

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 1 / 11

Registre de canvis del document

Revisió	Redactat per	Revisat per	Aprobat per	Data aprovació	Data publicació

Revisió	Apartat	Data Modificació	Motiu del canvi
1.0	-	12/06/2026	Primera versió del disseny tècnic de la política ctti-validate-ip 2.0.0.

RESPONSABLE DEL DOCUMENT: Accenture

Í N D E X

1. INTRODUCCIÓ	2
1.1 Propòsit	2
1.2 Abast	2
1.3 Definicions, acrònims i abreviatures	2
1.4 Referències	3
2. DISSENY DETALLAT	4
2.1 Component ctti-validate-ip	4
2.1.1 Disseny del component	4
2.1.2 Escenaris i algorismes	5
2.1.3 Altres vistes i informació addicional.....	6
ANNEXOS	8
Annex A — Seguretat i controls	8
Annex B — Consideracions de rendiment	8
Annex C — Versionat i compatibilitat	8
Annex D — Traçabilitat amb codi, tests i Postman	9
Annex E — Configuració d'API consumidora i cabeceres suportades	10
Annex F — Parametrització i rols	11

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)	N. revisió doc.: 1.0
	Disseny detallat de la solució	
	N. versió aplicació: 2.0.0	Build: 001 Pàg. 2 / 11

1. INTRODUCCIÓ

El present document descriu el disseny tècnic detallat de la política ctti-validate-ip versió 2.0.0, desplegada sobre IBM API Connect 10.0.8.8 i IBM DataPower API Gateway 10.6.0.6 (compatible també amb la versió 10.6.0.9 prevista)... La informació aquí recollida ha de ser suficient perquè la fase de construcció no requereixi prendre decisions addicionals més enllà de la pròpia sintaxi.

1.1 Propòsit

El propòsit d'aquesta política és validar l'adreça IP d'origen de les peticions que arriben al gateway, comparant-la amb una llista blanca configurable per API. La versió 2.0.0 amplia la funcionalitat de la versió 1.0.0 amb suport multi-capçalera, rangs CIDR (IPv4 i IPv6) i normalització d'adreces IPv4-mapped IPv6, mantenint la retrocompatibilitat amb les APIs que ja consumeixen la versió anterior. L' objectiu d' aquest disseny és documentar formalment la nova versió, perquè pugui ser utilitzada com a base contractual entre l' equip de plataforma i els equips d' aplicació consumidors.

1.2 Abast

Aquest document cobreix els aspectes tècnics següents:

- Arquitectura i ubicació de la política dins l' acoblament d' una API.
- Estructura del GatewayScript (codi font) i del YAML de definició de política.
- Algoritmes de validació IPv4 / IPv6 / CIDR / IPv4-mapped IPv6.
- Gestió d' errors controlats i integració amb la política ctti-error-management.
- Propietats consumides per la política i contracte amb l' API consumidora.
- Bateria de proves unitàries i de proves funcionals (Postman).
- Procediment de versionat i migració des de la versió 1.0.0.

Queden fora de l' abast d' aquest document:

- La política nativa d'IBM "ip-validation" inclosa per defecte en API Connect (es manté com a alternativa, però CTTI conserva la seva pròpia política per obtenir funcionalitat addicional).
- Altres polítiques CTTI invocades en fluxos nominals (ctti-error-management, ctti-validate-request, etc.), que es documenten en dissenys tècnics propis.
- La infraestructura DataPower (clústers, gateways, certificats), responsabilitat de l'equip d'infraestructura.

1.3 Definicions, acrònims i abreviatures

Terme	Descripció
API Connect	Producte d' IBM per a la gestió, publicació i seguretat d' APIs REST i SOAP. Versió actual: 10.0.8.8.
DataPower	Gateway d'aplicació d'IBM (DataPower API Gateway) que executa les polítiques d'API Connect. Versió actual: 10.6.0.6, prevista 10.6.0.9.
GatewayScript	Llenguatge basat en JavaScript ES5/V8 que s'executa dins del motor de DataPower. La política està escrita a GatewayScript v2.0.
Política	Component d' API Connect que aporta funcionalitat reutilitzable a les APIs. Es defineix mitjançant un YAML que conté el codi GatewayScript encastat.
Acoblat	Seqüència ordenada de polítiques que defineix el comportament d' una API.
CIDR	Classless Inter-Domain Routing. Notació per representar rangs d'adreces IP (p. ex. 10.0.0.0/24).
IPv4-mapped IPv6	Adreça IPv6 amb format ::ffff:x.x.x.x que representa una adreça IPv4 sobre infraestructura dual-stack.
RFC 7239	Estàndard que defineix la capçalera HTTP Forwarded per indicar l' origen real d' una petició a través de proxies.
Whitelist	Llista d' elements explícitament permesos; en aquest cas adreces IP o rangs

Finançat per



GOBIERNO
DE ESPAÑA



Plan de
Recuperación,
Transformación
y Resiliencia



Next Generation
Catalunya



Generalitat
de Catalunya

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 3 / 11

Terme	Descripció
	CIDR.

1.4 Referències

- Documentació corporativa API Connect CTTI (<https://canigo.ctti.gencat.cat/plataformes/apim/documentacio/>).
- IBM API Connect 10.0.8 KC (<https://www.ibm.com/docs/en/api-connect/10.0.8>).
- IBM DataPower Gateway 10.6 KC (<https://www.ibm.com/docs/en/datapower-gateway/10.6>).
- RFC 7239: Forwarded HTTP Extension (<https://datatracker.ietf.org/doc/html/rfc7239>).
- RFC 4291: IP Version 6 Addressing Architecture (<https://datatracker.ietf.org/doc/html/rfc4291>).
- RFC 4632: Classless Inter-domain Routing (CIDR) (<https://datatracker.ietf.org/doc/html/rfc4632>).

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)	N. revisió doc.: 1.0
	Disseny detallat de la solució	
	N. versió aplicació: 2.0.0	Build: 001 Pàg. 4 / 11

2. DISSENY DETALLAT

2.1 Component ctti-validate-ip

2.1.1 Disseny del component

Visió general de la política

ctti-validate-ip és una política de tipus gatewayscript que s'executa dins l'acoblament d'una API d'API Connect. La seva responsabilitat, única i ben delimitada, és determinar si l'adreça IP del client originador de la petició està autoritzada per consumir l' API.

La política llegeix la IP d'origen d'una llista ordenada de capçaleres HTTP, normalitza el seu format quan és necessari i la compara amb la llista blanca declarada a la propietat api.properties-ips-validas. Si la direcció no es troba a la llista, o si no es pot determinar la IP d'origen, la política rebutja la petició mitjançant un error controlat que la política ctti-error-management transformarà en la resposta final al client.

Posició dins de l'assemblatge

La política s'invoca normalment al principi de l'acoblament d'una API, just després de les polítiques de seguretat bàsiques (autenticació) i abans de qualsevol política de transformació o invocació al backend. La seva execució primerenca garanteix que les peticions no autoritzades es rebutgin abans de consumir recursos addicionals del gateway.

Ordre recomanat dins l'acoblament:

- global-policy-prehooks: assignació de Traceld i validacions globals.
- ctti-validate-ip (aquesta política): validació d'IP origen.
- ctti-validate-request: validació del cos i paràmetres de la petició.
- invoke / gatewayscript de lògica de negoci: invocació al backend.
- ctti-validate-response: validació de la resposta del backend.
- global-policy-posthooks: postprocessat i capçaleres de seguretat.

Diagrama de components

Representació textual del flux d'execució de la política, des de la recepció de la petició fins a la decisió de continuar l'acoblament o rebutjar-la:

```
[Petició HTTP entrant]
v
[DataPower API Gateway . context.message]
v
[Política ctti-validate-ip v2.0.0]
|- obtenirIpOrigen() ----> header-metadata . llegeix N capçaleres
|- extraerIp() ----> normalitza format (Forwarded / llista / port / corxets)
|- esIPv4MappedIPv6() ----> transforma ::ffff:x.x.x.x -> x.x.x.x
|- validarIP() ----> compara contra ips-validas (exacte o CIDR)
|   |- ipv4EnCidr() / ipv4ToLong()
|   |- ipv6EnCidr() / ipv6ToArray() / parseGrupoIPv6()
|- throwPolicyError() ----> context.reject + context.message.statusCode
v
[Continua l'acoblament] o [catch -> ctti-error-management]
```

Components i mòduls del GatewayScript

El codi font de la política s'estructura en set seccions lògiques numerades. Cada secció té una responsabilitat única i pot ser auditada de forma independent, la qual cosa facilita el manteniment i l'execució dels tests funcionals.

Secció	Identificador en el codi	Responsabilitat
1	Configuració · IP_HEADERS	Defineix l'ordre de prioritat de les capçaleres d'IP que es lligiran.
2	Flux principal (IIFE)	Orquestra l'execució: obté la IP, normalitza, valida i

Finançat per



Unió Europea
Fons Europeu
Next Generation



GOBIERNO
DE ESPAÑA



Plan de
Recuperación,
Transformación
y Resiliencia



Next Generation
Catalunya



Generalitat
de Catalunya

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)	N. revisió doc.: 1.0
	Disseny detallat de la solució	
	N. versió aplicació: 2.0.0	Build: 001 Pàg. 5 / 11

Secció	Identificador en el codi	Responsabilitat
		decideix continuar o rebutjar.
3	obtenirIpOrigen / extraerIp / esIPv4MappedIPv6	Lectura i normalització de la IP d' origen.
4	validarIP	Comparació de la IP contra la llista permesa, amb suport d' IPs exactes i rangs CIDR.
5	ipv4EnCidr / ipv4ToLong	Aritmètica IPv4 (conversió a sencer sense signe i comparació amb màscara).
6	ipv6EnCidr / ipv6ToArray / parseGrupIpv6	Aritmètica IPv6 (expansió de ":" i comparació grup a grup).
7	throwPolicyError	Helper per a l'emissió d'errors controlats (context.reject + statusCode).

Estructura del fitxer YAML de la política

El fitxer ctti-validate-ip-2.0.0.yaml conté la definició completa de la política llista per ser desplegada en un catàleg d'API Connect mitjançant apic policies:publish. Els blocs principals són:

Bloc YAML	Contingut
policy	Versió del schema de política (1.0.0).
info	title, name (ctti-validate-ip), version (2.0.0), descripció corporativa.
attach	rest, soap. La política aplica a APIs REST i SOAP.
gateways	datapower-api-gateway. La política només funciona en el gateway de DataPower v10.
assembly.execute	Conté un únic element gatewayscript v2.0.0 amb el codi font de la política encastat com a bloc literal indentat correctament.

2.1.2 Escenaris i algorismes

Flux nominal (IP)

- La política s'invoca des de l'acoblament de l'API.
- S'itera sobre l'arrelament IP_HEADERS en ordre i s'invoca header-metadata.original.get() per capçalera. La primera capçalera amb un valor no nul s'envia a extraerIp() per a la seva normalització.
- Si la IP resultant és IPv4-mapped IPv6 (::ffff:x.x.x.x), es transforma en la seva forma IPv4 equivalent.
- Es llegeix la propietat api.properties.ips-validas i es valida que sigui una cadena no buida.
- S'invoca la llista d'entrades permeses i intenta matisar la IP rebuda contra cadascuna, ja sigui per igualtat exacta o per inclusió en un rang CIDR.
- Si la validació té èxit, la política finalitza sense efecte i l'acoblament continua amb la següent política.

Flux d'error: cap capçalera d'IP

- Si cap de les capçaleres de IP_HEADERS retorna un valor, obtenirIpOrigen() retorna null.
- La política invoca throwPolicyError amb errorCode E0400 i statusCode "400 Bad Request".
- L'execució de l'script s'apèn i el catch de l'API recull l'error per generar la resposta amb ctti-error-management.

Flux d'error: IP no autoritzada

- La IP s'ha pogut determinar però cap entrada de la llista permesa la conté.
- throwPolicyError amb errorCode E0401 i statusCode "401 Unauthorized".

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 6 / 11

- No queda rastre de la IP rebutjada en logs propis: el control d'auditoria recau sobre Analytics i la política de log.

Flux d'error: propietat no informada

- Si la propietat ips-validas no està definida o no és una cadena, es considera un error de configuració.
- throwPolicyError amb errorCode E0500 i statusCode "500 Internal Server Error".

Algorisme de comparació IPv4 amb CIDR

La política implementa la comparació per màscara binària. La IP origen i la direcció de xarxa es transformen en enters de 32 bits sense signe mitjançant la funció ipv4ToLong, que rebutja octets fora de rang i cadenes mal formades (per exemple "999.999.999.999" o "1.2.3"). La màscara es calcula a partir del prefix mitjançant l'operació $((2^{\text{prefix}} - 1) * 2^{(32 - \text{prefix})})$, evitant l'ús de desplaçaments bit a bit que en JavaScript treballen amb sencers amb signe i causarien resultats incorrectes per a prefixos grans. Comparació final: $(\text{ipLong AND mask}) === (\text{netLong AND mask})$.

Algorisme de comparació IPv6 amb CIDR

La IP IPv6 i la xarxa es transformen en arrays de 8 enters de 16 bits mitjançant ipv6ToArray, que gestiona correctament la sintaxi "::" (compressió de zeros). El recorregut compara grup a grup: mentre el comptador de bits restants és superior o igual a 16, els dos grups complets han de ser idèntics; quan el comptador queda entre 1 i 15 bits, s'aplica una màscara parcial al grup corresponent.

Algorisme de normalització d'adreces IPv4-mapped IPv6

Una adreça IPv4-mapped IPv6 té el format ::ffff:x.x.x.x i representa una adreça IPv4 vista des d'una infraestructura dual-stack. La política detecta aquest cas amb una expressió regular i extreu la part IPv4 (x.x.x.x), de manera que la validació es realitza contra les regles IPv4 definides per l'usuari, sense necessitat de duplicar les entrades en format IPv6.

2.1.3 Altres vistes i informació addicional

Integracions i dependències — Mòduls DataPower utilitzats

Mòdul	Mètode utilitzat	Finalitat
header-metadata	original.get(name)	Lectura case-insensitive de capçaleres HTTP de la petició entrant.
context (global)	get(key)	Lectura de propietats d'API (api.properties.ips-validas).
context.reject	reject(errorName, errorMessage)	Emissió d' error controlat que serà capturat pel catch de l' API.
context.message	statusCode (set)	Assignació del statusCode HTTP que es retornarà al client.

Propietats consumides

Nom de la propietat	ips-validas
Tipus	string
Obligatorietat	Obligatòria
Descripció	Llista d' adreces IP o rangs CIDR permesos, separats per comes. Accepta IPv4, IPv6, IPv4 CIDR (10.0.0.0/24), IPv6 CIDR (2001:db8::/32) i mesclades. Els espais al voltant de les comes s'ignoren.
Exemples vàlids	"10.0.0.1, 10.0.0.2" · "10.0.0.0/24" · "2001:db8::/32, 192.168.1.5" · "::1, 127.0.0.1"
Origen	api.properties.ips-validas en la definició del swagger / OpenAPI de l'API consumidora.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 7 / 11

Dependències amb altres polítiques CTTI

La política depèn directament de la presència de ctti-error-management en el catch de l' API consumidora per a la generació de la resposta d' error final:

Política dependent	Tipus de dependència	Notes
ctti-error-management	Fort (contracte d'error controlat)	Captura els errors emesos amb context.reject i genera la resposta JSON / XML / SOAP segons FormatoRespuesta.
global-policy-prehooks	Dèbil (no requerida, però recomanada)	Genera el Traceld que apareix als logs si la política rebutja.
ctti-invoke-log	Cap	No hi ha interacció directa.

Gestió d'errors — Taula d'errors controlats

La política emet exclusivament errors controlats mitjançant la convenció CTTI (tipoError = "controlled", errorCode, moreInformation), de manera que ctti-error-management pugui resoldre el missatge final basant-se en el codi.

errorCode	HTTP	statusCode	moreInformation	Condicció
E0400	400	400 Bad Request	No se ha encontrado informada ninguna cabecera de IP de cliente.	Cap de les 8 capçaleres prioritàries retorna valor.
E0401	401	401 Unauthorized	IP no válida.	La IP determinada no es troba en cap entrada d' ips-validas.
E0500	500	500 Internal Server Error	La propiedad "ips-validas" no está definida o tiene un tipo inválido.	Error de configuració de l' API consumidora.

Integració amb ctti-error-management

L'error s'eleva amb la sintaxi: context.reject("JavaScriptError", JSON.stringify(payload)). El payload és sempre un objecte amb tres claus: tipoError ("controlled"), errorCode i moreInformation. Immediatament després s'assigna context.message.statusCode amb el format requerit per DataPower ("400 Bad Request", no només 400).

És crític que cada invocació de throwPolicyError vagi seguida d'un return explícit en la funció principal, ja que context.reject no até per si mateix l' execució de l' script.

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 8 / 11

ANNEXOS

Annex A — Seguretat i controls

La política implementa el patró clàssic de whitelist d'IP origen. Els controls de seguretat que aporta i les seves limitacions són els següents:

Controls aportats

- Filtrat precoç dins de l'acoblament: les peticions d'IPs no autoritzades es rebutgen abans de qualsevol invocació al backend, reduint la superfície d'atac.
- Suport de llista positiva (whitelist): la política rebutja per defecte; només autoritza les entrades explícitament declarades.
- Suport de rangs CIDR: permet declarar subredes completes sense haver d'enumerar IPs una a una, evitant errors humans a mantenir llistes llargues.
- Normalització d'IPv4-mapped IPv6: evita que un atacant pugui burlar el filtre simplement codificant la IPv4 en format dual-stack.
- Validació estricta d'octets IPv4: cadenes mal formades són rebutjades, eliminant la possibilitat d'IPs ambigües que matxin per accident.

Limitacions conegudes

- La política llegeix la IP de capçaleres HTTP enviades pel client. En entorns sense proxy de confiança, un client malintencionat podria suplantar capçaleres com X-Forwarded-For. La política assumeix que el gateway opera darrere d'un balancejador o proxy que normalitza aquestes capçaleres.
- La política no implementa rate-limiting ni detecció d'anomalies. Aquests controls s'han d'aportar per altres polítiques (rate-limit, security-policy).
- No es genera log explícit de les IPs rebutjades. L'auditoria de seguretat es delega a Analytics i a la política de logging.
- Les adreces IPv4-mapped IPv6 amb port (format ::ffff:x.x.x.x:port) no es normalitzen completament; aquesta combinació és rara i no s'ha trobat en l'ecosistema CTTI actual.

Annex B — Consideracions de rendiment

La política s'executa íntegrament en memòria, sense invocacions externes ni accés a disc. El cost computacional per petició és $O(N \times M)$, on N és el nombre de capçaleres d'IP rebudes (màxim 8) i M és el nombre d'entrades a la llista ips-validas. Per a una configuració típica (1-2 capçaleres rebudes, 5-10 entrades a la llista), el temps d'execució és inferior a 1 ms al maquinari de DataPower estàndard.

Recomanacions de configuració

- Mantenir la propietat ips-validas amb un nombre raonable d'entrades (recomanat < 50). Per a llistes molt grans, considerar agrupar amb rangs CIDR.
- Preferir rangs CIDR a llistes d'IPs individuals sempre que la topologia ho permeti.
- No utilitzar la política en posicions tardanes de l'acoblament (per exemple després d'una invocació al backend), ja que perd part del seu valor defensiu.
- A APIs amb molt volum (>1000 RPS), validar amb tests de càrrega que la configuració concreta no introdueix latència significativa.

Annex C — Versionat i compatibilitat

Versions de DataPower suportades

Versió DataPower	Estat de compatibilitat	Notes
10.6.0.6	Compatible (versió actual de CTTI)	Validada amb la col·lecció Postman de tests funcionals desplegada al toolkit local.

Finançat per



GOBIERNO
DE ESPAÑA



Plan de
Recuperación,
Transformación
y Resiliencia



Next Generation
Catalunya



Generalitat
de Catalunya

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 9 / 11

Versió DataPower	Estat de compatibilitat	Notes
10.6.0.9	Compatible (versió prevista post-upgrade)	GatewayScript v2.0 estable entre fix packs. Re-execució de la col·lecció Postman recomanada després de l'upgrade.
10.5.x	No suportada	Carència de funcionalitats del motor V8 utilitzades per la política.
v5 (legacy)	No suportada	Arquitectura completament diferent.

Política de versionat semàntic

La política segueix el versionat semàntic MAJOR. MINOR. PATCH:

- **MAJOR:** canvis incompatibles en el contracte (per exemple, format diferent de la propietat ips-validas).
- **MINOR:** noves funcionalitats que mantenen retrocompatibilitat (per exemple, suport de noves capçaleres).
- **PATCH:** correccions de bugs sense alteració del contracte.

Migració des de la versió 1.0.0

La versió 2.0.0 manté íntegrament el contracte de la 1.0.0 quant a la propietat consumida: ips-validas continua sent una cadena CSV. No és necessari cap canvi en el swagger de les APIs consumidores per actualitzar la referència de la política.

Canvis de comportament a tenir en compte:

Aspecte	Versió 1.0.0	Versió 2.0.0
Capçaleres lligides	Només X-Client-IP	8 capçaleres en ordre de prioritat
Rangs CIDR	No suportats	Suportats per a IPv4 i IPv6
IPv6	No suportat	Suportat (exacte i CIDR)
IPv4-mapped IPv6	No suportat (rebutja)	Normalitzat com a IPv4
Sense capçalera d' IP	errorCode E0500 (500)	errorCode E0400 (400 Bad Request)
statusCode emès	Numèric (incorrecte per a DataPower)	Cadena amb format "401 Unauthorized" (correcte)

L'únic canvi potencialment incompatible és el codi d'error quan falta la capçalera (E0500 → E0400). Els consumidors que capturaven exclusivament HTTP 500 com a "falta capçalera" han de ser actualitzats per capturar també HTTP 400.

Annex D — Traçabilitat amb codi, tests i Postman

Mapeig codi font – requisits tècnics

Logotip tècnic	Funció / Bloc en el codi	Test funcional Postman	Test Postman
Lectura multi-capçalera	IP_HEADERS obtenirIpOrigen()	Grup 6 (6 casos)	D07, D08, D09, E01, E02, E03
Normalització Forwarded RFC 7239	extraerIp() – regex for=	Grup 6, cas "Forwarded ..."	D03, D04
IPv4-mapped IPv6	esIPv4MappedIPv6() replace	Grup 5 (3 casos), Grup 9	B01, B02, B03
Validació CIDR IPv4	ipv4EnCidr() + ipv4ToLong()	Grup 2 (6 casos), Grup 3	A01, C01, C02, C03
Validació CIDR IPv6	ipv6EnCidr() + ipv6ToArray()	Grup 4 (6 casos)	A04, A05, C04, C05, C06
Trim de la llista	split + replace en validarIP	Grup 1, cas "espais"	cobert per A01

Finançat per



GOBIERNO
DE ESPAÑA



Plan de
Recuperación,
Transformación
y Resiliencia



Next Generation
Catalunya



Generalitat
de Catalunya

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 10 / 11

Logotip tècnic	Funció / Bloc en el codi	Test funcional Postman	Test Postman
Return tras reject	flux principal	Grup 9, cas "no sobreescritura"	cobert per A03
statusCode com a string	throwPolicyError	Grup 9, cas "statusCode string"	cobert per A02
errorCode E0400 si falta capçalera	flux principal	Grup 8, cas "cap capçalera"	A03
Extracció IPv4 amb port	extraerIp()	Grup 7, cas "port"	D06
Extracció IPv6 amb corxets i port	extraerIp()	Grup 7	D05
Validació d' octets IPv4	ipv4ToLong()	Grup 3 (2 casos)	F01, F02, F03, F04
IPs/capçaleres buides o escombraries	flux principal / obtenirIpOrigen	Grup 8	F05, F06, F07, F08

Col·lecció Postman de tests funcionals

La col·lecció Postman (ctti-validate-ip 2.0.0 - Tests funcionals) conté 35 escenaris funcionals agrupats en 7 carpetes temàtiques (A a G) i s'executa contra una API de prova real (api-test-validate-ip, GET /ping) desplegada en el toolkit local de DataPower o en l'entorn d'integració. No s'utilitzen shims ni simulacions de mòduls: els tests validen el comportament real de la política sobre el motor GatewayScript. El resultat esperat és 35/35 tests passats. L'execució es pot llançar des de la interfície de Postman o mitjançant Newman parametritzant la URL base i les IPs de prova.

Grup	Descripció	Nº casos
A	Tests funcionals bàsics (IPv4/IPv6 OK/KO)	5
B	IPv4-mapped IPv6 (::ffff:x.x.x.x)	3
C	Límits de CIDR (bordes exactes IPv4 i IPv6)	6
D	Extracció i parseu de capçaleres (formats, multi-capçalera)	9
E	Prioritat de capçaleres (IP_HEADERS)	3
F	IPs malformades i casos límit	8
G	Match exacte (sense CIDR)	1

Annex E — Configuració d'API consumidora i cabeceres suportades

Configuració d'API consumidora (exemple)

Perquè una API consumeixi la nova versió de la política, n'hi ha prou amb afegir el bloc següent al seu swagger:

```
x-ibm-configuration:
  properties:
    ips-validas:
      value: "10.0.0.0/24, 2001:db8::/32, 192.168.1.5"
      encoded: false
  assembly:
    execute:
      - ctti-validate-ip:
          version: 2.0.0
          title: ctti-validate-ip
      # ... resta de polítiques de l'API ...
```

Cabeceres d'IP suportades amb ordre de prioritats

Prioritat	Capçalera	Origen típic	Format esperat
-----------	-----------	--------------	----------------

Finançat per



Unió Europea
Fons Europeu
Next Generation



GOBIERNO
DE ESPAÑA



Plan de
Recuperación,
Transformación
y Resiliencia



Next Generation
Catalunya



Generalitat
de Catalunya

 Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació	ctti-validate-ip (Política de validació d'IP)		N. revisió doc.: 1.0
	Disseny detallat de la solució		
	N. versió aplicació: 2.0.0	Build: 001	Pàg. 11 / 11

Prioritat	Capçalera	Origen típic	Format esperat
1	Forwarded	Proxies RFC 7239	for ="192.0.2.43"; proto =https
2	X-Forwarded-For	Proxies HTTP de facto	192.0.2.43, 10.0.0.1, 172.16.0.1
3	CF-Connecting-IP	Cloudflare	192.0.2.43
4	True-Client-IP	Akamai / Cloudflare Enterprise	192.0.2.43
5	X-Real-IP	Nginx	192.0.2.43
6	X-Client-IP	Apache / legacy CTTI	192.0.2.43
7	X-Cluster-Client-IP	Balancejadors	192.0.2.43
8	X-Originating-IP	Altres proxies	192.0.2.43

Annex F — Parametrització i rols

No aplica a aquesta política: ctti-validate-ip és un component de gateway que no defineix transaccions, rols ni taules de parametrització pròpies. Es deixa indicat com a pendent / no aplicable.

Transaccions	Descripció
(No aplica)	(No aplica)

Rols	Descripció
(No aplica)	(No aplica)

Taules de parametrització	Descripció
(No aplica)	(No aplica)