

Push SGACL for Critical SGT sur tous les commutateurs Edge et Border à l'aide du modèle DNAC

cts role-based permissions from 0 to 3999 FALLBACK

cts role-based permissions from 3999 to 0 FALLBACK Ces commandes sont ajoutées à la section de configuration.

Note: Toutes les commandes peuvent être combinées en un seul modèle et peuvent être poussées pendant le provisionnement.

Problème 4. VLAN critique de la liste déroulante de paquets.

Une fois que la machine est dans le VLAN critique en raison de noeuds ISE en panne, il y a une perte de paquet toutes les 3 à 4 minutes (10 pertes max. observées) pour tous les points d'extrémité du VLAN critique.

Observations : Compteurs d'authentification en augmentation lorsque les serveurs sont DEAD. Les clients tentent de s'authentifier auprès de PSN lorsque les serveurs sont marqués comme DEAD. Solution/Solution :

Idéalement, il ne devrait pas y avoir de demande d'authentification d'un point de terminaison si les noeuds PSN ISE sont hors service.

Poussez cette commande dans radius server avec DNAC :

automate-testeur username auto-test probe-on

Avec cette commande dans le commutateur, il envoie des messages d'authentification de test périodiques au serveur RADIUS. Il recherche une réponse RADIUS à partir du serveur. Un message de réussite n'est pas nécessaire : une authentification échouée suffit car elle indique que le serveur est actif.

Additional Information

Modèle final DNAC :

```
interface range $uplink1
no cts role-based enforcement
1 .
cts role-based sgt-map <ISE Primary IP> sgt 1102
cts role-based sgt-map <Underlay Subnet> sgt 2
cts role-based sgt-map <Wireless OTT Subnet>sgt 1102
cts role-based sgt-map <DNAC IP> sgt 1102
cts role-based sgt-map <SXP Subnet> sgt 2
cts role-based sgt-map <Network Monitoring Tool IP> sgt 1102
cts role-based sgt-map vrf CORP_VN <Voice Gateway Subnet> sgt 1102
!
ip access-list role-based FALLBACK
permit ip
1
cts role-based permissions from 2 to 1102 FALLBACK
cts role-based permissions from 1102 to 2 FALLBACK
cts role-based permissions from 2 to 2 FALLBACK
cts role-based permissions from 0 to 3999 FALLBACK
cts role-based permissions from 3999 to 0 FALLBACK
```

Note: Toutes les interfaces de liaison ascendante dans les noeuds de périphérie sont

configurées sans application et on suppose que la liaison ascendante se connecte uniquement au noeud de périphérie. Sur les noeuds de périphérie, les interfaces de liaison ascendante vers les noeuds de périphérie doivent être configurées sans application et cela doit être fait manuellement.