Informazioni su BGP RPKI con white paper su XR7 Cisco8000

Sommario

Introduzione

Questo documento descrive la funzionalità Border Gateway Protocol (BGP) Resource Public Key Infrastructure (RPKI) sulla piattaforma Cisco IOS® XR.

Premesse

Prefazione

In questo documento viene descritta la funzionalità BGP RPKI e la relativa protezione da aggiornamenti dei prefissi BGP falsi o dannosi.

Ambito

Questo documento utilizza Cisco 8000 con XR 7.3.1 per la dimostrazione. Tuttavia, BGP RPKI è una funzionalità indipendente dalla piattaforma. I concetti discussi in questo documento si applicano ad altre piattaforme Cisco (con Cisco IOS, Cisco IOS-XE .) con conversioni CLI appropriate equivalenti. Il presente documento non disciplina la procedura per aggiungere autorizzazioni all'origine delle rotte (ROA) nei registri Internet regionali.

Prerequisiti

Il lettore richiede la conoscenza del protocollo BGP.

Esclusione di responsabilità

Gli indirizzi IP (Internet Protocol) utilizzati in questo documento non sono indirizzi effettivi. Tutti gli esempi, l'output del comando display e le figure incluse nel documento sono mostrati solo a scopo illustrativo. L'utilizzo di indirizzi IP reali in contenuti illustrativi è involontario e casuale.

Problemi BGP causati da annuncio di prefisso errato

Il BGP è la backbone del traffico Internet. Sebbene sia il componente più importante del core Internet, non è in grado di verificare se l'annuncio BGP in entrata ha avuto origine da un sistema autonomo autorizzato.

Questa limitazione del BGP lo rende un facile candidato per vari tipi di attacchi. Un attacco comune si chiama "dirottamento". Questo attacco può essere utilizzato per:

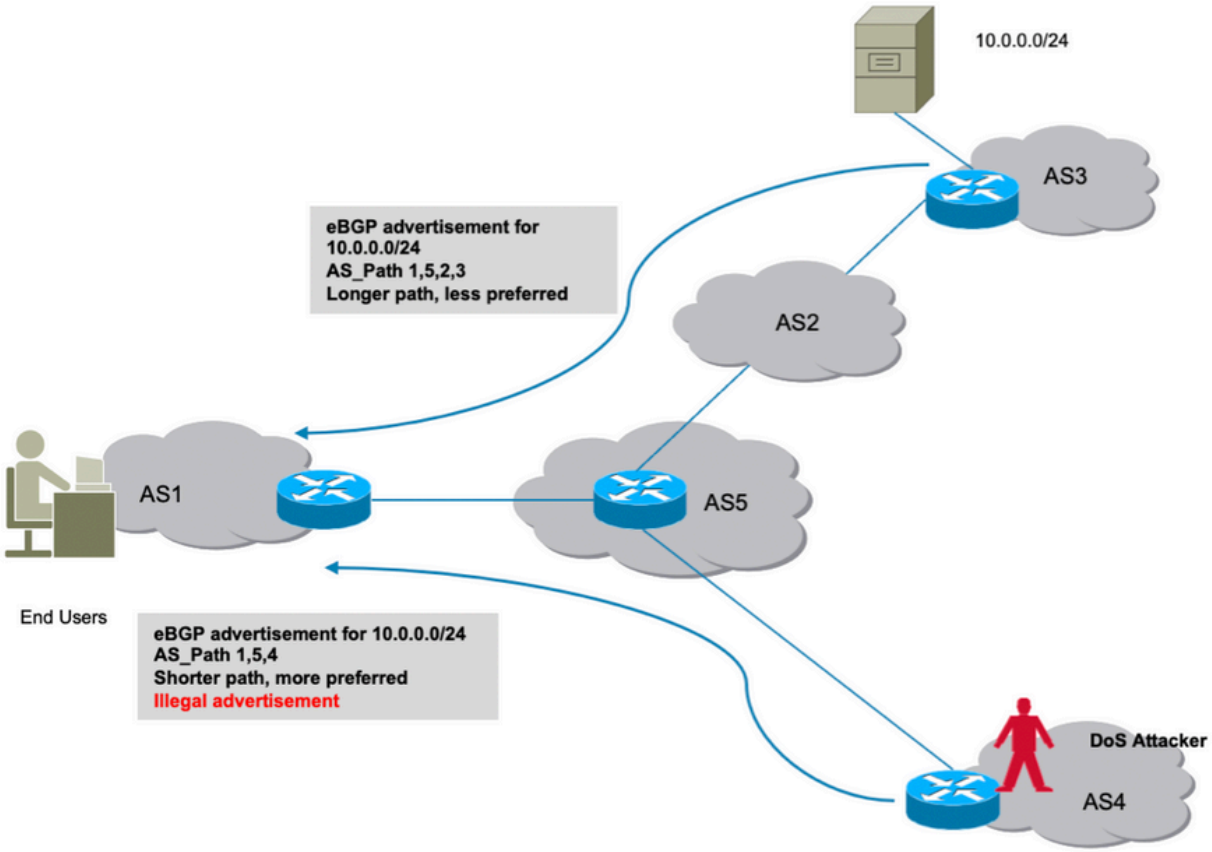
- L'intercettazione degli IP per inviare i risultati della posta indesiderata viene rifiutata e, di conseguenza, il servizio viene rifiutato.
- Controlla il traffico per ottenere informazioni riservate come le password.
- Interruzioni causate da configurazioni errate da parte dell'amministratore.
- Impedire la consegna del traffico con l'attivazione di server falsi garantisce la negazione del servizio.

L'attacco Denial of Service (comunemente noto come DoS) è un tentativo dannoso di interrompere il normale traffico diretto a un router, uno switch, un server e così via. Esistono diversi tipi di attacchi DoS e pochi sono discussi in questa sede.

Hijacking route

Si consideri lo scenario illustrato di seguito. Autonomous System 3 (AS3) invia un annuncio BGP legale per il prefisso 10.0.0.0/24. Secondo il progetto di BGP, non c'è nulla in BGP che impedisca a un aggressore di pubblicizzare lo stesso prefisso su Internet.

Come mostrato, l'utente non autorizzato in AS4 annuncia lo stesso prefisso 10.0.0.0/24. L'algoritmo per il miglior percorso BGP preferisce un percorso con AS_Path più breve. AS_Path 1,5,4 prevale sul percorso più lungo tramite AS 1,5,2,3. Pertanto, il traffico proveniente dai client verrà ora reindirizzato all'ambiente dell'autore dell'attacco e può essere interrotto, il che comporta la negazione del servizio ai client finali.

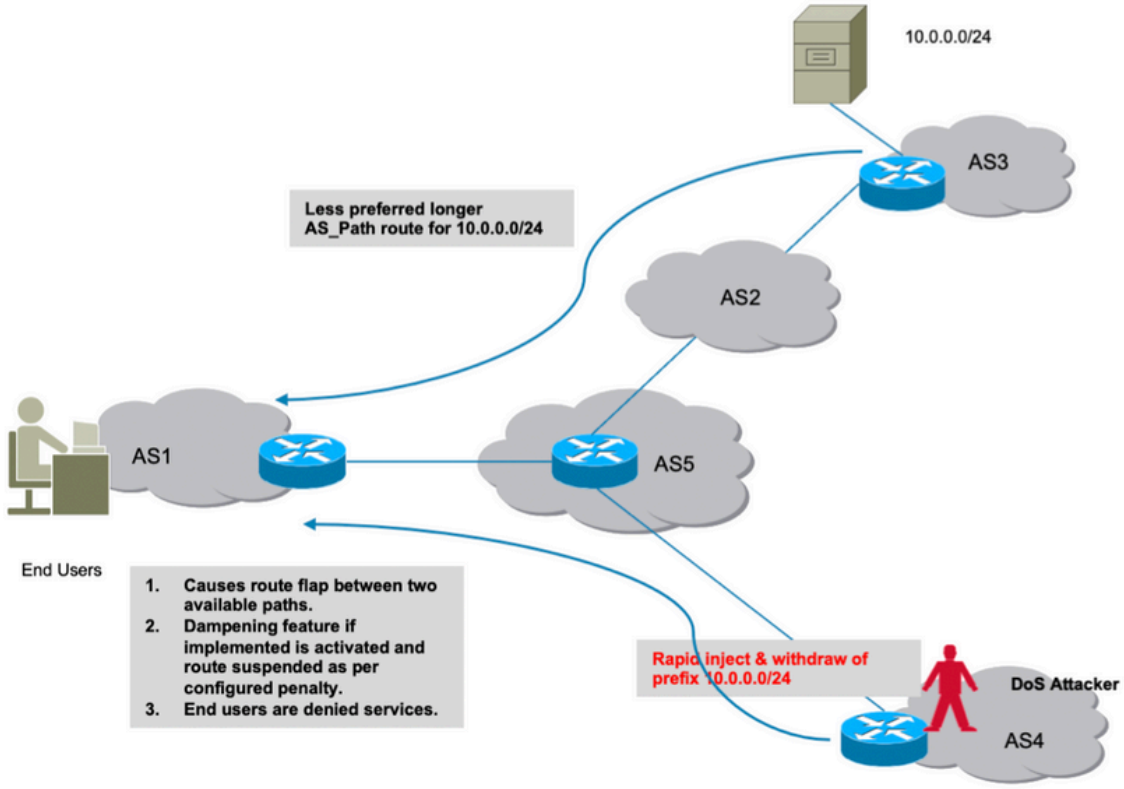


Dirottamento

Prestazioni del sistema ridotte

In questa sezione viene illustrato un altro modo in cui è possibile negare i servizi. Se la funzione di attenuazione dell'impatto delle route BGP di Cisco è configurata, potrebbe essere sfruttata se l'utente malintenzionato introduce rapidi flap delle route nella rete che causano una varianza costante.

La funzione di attenuazione comporterà sanzioni per il percorso legittimo e lo renderà non disponibile per il traffico effettivo. Inoltre, questo tipo di flap indotti in modo non etico provocherà uno stress sulle risorse del router, come la CPU, la memoria e così via.

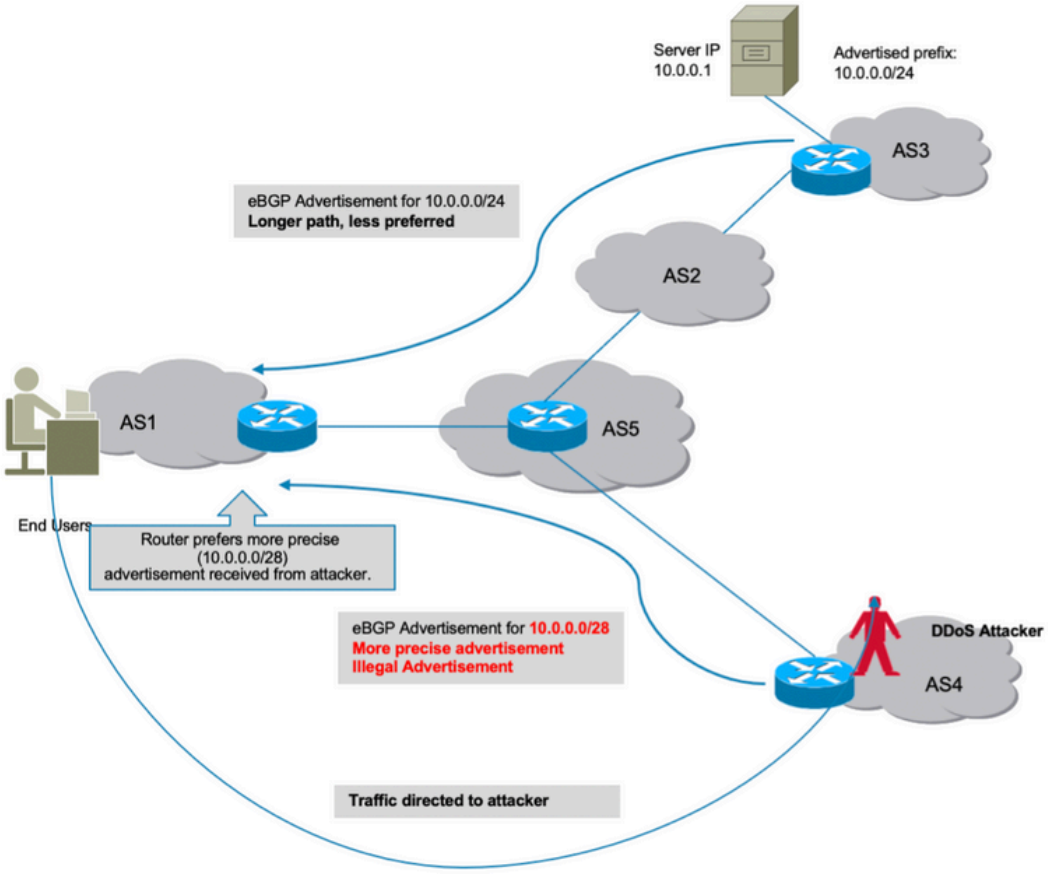


Attenuazione route

Hijacking del sottoprefisso

Come accennato nella sezione precedente, in che modo un utente non autorizzato può creare un prefisso in modo illegale e causare un'interruzione del traffico. Sfortunatamente, una perturbazione non è l'unica causa di preoccupazione. In tali attacchi, i dati effettivi possono essere compromessi quando un utente malintenzionato può scansionare i dati ricevuti per un utilizzo non etico.

Allo stesso modo, il dirottamento di un percorso potrebbe essere fatto pubblicizzando illegalmente un percorso più preciso. BGP preferisce prefissi più lunghi e questo comportamento può essere sfruttato in modo errato, come mostrato nell'immagine.



Dirottamento sub-prefisso

Tutti gli attacchi discussi derivano dal fatto che BGP non era in grado di identificare se l'origine AS di questi prefissi annunciati maliziosamente fosse valida o meno. Per risolvere questo problema, è necessaria una fonte di dati "vera" e "attendibile" che un router possa conservare nel proprio database. In seguito, a ogni ricezione di un nuovo annuncio, il router diventa in grado di verificare in modo incrociato le informazioni sull'origine del prefisso AS ricevute dal peer BGP con le informazioni sul database locale ricevute dal validator.

Pertanto, il router è in grado di distinguere gli annunci buoni da quelli cattivi (illegali) e la capacità di evitare tutti gli attacchi discussi in precedenza viene aggiunta automaticamente al router. BGP RPKI fornisce la fonte attendibile di informazioni necessaria.

RKI

RPKI utilizza un repository che contiene ROA. Un ROA contiene informazioni sul prefisso e il numero BGP AS associato. L'autorizzazione dell'origine della route è un'istruzione con firma crittografica.

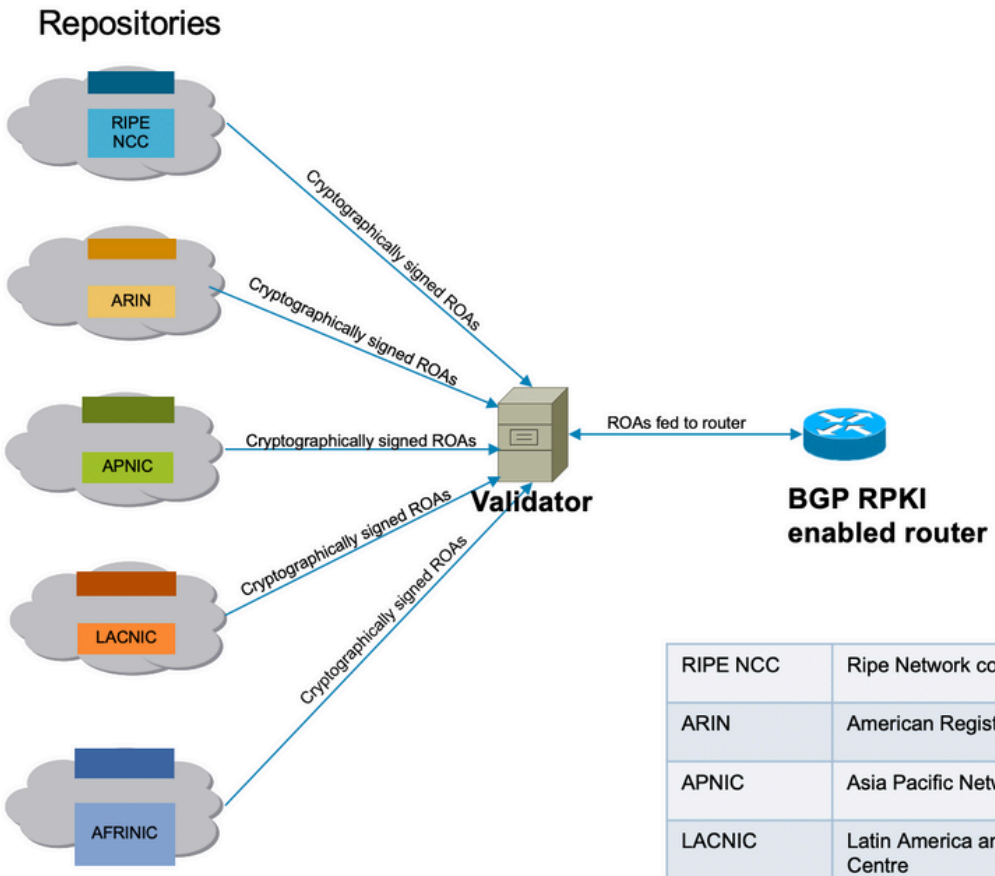
I 5 registri regionali Internet (RIR) sono i trust anchor dell'RPKI. IANA (Internet Assigned Numbers Authority) è la parte superiore della struttura ad albero che distribuisce i prefissi IP. I RIR sono il successivo nella gerarchia. Assegnano i sottoprefissi ai registri Internet locali (LIR) e ai provider di servizi Internet (ISP) di grandi dimensioni. Firmano un certificato per questi prefissi. Il livello successivo alloca i sottoprefissi di questi e utilizza i certificati riportati sopra per firmare i propri certificati e certificare le proprie allocazioni. In genere utilizzano i propri punti di pubblicazione per ospitare i certificati e i ROA. Ogni certificato elenca i punti di pubblicazione dei certificati figlio

firmati. RPKI forma quindi una struttura di certificati che rispecchia la struttura delle allocazioni di indirizzi IP. I validatori RPKI di proprietà dei relying party eseguono il polling di tutti i punti di pubblicazione per trovare i certificati e i ROA aggiornati (e i CRL e i manifesti). Le relazioni iniziano in corrispondenza dei trust anchor e seguono i collegamenti ai punti di pubblicazione dei certificati figlio.

I ROA vengono inseriti nel repository attraverso i RIR, ma lo stesso può essere fatto attraverso altri registri (nazionali o locali). Questa responsabilità può essere delegata anche agli ISP con un'adeguata supervisione e verifica da parte dei RIR.

Al momento, ci sono cinque repository ROA gestiti da RIPE NCE, ARIN, APNIC, LACNIC e AFRINIC.

Un validator presente nella rete comunica con questi repository e scarica un database ROA attendibile per crearne la cache. Si tratta di una copia unificata della RPKI, che viene periodicamente recuperata/aggiornata direttamente o indirettamente dalla RPKI globale. Validator invia quindi queste informazioni ai router consentendo loro di confrontare gli annunci BGP in arrivo con la tabella RPKI per prendere una decisione sicura.



RIPE NCC	Ripe Network coordination center
ARIN	American Registry for Internet Numbers
APNIC	Asia Pacific Network Information Centre
LACNIC	Latin America and Caribbean Network Information Centre
AFRINIC	African Network Information Centre

Connettività infrastruttura RPKI

Convalida

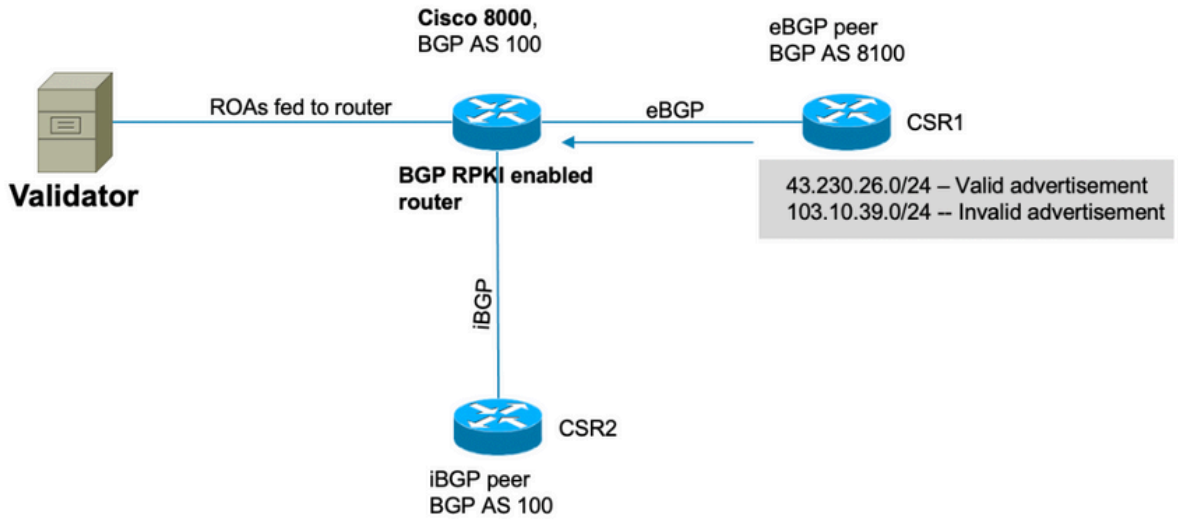
In questa dimostrazione viene utilizzato il validator RIPE. Il validator comunica con il router stabilendo una sessione TCP. In questa dimostrazione, il validator rimane in ascolto sulla porta IP 192.168.122.120 e sulla porta 3323.

```
routinator server --rtr 192.168.122.120:3323 --refresh=900
```

IANA ha specificato la porta 3323 per questa comunicazione. Il timer di aggiornamento definisce l'intervallo di tempo trascorso il quale il repository locale verrà sincronizzato e aggiornato per rimanere aggiornato.

Dimostrazione BGP RPKI

Topologia



Topologia

> **Nota**: in questa dimostrazione vengono utilizzati numeri e prefissi ASA pubblici casuali allo scopo di illustrare la meccanica BGP RPKI. Gli IP pubblici vengono utilizzati a causa di RPKI principalmente per la protezione dei prefissi pubblici e tutti gli ACR creati sui RIR sono prefissi pubblici. Infine, nessuna delle azioni, configurazioni, ecc. descritte in questo documento ha alcun effetto su questi IP pubblici e ASA.

Configurazione

```
router bgp 100

bgp router-id 10.1.1.1

rpki server 192.168.122.120

transport tcp port 3323

refresh-time 900
```

```
address-family ipv4 unicast
 !
 neighbor 10.0.12.2
 remote-as 8100
 address-family ipv4 unicast
  route-policy Pass in
  route-policy Pass out
 !
 !
 neighbor 10.0.13.3
 remote-as 100
 address-family ipv4 unicast
 !
 !
// 'Pass' is a permit all route-policy.
```

Sessione BGP RPKI

Il router stabilisce una sessione TCP con un validator (IP: 192.168.122.120, porta 3323) per scaricare la cache ROA nella memoria del router.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server 192.168.122.120
Wed Jan 20 22:54:15.763 UTC

RPKI Cache-Server 192.168.122.120
 Transport: TCP port 3323
 Bind source: (not configured)
 Connect state: ESTAB
 Conn attempts: 1
 Total byte RX: 4428792
 Total byte TX: 1400
 Last reset
   Timest: Jan 20 05:59:58 (16:54:17 ago)
   Reason: protocol error
```

Download ROA su router

La funzione di convalida invia le informazioni sul ROA al router. Questa cache viene aggiornata periodicamente per ridurre al minimo la possibilità che il router conservi informazioni non aggiornate. In questa dimostrazione, è stato configurato un tempo di aggiornamento di 900 secondi. Come mostrato di seguito, il router Cisco 8000 ha scaricato 172632 IPv4 e 28350 IPv6 ROA dal validator.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Wed Jan 20 23:01:59.432 UTC

Hostname/Address        Transport       State           Time                ROAs (IPv4/IPv6)

192.168.122.120         TCP:3323        ESTAB           17:00:21        172632/28350

RP/0/RP0/CPU0:Cisco8000#show bgp rpki table ipv4

Wed Jan 20 23:09:26.899 UTC

>>>Snipped output<<<

 Network               Maxlen      Origin-AS         Server

 10.0.0.0/24            24              13335             192.168.122.120

 10.0.4.0/22            22              38803             192.168.122.120

 10.0.4.0/24            24              38803             192.168.122.120

 10.0.5.0/24            24              38803             192.168.122.120

 10.0.6.0/24            24              38803             192.168.122.120

 10.0.7.0/24            24              38803             192.168.122.120

 10.1.1.0/24            24              13335             192.168.122.120

 10.1.4.0/22            22              4134              192.168.122.120

 10.1.16.0/20           20              4134              192.168.122.120

 10.2.9.0/24            24              4134              192.168.122.120

 10.2.10.0/24           24              4134              192.168.122.120

 10.2.11.0/24           24              4134              192.168.122.120

 10.2.12.0/22           22              4134              192.168.122.120

 10.3.0.0/16            16              4134              192.168.122.120

 10.6.0.0/22            24              9583              192.168.122.120
```

Verifica

In questa sezione viene mostrato come BGP RPKI in azione e come impedisce al router di inviare annunci errati o non validi.

Abilitazione della validità come origine

Per impostazione predefinita, il router recupera i ROA dal validator, ma non inizia a utilizzarli finché non è configurato per farlo. Di conseguenza, questi prefissi sono contrassegnati come "D" o disabilitati.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Wed Jan 20 23:27:37.268 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 30

BGP main routing table version 30

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs


Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

D*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

D*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

D*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Per abilitare il router per il controllo della validità come origine, attivare questo comando per la famiglia di indirizzi interessata.

```
router bgp 100

 address-family ipv4 unicast
```

```
 bgp origin-as validation enable

 !
```

Quando si attiva questo comando, il router analizza i prefissi presenti nella tabella BGP in base alle informazioni ROA ricevute dal validator e uno dei tre stati viene assegnato ai prefissi.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 00:04:58.136 UTC

Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*  203.0.113.1/24     10.0.12.2                0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Per consentire al router di utilizzare le informazioni sullo stato di convalida del prefisso durante il miglior calcolo del percorso, è necessario eseguire questo comando. Questa opzione non è attivata per impostazione predefinita in quanto consente di non utilizzare le informazioni di validità per il calcolo del miglior percorso, ma di utilizzarle comunque nei criteri di instradamento descritti più avanti in questo documento.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Stati di validità prefisso

In è possibile trovare un prefisso in tre stati.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 00:04:58.136 UTC



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*  203.0.113.1/24     10.0.12.2                0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

- Non valido: indica che il prefisso soddisfa una delle due condizioni seguenti: 1. Corrisponde a una o più **autorizzazioni ROA** (Route Origin Authorizations), ma non esiste corrispondenza ROA in cui l'AS di origine corrisponde all'AS di origine in AS-PATH. 2. Corrisponde a uno o più ROA alla lunghezza minima specificata nel ROA, ma per tutti i ROA in cui corrisponde alla lunghezza minima, è più lunga della lunghezza massima specificata. L'origine AS non è rilevante per la condizione #2.
- Valido: indica che il prefisso e la coppia AS sono stati trovati nella tabella della cache RPKI.
- Non trovato: indica che il prefisso non è compreso tra i prefissi validi o non validi.

In questa sezione vengono descritti in dettaglio i singoli prefissi e il relativo stato.

1. 203.0.113.0/24 - Valido

Il peer eBGP in AS 8100 ha creato questa route e l'ha annunciata al nodo Cisco8000. Poiché l'AS di origine (8100) corrisponde all'AS di origine nel ROA (ricevuto dal validator), questo prefisso è contrassegnato come valido e viene installato nella tabella di routing del router.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki table | in "203.0.113.0|Max"

Thu Jan 21 00:21:26.026 UTC

 Network               Maxlen          Origin-AS         Server

 203.0.113.0/24                24       8100              192.168.122.120
```

La route viene installata nella tabella BGP.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.0/24

Thu Jan 21 05:30:13.858 UTC

BGP routing table entry for 203.0.113.0/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 31          31

Last Modified: Jan 21 00:03:33.344 for 05:26:40

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer
```

```
 8100
   10.0.12.2 from 10.0.12.2 (192.168.122.105)
     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best
     Received Path ID 0, Local Path ID 1, version 31
     Origin-AS validity: valid
```

Poiché si tratta del prefisso BGP migliore e valido anche per RPKI, viene installato correttamente nella tabella di routing.

```
RP/0/RP0/CPU0:Cisco8000#show route 203.0.113.0/24
Thu Jan 21 00:29:43.667 UTC



Routing entry for 203.0.113.0/24
 Known via "bgp 100", distance 20, metric 0
 Tag 8100, type external
 Installed Jan 21 00:03:33.731 for 00:26:10
 Routing Descriptor Blocks
   10.0.12.2, from 10.0.12.2, BGP external
     Route metric is 0
 No advertising protos.
```

2. 203.0.113.1/24 - Non valido

Questo prefisso non è valido perché si è verificato un conflitto tra le informazioni sull'origine AS contenute nella ROA e le informazioni sull'origine AS ricevute tramite il messaggio BGP dal peer eBGP. 203.0.113.1/24 è ricevuto tramite BGP con origine AS 8100.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity invalid
Thu Jan 21 00:34:38.171 UTC
BGP router identifier 10.1.1.1, local AS number 100
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000000   RD version: 33
BGP main routing table version 33
BGP NSR Initial initsync version 2 (Reached)
```

```
BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs


Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop            Metric LocPrf Weight Path

*  203.0.113.1/24     10.0.12.2                0             0 8100 ?
```

Tuttavia, il ROA ricevuto dal validator mostra che questo prefisso appartiene a AS 10021.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki table 203.0.113.1/24 max 24

Thu Jan 21 00:37:05.615 UTC


RPKI ROA entry for 203.0.113.1/24-24

 Origin-AS: 10021 from 192.168.122.120

Version: 124211
```

Poiché le informazioni sull'origine AS nell'annuncio BGP ricevuto (AS 8100) non corrispondono all'origine AS effettiva ricevuta in ROA (AS 10021), il prefisso viene contrassegnato come Non valido e non viene installato nella tabella di routing.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24

Thu Jan 21 05:37:26.714 UTC

BGP routing table entry for 203.0.113.1/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 32          32

Last Modified: Jan 21 00:03:33.344 for 05:33:53

Paths: (1 available, no best path)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external

     Received Path ID 0, Local Path ID 0, version 0
```

```
     Origin-AS validity: invalid
```

3. 192.168.122.1/32 Non trovato

Questo è un prefisso privato e non è presente nella cache ROA. BGP ha dichiarato questo prefisso come 'Non trovato'.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 192.168.122.1/32

Thu Jan 21 05:44:39.861 UTC

BGP routing table entry for 192.168.122.1/32

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 33          33

Last Modified: Jan 21 00:03:33.344 for 05:41:06

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 33

     Origin-AS validity: not-found
```

Poiché RPKI viene ancora adottato, i prefissi 'not found' vengono installati nella tabella di routing. In caso contrario, BGP ignorerà questi prefissi legittimi non registrati nel database RPKI.

Consenti prefisso non valido

Sebbene non sia consigliato, il software fornisce una manopola per consentire ai prefissi non validi di partecipare all'algoritmo di calcolo del miglior percorso.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as allow invalid

 !
```

Con questa configurazione, il router non considera i prefissi non validi per il calcolo del miglior percorso, mentre l'opzione è contrassegnata come "non valida". In questo output viene

visualizzato il percorso "203.0.113.1/24" contrassegnato come migliore.

```
RP/0/RP0/CPU0:Cisco8000#show bgp

Thu Jan 21 06:21:34.294 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 34

BGP main routing table version 34

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop            Metric LocPrf Weight Path

*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Come mostrato in questo output, il prefisso è contrassegnato come migliore nonostante non sia più valido.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24

Thu Jan 21 06:23:26.994 UTC

BGP routing table entry for 203.0.113.1/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                34          34

Last Modified: Jan 21 06:05:31.344 for 00:17:55

Paths: (1 available, best #1)

 Not advertised to any peer
```

```
 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 34

     Origin-AS validity: invalid
```

Si noti che un router considera ancora il prefisso non valido come l'ultima opzione e preferisce sempre un prefisso valido a un prefisso non valido, se disponibile.

Configurazione manuale del ROA sul router

Se per qualche motivo non viene ancora creato, ricevuto o ritardato un ROA per un determinato prefisso, è possibile configurare un ROA manuale sul router. Ad esempio, il prefisso "192.168.122.1/32" è contrassegnato come "Non trovato" come mostrato di seguito.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 06:36:31.041 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 34

BGP main routing table version 34

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?
```

```
I*> 203.0.113.1/24     10.0.12.2               0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2               0             0 8100 ?
```

Èpossibile configurare un ROA manuale come illustrato di seguito. Questo comando associa il prefisso ‘192.168.122.1/32’ a AS 8100.

```
router bgp 100

 rpki route 192.168.122.1/32 max 32 origin 8100
```

Con questa configurazione, lo stato del prefisso cambia da "N" a "V".

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 06:36:34.151 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 35

BGP main routing table version 35

BGP NSR Initial initsync version 2 (Reached)



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2               0             0 8100 ?

I*> 203.0.113.1/24     10.0.12.2               0             0 8100 ?

V*> 192.168.122.1/32   10.0.12.2               0             0 8100 ?
```

Stato convalida prefisso e criteri di route

Il risultato dello stato del prefisso può essere utilizzato per creare criteri di route. Questi stati possono essere utilizzati in un'istruzione match ed è possibile eseguire le azioni desiderate dall'amministratore. In questo esempio tutti i prefissi vengono associati a uno stato non valido e per essi viene impostato il valore di rilevanza 12345.

```
route-policy Invalid
```

```
 if validation-state is invalid then
   set weight 12345
 endif
end-policy
!



router bgp 100
 remote-as 8100
 address-family ipv4 unicast
  route-policy Invalid in
 !
 !
!
```

Questo output mostra un peso applicato prefisso non valido di 12345.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24
Thu Jan 21 06:57:33.816 UTC
BGP routing table entry for 203.0.113.1/24
Versions:
 Process           bRIB/RIB  SendTblVer
 Speaker                 38          38
Last Modified: Jan 21 06:54:04.344 for 00:03:29
Paths: (1 available, best #1)
 Not advertised to any peer
 Path #1: Received by speaker 0
 Not advertised to any peer
 8100
   10.0.12.2 from 10.0.12.2 (192.168.122.105)
     Origin incomplete, metric 0, localpref 100, weight 12345, valid, external, best, group-best
     Received Path ID 0, Local Path ID 1, version 38
     Origin-AS validity: invalid
```

Condivisione delle informazioni di convalida del prefisso tramite la community estesa

Poiché il router BGP può anche condividere lo stato di convalida del prefisso con altri router (senza cache locale da validator) tramite la community estesa BGP. In questo modo si risparmia il sovraccarico di ogni router della rete con una sessione di convalida e si scaricano tutti i ROA.

Ciò è reso possibile dalla comunità estesa BGP.

Questo comando consente al router di condividere le informazioni di 'convalida del prefisso' con i peer iBGP.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation signal ibgp
```

Dopo aver configurato il router Cisco 8000 come mostrato, il protocollo BGP aggiorna i peer per includere le informazioni sulla convalida del prefisso. In questo caso, il router iBGP adiacente è un router IOS-XE.

```
csr2#show ip bgp 203.0.113.1/24

BGP routing table entry for 203.0.113.1/24, version 14

Paths: (1 available, best #1, table default)

 Not advertised to any peer

 Refresh Epoch 1

 8100

   10.0.12.2 from 10.0.13.1 (10.1.1.1)

     Origin IGP, metric 0, localpref 100, valid, internal, best

     Extended Community: 0x4300:0:2

     rx pathid: 0, tx pathid: 0x0

     Updated on Jan 21 2021 18:16:56 UTC
```

Questa mappatura della community estesa può essere compresa usando 0x4300 0x0000 (4 byte che indicano lo stato).

I quattro byte che indicano lo stato vengono considerati come un numero intero senza segno a 32 bit con uno dei valori seguenti:

- 0 - Valido
- 1 - Non trovato
- 2 - Non valido

Il prefisso della community 203.0.113.1/24 è 0x4300:0:2, che corrisponde al prefisso "Non valido". In questo modo, il router csr2, nonostante non disponga di una cache locale propria, è ancora in grado di prendere decisioni in base allo stato di convalida del prefisso.

Èora possibile utilizzare lo stato di convalida del prefisso per trovare una corrispondenza in una route-map o nell'algoritmo per il miglior percorso BGP.

Suggerimenti per l'implementazione di BGP RPKI

Buone pratiche per la creazione di ROA

Queste sono alcune raccomandazioni basate su reti irraggiungibili osservate presso l'Osservatorio RPKI. L'Osservatorio RPKI analizza diversi aspetti del paesaggio RPKI.

- Se viene creato un ROA per un prefisso qualsiasi, si consiglia di annunciare tale prefisso in BGP. In assenza di tale certificato, qualcun altro può annunciarlo semplicemente fingendo di essere un ASN contenuto in tale ROA e utilizzare il prefisso.
- Se il valore di ROA viene creato con un valore di maxlen maggiore della lunghezza del prefisso, equivale a creare un valore di ROA per tutti i possibili prefissi al di sotto del prefisso originale fino al valore di maxlen. Si consiglia di annunciare tutti questi prefissi in BGP.
- Se viene creato un ROA per un prefisso e il proprietario del prefisso annuncia un sottoprefisso del prefisso originale, il ROA invaliderà quel sottoprefisso. Un ROA per il prefisso secondario e il massimo del ROA originale devono essere estesi per coprire il prefisso secondario.
- Se un'organizzazione è proprietaria di un prefisso, ma si prevede di non annunciarlo in BGP, è necessario creare un ROA per il prefisso AS0. Ciò invaliderà qualsiasi annuncio di prefisso in quanto AS0 non può apparire in alcun percorso AS.
- Se esistono più ASN che hanno origine nello stesso prefisso, è necessario creare gli ACL per tale prefisso per ciascuno degli ASN. Di conseguenza, se un router ha più ROA per lo stesso prefisso, sarà valido un annuncio BGP che corrisponda a uno di essi. Più ROA per lo stesso prefisso non sono in conflitto tra loro.
- Se "A" genera un prefisso per il cliente "B" e crea un ROA per tale prefisso per conto di "B", "A" deve anteporre l'ASN "B" all'annuncio o fare in modo che "B" generi il prefisso stesso.

Impatto delle prestazioni di RPKI sui router XR BGP

Effetto dell'aggiornamento ROA sulla CPU con Route-Policy

Quando si aggiornano i ROA e se il router dispone di una route-policy in entrata locale per un router adiacente che contiene un "lo stato di convalida è", diventa importante riconvalidare lo stato dei prefissi in base ai nuovi ROA aggiornati. A tale scopo, il router invia una richiesta BGP REFRESH al proprio peer.

Quando i vicini BGP ricevono questo messaggio come mostrato, i vicini inviano nuovamente i prefissi e i criteri di route in ingresso possono riconvalidare i prefissi in ingresso.

```
Jan 22 18:28:41.360: BGP: 10.0.12.1 rcv message type 5, length (excl. header) 4

Jan 22 18:28:41.360: BGP: 10.0.12.1 rcvd REFRESH_REQ for afi/safi: 1/1, refresh code is 0
```

Il problema si amplifica quando molti vicini si aggiornano contemporaneamente ogni volta che vengono aggiornati i conti di ritorno. Se i criteri di route in entrata per i router adiacenti sono

complessi e richiedono un'elevata elaborazione, dopo un aggiornamento del ROA la CPU risulterà elevata per alcuni minuti. Questi messaggi REFRESH non vengono visualizzati se i criteri di route in ingresso del router adiacente non contengono un comando "validation-state is".

Se per un router adiacente è configurata la "riconfigurazione soft sempre in entrata", i messaggi BGP REFRESH non verranno inviati, ma verranno comunque eseguiti gli stessi criteri di route alla stessa velocità ed è possibile prevedere lo stesso utilizzo della CPU.

Si consiglia di preferire l'approccio "bgp bestpath origin-as use invalid" rispetto alla configurazione di una policy di route per i motivi illustrati al punto 6.2.2.

Riduzione al minimo dell'impatto della CPU causato dall'aggiornamento ROA

Il modo migliore per evitare il problema qui illustrato consiste nell'utilizzare la **validità dell'origine del percorso migliore** senza **lo stato di convalida** nel criterio.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Questo comando mantiene un percorso non valido ricevuto sul router, ma impedisce che diventi il percorso migliore. Non verrà installata né annunciata in seguito. È meglio lasciarlo cadere. Se con il successivo aggiornamento del ROA diventa valido, non è necessario alcun REFRESH e diventa automaticamente idoneo per il miglior percorso senza che sia necessaria l'esecuzione di regole.

Se l'utente preferisce consentire i prefissi "non validi" e non li utilizza, oltre alla **validità dell'origine del percorso migliore**, utilizzare la configurazione **origine del percorso migliore come non valido**.

In questo caso, quando un ROA cambia, il percorso migliore viene automaticamente aggiornato senza che sia necessario un messaggio REFRESH. Per annullare la preferenza, una route indica che durante la selezione della route BGP il percorso non valido RPKI è considerato meno preferibile di qualsiasi altro percorso alla stessa destinazione. È simile all'assegnazione di un peso o di una preferenza locale minore di 0.

Il numero di invalidamenti RPKI è relativamente ridotto e mantenuto nella tabella non determina un impatto significativo sulle risorse.

> **Nota**: per utilizzare la "validità origine percorso migliore come utilizzo", tutti i percorsi di una route, inclusi i percorsi IBGP, devono avere la validità RPKI corretta. In caso contrario, è comunque possibile eseguire il test dello stato di convalida in route-policy.

Le route IBGP non vengono convalidate dal router sul database ROA. Le route IBGP ottengono una validità RPKI dalla community estesa RPKI. Se la route IBGP viene ricevuta senza questa community estesa, il relativo stato di convalida viene impostato su non trovato.

Ingombro della memoria RPKI BGP

Ciascun ROA consuma memoria per l'indice e i dati. Se due server ROA fanno riferimento allo stesso prefisso IP, ma hanno max_len diverso o sono ricevuti da server RPKI diversi, condividono lo stesso indice ma hanno dati separati. I requisiti di memoria possono variare perché il sovraccarico di memoria non è costante. Si raccomanda un superamento del 10%. Le piattaforme a 64 bit richiedono più memoria per ogni oggetto di memoria rispetto alle piattaforme a 32 bit. Utilizzo di memoria IOS-XR in byte per un oggetto indice e un oggetto dati nella tabella. Alcuni costi comuni, per lo più costanti, sono inclusi nei numeri.

	Piattaforma a 32 bit (byte)	Piattaforma a 64 bit (byte)
Indice IPv4	74	111
Indice IPv6	86	125
dati	34	53

In questa sezione vengono illustrati due scenari per spiegare in che modo i server ROA utilizzano la memoria.

Scenario 1. Tre server RPKI configurati sul router

Si prenda in considerazione un router che utilizza 3 server RPKI, ognuno dei quali fornisce 200.000 ROA IPv4 e 20.000 ROA IPv6 su un processore di routing a 64 bit e richiederà la seguente memoria:

20000 * (125 + 3*53) + 200000 * (111 + 3*53) byte = 59,68 milioni di byte

Durante il calcolo della memoria, il ROA per lo stesso prefisso di tre validatori diversi condivideva lo stesso valore di indice.

Scenario 2. Server RPKI singoli configurati sul router

Memoria di processo BGP senza ROA:

```
RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:19:57.945 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot
 Process

1069           2M        71M       132K        25M      7447M        50M        74M        bgp


RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:12:09.073 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      NONE          00:00:25      N/A
```

Il processo BGP consuma 25 MB di memoria senza ROA.

Memoria di processo BGP con ROA:

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:23:46.769 UTC


Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      ESTAB         00:02:42      172796/28411


RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:24:14.659 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot     Process

1069          2M        99M       132K        53M      7447M        50M       102M       bgp
```

Il processo BGP consuma 25 MB di memoria senza ROA.

Memoria di processo BGP con ROA:


```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:23:46.769 UTC


Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      ESTAB         00:02:42      172796/28411

RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:24:14.659 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot     Process

1069          2M        99M       132K        53M      7447M        50M       102M       bgp
```


Il router Cisco 8000 esegue un sistema operativo a 64 bit. Ricevette 172796 IPv4 ROA e 28411 ROA.

Memoria (byte) = 172.796 x [111 (indice) + 53 (dati)] + 2841 x [125 (indice) + 53 (dati)].

Questi calcoli danno circa 27 MB, che è approssimativamente l'incremento osservato sulla memoria del router sopra.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).