



Guida per l'utente

# Amazon Inspector Classic



Version Latest

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Inspector Classic: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

---

# Table of Contents

.....	viii
Cos'è Amazon Inspector Classic? .....	1
Vantaggi di Amazon Inspector Classic .....	2
Caratteristiche di Amazon Inspector Classic .....	2
Accesso ad Amazon Inspector Classic .....	3
Concetti e terminologia .....	4
Limiti del servizio .....	6
Prezzi .....	7
Prezzi per il pacchetto di regole di raggiungibilità della rete .....	7
Prezzi dei pacchetti di regole di valutazione degli host .....	8
Sistemi operativi e regioni supportati .....	9
Sistemi operativi basati su Linux supportati per l'agente Amazon Inspector Classic .....	10
Sistemi operativi basati su Windows supportati per l'agente Amazon Inspector Classic .....	10
Regioni AWS supportate .....	11
Fine del supporto per Amazon Inspector Classic .....	12
Fase 1: (Facoltativo) Esportazione dei report e dei risultati della valutazione .....	13
Fase 2: Eliminare tutte le esecuzioni di valutazione pianificate in Amazon Inspector Classic .....	14
Fase 3: abilitare il nuovo Amazon Inspector .....	14
Nozioni di base .....	15
Impostazione One-Click .....	15
Configurazione avanzata .....	16
Esercitazioni .....	18
Tutorial su Amazon Inspector Classic - Red Hat Enterprise Linux .....	18
Fase 1: configurare un'istanza Amazon EC2 da utilizzare con Amazon Inspector Classic .....	19
Fase 2: modifica la tua istanza Amazon EC2 .....	19
Fase 3: Creazione di un target di valutazione e installazione di un agente su un'istanza EC2 .....	19
Fase 4: Creazione ed esecuzione di un modello di valutazione .....	21
Fase 5: Individuazione e analisi dei risultati .....	21
Fase 6: Applicazione della correzione consigliata al target di valutazione .....	23
Tutorial di Amazon Inspector Classic - Ubuntu Server .....	23
Fase 1: configurare un'istanza Amazon EC2 da utilizzare con Amazon Inspector Classic .....	24
Passaggio 2: crea un obiettivo di valutazione e installa un agente sull'istanza EC2 .....	24
Passaggio 3: crea ed esegui il modello di valutazione .....	25

Fase 4: Individua e analizza i risultati generati .....	26
Fase 5: applica la correzione consigliata al tuo obiettivo di valutazione .....	27
Sicurezza .....	28
Protezione dei dati .....	29
Crittografia dei dati a riposo .....	30
Crittografia dei dati in transito .....	30
Identity and Access Management .....	31
Destinatari .....	31
Autenticazione con identità .....	32
Gestione dell'accesso tramite policy .....	33
Come funziona Amazon Inspector Classic con IAM .....	35
Esempio 2: consentire a un utente di eseguire operazioni di descrizione ed elenco solo sui risultati di Amazon Inspector .....	38
Risorse relative alle policy .....	39
Chiavi di condizione delle policy .....	39
ACLs .....	40
ABAC .....	40
Credenziali temporanee .....	41
Autorizzazioni dell'entità principale .....	41
Ruoli di servizio .....	41
Ruoli collegati ai servizi .....	41
Esempi di policy basate su identità .....	42
Uso di ruoli collegati ai servizi .....	45
Risoluzione dei problemi .....	48
Registrazione di log e monitoraggio .....	50
Risposta agli incidenti .....	50
Convalida della conformità .....	50
Resilienza .....	51
Sicurezza dell'infrastruttura .....	52
Analisi della configurazione e delle vulnerabilità .....	52
Best practice di sicurezza .....	53
Agenti di Amazon Inspector Classic .....	54
Privilegi di agente Amazon Inspector Classic .....	55
Sicurezza della rete e degli agenti Amazon Inspector Classic .....	55
Aggiornamenti degli agenti Amazon Inspector Classic .....	56
Ciclo di vita dei dati telemetrici .....	56

Controllo degli accessi da Amazon Inspector Classic agli account AWS .....	57
Limiti per gli agenti di Amazon Inspector Classic .....	57
Installazione degli agenti Amazon Inspector Classic .....	57
Installazione dell'agente su più istanze EC2 usando Systems Manager Run Command .....	58
Installazione dell'agente su un'istanza EC2 basata su Linux .....	59
Installazione dell'agente su un'istanza EC2 basata su Windows .....	61
Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Linux .....	62
Verifica dell'esecuzione dell'agente Amazon Inspector Classic .....	63
Interruzione dell'agente Amazon Inspector Classic .....	63
Avvio dell'agente Amazon Inspector Classic .....	63
Modifica delle impostazioni degli agenti Amazon Inspector Classic .....	63
Configurazione del supporto proxy per un agente Amazon Inspector Classic .....	64
Disinstallazione dell'agente Amazon Inspector Classic .....	65
Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Windows .....	66
Avvio o arresto di un agente Amazon Inspector Classic o verifica che l'agente sia in esecuzione .....	67
Modifica delle impostazioni dell'agente Amazon Inspector Classic .....	67
Configurazione del supporto proxy per un agente Amazon Inspector Classic .....	68
Disinstallazione dell'agente Amazon Inspector Classic .....	69
(Facoltativo) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Linux .....	69
Installazione degli strumenti GPG .....	70
Autenticazione e importazione della chiave pubblica .....	71
Verifica della firma del pacchetto .....	73
(Facoltativo) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Windows .....	74
Obiettivi di valutazione di Amazon Inspector Classic .....	76
Tagging delle risorse per la creazione di un target di valutazione .....	76
Limiti degli obiettivi di valutazione di Amazon Inspector Classic .....	77
Creazione di un target di valutazione .....	77
Eliminazione di un target di valutazione .....	79
Regole, pacchetti e regole di Amazon Inspector Classic .....	80
Livelli di severità per le regole in Amazon Inspector Classic .....	80
Pacchetti di regole in Amazon Inspector Classic .....	81
Network Reachability .....	81
Configurazioni analizzate .....	82

Route di raggiungibilità .....	83
Tipi di risultati .....	83
Common vulnerabilities & exposures (CVE) .....	86
Center for Internet Security (CIS) Benchmarks .....	87
Best practice di sicurezza per Amazon Inspector Classic .....	90
Disabilita l'accesso root tramite SSH .....	91
Supporta solo SSH versione 2 .....	92
Disabilita autenticazione password tramite SSH .....	92
Configura età massima della password .....	93
Configura lunghezza minima della password .....	93
Configura complessità della password .....	94
Enable ASLR .....	95
Enable DEP .....	95
Configura le autorizzazioni per le directory del sistema .....	96
Modelli di valutazione ed esecuzioni di valutazione di Amazon Inspector Classic .....	97
Modelli di valutazione Amazon Inspector Classic .....	97
Limiti dei modelli di valutazione Amazon Inspector Classic .....	98
Creazione di un modello di valutazione .....	98
Eliminazione di un modello di valutazione .....	100
Esecuzioni di valutazioni .....	101
Eliminazione di un'esecuzione di valutazioni .....	101
Limiti dei cicli di valutazione di Amazon Inspector Classic .....	102
L'impostazione della valutazione automatica avviene tramite una funzione Lambda .....	102
Configurazione di un argomento SNS per le notifiche di Amazon Inspector Classic .....	104
Risultati di Amazon Inspector Classic .....	107
Uso dei risultati .....	107
Rapporti di valutazione .....	110
Esclusioni in Amazon Inspector Classic .....	112
Tipi di esclusione .....	112
Anteprima delle esclusioni .....	125
Visualizzazione delle esclusioni post-valutazione .....	126
Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati .....	127
Registrazione delle chiamate API Amazon Inspector Classic con AWS CloudTrail .....	132
Informazioni su Amazon Inspector Classic in CloudTrail .....	132
Informazioni sulle voci dei file di log di Amazon Inspector Classic .....	133
Monitoraggio di Amazon Inspector Classic tramite Amazon CloudWatch .....	136

Metriche di Amazon Inspector Classic CloudWatch .....	136
Configurazione di Amazon Inspector Classic tramite AWS CloudFormation .....	138
Integrazioni CSPM di Security Hub .....	139
In che modo Amazon Inspector invia i risultati al Security Hub CSPM .....	139
Tipi di risultati inviati da Amazon Inspector .....	140
Latenza per l'invio degli esiti .....	140
Riprovare quando Security Hub CSPM non è disponibile .....	140
Aggiornamento degli esiti esistenti CSPM Security Hub .....	140
Risultati tipici di Amazon Inspector .....	141
Abilitazione e configurazione dell'integrazione .....	143
Come interrompere l'invio degli esiti .....	143
Amazon Inspector Classic ARNs .....	144
ARNs per le risorse di Amazon Inspector Classic .....	144
Amazon Inspector Classic ARNS per pacchetti di regole .....	145
Stati Uniti orientali (Ohio) .....	146
Stati Uniti orientali (Virginia settentrionale) .....	146
Stati Uniti occidentali (California settentrionale) .....	147
Stati Uniti occidentali (Oregon) .....	148
Asia Pacifico (Mumbai) .....	149
Asia Pacifico (Seul) .....	149
Asia Pacifico (Sydney) .....	150
Asia Pacifico (Tokyo) .....	151
Europa (Francoforte) .....	151
Europa (Irlanda) .....	152
Europa (Londra) .....	153
Europa (Stoccolma) .....	154
AWS GovCloud (Stati Uniti orientali) .....	154
AWS GovCloud (Stati Uniti occidentali) .....	155
Cronologia dei documenti .....	156
AWS Glossario .....	163

Avviso di fine del supporto: il 20 maggio 2026, AWS terminerà il supporto per Amazon Inspector Classic. Dopo il 20 maggio 2026, non potrai più accedere alla console Amazon Inspector Classic o alle risorse di Amazon Inspector Classic. Amazon Inspector Classic non è più disponibile per i nuovi account e per gli account che non hanno completato una valutazione negli ultimi 6 mesi. Per tutti gli altri account, l'accesso rimarrà valido fino al 20 maggio 2026, dopodiché non potrai più accedere alla console Amazon Inspector Classic o alle risorse Amazon Inspector Classic. Per ulteriori informazioni, consulta la [fine del supporto di Amazon Inspector Classic](#).

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.

# Cos'è Amazon Inspector Classic?

## Note

Il nuovo Amazon Inspector, una versione completamente riprogettata e riprogettata di Amazon Inspector Classic, è ora disponibile ovunque. Regioni AWS Il nuovo Amazon Inspector ha ampliato la copertura per aggiungere il supporto per le immagini dei container che risiedono in Amazon Elastic Container Registry (Amazon ECR) oltre alle istanze. EC2 Il nuovo Amazon Inspector offre supporto multi-account attraverso l'integrazione e la scansione continua delle vulnerabilità del software e della raggiungibilità della rete in base a vulnerabilità ed esposizioni comuni (). AWS Organizations CVEs Ti invitiamo a esplorare e utilizzare queste e altre funzionalità nuove e migliorate e a trarre vantaggio dal valore della sicurezza notevolmente migliorato. Per informazioni sulle caratteristiche e sui prezzi del nuovo Amazon Inspector, consulta [Amazon Inspector](#). Per informazioni su come passare al nuovo Amazon Inspector, consulta. [Fine del supporto per Amazon Inspector Classic](#)

Amazon Inspector Classic verifica l'accessibilità di rete EC2 delle istanze Amazon e lo stato di sicurezza delle applicazioni eseguite su tali istanze. Amazon Inspector Classic valuta le applicazioni in base all'esposizione, alle vulnerabilità e alle deviazioni dalle best practice. Dopo aver eseguito una valutazione, Amazon Inspector Classic produce un elenco dettagliato dei risultati di sicurezza organizzato per livello di gravità.

Con Amazon Inspector Classic, puoi automatizzare le valutazioni delle vulnerabilità di sicurezza in tutte le tue pipeline di sviluppo e distribuzione o per i sistemi di produzione statici. In questo modo, il test di sicurezza diventa parte integrante delle operazioni IT e di sviluppo.

Amazon Inspector Classic offre anche un software predefinito chiamato agente che puoi installare facoltativamente nel sistema operativo delle EC2 istanze che desideri valutare. L'agente monitora il comportamento delle EC2 istanze, inclusa l'attività di rete, del file system e dei processi. Raccoglie anche un ampio set di dati di comportamento e configurazione (telemetria).

## Important

AWS non garantisce che seguendo i consigli forniti si risolvano tutti i potenziali problemi di sicurezza. I risultati generati da Amazon Inspector Classic dipendono dalla scelta dei pacchetti di regole inclusi in ogni modello di valutazione, dalla presenza di componenti

non AWS componenti nel sistema e da altri fattori. Sei responsabile della sicurezza delle applicazioni, dei processi e degli strumenti eseguiti sui AWS servizi. Per ulteriori informazioni, consulta il [modello di responsabilitàAWS condivisa](#) per la sicurezza.

#### Note

AWS è responsabile della protezione dell'infrastruttura globale che gestisce i servizi offerti nel AWS Cloud. Questa infrastruttura è composta da hardware, software, rete e strutture che eseguono AWS i servizi. AWS fornisce diversi report di revisori di terze parti che hanno verificato la nostra conformità a una serie di standard e normative sulla sicurezza informatica. Per ulteriori informazioni, consulta [AWS Cloud Compliance](#).

Per informazioni sulla terminologia di Amazon Inspector Classic, consulta [Terminologia e concetti di Amazon Inspector Classic](#)

## Vantaggi di Amazon Inspector Classic

Ecco alcuni dei principali vantaggi di Amazon Inspector Classic:

- Integra i controlli di sicurezza automatizzati nei tuoi normali processi di distribuzione e produzione: valuta la sicurezza delle tue AWS risorse per scopi forensi, risoluzione dei problemi o audit attivi. Esegui le valutazioni durante il processo di sviluppo o in un ambiente di produzione stabile.
- Individua i problemi di sicurezza delle applicazioni: automatizza la valutazione della sicurezza delle tue applicazioni e identifica in modo proattivo le vulnerabilità. In questo modo puoi procedere allo sviluppo e ripetere le stesse operazioni sulle nuove applicazioni, verificando la conformità con best practice e policy.
- Acquisisci una comprensione più approfondita delle tue AWS risorse: tieniti informato sull'attività e sui dati di configurazione AWS delle tue risorse esaminando i risultati prodotti da Amazon Inspector Classic.

## Caratteristiche di Amazon Inspector Classic

Ecco alcune delle caratteristiche principali di Amazon Inspector Classic:

- **Motore di scansione della configurazione e monitoraggio delle attività:** Amazon Inspector Classic fornisce un agente che analizza la configurazione del sistema e delle risorse. Inoltre, monitora l'attività per determinare l'aspetto di un target di valutazione, il comportamento e le componenti dipendenti. La combinazione di questi dati telemetrici fornisce un quadro completo del target e dei relativi potenziali problemi di sicurezza o conformità.
- **Libreria di contenuti integrata:** Amazon Inspector Classic include una libreria integrata di regole e report. In questa libreria sono disponibili controlli basati su best practice, nonché standard e vulnerabilità comuni a livello di conformità. I controlli includono procedure raccomandate dettagliate per la risoluzione dei potenziali problemi di sicurezza.
- **Automazione tramite un'API:** Amazon Inspector Classic può essere completamente automatizzato tramite un'API. Ciò ti consente di integrare test di sicurezza nei processi di progettazione e sviluppo, tra cui la selezione, l'esecuzione e la segnalazione dei risultati di tali test.

## Accesso ad Amazon Inspector Classic

Puoi utilizzare il servizio Amazon Inspector Classic in uno dei seguenti modi:

### Console Amazon Inspector Classic

Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo.

<https://console.aws.amazon.com/inspector/>

La console è un'interfaccia basata su browser che consente di accedere e utilizzare il servizio Amazon Inspector Classic.

### AWS SDKs

AWS fornisce kit di sviluppo software (SDKs) costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione. Sono supportati i linguaggi Java, Python, Ruby, .NET, iOS, Android e altri. SDKs Forniscono un modo pratico per creare un accesso programmatico al servizio Amazon Inspector Classic. Per informazioni su AWS SDKs, incluso come scaricarli e installarli, consulta [Tools for Amazon Web Services](#).

### API HTTPS Amazon Inspector Classic

Puoi accedere ad Amazon Inspector Classic e in modo AWS programmatico utilizzando l'API HTTPS di Amazon Inspector Classic, che consente di inviare richieste HTTPS direttamente al servizio. Per ulteriori informazioni, consulta [Amazon Inspector Classic API Reference](#).

## AWS Strumenti da riga di comando

Puoi utilizzare gli strumenti della AWS riga di comando per eseguire comandi dalla riga di comando del tuo sistema per eseguire attività di Amazon Inspector Classic. Gli strumenti da riga di comando sono utili anche se desideri creare script che eseguano attività AWS . Per ulteriori informazioni, consulta l'interfaccia a [riga di AWS comando di Amazon Inspector Classic](#).

## Terminologia e concetti di Amazon Inspector Classic

Quando inizi a usare Amazon Inspector Classic, puoi trarre vantaggio dall'apprendimento dei suoi concetti chiave.

### Agente Amazon Inspector Classic

Un agente software che puoi installare sulle EC2 istanze incluse nell'obiettivo di valutazione. L'agente raccoglie anche un ampio set di dati di configurazione (telemetria). Per ulteriori informazioni, consulta [Agenti di Amazon Inspector Classic](#).

### Esecuzione di valutazioni

Processo che porta alla scoperta di potenziali problematiche di sicurezza attraverso l'analisi della configurazione del target di valutazione rispetto ai pacchetti di regole specificati. Durante un'esecuzione di valutazioni, Amazon Inspector monitora, raccoglie e analizza i dati di configurazione (telemetria) dalle risorse all'interno del target specificato. Quindi, Amazon Inspector analizza i dati e li confronta con un set di pacchetti di regole di sicurezza specificati nel modello di valutazione utilizzato durante l'esecuzione di valutazioni. Un'esecuzione di valutazioni completata genera un elenco di risultati, ovvero un elenco di potenziali problemi di sicurezza di vari livelli di gravità. Per ulteriori informazioni, consulta [Modelli di valutazione ed esecuzioni di valutazione di Amazon Inspector Classic](#).

### Target di valutazione

Nel contesto di Amazon Inspector Classic, una raccolta di risorse AWS che interagiscono come un'unica unità per aiutarti a raggiungere i tuoi obiettivi aziendali. Amazon Inspector Classic valuta lo stato di sicurezza delle risorse che costituiscono l'obiettivo di valutazione.

**⚠ Important**

Attualmente, gli obiettivi di valutazione di Amazon Inspector Classic possono essere costituiti solo da istanze EC2. Per ulteriori informazioni, consulta [Limiti del servizio Amazon Inspector Classic](#)

Per creare un obiettivo di valutazione di Amazon Inspector Classic, devi prima etichettare EC2 le istanze con coppie chiave-valore di tua scelta. Successivamente, puoi creare una visualizzazione di queste EC2 istanze con tag che hanno chiavi o valori comuni. Per ulteriori informazioni, consulta [Obiettivi di valutazione di Amazon Inspector Classic](#).

### Modello di valutazione

Una configurazione utilizzata durante un'esecuzione di valutazioni. Il modello include quanto segue:

- Pacchetti di regole utilizzati da Amazon Inspector Classic per valutare l'obiettivo di valutazione
- Argomenti di Amazon SNS a cui desideri che Amazon Inspector Classic invii notifiche sugli stati e i risultati delle esecuzioni di valutazione
- I tag (coppie chiave-valore) che è possibile assegnare ai risultati generati dall'esecuzione di valutazioni
- La durata dell'esecuzione di valutazioni

### Risultato

Un potenziale problema di sicurezza che Amazon Inspector Classic rileva durante un'esecuzione di valutazione dell'obiettivo specificato. I risultati vengono visualizzati nella console Amazon Inspector Classic o recuperati tramite l'API. Contengono una descrizione dettagliata del problema di sicurezza e un consiglio su come risolverlo. Per ulteriori informazioni, consulta [Risultati di Amazon Inspector Classic](#).

### Regola

Nel contesto di Amazon Inspector Classic, un controllo di sicurezza eseguito durante un'esecuzione di valutazione. Quando una regola rileva un potenziale problema di sicurezza, Amazon Inspector Classic genera un risultato che descrive il problema.

### Pacchetto di regole

Nel contesto di Amazon Inspector Classic, una raccolta di regole. Un pacchetto di regole corrisponde a un obiettivo di sicurezza associato all'utente corrente. Puoi specificare il tuo

obiettivo di sicurezza selezionando il pacchetto di regole appropriato quando crei un modello di valutazione Amazon Inspector Classic. Per ulteriori informazioni, consulta [Regole, pacchetti e regole di Amazon Inspector Classic](#).

## Telemetria

Informazioni sul pacchetto installato e configurazione del software per un' EC2 istanza. Amazon Inspector Classic raccoglie i dati durante un'esecuzione di valutazione.

## Limiti del servizio Amazon Inspector Classic

La tabella seguente mostra i limiti di Amazon Inspector Classic per un account AWS.

### Important

Attualmente, gli obiettivi di valutazione possono consistere solo in EC2 istanze.

Di seguito sono riportati i limiti di Amazon Inspector Classic per account AWS per regione:

Risorsa	Limite predefinito	Commenti
Istanze nelle valutazioni in esecuzione	500	Il numero massimo di EC2 istanze che possono essere incluse in tutte le valutazioni in esecuzione per account per regione.
Esecuzioni di valutazioni	50000	Numero massimo di esecuzioni di valutazioni che puoi creare per account per regione. È possibile eseguire più esecuzioni di valutazione

Risorsa	Limite predefinito	Commenti
		contemporaneamente , purché gli obiettivi di valutazione utilizzati per queste esecuzioni non contengano o istanze EC2 sovrapposte.
Modelli di valutazione	500	Numero massimo di modelli di valutazione che è possibile avere in un dato momento per account per regione.
Target di valutazione	50	Numero massimo di target di valutazione che è possibile avere in un dato momento per account per regione.

[Salvo diversa indicazione, questi limiti possono essere aumentati su richiesta contattando il Centro.Supporto AWS](#)

## Prezzi di Amazon Inspector Classic

I prezzi di Amazon Inspector Classic si basano sul numero di EC2 istanze incluse in ciascuna valutazione e sui pacchetti di regole utilizzati in tali valutazioni.

### Prezzi per il pacchetto di regole di raggiungibilità della rete

Le valutazioni di Amazon Inspector Classic con i pacchetti di regole di raggiungibilità della rete hanno un prezzo mensile per istanza per valutazione (valutazione dell'istanza). Ad esempio, se esegui 1 valutazione su 1 istanza, si tratta di una valutazione di 1 istanza. Se si esegue 1 valutazione su 10

istanze, si tratta di 10 valutazioni di istanza. Il prezzo parte da 0,15 USD per valutazione dell'istanza al mese, con sconti sui volumi fino a raggiungere un minimo di 0,04 USD per valutazione dell'istanza al mese.

## Dettagli della prova gratuita

Primi 90 giorni con Amazon Inspector Classic	Prezzo di valutazione per istanza
Prime 250 valutazioni di istanza	\$0,00

## Dettagli prezzi

In un determinato mese	Prezzo di valutazione per istanza
Prime 250 valutazioni di istanza	0,15\$
Prossime 750 valutazioni dell'istanza	\$0,13
Prossime 4.000 valutazioni dell'istanza	0,10 \$
Prossime 45.000 valutazioni delle istanze	0,07\$
Tutte le altre valutazioni delle istanze	0,04\$

## Prezzi dei pacchetti di regole di valutazione degli host

Per qualsiasi combinazione di Common Vulnerabilities and Exposures (CVE), benchmark Center for Internet Security (CIS), best practice di sicurezza e analisi del comportamento in fase di esecuzione incluse nelle valutazioni

I pacchetti di regole di valutazione degli host di Amazon Inspector Classic utilizzano un agente distribuito sulle EC2 istanze Amazon che esegue le applicazioni che desideri valutare. Le valutazioni con i pacchetti di regole host hanno un prezzo mensile per agente per valutazione (agent-assessment). Ad esempio, se si esegue 1 valutazione contro 1 agente, si tratta di 1 valutazione agente. Se si esegue 1 valutazione contro 10 agenti, si tratta di 10 valutazioni tra agenti. Il prezzo parte da 0,30 USD per agente di valutazione al mese, con sconti sui volumi fino a raggiungere un minimo di 0,05 USD per agente di valutazione al mese.

## Dettagli della prova gratuita

Primi 90 giorni con Amazon Inspector Classic	Prezzo di valutazione per agente
Prime 250 valutazioni effettuate da un agente	\$0,00

## Dettagli prezzi

In un determinato mese	Prezzo di valutazione per agente
Prime 250 valutazioni effettuate da un agente	0,30\$
Prossime 750 valutazioni degli agenti	0,25\$
Prossime 4.000 valutazioni degli agenti	0,15\$
Prossime 45.000 valutazioni degli agenti	0,10 \$
Tutte le altre valutazioni degli agenti	0,05 \$

## Regioni e sistemi operativi supportati da Amazon Inspector Classic

Questo capitolo fornisce informazioni sui sistemi operativi e sulle regioni AWS supportati da Amazon Inspector Classic.

### Important

Attualmente, gli obiettivi di valutazione di Amazon Inspector Classic possono essere costituiti solo da istanze EC2. Puoi eseguire una valutazione senza agenti con il pacchetto di regole di [raggiungibilità della rete](#) su qualsiasi istanza EC2 indipendentemente dal sistema operativo.

Per informazioni sui pacchetti di regole di Amazon Inspector Classic disponibili nei sistemi operativi supportati, consulta. [Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati](#)

### Argomenti

- [Sistemi operativi basati su Linux supportati per l'agente Amazon Inspector Classic](#)

- [Sistemi operativi basati su Windows supportati per l'agente Amazon Inspector Classic](#)
- [Regioni AWS supportate](#)

## Sistemi operativi basati su Linux supportati per l'agente Amazon Inspector Classic

Puoi utilizzare l'agente Amazon Inspector Classic su istanze x86 a 64 bit e [Arm](#) EC2. L'agente è compatibile con le seguenti versioni dei sistemi operativi basati su Linux:

- istanze x86 a 64 bit
  - Amazon Linux 2
  - Amazon Linux (2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
  - Ubuntu (20.04 LTS, 18.04 LTS, 16.04 LTS, 14.04 LTS)
  - Debian (10.x, 9.0 - 9.5, 8.0 - 8.7)
  - Red Hat Enterprise Linux (8.x, 7.2, 6.2 - 6.9)
  - CentOS (7.2 - 7.x, 6.2 - 6.9)
- Istanze ARM
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS, 16.04 LTS)

## Sistemi operativi basati su Windows supportati per l'agente Amazon Inspector Classic

Puoi utilizzare l'agente Amazon Inspector Classic solo su istanze EC2 che eseguono la versione a 64 bit dei seguenti sistemi operativi basati su Windows:

- Windows Server 2019 Base
- Windows Server 2016 Standard
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

## Regioni AWS supportate

Amazon Inspector Classic è supportato nelle seguenti regioni AWS:

- Stati Uniti orientali (Ohio) us-east-2
- Stati Uniti orientali (Virginia settentrionale) us-east-1
- Stati Uniti occidentali (California settentrionale) us-west-1
- Stati Uniti occidentali (Oregon) us-west-2
- Asia Pacifico (Mumbai) ap-south-1
- Asia Pacifico (Seoul) ap-northeast-2
- Asia Pacifico (Sydney) ap-southeast-2
- Asia Pacifico (Tokyo) ap-northeast-1
- Europa (Francoforte) eu-central-1
- Europa (Irlanda) eu-west-1
- Europa (Londra) eu-west-2
- Europa (Stoccolma) eu-north-1
- AWS GovCloud (Stati Uniti orientali) -1 gov-us-east
- AWS GovCloud (Stati Uniti occidentali) -1 gov-us-west

### Note

Il pacchetto di regole [di raggiungibilità della rete](#) non è disponibile nelle regioni AWS GovCloud (Stati Uniti).

# Fine del supporto per Amazon Inspector Classic

Dopo un'attenta valutazione, abbiamo deciso di interrompere il supporto per Amazon Inspector Classic a partire dal 20 maggio 2026. Amazon Inspector Classic non accetterà più nuovi clienti a partire dal 20 maggio 2025. In qualità di cliente esistente con un account registrato al servizio prima del 20 maggio 2025, puoi continuare a utilizzare le funzionalità di Amazon Inspector Classic. Dopo il 20 maggio 2026, non potrai più utilizzare Amazon Inspector Classic.

Il nuovo Amazon Inspector è ora disponibile a livello globale in. Regioni AWS Il nuovo Amazon Inspector è una versione completamente riprogettata e riprogettata dell'esistente Amazon Inspector, ora chiamato Amazon Inspector Classic. Le seguenti funzionalità sono i principali miglioramenti di Amazon Inspector:

- **Progettato per la scalabilità:** il nuovo Amazon Inspector è progettato per la scalabilità e l'ambiente cloud dinamico. Non c'è limite al numero di istanze o immagini che possono essere scansionate in un account.
- **Supporto per immagini di container:** il nuovo Amazon Inspector analizza anche le immagini dei container che risiedono in Amazon Elastic Container Registry (Amazon ECR) alla ricerca di vulnerabilità del software.
- **Supporto per la gestione di più account:** il nuovo Amazon Inspector è integrato con Organizations. Ciò ti consente di delegare un account amministratore per Amazon Inspector dalla tua organizzazione. L'account amministratore delegato è un account centralizzato che consolida tutti i risultati e può configurare tutti gli account dei membri.
- **Utilizza un AWS Systems Manager agente (agente SSM):** con il nuovo Amazon Inspector, non è più necessario installare e gestire un agente Amazon Inspector autonomo su tutte le istanze. EC2 Il nuovo Amazon Inspector sfrutta l'agente SSM ampiamente distribuito.
- **Scansione automatica e continua:** con Amazon Inspector Classic, puoi impostare manualmente obiettivi di valutazione, modelli di valutazione e configurare la frequenza delle valutazioni. Tuttavia, la nuova versione di Amazon Inspector rileva automaticamente tutte le EC2 istanze appena lanciate e le immagini di container idonee inviate ad Amazon ECR e le analizza immediatamente per individuare vulnerabilità del software ed esposizione involontaria alla rete. Le risorse vengono scansionate nuovamente automaticamente in base a diversi trigger, tra cui l'avvio di una nuova EC2 istanza, l'invio di un'immagine del contenitore ad Amazon ECR, l'installazione di un nuovo pacchetto in EC2 un'istanza, l'installazione di una patch o la pubblicazione di un nuovo Common Vulnerabilities and Exposure (CVE) che influisce sulla risorsa.

- **Punteggio di rischio Amazon Inspector:** il nuovo Amazon Inspector calcola un punteggio di rischio Amazon Inspector per aiutarti a dare priorità ai risultati. Il punteggio di rischio viene calcolato correlando le informazioni up-to-date CVE con fattori temporali e ambientali come l'accessibilità della rete e le informazioni sulla sfruttabilità.
- **Altre integrazioni:** tutti i risultati vengono aggregati in una console Amazon Inspector di nuova concezione e inviati AWS Security Hub CSPM ad Amazon per automatizzare i flussi di lavoro EventBridge , come l'emissione di ticket. I risultati relativi alle immagini dei container vengono inoltre inviati ad Amazon ECR.

Per informazioni su tutte le caratteristiche e i prezzi del nuovo Amazon Inspector, consulta la [Amazon Inspector User Guide](#).

Sebbene continueremo a supportare Amazon Inspector Classic per qualche tempo e i clienti potranno utilizzare sia il nuovo Amazon Inspector che Amazon Inspector Classic nello stesso account, ti consigliamo vivamente di migrare al nuovo Amazon Inspector. Le seguenti sezioni illustrano il processo di passaggio da Amazon Inspector Classic al nuovo Amazon Inspector.

#### Argomenti

- [Fase 1: \(Facoltativo\) Esportazione dei report e dei risultati della valutazione](#)
- [Fase 2: Eliminare tutte le esecuzioni di valutazione pianificate in Amazon Inspector Classic](#)
- [Fase 3: abilitare il nuovo Amazon Inspector](#)

## Fase 1: (Facoltativo) Esportazione dei report e dei risultati della valutazione

Per salvare i report di valutazione e i risultati in Amazon Inspector Classic, genera un rapporto di valutazione.

Per generare un report di valutazione

1. Nella pagina Assessment runs (Esecuzioni di valutazioni) individuare l'esecuzione di valutazioni per cui si desidera generare un report. Assicurati che lo stato sia Analisi completa.
2. Nella colonna Reports (Report) per l'esecuzione di valutazioni desiderata, scegliere l'icona dei report.

**⚠ Important**

L'icona dei report è presente nella colonna Reports (Report) solo per le esecuzioni di valutazioni eseguite dopo il 25 aprile 2017. È stato allora che sono diventati disponibili i report di valutazione in Amazon Inspector Classic.

3. Nella finestra di dialogo del rapporto di valutazione, scegli il tipo di rapporto che desideri visualizzare (un rapporto sui risultati o un rapporto completo) e il formato del rapporto (HTML o PDF). Scegliere quindi Generate report (Genera report).

## Fase 2: Eliminare tutte le esecuzioni di valutazione pianificate in Amazon Inspector Classic

Per disabilitare Amazon Inspector Classic, elimina tutti i modelli di valutazione presenti nel tuo account quando sono attivi. Regioni AWS L'eliminazione dei modelli di valutazione interrompe tutte le future esecuzioni di valutazione pianificate.

Come eliminare un modello di valutazione

- Nella pagina Assessment Templates (Modelli di valutazione) scegliere il modello da eliminare, quindi Delete (Elimina). Quando viene richiesta la conferma, scegli Sì.

**⚠ Important**

Quando elimini un modello di valutazione, verranno eliminati anche tutti i modelli di valutazione, tutte le valutazioni eseguite, tutti i risultati e tutte le versioni dei report associati al modello.

## Fase 3: abilitare il nuovo Amazon Inspector

Puoi abilitare il nuovo Amazon Inspector utilizzando Console di gestione AWS o il nuovo Amazon Inspector. APIs Per iniziare a usare il nuovo Amazon Inspector, consulta la [Guida introduttiva](#) nella Amazon Inspector User Guide.

# Guida introduttiva ad Amazon Inspector Classic

Questo tutorial mostra come configurare Amazon Inspector Classic e iniziare a creare ed eseguire la prima valutazione.

## Impostazione One-Click

La procedura seguente mostra come creare ed eseguire una valutazione automatica utilizzando un modello predefinito e parametri di pianificazione predefiniti (una volta alla settimana o solo una volta) su tutte le istanze Amazon Elastic Compute Cloud (Amazon EC2) disponibili nell'attuale e. Account AWS Regione AWS

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo.  
<https://console.aws.amazon.com/inspector/>
2. Nella pagina Welcome (Benvenuto) scegliere il tipo di valutazione da eseguire. Le valutazioni di rete analizzano le configurazioni di rete del tuo AWS ambiente alla ricerca di vulnerabilità e non richiedono un agente Amazon Inspector Classic. Gli Host Assessments analizzano il software e le configurazioni on-host delle EC2 istanze alla ricerca di vulnerabilità e richiedono l'installazione di un agente sulle istanze. EC2

Scegli Run weekly (recommended) (Esegui settimanalmente) (opzione consigliata) o Run once (Esegui una volta). Quando esegui la tua scelta, il servizio crea automaticamente la valutazione per te. Nello specifico, il servizio effettua quanto segue:

- a. Crea un [ruolo collegato al servizio](#).

### Note

Per identificare le EC2 istanze specificate negli obiettivi di valutazione, Amazon Inspector Classic deve EC2 enumerare le istanze e i tag. Amazon Inspector Classic ottiene l'accesso a queste risorse direttamente dall'utente Account AWS tramite un ruolo collegato al servizio chiamato `AWSServiceRoleForAmazonInspector`. Per ulteriori informazioni sui ruoli collegati ai servizi, consulta [Utilizzo di ruoli collegati ai servizi per Amazon Inspector Classic](#) e [Utilizzo dei ruoli collegati ai servizi](#).

- b. Se applicabile, installa un agente [Amazon Inspector Classic](#) su tutte le istanze EC2 disponibili nella tua regione e nella Account AWS tua regione.

**Note**

Il servizio installa un agente Amazon Inspector Classic solo nelle istanze che AWS Systems Manager consentono EC2 Run Command. Per utilizzare questa opzione, assicurati che tutte le EC2 istanze siano nella versione corrente Account AWS e Regione AWS abbiano installato l'agente SSM e abbiano un ruolo IAM che consenta Run Command. Per ulteriori informazioni, consulta [Installazione dell'agente su più istanze EC2 usando Systems Manager Run Command](#).

- c. Aggiunge le istanze per un [target di valutazione](#).
  - d. Include il target in un modello di [valutazione](#) con un set di pacchetti di regole standardizzati.
  - e. Esegue le valutazioni settimanalmente o solo una tantum, a seconda che si scelga Run weekly (Esegui settimanalmente) (opzione consigliata) o Run once (Esegui una tantum).
3. Nella finestra di dialogo di conferma, scegli OK. Amazon Inspector Classic esegue automaticamente la valutazione.

## Configurazione avanzata

La procedura seguente mostra come scegliere EC2 istanze Amazon, pacchetti di regole e parametri di pianificazione specifici da includere in un obiettivo e modello di valutazione.

1. Nella pagina Welcome (Benvenuto), seleziona Advanced setup (Configurazione avanzata).
2. Sulla pagina Define an assessment target (Definisci un target di valutazione), inserire il nome del proprio target valutazione.
3. Per Tutte le istanze, puoi mantenere selezionata la casella di controllo per includere tutte le EC2 istanze della tua regione nell' Account AWS obiettivo di valutazione. Se desideri scegliere quali EC2 istanze includere, deseleziona la casella di controllo Tutte le istanze e inserisci i tag Chiave e Value associati alle istanze di destinazione. EC2 Per ulteriori informazioni sull'etichettatura delle EC2 istanze, consulta [Tagging Your Amazon Resources](#). EC2
4. Per Install Agents, puoi mantenere la casella di controllo selezionata per impostazione predefinita se le istanze consentono l'esecuzione del comando di esecuzione di [System Manager](#). Il servizio installa un agente Amazon Inspector Classic su EC2 tutte le istanze del target di valutazione che lo consentono. AWS Systems Manager Per utilizzare questa opzione, assicurati che tutte le EC2 istanze siano nella versione corrente Account AWS e Regione AWS abbiano installato l'agente SSM e abbiano un ruolo IAM che consenta Run Command. Per

ulteriori informazioni, consulta [Installazione dell'agente su più istanze EC2 usando Systems Manager Run Command](#). Per installare manualmente l'agente, consulta [Installazione di agenti Amazon Inspector](#).

5. Scegli Next (Successivo).
6. Sulla pagina Define an assessment template (Definisci un modello di valutazione), inserire il nome del proprio modello di valutazione.
7. In Rules packages (Pacchetti di regole), scegliere uno o più pacchetti di regole da includere nel modello di valutazione. Per ulteriori informazioni sui pacchetti di regole, consulta [Regole e pacchetti di regole Amazon Inspector](#).
8. Per Duration (Durata), selezionare la durata dell'esecuzione di valutazione.
9. (Facoltativo) Per Assessment Schedule, imposta una pianificazione per le esecuzioni di valutazione ricorrenti.
10. Scegli Next (Successivo).
11. Nella pagina Review (Revisione), rivedere le opzioni per i target di valutazione e il modello. Se sei soddisfatto della configurazione, scegli Crea. Se si imposta una pianificazione di valutazione per il modello di valutazione, la valutazione viene eseguita automaticamente dopo aver scelto Create (Crea).

#### Note

Per identificare le EC2 istanze specificate negli obiettivi di valutazione, Amazon Inspector Classic deve enumerare le istanze e i tag. Amazon Inspector Classic ottiene l'accesso a queste risorse direttamente dall'utente Account AWS tramite un ruolo collegato al servizio chiamato `AWSServiceRoleForAmazonInspector`. Per ulteriori informazioni sull'utilizzo dei ruoli collegati ai servizi in Amazon Inspector Classic, consulta [Utilizzo di ruoli collegati ai servizi per Amazon Inspector Classic](#). Per informazioni dettagliate sull'utilizzo dei ruoli collegati ai servizi, consulta Using service-linked roles nella [Guida](#) per l'utente AWS Identity and Access Management.

12. Se è stata configurata una pianificazione di valutazione, accedere al modello di valutazione tramite la console e selezionare Run (Esegui).
13. Per monitorare l'avanzamento dell'esecuzione di valutazione, nel riquadro di navigazione della console, scegliere Assessment runs (Esecuzioni di valutazione), quindi scegliere Findings (Risultati). Per ulteriori informazioni sui risultati, consulta [Risultati di Amazon Inspector Classic](#).

# Tutorial per Amazon Inspector Classic

I seguenti tutorial mostrano come eseguire le esecuzioni di valutazione di Amazon Inspector Classic sui sistemi operativi Red Hat Enterprise Linux e Ubuntu.

## Tutorial

- [Tutorial: Utilizzo di Amazon Inspector Classic con Red Hat Enterprise Linux](#)
- [Tutorial: utilizzo di Amazon Inspector Classic con Ubuntu Server](#)

## Tutorial su Amazon Inspector Classic - Red Hat Enterprise Linux

Prima di seguire le istruzioni in questo tutorial, ti consigliamo di familiarizzare con le informazioni riportate nella sezione [Terminologia e concetti di Amazon Inspector Classic](#).

Questo tutorial mostra come utilizzare Amazon Inspector Classic per analizzare il comportamento di un'istanza EC2 che esegue il sistema operativo Red Hat Enterprise Linux 7.5. Fornisce step-by-step istruzioni su come navigare nel flusso di lavoro di Amazon Inspector Classic. Il flusso di lavoro include la preparazione delle istanze Amazon EC2, l'esecuzione di un modello di valutazione e l'esecuzione delle correzioni di sicurezza consigliate generate nei risultati della valutazione. Se sei un utente alle prime armi e desideri configurare ed eseguire una valutazione di Amazon Inspector Classic con un clic, [consulta Creazione](#) di una valutazione di base.

## Argomenti

- [Fase 1: configurare un'istanza Amazon EC2 da utilizzare con Amazon Inspector Classic](#)
- [Fase 2: modifica la tua istanza Amazon EC2](#)
- [Fase 3: Creazione di un target di valutazione e installazione di un agente su un'istanza EC2](#)
- [Fase 4: Creazione ed esecuzione di un modello di valutazione](#)
- [Fase 5: Individuazione e analisi dei risultati](#)
- [Fase 6: Applicazione della correzione consigliata al target di valutazione](#)

## Fase 1: configurare un'istanza Amazon EC2 da utilizzare con Amazon Inspector Classic

Per questo tutorial, crea un'istanza EC2 che esegua Red Hat Enterprise Linux 7.5 e taggala utilizzando la chiave Name e il valore di **InspectorEC2InstanceLinux**

### Note

Per ulteriori informazioni sul tagging delle istanze EC2, consulta [Risorse e tag](#).

## Fase 2: modifica la tua istanza Amazon EC2

In questo tutorial, modifichi l'istanza EC2 di destinazione per esporla al potenziale problema di sicurezza CVE-2018-1111. [Per ulteriori informazioni, consulta https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111) e [Common vulnerabilities & exposures \(CVE\)](#)

Connettiti alla tua istanza, **InspectorEC2InstanceLinux**, ed esegui questo comando:

```
sudo yum install dhclient-12:4.2.5-68.el7
```

Per istruzioni su come connettersi a un'istanza EC2, consulta [Connect to Your Instance](#) nella Amazon EC2 User Guide.

## Fase 3: Creazione di un target di valutazione e installazione di un agente su un'istanza EC2

Amazon Inspector Classic utilizza obiettivi di valutazione per designare le risorse AWS da valutare.

Per creare un target di valutazione e installare un agente su un'istanza EC2

1. Accedi Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo. <https://console.aws.amazon.com/inspector/>
2. Nel riquadro di navigazione scegli Assessment targets (Target di valutazione), quindi Create (Crea).

Esegui questa operazione:

- a. Nel campo Name (Nome) inserisci il nome del target di valutazione.

Per questo tutorial, digita **MyTargetLinux**.

- b. Per i tag di utilizzo, scegli le istanze EC2 che desideri includere in questo obiettivo di valutazione inserendo i valori nei campi Chiave e Valore.

Per questo tutorial, scegliere l'istanza EC2 creata nella fase precedente immettendo **Name** nel campo Key (Chiave) e **InspectorEC2InstanceLinux** nel campo Value (Valore).

Per includere nel target di valutazione tutte le istanze EC2 nella regione e nell'account AWS, seleziona la casella All Instances (Tutte le istanze).

- c. Scegli Save (Salva).
- d. Installa un agente Amazon Inspector Classic sulla tua istanza EC2 con tag. Per installare un agente su tutte le istanze EC2 incluse in un target di valutazione, seleziona la casella Install Agents (Installa agenti).

#### Note

Puoi anche installare l'agente Amazon Inspector Classic utilizzando il [comando AWS Systems Manager Run](#). Per installare l'agente su tutte le istanze incluse nel target di valutazione, puoi specificare gli stessi tag che hai usato per creare il target di valutazione. Oppure puoi installare manualmente l'agente Amazon Inspector Classic sulla tua istanza EC2. Per ulteriori informazioni, consulta [Installazione degli agenti Amazon Inspector Classic](#).

- e. Scegli Save (Salva).

#### Note

A questo punto, Amazon Inspector Classic crea un ruolo collegato al servizio chiamato `AWSServiceRoleForAmazonInspector`. Il ruolo garantisce ad Amazon Inspector Classic l'accesso necessario alle tue risorse. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi per Amazon Inspector Classic](#).

## Fase 4: Creazione ed esecuzione di un modello di valutazione

Per creare ed eseguire il modello

1. Nel riquadro di navigazione selezionare Assessment templates (Modelli di valutazione), quindi Create (Crea).
2. Nel campo Name (Nome), inserire il nome del modello di valutazione. Per questo tutorial, digita **MyFirstTemplateLinux**.
3. Per Target name (Nome target), selezionare il target di valutazione creato sopra, **MyTargetLinux**.
4. In Rules packages (Pacchetti di regole), scegliere uno o più pacchetti di regole da utilizzare in questo modello di valutazione.

Per questo tutorial, selezionare Common Vulnerabilities and Exposures – 1.1.

5. Nel campo Duration (Durata) specifica la durata del modello di valutazione.

Per questo tutorial, selezionare 15 minuti.

6. Scegli Create and run (Crea ed esegui).

## Fase 5: Individuazione e analisi dei risultati

Un ciclo di valutazione completato produce una serie di risultati o potenziali problemi di sicurezza che Amazon Inspector Classic rileva nel tuo obiettivo di valutazione. Puoi rivedere i risultati e seguire la procedura consigliata per risolvere i potenziali problemi di sicurezza.

In questo tutorial, se completi i passaggi precedenti, l'esecuzione di valutazioni genera un risultato riferito alla vulnerabilità comune [CVE-2018-1111](#).

Per individuare e analizzare i risultati

1. Nel riquadro di navigazione selezionare Assessment runs (Esecuzioni di valutazione). Verifica che lo stato dell'esecuzione del modello di valutazione chiamato MyFirstTemplateLinux sia impostato su Raccolta di dati. Questo stato indica che l'esecuzione di valutazioni è attualmente in corso e che i dati telemetrici relativi al target vengono raccolti e analizzati in base ai pacchetti di regole selezionati.

2. Non puoi visualizzare i risultati generati dall'esecuzione di valutazioni in corso. Consenti all'esecuzione di valutazioni di completare l'intero processo. Tuttavia, per questo tutorial puoi arrestare l'esecuzione dopo alcuni minuti.

Lo stato dell'analisi MyFirstTemplateLinuxcambia prima in Interruzione, poi in pochi minuti in Analisi e infine in Analisi completa. Per visualizzare queste variazioni di stato, selezionare l'icona Refresh (Aggiorna).

3. Nel riquadro di navigazione, seleziona Esiti.

Puoi vedere che una nuova scoperta di High Severity chiamata Instance Inspector EC2 InstanceLinux è vulnerabile a CVE-2018-1111.

#### Note

Se il nuovo risultato non è visualizzato, selezionare l'icona Refresh (Aggiorna).

Per espandere la visualizzazione e visualizzare i dettagli di questo risultato, scegli la freccia a sinistra del risultato. I dettagli del risultato includono i seguenti elementi:

- ARN del risultato
- Nome dell'esecuzione di valutazioni che ha generato il risultato
- Nome del target di valutazione che ha generato il risultato
- Nome del modello di valutazione che ha generato il risultato
- Ora di inizio dell'esecuzione di valutazioni
- Ora di fine dell'esecuzione di valutazioni
- Stato dell'esecuzione di valutazioni
- Nome del pacchetto di regole contenente la regola che ha attivato questo risultato
- ID agente Amazon Inspector Classic
- Nome del risultato
- Gravità del risultato
- Descrizione del risultato
- Procedure consigliate che puoi eseguire per correggere il potenziale problema di sicurezza descritto dal risultato

## Fase 6: Applicazione della correzione consigliata al target di valutazione

In questo tutorial, hai modificato il target di valutazione in modo da esporlo a potenziali problemi di sicurezza CVE-2018-1111. In questa procedura, applica la correzione consigliata per il problema.

Per applicare la correzione al target

1. Connettiti all'istanza **InspectorEC2InstanceLinux** creata nella precedente sezione ed esegui questo comando:

```
sudo yum update dhclient-12:4.2.5-68.e17
```

2. Nella pagina Modelli di valutazione, scegli MyFirstTemplateLinux, quindi scegli Esegui per iniziare una nuova esecuzione di valutazione utilizzando questo modello.
3. Segui i passaggi indicati [Fase 5: Individuazione e analisi dei risultati](#) per visualizzare i risultati risultanti da questa successiva esecuzione del MyFirstTemplateLinuxmodello.

Poiché hai risolto il problema di sicurezza CVE-2018-1111, non dovresti più visualizzare alcun risultato.

## Tutorial di Amazon Inspector Classic - Ubuntu Server

Prima di seguire le istruzioni in questo tutorial, ti consigliamo di familiarizzare con le informazioni riportate nella sezione [Terminologia e concetti di Amazon Inspector Classic](#).

Questo tutorial mostra come utilizzare Amazon Inspector Classic per analizzare il comportamento di un'istanza EC2 che esegue il sistema operativo Ubuntu Server 16.04 LTS. Fornisce step-by-step istruzioni su come navigare nel flusso di lavoro di Amazon Inspector Classic.

Se sei un utente alle prime armi e desideri configurare ed eseguire una valutazione di Amazon Inspector Classic con un clic, [consulta Creazione](#) di una valutazione di base.

Argomenti

- [Fase 1: configurare un'istanza Amazon EC2 da utilizzare con Amazon Inspector Classic](#)
- [Passaggio 2: crea un obiettivo di valutazione e installa un agente sull'istanza EC2](#)
- [Passaggio 3: crea ed esegui il modello di valutazione](#)
- [Fase 4: Individua e analizza i risultati generati](#)
- [Fase 5: applica la correzione consigliata al tuo obiettivo di valutazione](#)

## Fase 1: configurare un'istanza Amazon EC2 da utilizzare con Amazon Inspector Classic

Per configurare un'istanza EC2

- Per questo tutorial, crea un'istanza EC2 che esegue Ubuntu Server 16.04 LTS e taggala utilizzando la chiave Name e il valore di **InspectorEC2InstanceUbuntu**

### Note

Per ulteriori informazioni sul tagging delle istanze EC2, consulta [Risorse e tag](#).

## Passaggio 2: crea un obiettivo di valutazione e installa un agente sull'istanza EC2

Amazon Inspector Classic utilizza obiettivi di valutazione per designare le risorse AWS da valutare.

Per creare un obiettivo di valutazione e installare un agente sull'istanza EC2

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo. <https://console.aws.amazon.com/inspector/>
2. Nel riquadro di navigazione scegli Assessment targets (Target di valutazione), quindi Create (Crea).
3. Nel campo Name (Nome) inserisci il nome del target di valutazione.


Ai fini di questo tutorial, digita **MyTargetUbuntu**.

4. Per i tag di utilizzo, scegli le istanze EC2 che desideri includere in questo obiettivo di valutazione inserendo i valori nei campi Chiave e Valore.

Per questo tutorial, scegliere l'istanza EC2 creata nella fase precedente immettendo **Name** nel campo Key (Chiave) e **InspectorEC2InstanceUbuntu** nel campo Value (Valore).


Per includere tutte le istanze EC2 nella regione e nell'account AWS nel target di valutazione, selezionare la casella All Instances (Tutte le istanze).

5. Installa un Amazon Inspector Classic Agent sulla tua istanza EC2 con tag. Per installare un agente su tutte le istanze EC2 incluse in un target di valutazione, selezionare la casella Install Agents (Installa agenti).

 Note

Puoi inoltre installare l'agente Amazon Inspector usando [Systems Manager Run Command](#). Per installare l'agente su tutte le istanze incluse nel target di valutazione, puoi specificare gli stessi tag utilizzati per creare tale target di valutazione. In alternativa, puoi installare Agente Amazon Inspector sull'istanza EC2 manualmente. Per ulteriori informazioni, consulta [Installazione degli agenti Amazon Inspector Classic](#).

6. Scegli Save (Salva).

 Note

A questo punto, `AWSServiceRoleForAmazonInspector` viene creato un ruolo collegato al servizio chiamato per concedere ad Amazon Inspector Classic l'accesso alle tue risorse. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi per Amazon Inspector Classic](#).

## Passaggio 3: crea ed esegui il modello di valutazione

Per creare ed eseguire il modello

1. Se si utilizza la Advanced setup (Configurazione avanzata), si verrà indirizzati alla pagina Define an assessment template (Definisci un modello di valutazione). In caso contrario, passare alla pagina Assessment templates (Modelli di valutazione) e scegliere Create (Crea).
2. Nel campo Name (Nome), inserire il nome del modello di valutazione. Per questo tutorial, digita **MyFirstTemplateUbuntu**.
3. Per Target name (Nome target), selezionare il target di valutazione creato sopra, **MyTargetUbuntu**.
4. Per Rules packages (Pacchetti di regole) usa il menu a discesa per scegliere i pacchetti di regole che desideri usare in questo modello di valutazione.

Per questo tutorial, selezionare Common Vulnerabilities and Exposures – 1.1.

5. Nel campo Duration (Durata) specifica la durata del modello di valutazione.

Per questo tutorial, scegliere 15 minuti.

6. Se si utilizza Advanced setup (Configurazione avanzata), selezionare Avanti. Nella pagina Review (Revisione), selezionare Create (Crea). In caso contrario scegliere Create and run (Crea ed esegui).

## Fase 4: Individua e analizza i risultati generati

Un ciclo di valutazione completato produce una serie di risultati o potenziali problemi di sicurezza che Amazon Inspector Classic rileva nel tuo obiettivo di valutazione. Puoi rivedere i risultati e seguire la procedura consigliata per risolvere i potenziali problemi di sicurezza.

1. Passare alla pagina Assessment Runs (Esecuzioni di valutazioni). Verifica che lo stato dell'esecuzione del modello di valutazione chiamato MyFirstTemplateUbutue creato nel passaggio precedente sia impostato su Raccolta di dati. Questo stato indica che l'esecuzione di valutazioni è attualmente in corso e che i dati telemetrici relativi al target vengono raccolti e analizzati in base ai pacchetti di regole selezionati.
2. Non puoi visualizzare i risultati generati dall'esecuzione di valutazioni in corso. Consenti all'esecuzione di valutazioni di completare l'intero processo.

Lo stato dell'analisi MyFirstTemplateUbutucambia prima in Interruzione, poi in pochi minuti in Analisi e infine in Analisi completa. Per visualizzare queste variazioni di stato, selezionare l'icona Refresh (Aggiorna).

3. Passare alla pagina Findings (Risultati).

Per espandere la visualizzazione e visualizzare i dettagli di un risultato, scegliete la freccia a sinistra del risultato. I dettagli del risultato includono i seguenti elementi:

- ARN del risultato
- Nome dell'esecuzione di valutazioni che ha generato il risultato
- Nome del target di valutazione che ha generato il risultato
- Nome del modello di valutazione che ha generato il risultato
- Ora di inizio dell'esecuzione di valutazioni
- Ora di fine dell'esecuzione di valutazioni
- Stato dell'esecuzione di valutazioni

- Nome del pacchetto di regole che include la regola che ha attivato il risultato
- ID agente Amazon Inspector Classic
- Nome del risultato
- Gravità del risultato
- Descrizione del risultato
- Procedure consigliate che puoi eseguire per correggere il potenziale problema di sicurezza descritto dal risultato

## Fase 5: applica la correzione consigliata al tuo obiettivo di valutazione

In questa procedura, si applica un aggiornamento per risolvere i problemi rilevati.

1. Connect all'istanza **InspectorEC2InstanceUbuntu** ed esegui un aggiornamento del pacchetto.
2. Nella pagina Modelli di valutazione, scegli MyFirstTemplateUbuntu, quindi scegli Esegui per iniziare una nuova esecuzione utilizzando questo modello.
3. Segui i passaggi indicati [Fase 4: Individua e analizza i risultati generati](#) per visualizzare i risultati risultanti da questa successiva esecuzione del MyFirstTemplateUbuntu modello.

L'aggiornamento del pacchetto avrebbe dovuto risolvere i risultati della prima esecuzione del modello.

# Sicurezza in Amazon Inspector Classic

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon Inspector Classic, consulta AWS [Services in Scope by Compliance Program AWS Services in Scope](#) Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon Inspector Classic. I seguenti argomenti mostrano come configurare Amazon Inspector Classic per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri servizi AWS che ti aiutano a monitorare e proteggere le tue risorse Amazon Inspector Classic.

## Argomenti

- [Protezione dei dati in Amazon Inspector Classic](#)
- [Identity and Access Management per Amazon Inspector Classic](#)
- [Registrazione e monitoraggio in Amazon Inspector Classic](#)
- [Risposta agli incidenti in Amazon Inspector Classic](#)
- [Convalida della conformità per Amazon Inspector Classic](#)
- [Resilienza in Amazon Inspector Classic](#)
- [Sicurezza dell'infrastruttura in Amazon Inspector Classic](#)
- [Analisi della configurazione e delle vulnerabilità in Amazon Inspector Classic](#)
- [Best practice di sicurezza per Amazon Inspector Classic](#)

# Protezione dei dati in Amazon Inspector Classic

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in Amazon Inspector Classic. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Inspector Classic o altro Servizi AWS utilizzando la console, l'API o AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un

server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

## Argomenti

- [Crittografia dei dati a riposo](#)
- [Crittografia dei dati in transito](#)

## Crittografia dei dati a riposo

I dati di telemetria generati da un agente Amazon Inspector Classic durante le esecuzioni di valutazione sono formattati in file JSON. Questi file vengono near-real-time consegnati tramite TLS ad Amazon Inspector Classic, dove vengono crittografati con per-assessment-run una chiave derivata temporanea AWS KMS.

I file vengono archiviati in modo sicuro in bucket S3 dedicati ad Amazon Inspector Classic. Il motore di regole di Amazon Inspector Classic esegue le seguenti operazioni:

- Accede ai dati di telemetria crittografati nel bucket S3
- Decrypta i dati in memoria
- Elabora i dati in base alle regole di valutazione configurate per generare risultati

## Crittografia dei dati in transito

In quanto servizio gestito, Amazon Inspector Classic è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizza chiamate API AWS pubblicate per accedere ad Amazon Inspector Classic attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

# Identity and Access Management per Amazon Inspector Classic

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuare l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon Inspector. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

## Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come funziona Amazon Inspector Classic con IAM](#)
- [Esempio 2: consentire a un utente di eseguire operazioni di descrizione ed elenco solo sui risultati di Amazon Inspector](#)
- [Risorse relative alle policy per Amazon Inspector](#)
- [Chiavi relative alle condizioni delle politiche per Amazon Inspector](#)
- [ACLs in Amazon Inspector](#)
- [ABAC con Amazon Inspector](#)
- [Utilizzo di credenziali temporanee con Amazon Inspector](#)
- [Autorizzazioni principali multiservizio per Amazon Inspector](#)
- [Ruoli di servizio per Amazon Inspector](#)
- [Ruoli collegati ai servizi per Amazon Inspector](#)
- [Esempi di policy basate sull'identità per Amazon Inspector Classic](#)
- [Utilizzo di ruoli collegati ai servizi per Amazon Inspector Classic](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Inspector Classic](#)

## Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Inspector Classic](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come funziona Amazon Inspector Classic con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [Esempi di policy basate sull'identità per Amazon Inspector Classic](#))

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

## Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

## Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

## Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

## Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

## Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

## Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

## Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

## Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- **Limiti delle autorizzazioni:** imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Politiche di controllo del servizio (SCPs):** specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .

- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

## Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

## Come funziona Amazon Inspector Classic con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon Inspector, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon Inspector.

### Funzionalità IAM che puoi utilizzare con Amazon Inspector Classic

Funzionalità IAM	Supporto per Amazon Inspector
<a href="#">Policy basate sull'identità</a>	Sì
<a href="#">Policy basate su risorse</a>	No
<a href="#">Operazioni di policy</a>	Sì
<a href="#">Risorse relative alle policy</a>	Sì
<a href="#">Chiavi di condizione della policy (specifica del servizio)</a>	Sì
<a href="#">ACLs</a>	No
<a href="#">ABAC (tag nelle policy)</a>	Parziale
<a href="#">Credenziali temporanee</a>	Sì

Funzionalità IAM	Supporto per Amazon Inspector
<a href="#">Autorizzazioni del principale</a>	Sì
<a href="#">Ruoli di servizio</a>	No
<a href="#">Ruoli collegati al servizio</a>	Sì

Per avere una visione di alto livello di come Amazon Inspector e AWS altri servizi funzionano con la maggior parte delle funzionalità IAM, [AWS consulta i servizi che funzionano con IAM](#) nella IAM User Guide.

## Politiche basate sull'identità per Amazon Inspector

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Esempi di policy basate sull'identità per Amazon Inspector

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta. [Esempi di policy basate sull'identità per Amazon Inspector Classic](#)

## Politiche basate sulle risorse all'interno di Amazon Inspector

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket

Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

## Azioni politiche per Amazon Inspector

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Amazon Inspector, consulta [Azioni definite da Amazon Inspector](#) Classic nel Service Authorization Reference.

Le azioni politiche in Amazon Inspector utilizzano il seguente prefisso prima dell'azione:

```
inspector
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
  "inspector:action1",  
  "inspector:action2"  
]
```

La seguente policy di autorizzazione concede a un utente l'autorizzazione per eseguire tutte le operazioni che iniziano con `Describe` e `List`. Queste operazioni mostrano informazioni su una

risorsa Amazon Inspector, ad esempio un obiettivo di valutazione o un risultato. Il carattere jolly (\*) nell'Resourceelemento indica che le operazioni sono consentite per tutte le risorse Amazon Inspector di proprietà dell'account:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:Describe*",
        "inspector:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

## Esempio 2: consentire a un utente di eseguire operazioni di descrizione ed elenco solo sui risultati di Amazon Inspector

La seguente policy di autorizzazione concede a un utente l'autorizzazione per eseguire solo le operazioni `ListFindings` e `DescribeFindings`. Queste operazioni mostrano informazioni sui risultati di Amazon Inspector. Il carattere jolly (\*) nell'Resourceelemento indica che le operazioni sono consentite per tutte le risorse Amazon Inspector di proprietà dell'account.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:DescribeFindings",
        "inspector:ListFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

```
    "Resource": "*"
  }
]
}
```

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta [Esempi di policy basate sull'identità per Amazon Inspector Classic](#)

## Risorse relative alle policy per Amazon Inspector

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (\*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"

```

Per visualizzare un elenco dei tipi di risorse Amazon Inspector e relativi ARNs, consulta [Risorse definite da Amazon Inspector Classic](#) nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta [Azioni definite da Amazon Inspector Classic](#).

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta [Esempi di policy basate sull'identità per Amazon Inspector Classic](#)

## Chiavi relative alle condizioni delle politiche per Amazon Inspector

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco dei codici di condizione di Amazon Inspector, consulta [Condition keys per Amazon Inspector](#) Classic nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Amazon Inspector Classic](#).

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta [Esempi di policy basate sull'identità per Amazon Inspector Classic](#)

## ACLs in Amazon Inspector

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

## ABAC con Amazon Inspector

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di

ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

## Utilizzo di credenziali temporanee con Amazon Inspector

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

## Autorizzazioni principali multiservizio per Amazon Inspector

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

## Ruoli di servizio per Amazon Inspector

Supporta i ruoli di servizio: no

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

### Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Amazon Inspector. Modifica i ruoli di servizio solo quando Amazon Inspector fornisce indicazioni in tal senso.

## Ruoli collegati ai servizi per Amazon Inspector

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi Amazon Inspector, consulta [Utilizzo di ruoli collegati ai servizi per Amazon Inspector Classic](#)

## Esempi di policy basate sull'identità per Amazon Inspector Classic

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse Amazon Inspector. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon Inspector, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per Amazon Inspector Classic](#) nel Service Authorization Reference.

### Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console Amazon Inspector](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Consenti a un utente di eseguire operazioni, descrivere ed elencare solo sui risultati di Amazon Inspector](#)

### Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon Inspector nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono

le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai clienti AWS specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel tuo Account AWS, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

## Utilizzo della console Amazon Inspector

Per accedere alla console Amazon Inspector Classic, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon Inspector presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto

alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS AI contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console Amazon Inspector, collega anche Amazon *ConsoleAccess* Inspector *ReadOnly* AWS o la policy gestita alle entità. Per maggiori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente di IAM.

## Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",

```

```
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

## Consenti a un utente di eseguire operazioni, descrivere ed elencare solo sui risultati di Amazon Inspector

La seguente policy di autorizzazione concede a un utente l'autorizzazione per eseguire solo le operazioni `ListFindings` e `DescribeFindings`. Queste operazioni mostrano informazioni sui risultati di Amazon Inspector. Il carattere jolly (\*) nell'elemento `Resource` indica che le operazioni sono consentite per tutte le risorse Amazon Inspector di proprietà dell'account.

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:DescribeFindings",
        "inspector:ListFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

## Utilizzo di ruoli collegati ai servizi per Amazon Inspector Classic

Amazon Inspector Classic utilizza ruoli collegati ai [servizi AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon

Inspector Classic. I ruoli collegati ai servizi sono predefiniti da Amazon Inspector Classic e includono tutte le autorizzazioni richieste dal servizio per chiamare altri utenti per tuo conto. Servizi AWS

Un ruolo collegato al servizio semplifica la configurazione di Amazon Inspector Classic perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon Inspector Classic definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon Inspector Classic può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi le tue risorse Amazon Inspector Classic perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano ruoli collegati ai servizi, consulta [AWS Servizi che funzionano con IAM](#) e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

## Autorizzazioni di ruolo collegate ai servizi per Amazon Inspector Classic

Amazon Inspector Classic utilizza il ruolo collegato al servizio denominato `- AWSServiceRoleForAmazonInspector ServiceLinkedRoleDescription`

Il ruolo `AWSService RoleForAmazonInspector` collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `inspector.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AmazonInspectorServiceRolePolicy` consente ad Amazon Inspector Classic di completare le seguenti azioni sulle risorse specificate:

- Operazione: `iam:CreateServiceLinkedRole` su `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`

È necessario configurare le autorizzazioni per consentire a un'entità IAM (come un utente, un gruppo o un ruolo IAM) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Creazione di un ruolo collegato ai servizi per Amazon Inspector Classic

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando utilizzi `CompleteThisCreateActionInThisService` l' AWS API Console di gestione AWS, Amazon Inspector Classic crea per te il ruolo collegato al servizio. AWS CLI

## Modifica di un ruolo collegato al servizio per Amazon Inspector Classic

Amazon Inspector Classic non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonInspector` servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

## Eliminazione di un ruolo collegato al servizio per Amazon Inspector Classic

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, consigliamo di eliminare il ruolo. In questo modo, non hai un'entità inutilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

### Note

Se il servizio Amazon Inspector Classic utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Amazon Inspector Classic utilizzate da **`AWSServiceRoleForAmazonInspector`**

- Elimina i tuoi obiettivi di valutazione Account AWS in tutti i Regioni AWS luoghi in cui è in esecuzione Amazon Inspector Classic. Per ulteriori informazioni, consulta [Obiettivi di valutazione di Amazon Inspector Classic](#).

Eliminazione manuale del ruolo collegato al servizio con IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSService RoleForAmazonInspector servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Regioni supportate per i ruoli collegati ai servizi Amazon Inspector Classic

Amazon Inspector Classic supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di AWS](#).

## Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Inspector Classic

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Inspector e IAM.

### Argomenti

- [Non sono autorizzato a eseguire un'azione in Amazon Inspector](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon Inspector](#)

## Non sono autorizzato a eseguire un'azione in Amazon Inspector

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM mateojackson prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *my-example-widget* fittizia ma non dispone di autorizzazioni `inspector:GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
inspector:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente mateojackson deve essere aggiornata per consentire l'accesso alla risorsa *my-example-widget* utilizzando l'azione `inspector:GetWidget`.

Se hai bisogno di assistenza, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole` azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon Inspector.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon Inspector. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon Inspector

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon Inspector supporta queste funzionalità, consulta [Come funziona Amazon Inspector Classic con IAM](#)
- Per sapere come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.

- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.

## Registrazione e monitoraggio in Amazon Inspector Classic

Amazon Inspector Classic è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon Inspector Classic. CloudTrail acquisisce tutte le chiamate API per Amazon Inspector Classic come eventi, incluse le chiamate dalla console Amazon Inspector Classic e le chiamate in codice alle operazioni dell'API Amazon Inspector Classic.

Per informazioni sull'utilizzo della CloudTrail registrazione in Amazon Inspector Classic, consulta [Registrazione delle chiamate API Amazon Inspector Classic con AWS CloudTrail](#)

Puoi monitorare Amazon Inspector Classic utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi in metriche leggibili e quasi in tempo reale. Per impostazione predefinita, Amazon Inspector Classic invia i dati delle metriche CloudWatch in periodi di 5 minuti.

Per informazioni sull'utilizzo CloudWatch con Amazon Inspector Classic, consulta [Monitoraggio di Amazon Inspector Classic tramite Amazon CloudWatch](#)

## Risposta agli incidenti in Amazon Inspector Classic

La risposta agli incidenti per Amazon Inspector Classic è una AWS responsabilità. AWS ha una politica e un programma formali e documentati che regolano la risposta agli incidenti.

AWS i problemi operativi di ampio impatto sono pubblicati nel [AWS Service Health Dashboard](#).

Le questioni operative sono anche registrate nei singoli account tramite Dashboard AWS Health. Per informazioni su come utilizzare Health Dashboard, consulta la [Guida per l'AWS Health utente](#).

## Convalida della conformità per Amazon Inspector Classic

Revisori di terze parti valutano la sicurezza e la conformità di Amazon Inspector Classic nell'ambito di AWS diversi programmi di conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco di AWS servizi nell'ambito di programmi di conformità specifici, consulta [Servizi AWS nell'ambito del programma di conformità](#) . Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Download dei report in AWS Artifact](#).

La tua responsabilità di conformità quando usi Amazon Inspector Classic è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità della tua azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Le guide rapide per la sicurezza e la conformità](#): queste guide all'implementazione illustrano considerazioni architettoniche e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- [Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi allo standard HIPAA.
- [AWS Risorse per la conformità Risorse per AWS](#) : questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua area geografica.
- [Valutazione delle risorse con le regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub CSPM](#)— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente di verificare la conformità agli standard e alle best practice del settore della sicurezza. AWS

## Resilienza in Amazon Inspector Classic

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

Amazon Inspector Classic è altamente disponibile ed esegue query utilizzando risorse di calcolo in più zone di disponibilità. Instrada automaticamente le query in modo appropriato se una particolare zona di disponibilità non è raggiungibile.

Amazon Inspector Classic utilizza Amazon S3 come archivio dati sottostante, il che rende i dati altamente disponibili e durevoli. Amazon S3 fornisce un'infrastruttura durevole per archiviare dati importanti. Concepita per la durabilità degli oggetti fino al 99,999999999%. I dati vengono archiviati in modo ridondante in più strutture e in più dispositivi all'interno di ogni struttura.

## Sicurezza dell'infrastruttura in Amazon Inspector Classic

In quanto servizio gestito, Amazon Inspector Classic è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizza chiamate API AWS pubblicate per accedere ad Amazon Inspector Classic attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Per ulteriori informazioni sulla sicurezza della rete e degli agenti di Amazon Inspector Classic, consulta [the section called “Sicurezza della rete e degli agenti Amazon Inspector Classic”](#)

## Analisi della configurazione e delle vulnerabilità in Amazon Inspector Classic

Amazon Inspector Classic offre un software predefinito chiamato agente che puoi installare facoltativamente nel sistema operativo delle istanze EC2 che desideri valutare. L'agente raccoglie un ampio set di dati di configurazione, noti come telemetria. Per ulteriori informazioni sugli agenti Amazon Inspector Classic, consulta [Agenti di Amazon Inspector Classic](#)

## Best practice di sicurezza per Amazon Inspector Classic

Amazon Inspector Classic offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, sono da considerare come considerazioni utili anziché prescrizioni.

Per l'elenco delle best practice di sicurezza per Amazon Inspector Classic, consulta [the section called "Best practice di sicurezza per Amazon Inspector Classic"](#)

# Agenti di Amazon Inspector Classic

L'agente Amazon Inspector Classic è un'entità che raccoglie informazioni sui pacchetti installati e sulla configurazione software per un'istanza Amazon EC2. Sebbene non sia necessario in tutti i casi, è necessario installare l'agente Amazon Inspector Classic su ciascuna delle istanze Amazon EC2 di destinazione per valutarne appieno la sicurezza.

Per ulteriori informazioni su come installare, disinstallare e reinstallare l'agente, su come verificare se l'agente installato è in esecuzione e su come configurare il supporto proxy per l'agente, consulta [Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Linux](#) e [Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Windows](#).

## Note

Non è necessario un agente Amazon Inspector Classic per eseguire il pacchetto di regole di [raggiungibilità della rete](#).

## Important

L'agente Amazon Inspector Classic si affida ai metadati delle istanze Amazon EC2 per funzionare correttamente. Accede ai metadati dell'istanza utilizzando la versione 1 o la versione 2 di Instance Metadata Service (o). IMDSv1 IMDSv2 Vedere [Metadati dell'istanza e dati utente](#) per ulteriori informazioni sui metadati delle istanze EC2 e sui metodi di accesso.

## Argomenti

- [Privilegi di agente Amazon Inspector Classic](#)
- [Sicurezza della rete e degli agenti Amazon Inspector Classic](#)
- [Aggiornamenti degli agenti Amazon Inspector Classic](#)
- [Ciclo di vita dei dati telemetrici](#)
- [Controllo degli accessi da Amazon Inspector Classic agli account AWS](#)
- [Limiti per gli agenti di Amazon Inspector Classic](#)
- [Installazione degli agenti Amazon Inspector Classic](#)
- [Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Linux](#)

- [Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Windows](#)
- [\(Facoltativo\) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Linux](#)
- [\(Facoltativo\) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Windows](#)

## Privilegi di agente Amazon Inspector Classic

È necessario disporre delle autorizzazioni amministrative o di root per installare l'agente Amazon Inspector Classic. Nei sistemi operativi supportati basati su Linux, l'agente è costituito da un eseguibile in modalità utente eseguito con accesso root. Nei sistemi operativi basati su Windows supportati, l'agente è costituito da un servizio di aggiornamento e da un servizio agente eseguiti in modalità utente con privilegi LocalSystem.

## Sicurezza della rete e degli agenti Amazon Inspector Classic

L'agente Amazon Inspector Classic avvia tutte le comunicazioni con il servizio Amazon Inspector Classic. Ciò significa che l'agente deve disporre di un percorso di rete in uscita verso un endpoint pubblico per poter inviare dati di telemetria. Ad esempio, l'agente potrebbe connettersi a `aarsenal.<region>.amazonaws.com`, o l'endpoint potrebbe essere un bucket Amazon S3 in `s3.dualstack.<region>.amazonaws.com`. Assicurati di sostituirlo `<region>` con la AWS regione effettiva in cui utilizzi Amazon Inspector Classic. Per ulteriori informazioni, consulta l'articolo sugli [intervalli di indirizzi IP AWS](#). Poiché tutte le connessioni dall'agente vengono stabilite in uscita, non è necessario aprire le porte dei gruppi di sicurezza per consentire le comunicazioni in entrata verso l'agente da Amazon Inspector Classic.

L'agente comunica periodicamente con Amazon Inspector Classic tramite un canale protetto da TLS, che viene autenticato utilizzando l'identità associata al ruolo AWS dell'istanza EC2 o, se non viene assegnato alcun ruolo, con il documento di metadati dell'istanza. Una volta autenticato, l'agente invia messaggi di heartbeat al servizio e riceve istruzioni dal servizio in risposta. Se una valutazione è stata pianificata, l'agente riceve le istruzioni per tale valutazione. Queste istruzioni sono file JSON strutturati e indicano all'agente di abilitare o disabilitare specifici sensori preconfigurati nell'agente. Ogni azione di istruzione è predefinita all'interno dell'agente. Non è possibile eseguire istruzioni arbitrarie.

Durante una valutazione, l'agente raccoglie i dati di telemetria dal sistema per inviarli ad Amazon Inspector Classic tramite un canale protetto da TLS. L'agente non modifica il sistema da cui raccoglie

dati. Dopo aver raccolto i dati di telemetria, l'agente li invia nuovamente ad Amazon Inspector Classic per l'elaborazione. Oltre ai dati di telemetria generati, l'agente non è in grado di raccogliere o trasmettere altri dati relativi al sistema o ai target di valutazione. Al momento, non è disponibile alcun metodo esposto per l'intercettazione e l'analisi dei dati di telemetria a livello di agente.

## Aggiornamenti degli agenti Amazon Inspector Classic

Man mano che gli aggiornamenti per l'agente Amazon Inspector Classic diventano disponibili, vengono scaricati automaticamente da Amazon S3 e applicati. Questa operazione aggiorna anche qualsiasi eventuale dipendenza obbligatoria. La funzionalità di aggiornamento automatico elimina la necessità di tracciare e gestire manualmente il controllo delle versioni degli agenti che hai installato sulle tue istanze EC2. Tutti gli aggiornamenti sono soggetti a processi Amazon di controllo delle modifiche per garantire la conformità con gli standard di sicurezza applicabili.

Per garantire la sicurezza dell'agente, tutte le comunicazioni tra l'agente e il sito di rilascio degli aggiornamenti automatici (S3) vengono eseguite tramite una connessione TLS e dopo l'autenticazione del server. Tutti i file binari coinvolti nel processo di aggiornamento automatico sono associati a una firma digitale e le firme vengono verificate dal servizio di aggiornamento prima dell'installazione. Il processo di aggiornamento automatico viene eseguito solo durante i periodi non di valutazione. Se vengono rilevati errori, il processo di aggiornamento può eseguire il rollback e un nuovo tentativo di aggiornamento. Infine, il processo di aggiornamento dell'agente si limita ad aggiornare le funzionalità dell'agente. Nessuna delle tue informazioni specifiche viene mai inviata dall'agente ad Amazon Inspector Classic come parte del flusso di lavoro di aggiornamento. Le uniche informazioni inviate durante il processo di aggiornamento sono i dati di telemetria di base relativi alla riuscita o meno dell'installazione e, se applicabile, qualsiasi informazione sulla diagnostica degli errori di aggiornamento.

## Ciclo di vita dei dati telemetrici

I dati di telemetria generati dall'agente Amazon Inspector Classic durante le esecuzioni di valutazione sono formattati in file JSON. I file vengono near-real-time consegnati tramite TLS ad Amazon Inspector Classic, dove vengono crittografati con per-assessment-run una chiave temporanea derivata da KMS. I file vengono archiviati in modo sicuro in un bucket Amazon S3 dedicato ad Amazon Inspector Classic. Il motore di regole di Amazon Inspector Classic accede ai dati di telemetria crittografati nel bucket S3, li decrittografa in memoria ed elabora i dati in base alle regole di valutazione configurate per generare risultati. I dati di telemetria archiviati in S3 vengono conservati solo con finalità di assistenza per le richieste di supporto. Non vengono usati né aggregati da Amazon

per altri scopi. Dopo 30 giorni, i dati di telemetria vengono eliminati definitivamente in base a una politica standard sul ciclo di vita dei bucket S3 per i dati di Amazon Inspector Classic. Attualmente, Amazon Inspector Classic non fornisce un'API o un meccanismo di accesso ai bucket S3 per la telemetria raccolta.

## Controllo degli accessi da Amazon Inspector Classic agli account AWS

Come servizio di sicurezza, Amazon Inspector Classic accede ai tuoi AWS account e alle tue risorse solo quando deve trovare istanze EC2 da valutare tramite query per i tag. Ciò avviene tramite l'accesso IAM standard tramite il ruolo creato durante la configurazione iniziale del servizio Amazon Inspector Classic. Durante una valutazione, tutte le comunicazioni con l'ambiente vengono avviate dall'agente Amazon Inspector Classic installato localmente sulle istanze EC2. Gli oggetti di servizio Amazon Inspector Classic che vengono creati, come obiettivi di valutazione, modelli di valutazione e risultati generati dal servizio, vengono archiviati in un database gestito e accessibile solo da Amazon Inspector Classic.

## Limiti per gli agenti di Amazon Inspector Classic

Per informazioni sui limiti degli agenti di Amazon Inspector Classic, consulta [Limiti del servizio Amazon Inspector Classic](#)

## Installazione degli agenti Amazon Inspector Classic


Puoi installare l'agente Amazon Inspector Classic utilizzando il [comando Systems Manager Run](#) su più istanze (incluse istanze basate su Linux e Windows). In alternativa, puoi installare l'agente singolarmente accedendo a ciascuna istanza EC2. Le procedure in questo capitolo forniscono le istruzioni per entrambi i metodi.

Come altra opzione, puoi installare rapidamente l'agente su tutte le istanze Amazon EC2 incluse in un obiettivo di valutazione selezionando la casella di controllo Installa agenti nella pagina Definisci un obiettivo di valutazione sulla console.

### Argomenti

- [Installazione dell'agente su più istanze EC2 usando Systems Manager Run Command](#)
- [Installazione dell'agente su un'istanza EC2 basata su Linux](#)


- [Installazione dell'agente su un'istanza EC2 basata su Windows](#)

 Note


Le procedure in questo capitolo si applicano a tutte le AWS regioni supportate da Amazon Inspector Classic.

## Installazione dell'agente su più istanze EC2 usando Systems Manager Run Command

Puoi installare l'agente Amazon Inspector Classic sulle tue istanze EC2 utilizzando il comando [Systems Manager Run Command](#). Ciò ti permetterà di installare contemporaneamente l'agente in remoto e su più istanze (istanze basate sia su Linux che su Windows) con lo stesso comando.

 Important

L'installazione dell'agente tramite il Systems Manager Run Command non è attualmente supportata per il sistema operativo Debian.

 Important

Per utilizzare questa opzione, assicurati che sull'istanza EC2 sia installato l'agente SSM e che abbia un ruolo IAM che consenta Run Command. L'agente SSM viene installato per impostazione predefinita nelle istanze Amazon EC2 basate su Windows e nelle istanze basate su Amazon Linux. Amazon EC2 Systems Manager richiede un ruolo IAM per le istanze EC2 che elabora i comandi e un ruolo separato per gli utenti che eseguono i comandi. [Per ulteriori informazioni, consulta Installazione e configurazione dell'agente SSM e Configurazione dei ruoli di sicurezza per SSM.](#)

Per installare l'agente su più istanze EC2 utilizzando il comando Systems Manager Run

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione sotto Node Tools, scegli Esegui comando.

3. Scegli Esegui comando.
4. Per il documento Command, scegli il documento denominato AmazonInspector-Manage AWSSAgent di proprietà di Amazon. Questo documento contiene lo script per l'installazione dell'agente Amazon Inspector Classic sulle istanze EC2.
5. Per Targets, puoi selezionare le istanze EC2 utilizzando metodi diversi. Per installare l'agente su tutte le istanze incluse nel target di valutazione, è possibile specificare gli stessi tag utilizzati per creare il target di valutazione.
6. Effettuare le scelte desiderate per le restanti opzioni disponibili utilizzando le istruzioni riportate nella sezione [Esecuzione di comandi dalla console](#) e quindi selezionare Run (Esegui).

#### Note

Puoi anche installare l'agente su più istanze EC2 (sia basate su Linux che su Windows) quando crei un target di valutazione, oppure puoi utilizzare il pulsante Installa agenti con comando Run per un target esistente. Per ulteriori informazioni, consulta [Creazione di un target di valutazione](#).

## Installazione dell'agente su un'istanza EC2 basata su Linux

Esegui la seguente procedura per installare l'agente Amazon Inspector Classic su un'istanza EC2 basata su Linux.

Per installare l'agente su un'istanza EC2 basata su Linux

1. Accedi alla tua istanza EC2 che esegue un sistema operativo basato su Linux in cui desideri installare l'agente Amazon Inspector Classic.

#### Note

Per informazioni sui sistemi operativi supportati da Amazon Inspector Classic, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#)

2. Scarica lo script di installazione dell'agente eseguendo uno dei seguenti comandi:
  - `wget https://inspector-agent.amazonaws.com/linux/latest/install`
  - `curl -O https://inspector-agent.amazonaws.com/linux/latest/install`

3. (Opzionale) Verificare che lo script di installazione dell'agente non sia alterato o danneggiato. Per ulteriori informazioni, consulta [\(Facoltativo\) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Linux.](#)
4. Per installare l'agente, eseguire `sudo bash install`.

#### Note

Se stai installando l'agente in un SELinux ambiente, Amazon Inspector Classic potrebbe essere rilevato come un demone non confinato. Puoi evitarlo modificando il dominio del processo agente da quello predefinito a `initrc_t bin_t`. Utilizza i seguenti comandi per assegnare il `bin_t` contesto agli script di esecuzione di Amazon Inspector Classic prima di installare l'agente per: SELinux

```
sudo semanage fcontext -a -t bin_t /etc/rc.d/init.d/awsagent
sudo semanage fcontext -a -t bin_t /etc/init.d/awsagent
```

#### Note

Man mano che gli aggiornamenti per l'agente diventano disponibili, vengono scaricati automaticamente da Amazon S3 e applicati. Per ulteriori informazioni, consulta [Aggiornamenti degli agenti Amazon Inspector Classic.](#)

Per ignorare questo processo di aggiornamento automatico, esegui questo comando quando installi l'agente:

```
sudo bash install -u false
```

#### Note

(Facoltativo) Per rimuovere lo script di installazione dell'agente, esegui `rm install`.

5. Verificare che vengano installati i seguenti file richiesti per la corretta installazione e il corretto funzionamento dell'agente:
  - `libcurl4` (necessario per installare l'agente su Ubuntu 18.04)
  - `libcurl3`
  - `libgcc1`

- `libc6`
- `libstdc++6`
- `libssl1.0.1`
- `libssl1.0.2` (necessario per installare l'agente su Debian 9)
- `libssl1.1` (necessario per installare l'agente su Ubuntu 20.04 LTS)
- `libpcap0.8`

## Installazione dell'agente su un'istanza EC2 basata su Windows

Esegui la seguente procedura per installare l'agente Amazon Inspector Classic su un'istanza EC2 basata su Windows.

Per installare l'agente su un'istanza EC2 basata su Windows

1. Accedi alla tua istanza EC2 che esegue un sistema operativo basato su Windows in cui desideri installare l'agente.

### Note

Per ulteriori informazioni sui sistemi operativi supportati da Amazon Inspector Classic, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#)

2. Scaricare il seguente file exe:

```
https://inspector-agent.amazonaws.com/windows/installer/latest/AWSAgentInstall.exe
```

3. Aprire una finestra del prompt dei comandi (con autorizzazioni di amministrazione), passare alla posizione in cui è stato salvato il file `AWSAgentInstall.exe` scaricato ed eseguire il file `.exe` per installare l'agente.

### Note

Man mano che gli aggiornamenti per l'agente diventano disponibili, vengono scaricati automaticamente da Amazon S3 e applicati. Per ulteriori informazioni, consulta [Aggiornamenti degli agenti Amazon Inspector Classic](#).

Per ignorare questo processo di aggiornamento automatico, esegui questo comando quando installi l'agente:

```
AWSAgentInstall.exe AUTOUPDATE=No
```

## Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Linux

Puoi installare, rimuovere, verificare e modificare il comportamento degli agenti Amazon Inspector Classic. Accedi alla tua istanza Amazon EC2 che esegue un sistema operativo basato su Linux ed esegui una delle seguenti procedure. Per ulteriori informazioni sui sistemi operativi supportati per Amazon Inspector Classic, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#)

### Important

L'agente Amazon Inspector Classic si affida ai metadati delle istanze Amazon EC2 per funzionare correttamente. Accede ai metadati dell'istanza utilizzando la versione 1 o la versione 2 di Instance Metadata Service (o). IMDSv1 IMDSv2 Vedere [Metadati dell'istanza e dati utente](#) per ulteriori informazioni sui metadati delle istanze EC2 e sui metodi di accesso.

### Note

I comandi di questa sezione funzionano in tutte le AWS regioni supportate da Amazon Inspector Classic.

### Argomenti

- [Verifica dell'esecuzione dell'agente Amazon Inspector Classic](#)
- [Interruzione dell'agente Amazon Inspector Classic](#)
- [Avvio dell'agente Amazon Inspector Classic](#)
- [Modifica delle impostazioni degli agenti Amazon Inspector Classic](#)
- [Configurazione del supporto proxy per un agente Amazon Inspector Classic](#)
- [Disinstallazione dell'agente Amazon Inspector Classic](#)

## Verifica dell'esecuzione dell'agente Amazon Inspector Classic

- Per verificare che l'agente sia installato e in esecuzione, accedi alla tua istanza EC2 ed esegui il seguente comando:

```
sudo /opt/aws/awsagent/bin/awsagent status
```

Questo comando restituisce lo stato dell'agente attualmente in esecuzione oppure un errore indicante che l'agente non può essere contattato.

## Interruzione dell'agente Amazon Inspector Classic

- Per arrestare l'agente, esegui questo comando:

```
sudo /etc/init.d/awsagent stop
```

## Avvio dell'agente Amazon Inspector Classic

- Per avviare l'agente, esegui questo comando:

```
sudo /etc/init.d/awsagent start
```

## Modifica delle impostazioni degli agenti Amazon Inspector Classic

Dopo l'installazione e l'esecuzione dell'agente Amazon Inspector Classic sull'istanza EC2, puoi modificare le impostazioni nel `agent.cfg` file per alterare il comportamento dell'agente. Nei sistemi operativi basati su Linux, il file `agent.cfg` si trova nella directory `/opt/aws/awsagent/etc`. Dopo avere modificato e salvato il file `agent.cfg`, dovrai arrestare e avviare l'agente per rendere effettive le modifiche.

### Important

È consigliabile modificare il file `agent.cfg` solo sotto la guida di AWS Support.

## Configurazione del supporto proxy per un agente Amazon Inspector Classic

Per ottenere il supporto proxy per un agente su un sistema operativo basato su Linux, usa un file di configurazione specifico dell'agente con specifiche variabili di ambiente. [Per ulteriori informazioni, consulta \[https://wiki.archlinux.org/index.php/proxy\\\_impostazioni\]\(https://wiki.archlinux.org/index.php/proxy\_impostazioni\)](#).

Completa una delle seguenti procedure:

Per installare un agente su un'istanza EC2 che utilizza un server proxy

1. Creare un file denominato `awsagent.env` e salvarlo nella directory `/etc/init.d/`.
2. Modificare il file `awsagent.env` in modo da includere queste variabili di ambiente nel formato seguente:
  - `export https_proxy=hostname:port`
  - `export http_proxy=hostname:port`
  - `export no_proxy=169.254.169.254`

### Note

Sostituire i valori negli esempi precedenti solo con combinazioni valide di nome host e numero di porta. Specificare l'indirizzo IP dell'endpoint dei metadati dell'istanza (169.254.169.254) per la variabile `no_proxy`.


3. Installa l'agente Amazon Inspector Classic completando i passaggi della procedura. [Installazione dell'agente su un'istanza EC2 basata su Linux](#)

Per configurare il supporto proxy su un'istanza EC2 con un agente in esecuzione

1. Per configurare il supporto proxy, la versione dell'agente in esecuzione sull'istanza EC2 deve essere 1.0.800.1 o successiva. Se è stato abilitato il processo di aggiornamento automatico per l'agente, è possibile verificare che la versione dell'agente sia 1.0.800.1 o superiore seguendo la procedura [Verifica dell'esecuzione dell'agente Amazon Inspector Classic](#). Se non hai abilitato il processo di aggiornamento automatico per l'agente, devi installare nuovamente l'agente su questa istanza EC2 seguendo la [Installazione dell'agente su un'istanza EC2 basata su Linux](#) procedura.
2. Creare un file denominato `awsagent.env` e salvarlo nella directory `/etc/init.d/`.

3. Modificare il file `awsagent.env` in modo da includere queste variabili di ambiente nel formato seguente:

- `export https_proxy=hostname:port`
- `export http_proxy=hostname:port`
- `export no_proxy=169.254.169.254`

 Note

Sostituire i valori negli esempi precedenti solo con combinazioni valide di nome host e numero di porta. Specificare l'indirizzo IP dell'endpoint dei metadati dell'istanza (169.254.169.254) per la variabile `no_proxy`.

4. Riavviare l'agente arrestandolo prima con il comando seguente:

```
sudo /etc/init.d/awsagent restart
```

Le impostazioni proxy vengono acquisite e utilizzate sia dall'agente che dal processo di aggiornamento automatico.

## Disinstallazione dell'agente Amazon Inspector Classic

Per disinstallare l'agente

1. Accedi alla tua istanza EC2 che esegue un sistema operativo basato su Linux in cui desideri disinstallare l'agente.

 Note

Per ulteriori informazioni sui sistemi operativi supportati per Amazon Inspector Classic, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#)

2. Per disinstallare l'agente, utilizza uno dei seguenti comandi:

- Su Amazon Linux, CentOS e Red Hat eseguire questo comando:

```
sudo yum remove 'AwsAgent*'
```

- Su Ubuntu Server eseguire questo comando:

```
sudo apt-get purge 'awsagent**'
```

## Utilizzo degli agenti Amazon Inspector Classic su sistemi operativi basati su Windows

Puoi avviare, arrestare e modificare il comportamento degli agenti Amazon Inspector Classic. Accedi alla tua istanza EC2 che esegue un sistema operativo basato su Windows ed esegui una delle procedure descritte in questo capitolo. Per ulteriori informazioni sui sistemi operativi supportati per Amazon Inspector Classic, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#)

### Important

L'agente Amazon Inspector Classic si affida ai metadati delle istanze Amazon EC2 per funzionare correttamente. Accede ai metadati dell'istanza utilizzando la versione 1 o la versione 2 di Instance Metadata Service (). IMDSv1 or IMDSv2 Vedere [Metadati dell'istanza e dati utente](#) per ulteriori informazioni sui metadati delle istanze EC2 e sui metodi di accesso.

### Note

I comandi di questo capitolo funzionano in tutte le AWS regioni supportate da Amazon Inspector Classic.

### Argomenti

- [Avvio o arresto di un agente Amazon Inspector Classic o verifica che l'agente sia in esecuzione](#)
- [Modifica delle impostazioni dell'agente Amazon Inspector Classic](#)
- [Configurazione del supporto proxy per un agente Amazon Inspector Classic](#)
- [Disinstallazione dell'agente Amazon Inspector Classic](#)

## Avvio o arresto di un agente Amazon Inspector Classic o verifica che l'agente sia in esecuzione

Per avviare, arrestare o verificare un agente

1. Sulla tua istanza EC2, scegli Start, Esegui, quindi inserisci. **services.msc**
2. Se l'agente è in esecuzione, vengono elencati due servizi con il relativo stato impostato su Started (Avviato) o Running (In esecuzione) nella finestra Services (Servizi): AWS Agent Service (Servizio agente AWS) e AWS Agent Updater Service (Servizio di aggiornamento agente AWS).
3. Per avviare l'agente, fare clic con il pulsante destro del mouse su AWS Agent Service (Servizio agente AWS) e quindi scegliere Start (Avvia). Se il servizio è stato avviato, lo stato viene aggiornato e impostato su Started (Avviato) o Running (In esecuzione).
4. Per arrestare l'agente, fare clic con il pulsante destro del mouse su AWS Agent Service (Servizio agente AWS) e quindi scegliere Stop (Arresta). Se il servizio è stato arrestato, lo stato viene cancellato (appare vuoto). Non è consigliabile arrestare AWS Service Agent Updater (Aggiornamento agente servizio AWS) perché questa operazione disabilita l'installazione di tutti i futuri miglioramenti e delle correzioni per l'agente.
5. Per verificare che l'agente sia installato e in esecuzione, accedi all'istanza EC2 e apri un prompt dei comandi utilizzando le autorizzazioni amministrative. Passare a `C:\Program Files\Amazon Web Services\AWS Agent` ed eseguire questo comando:

```
AWSAgentStatus.exe
```

Questo comando restituisce lo stato dell'agente attualmente in esecuzione oppure un errore indicante che l'agente non può essere contattato.

## Modifica delle impostazioni dell'agente Amazon Inspector Classic

Dopo l'installazione e l'esecuzione dell'agente Amazon Inspector Classic sull'istanza EC2, puoi modificare le impostazioni nel `agent.cfg` file per alterare il comportamento dell'agente. Nei sistemi operativi basati su Windows, il file si trova nella directory `C:\ProgramData\Amazon Web Services\AWS Agent`. Dopo avere modificato e salvato il file `agent.cfg`, dovrai arrestare e avviare l'agente per rendere effettive le modifiche.

**⚠ Important**

È consigliabile modificare il file `agent.cfg` solo sotto la guida di AWS Support.

## Configurazione del supporto proxy per un agente Amazon Inspector Classic

Per ottenere il supporto proxy per un agente in un sistema operativo basato su Windows, usa il proxy WinHTTP. Per configurare il proxy WinHTTP utilizzando l'utilità `netsh`, consulta [Netsh Commands for Windows Hypertext Transfer Protocol \(WINHTTP\)](#).

**⚠ Important**

Per le istanze basate su Windows sono supportati solo i proxy HTTPS.

Completa una delle seguenti procedure:

Per installare un agente su un'istanza EC2 che utilizza un server proxy

1. Scaricare il seguente file exe: `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`
2. Aprire una finestra o PowerShell una finestra del prompt dei comandi (utilizzando le autorizzazioni amministrative). Passare alla posizione in cui è stato salvato il file scaricato `AWSAgentInstall.exe` e quindi eseguire questo comando:

```
.\AWSAgentInstall.exe /install USEPROXY=1
```

Per configurare il supporto proxy su un'istanza EC2 con un agente in esecuzione

1. Per configurare il supporto proxy, la versione dell'agente Amazon Inspector Classic in esecuzione sull'istanza EC2 deve essere 1.0.0.59 o successiva. Se è stato abilitato il processo di aggiornamento automatico per l'agente, è possibile verificare che la versione dell'agente sia 1.0.0.59 o superiore seguendo la procedura [Avvio o arresto di un agente Amazon Inspector Classic o verifica che l'agente sia in esecuzione](#). Se non hai abilitato il processo di aggiornamento automatico per l'agente, devi installare nuovamente l'agente su questa istanza EC2 seguendo la [Installazione dell'agente su un'istanza EC2 basata su Windows](#) procedura.
2. Aprire l'editor del Registro di sistema (`regedit.exe`).

3. Passare alla seguente chiave del Registro di sistema: "HKEY\_LOCAL\_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater".
4. Al suo interno, creare un valore DWORD(32bit) denominato "UseProxy".
5. Fare doppio clic sul valore e impostarlo su 1.
6. Immettere **services.msc**, individuare le voci AWS Agent Service (Servizio agente AWS) e AWS Agent Updater Service (Aggiornamento agente servizio AWS) nella finestra Services (Servizi) e quindi riavviare ciascun processo. Dopo il riavvio di entrambi i processi, eseguire il file `AWSAgentStatus.exe` (vedi il passaggio 5 in [Avvio o arresto di un agente Amazon Inspector Classic o verifica che l'agente sia in esecuzione](#)). Visualizzare lo stato dell'agente e verificare che stia utilizzando il proxy configurato.

## Disinstallazione dell'agente Amazon Inspector Classic

Per disinstallare l'agente

1. Accedi alla tua istanza EC2 che esegue un sistema operativo basato su Windows in cui desideri disinstallare l'agente Amazon Inspector Classic.

### Note

Per ulteriori informazioni sui sistemi operativi supportati per Amazon Inspector Classic, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#)

2. Nell'istanza EC2, passa a Control Panel (Pannello di controllo), Add/Remove Programs (Installazione applicazioni).
3. Nell'elenco dei programmi installati scegliere AWS Agent (Agente AWS) e quindi Disinstalla.

## (Facoltativo) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Linux

Questo argomento descrive il processo consigliato per verificare la validità dello script di installazione dell'agente Amazon Inspector Classic per i sistemi operativi basati su Linux.

Quando si esegue il download di un'applicazione da Internet, ti consigliamo di autenticare l'identità dell'autore del software e controllare che l'applicazione non risulti modificata o danneggiata

rispetto alla versione pubblicata. Ciò consente di evitare di installare una versione dell'applicazione contenente un virus o altro malware.

Se dopo aver eseguito i passaggi descritti in questo argomento, stabilisci che il software per l'agente Amazon Inspector Classic è alterato o danneggiato, **NON** eseguire il file di installazione. Contatta AWS Support.

I file agente Amazon Inspector Classic per i sistemi operativi basati su Linux vengono firmati utilizzando GnuPG, un'implementazione open source dello standard Pretty Good Privacy (OpenPGP) per firme digitali sicure. GnuPG (noto anche come GPG) fornisce l'autenticazione e il controllo dell'integrità tramite una firma digitale. Amazon EC2 pubblica una chiave pubblica e firme che puoi utilizzare per verificare gli strumenti dell'interfaccia a riga di comando di Amazon EC2 scaricati. Per ulteriori informazioni su PGP e GnuPG (GPG), consulta <http://www.gnupg.org>.

La prima fase prevede la verifica dell'affidabilità dell'autore del software. Scarica la chiave pubblica dell'autore del software, controlla l'autenticità di tale proprietario e quindi aggiungi la chiave pubblica al tuo keyring. Il keyring è una raccolta di chiavi pubbliche nota. Dopo aver confermato l'autenticità della chiave pubblica, puoi usarla per verificare la firma dell'applicazione.

## Argomenti

- [Installazione degli strumenti GPG](#)
- [Autenticazione e importazione della chiave pubblica](#)
- [Verifica della firma del pacchetto](#)

## Installazione degli strumenti GPG

Se il sistema operativo è Linux o Unix, gli strumenti GPG probabilmente sono già installati. Per sapere se gli strumenti sono installati nel sistema, digita `gpg` al prompt dei comandi. Se gli strumenti GPG sono installati, viene visualizzato un prompt dei comandi GPG. Se gli strumenti GPG non sono installati, verrà visualizzato un messaggio di errore che indica che il comando non è disponibile. Puoi installare il pacchetto GnuPG da un repository.

Per installare gli strumenti GPG su un computer Linux basato su Debian

- Da un terminale, esegui il comando seguente: `apt-get install gnupg`.

## Per installare gli strumenti GPG su un computer Linux basato su Red Hat

- Da un terminale, esegui il comando seguente: `yum install gnupg`.

## Autenticazione e importazione della chiave pubblica

La fase successiva del processo consiste nell'autenticare la chiave pubblica Amazon Inspector Classic e aggiungerla come chiave affidabile nel GPG tuo portachiavi.

Per autenticare e importare la chiave pubblica di Amazon Inspector Classic

1. Recupera una copia della chiave pubblica GPG in uno dei modi seguenti:
  - [Scaricala da `https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg`](https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg).
  - Copia la chiave dal seguente testo e incollala in un file denominato `inspector.gpg`. Assicurati di includere quanto segue:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: GnuPG v2.0.18 (GNU/Linux)
```

```
mQINBFYDlFEBEADFPfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3B0z1e/MXI  
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90  
gf9m1iKVHjdVQ9qNH1B20FknPDxMDRHcrlJYDKYCX3+MODEHn1K25tIH2KWezXP  
FPSU+TkWjLRzSMYH1L8IwjFUIIi78jQS9a31R/c014zuC5f0VghY1SomLI8irfoD  
JSa3csVRujSm0Af9o3beiMR/kNDMpgD0xgiQTu/Kh39c16o8AKe+QKK48kq07hra  
h1dpzLbfeZEVU6dWMZt1UksG/zKxuzD6d8vXYH7Z+x09POPFALQCQMC3WisIKgj  
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr  
PgwnUvDZuazxuuPzucZG0J5kbptat3DcUpstjdmGAIId3JawBbps77qRZdA+swr  
o9o3jbowgmf0y5ZS6KwvZnC6XyTAKXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X  
10rf0m1VufMzAyTu0YQGBWaqKzSB8tCkvFw54PrRuUTCv826XU7SIJNzmNQo58uL  
bKyLVBSCVabfs0lkECIESq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB  
tCdBbWF6b24gSW5zcGVjdG9yIDxpbNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC  
ACIFAlYDlFEcGwMGcWkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAoJECR0CWBYNgQY  
8yUP/2GpI140f3mKBUIsTe0XQLvwiBCHmY+V9f0uKqDTinxssjEMCnz0vsKeCZF/  
L35pwNa/oW00Ja8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF  
x4hWS0jUVEHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WT1P/0r/  
HIkKzzqQ0aa0f5t9zc5DKwi+dFmJbRUyaq22xs8C81U0DjHunhHdZ21cnsGk91S  
fvuaum9aR4/uVIY0TVWnjC5J3+V1czyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu  
DPn0/+zxb7Jz3QCHXnuTbxZTjvv1600i8//uRtnPXjz4wZLwQfibgHmk1++hzND7  
w0YA02Js6v5FZQ1LQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyx1mNVRpVZY4L1  
D0HyqGQhpkyV3drjjNZ1Eofwbfu7m60DwsgM15ynzhKk1JzwpJFFB3mMc7qLi+qX  
MJtEX8KJ/iVUQStHHAG7daL1bXpWSI3BRuaHsWbBGQ/mcHBgUU0QJyEp5LAdg9Fs
```

```
VP55gWtF7pIqifiqlcfgG00v+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
Lf09+3sEi1NrsMib0KRLDeBt3EuDsaBZg0kqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

- Al prompt dei comandi nella directory in cui hai salvato `inspector.gpg`, usa il seguente comando per importare la chiave pubblica Amazon Inspector Classic nel tuo portachiavi:

```
gpg --import inspector.gpg
```

I risultati restituiti dal comando saranno simili a quanto segue:

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

Annota il valore della chiave. Tale valore verrà usato nel passaggio successivo. Nell'esempio precedente, il valore della chiave è `58360418`.

- Verifica l'impronta eseguendo il comando seguente, sostituendo `key-value` con il valore annotato nella fase precedente:

```
gpg --fingerprint key-value
```

Questo comando restituisce risultati simili ai seguenti:

```
pub 4096R/58360418 2015-09-24
    Key fingerprint = DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836
0418
    uid Amazon Inspector <inspector@amazon.com>
```

Inoltre, la stringa dell'impronta deve essere uguale al valore `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418` riportato nell'esempio precedente. Confronta l'impronta della chiave restituita con quella pubblicata in questa pagina. Le chiavi devono corrispondere. Se non corrispondono, non installare lo script di installazione dell'agente Amazon Inspector Classic e contatta AWS Support.

## Verifica della firma del pacchetto

Dopo aver installato gli GPG strumenti, autenticato e importato la chiave pubblica Amazon Inspector Classic e verificato che la chiave pubblica sia attendibile, sei pronto per verificare la firma dello script di installazione.

Per verificare la firma dello script di installazione di

1. Al prompt dei comandi esegui il comando seguente per scaricare il file SIGNATURE per lo script di installazione:

```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
```

2. Verifica la firma eseguendo il comando seguente al prompt dei comandi nella directory in cui hai salvato il file di `install.sig` installazione di Amazon Inspector Classic. Entrambi i file devono essere presenti.

```
gpg --verify ./install.sig
```

L'output deve essere simile al seguente:

```
gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418
```

Se l'output contiene la frase `Good signature from "Amazon Inspector <inspector@amazon.com>"`, significa che la firma è stata verificata con successo e puoi procedere con l'esecuzione dello script di installazione di Amazon Inspector Classic.

Se l'output include la frase `BAD signature`, controllare di avere eseguito la procedura correttamente. Se il problema persiste, non eseguire il file di installazione scaricato in precedenza e contatta AWS Support.

Di seguito sono elencati i dettagli sugli avvisi che potrebbero essere visualizzati:

- **ATTENZIONE:** questa chiave non è certificata con una firma affidabile! Non vi è alcuna indicazione che la firma appartenga al proprietario. Si riferisce al tuo livello di fiducia personale nella

convinzione di possedere una chiave pubblica autentica per Amazon Inspector Classic. In un mondo ideale, ti recheresti in un ufficio AWS e riceveresti la chiave personalmente. Tuttavia, la prassi normale è scaricare la chiave da un sito Web. In questo caso, il sito Web è un sito Web di AWS.

- gpg: no ultimately trusted keys found. (gpg: nessuna chiave affidabile trovata) Questo messaggio indica che la chiave specifica non è ritenuta affidabile da te o da un'altra persona da te considerata affidabile.

Per ulteriori informazioni, consulta <http://www.gnupg.org>.

## (Facoltativo) Verifica la firma dello script di installazione dell'agente Amazon Inspector Classic sui sistemi operativi basati su Windows

Questo argomento descrive il processo consigliato per verificare la validità dello script di installazione dell'agente Amazon Inspector Classic per i sistemi operativi basati su Windows.

Quando si esegue il download di un'applicazione da Internet, ti consigliamo di autenticare l'identità dell'autore del software e controllare che l'applicazione non risulti modificata o danneggiata rispetto alla versione pubblicata. Ciò consente di evitare di installare una versione dell'applicazione contenente un virus o altro malware.

Se dopo aver eseguito i passaggi descritti in questo argomento, stabilisci che il software per l'agente Amazon Inspector Classic è alterato o danneggiato, NON eseguire il file di installazione. Contatta AWS Support.

Per verificare la validità dello script di installazione dell'agente scaricato nei sistemi operativi basati su Windows, accertarti che l'identificazione del relativo certificato firmatario di Amazon Services LLC sia uguale al seguente valore:

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B36

Per verificare questo valore, esegui la procedura seguente:

1. Clicca con il pulsante destro del mouse sul file `AWSAgentInstall.exe`, e apri la finestra Proprietà.
2. Scegli la scheda Firme digitali.
3. Dall'elenco delle firme, scegli Amazon Web Services, Inc., quindi scegli Dettagli.

4. Scegli la scheda Generale, se non è già selezionata, quindi scegli Visualizza certificato.
5. Scegli la scheda Dettagli, quindi seleziona Tutto nell'elenco a discesa Mostra, se non è già selezionato.
6. Scorri fino a visualizzare il campo Identificazione personale, quindi scegli Identificazione personale. In questo modo viene visualizzato l'intero valore dell'identificazione personale nella finestra inferiore.
  - Se il valore dell'identificazione personale nella finestra inferiore è identico al valore seguente:

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

significa che lo script di installazione dell'agente scaricato è autentico e può essere installato in modo sicuro.

- Se il valore dell'identificazione personale nella finestra inferiore dei dettagli non è identico al valore precedente, non eseguire `AWSAgentInstall.exe`.

# Obiettivi di valutazione di Amazon Inspector Classic

Puoi utilizzare Amazon Inspector Classic per valutare se i tuoi obiettivi di AWS valutazione (le tue raccolte di AWS risorse) presentano potenziali problemi di sicurezza da risolvere.

## Important

Attualmente i target di valutazione possono essere composti solo da istanze EC2 eseguite sui sistemi operativi supportati. Per informazioni sui sistemi operativi supportati e sulle regioni AWS supportate, consulta [the section called "Sistemi operativi e regioni supportati"](#).

## Note

Per informazioni sul lancio di istanze EC2, consulta la documentazione di [Amazon Elastic Compute Cloud](#).

## Argomenti

- [Tagging delle risorse per la creazione di un target di valutazione](#)
- [Limiti degli obiettivi di valutazione di Amazon Inspector Classic](#)
- [Creazione di un target di valutazione](#)
- [Eliminazione di un target di valutazione](#)

## Tagging delle risorse per la creazione di un target di valutazione

Per creare un obiettivo di valutazione da sottoporre ad Amazon Inspector Classic, devi innanzitutto etichettare le istanze EC2 che desideri includere nel tuo obiettivo. I tag sono parole o frasi che fungono da metadati per identificare e organizzare le istanze e altre risorse. AWS Amazon Inspector Classic utilizza i tag che crei per identificare le istanze che appartengono al tuo target.

Ogni AWS tag è costituito da una coppia chiave e valore a tua scelta. Ad esempio, potresti scegliere di denominare la tua chiave «Nome» e il tuo valore "MyFirstInstance». Dopo aver taggato le istanze, utilizzi la console Amazon Inspector Classic per aggiungere le istanze al tuo obiettivo di valutazione. Non è necessario che un'istanza qualsiasi corrisponda a più di una coppia chiave-valore.

Quando tagghi le tue istanze EC2 per creare obiettivi di valutazione, puoi creare chiavi di tag personalizzate o utilizzare chiavi di tag create da altri utenti nello stesso account. AWS Puoi anche utilizzare le chiavi di tag che AWS vengono create automaticamente. Ad esempio, crea AWS automaticamente una chiave Name tag per le istanze EC2 che avvii.

Puoi aggiungere tag alle istanze EC2 quando le crei oppure puoi aggiungere, modificare o rimuovere tali tag uno alla volta nella pagina della console per ogni istanza EC2. Puoi anche aggiungere tag a più istanze EC2 contemporaneamente utilizzando il Tag Editor.

Per ulteriori informazioni, consulta [Editor di tag](#). Per ulteriori informazioni sul tagging delle istanze EC2, consulta [Risorse e tag](#).

## Limiti degli obiettivi di valutazione di Amazon Inspector Classic

Puoi creare fino a 50 obiettivi di valutazione per AWS account. Per ulteriori informazioni, consulta [Limiti del servizio Amazon Inspector Classic](#).

## Creazione di un target di valutazione

Puoi utilizzare la console Amazon Inspector Classic per creare obiettivi di valutazione.


Come creare una destinazione di valutazione

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo. <https://console.aws.amazon.com/inspector/>
2. Nel riquadro di navigazione scegli Assessment Targets (Target di valutazione), quindi Create (Crea).
3. Nel campo Name (Nome) immetti un nome per il target di valutazione.
4. Esegui una delle seguenti operazioni:
  - Per includere tutte le istanze EC2 in questo AWS account e nella regione in questo obiettivo di valutazione, seleziona la casella di controllo Tutte le istanze.


### Note

Il limite relativo al numero massimo di agenti che puoi includere nell'esecuzione di una valutazione si applica quando utilizzi questa opzione. Per ulteriori informazioni, consulta [Limiti del servizio Amazon Inspector Classic](#).

- Per scegliere le istanze EC2 da includere in questo obiettivo di valutazione, in Usa tag, inserisci i nomi chiave e le coppie chiave-valore dei tag.
5. (Facoltativo) Durante la creazione di una destinazione, puoi selezionare la casella di controllo **Installa agenti** per installare l'agente su tutte le istanze EC2 di questa destinazione. Per utilizzare questa opzione, le istanze EC2 devono avere installato l'agente SSM e un ruolo IAM che consenta Run Command. L'agente SSM viene installato per impostazione predefinita nelle istanze Amazon EC2 basate su Windows e nelle istanze basate su Amazon Linux. Amazon EC2 Systems Manager richiede un ruolo IAM per le istanze EC2 che elaborano i comandi e un ruolo separato per gli utenti che eseguono i comandi. Per ulteriori informazioni, consulta [Installazione e configurazione dell'agente SSM](#) e [Configurazione dei ruoli di sicurezza per Systems Manager](#).

 Important

Se un'istanza EC2 dispone già di un agente in esecuzione, l'utilizzo di questa opzione sostituisce l'agente attualmente in esecuzione sull'istanza con l'agente della versione più recente.


 Note

Per gli obiettivi di valutazione esistenti, puoi scegliere il pulsante **Installa agenti con Run Command** per installare l'agente su tutte le istanze EC2 di questa destinazione.

 Note

Puoi anche installare l'agente su più istanze EC2 (sia istanze basate su Linux che su Windows con lo stesso comando) in remoto utilizzando il comando Systems Manager Run. Per ulteriori informazioni, consulta [Installazione dell'agente Amazon Inspector su più istanze EC2 con Systems Manager Run Command](#).

6. Scegli **Save (Salva)**.

 Note


Puoi utilizzare il pulsante Preview Target nella pagina Assessment Targets per esaminare tutte le istanze EC2 incluse nell'obiettivo di valutazione. Per ogni istanza EC2, puoi esaminare il nome host, l'ID dell'istanza, l'indirizzo IP e, se applicabile, lo stato dell'agente. Lo stato dell'agente può avere i seguenti valori: HEALTHY, UNHEALTHY e UNKNOWN. Amazon Inspector Classic mostra uno stato UNKNOWN quando non è in grado di determinare se c'è un agente in esecuzione sull'istanza EC2.

## Eliminazione di un target di valutazione

Per eliminare un target di valutazione, esegui questa procedura.

Come eliminare un target di valutazione

- Nella pagina Assessment targets (Target di valutazione) scegliere il target da eliminare, quindi Delete (Elimina). Quando viene richiesta la conferma, scegli Sì.

 Important

Quando elimini un target di valutazione, vengono eliminati anche tutti i modelli di valutazione, tutte le esecuzioni di valutazioni, tutti i risultati e tutte le versioni dei report associati al target.

Puoi eliminare un target di valutazione anche usando l'API [DeleteAssessmentTarget](#).

# Regole, pacchetti e regole di Amazon Inspector Classic

Puoi utilizzare Amazon Inspector Classic per valutare i tuoi obiettivi di valutazione (raccolte di risorse AWS) per potenziali problemi di sicurezza e vulnerabilità. Amazon Inspector Classic confronta il comportamento e la configurazione di sicurezza degli obiettivi di valutazione con pacchetti di regole di sicurezza selezionati. Nel contesto di Amazon Inspector Classic, una regola è un controllo di sicurezza che Amazon Inspector Classic esegue durante l'esecuzione della valutazione.

In Amazon Inspector Classic, le regole sono raggruppate in pacchetti di regole distinti per categoria, gravità o prezzo. Questa suddivisione mette a disposizione vari tipi di analisi che è possibile eseguire. Ad esempio, Amazon Inspector Classic offre un gran numero di regole che puoi utilizzare per valutare le tue applicazioni. Tuttavia, puoi decidere di includere un numero ridotto di regole disponibili per gestire un'area problematica particolare o per rilevare problemi specifici a livello di sicurezza. Le aziende con grandi reparti IT possono avere l'esigenza di stabilire se un'applicazione è esposta a una minaccia di sicurezza. Altre potrebbero avere bisogno di concentrarsi solo sui problemi con livello di gravità Elevata.

- [Livelli di severità per le regole in Amazon Inspector Classic](#)
- [Pacchetti di regole in Amazon Inspector Classic](#)

## Livelli di severità per le regole in Amazon Inspector Classic

A ogni regola di Amazon Inspector Classic è assegnato un livello di gravità. Ciò riduce la necessità di dare priorità a una regola rispetto a un'altra nell'analisi. Ciò semplifica inoltre il processo decisionale durante la fase di risoluzione quando una regola evidenzia un potenziale problema.

I livelli High (Alta), Medium (Media) e Low (Bassa) indicano un problema di sicurezza che potrebbe compromettere la riservatezza, l'integrità e la disponibilità delle informazioni all'interno del target di valutazione. I livelli si distinguono in base alla probabilità che il problema porti a un compromesso e all'urgenza della risoluzione del problema.

Il livello Informational (Informativa) evidenzia un dettaglio della configurazione della sicurezza di un target di valutazione specifico.

Ecco i metodi consigliati per rispondere ai problemi in base alla loro gravità:

- **Elevato:** i problemi di elevata gravità sono estremamente urgenti. Amazon Inspector Classic consiglia di trattare questo problema di sicurezza come un'emergenza e di implementare una soluzione immediata.
- I problemi di gravità medio-media sono piuttosto urgenti. Amazon Inspector Classic consiglia di risolvere questo problema alla prossima occasione possibile, ad esempio durante il prossimo aggiornamento del servizio.
- **Basso:** i problemi di bassa gravità sono meno urgenti. Amazon Inspector Classic consiglia di risolvere questo problema nell'ambito di uno dei futuri aggiornamenti del servizio.
- **Informativo:** questi problemi sono puramente informativi. In base agli obiettivi aziendali e organizzativi, puoi semplicemente prendere nota di queste informazioni o utilizzarle per migliorare la sicurezza del tuo target di valutazione.

## Pacchetti di regole in Amazon Inspector Classic

Una valutazione di Amazon Inspector può usare qualsiasi combinazione dei seguenti pacchetti di regole:

Valutazioni di rete:

- [Network Reachability](#)

Valutazioni dell'host:

- [Common vulnerabilities & exposures \(CVE\)](#)
- [Center for Internet Security \(CIS\) Benchmarks](#)
- [Best practice di sicurezza per Amazon Inspector Classic](#)

## Network Reachability

Le regole del pacchetto Network Reachability analizzano le configurazioni di rete per individuare le vulnerabilità di sicurezza delle istanze EC2. I risultati generati da Amazon Inspector costituiscono anche una guida per la limitazione dell'accesso non protetto.

[Il pacchetto di regole di Network Reachability utilizza la tecnologia più recente dell'iniziativa Provable Security. AWS](#)

I risultati generati da queste regole mostrano se le tue porte sono raggiungibili da Internet tramite un Internet gateway (comprese le istanze con Application Load Balancer o Classic Load Balancer), una connessione peering VPC o una VPN tramite un gateway virtuale. Questi risultati evidenziano anche configurazioni di rete che consentono accessi potenzialmente dannosi, come gruppi di sicurezza mal gestiti e così ACLs via IGWs.

Queste regole aiutano ad automatizzare il monitoraggio delle reti AWS e a identificare i punti in cui l'accesso di rete alle istanze EC2 potrebbe essere configurato in modo errato. Includendo questo pacchetto nel ciclo di valutazione, è possibile implementare controlli di sicurezza di rete dettagliati senza dover installare scanner e inviare pacchetti, che sono complessi e costosi da mantenere, in particolare su connessioni peering VPC e. VPNs

#### Important

Non è necessario un agente Amazon Inspector Classic per valutare le istanze EC2 con questo pacchetto di regole. Tuttavia, un agente installato può fornire informazioni sulla presenza di processi in ascolto sulle porte. Non installare un agente su un sistema operativo non supportato da Amazon Inspector Classic. Se un agente è presente in un'istanza che esegue un sistema operativo non supportato, il pacchetto di regole Network Reachability non funzionerà su tale istanza.

Per ulteriori informazioni, consulta [Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati](#).

## Configurazioni analizzate

Le regole di Network Reachability analizzano la configurazione delle seguenti entità per cercare le vulnerabilità:

- [Istanze Amazon EC2](#)
- [Application Load Balancer](#)
- [Direct Connect](#)
- [Elastic Load Balancer](#)
- [Interfacce di rete elastiche](#)
- [Gateway Internet \(\) IGWs](#)
- [Elenchi di controllo degli accessi alla rete \(\) ACLs](#)

- [Tabelle di routing](#)
- [Gruppi di sicurezza \(SGs\)](#)
- [Sottoreti](#)
- [Cloud privati virtuali \(VPCs\)](#)
- [Gateway privati virtuali \(\) VGWs](#)
- [Connessioni in peering di VPC](#)

## Route di raggiungibilità

Le regole di Network Reachability controllano le seguenti route di raggiungibilità che corrispondono ai modi in cui è possibile accedere alle porte dall'esterno del VPC:

- **Internet** - Internet gateway (tra cui Application Load Balancer e Classic Load Balancer)
- **PeeredVPC** – Connessioni in peering di VPC
- **VGW** - Gateway privati virtuali

## Tipi di risultati

Una valutazione che include il pacchetto di regole Network Reachability può restituire i seguenti tipi di risultati per ogni route di raggiungibilità:

- [RecognizedPort](#)
- [UnrecognizedPortWithListener](#)
- [NetworkExposure](#)

### RecognizedPort

Una porta che viene in genere utilizzata per un servizio noto è raggiungibile. Se sull'istanza EC2 di destinazione è presente un agente, i risultati generati indicheranno anche se esiste un processo di ascolto attivo sulla porta. I risultati di questo tipo vengono valutati in base all'impatto sulla sicurezza del servizio noto:

- **RecognizedPortWithListener**— Una porta riconosciuta è raggiungibile esternamente dalla rete Internet pubblica tramite uno specifico componente di rete e un processo è in ascolto sulla porta.

- **RecognizedPortNoListener**— Una porta è raggiungibile esternamente dalla rete Internet pubblica tramite uno specifico componente di rete e non vi sono processi in ascolto sulla porta.
- **RecognizedPortNoAgent**— Una porta è raggiungibile esternamente dalla rete Internet pubblica tramite uno specifico componente di rete. La presenza di un processo in ascolto sulla porta non può essere determinata senza installare un agente sull'istanza di destinazione.

La tabella seguente mostra un elenco di porte riconosciute:

Servizio	Porte TCP	Porte UDP
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP over TLS	636	
Global catalog LDAP	3268	
Global catalog LDAP over TLS	3269	
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752
RPC	111, 135, 530	111, 135, 530
WINS	1512, 42	1512, 42
DHCP	67, 68, 546, 547	67, 68, 546, 547
Syslog	601	514
Servizi di stampa	515	
Telnet	23	23

Servizio	Porte TCP	Porte UDP
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017, 27018, 27019, 28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521, 1630	
Elasticsearch	9300, 9200	
HTTP	80	80
HTTPS	443	443

## UnrecognizedPortWithListener

Se una porta non è elencata nella tabella precedente significa che è raggiungibile e ha un processo attivo in ascolto. Poiché i risultati di questo tipo mostrano informazioni sui processi di ascolto, possono essere generati solo quando un agente Amazon Inspector è installato sull'istanza EC2 di destinazione. I risultati di questo tipo hanno il livello di gravità Low (Bassa).

## NetworkExposure

I risultati di questo tipo mostrano informazioni aggregate sulle porte raggiungibili sull'istanza EC2. Per ogni combinazione di interfacce di rete elastiche e gruppi di sicurezza su un'istanza EC2, questi risultati mostrano l'insieme raggiungibile di intervalli di porte TCP e UDP. I risultati di questo tipo hanno il livello di gravità Informational (Informativo).

## Common vulnerabilities & exposures (CVE)

Le regole di questo pacchetto aiutano a verificare se le EC2 istanze degli obiettivi di valutazione sono esposte a vulnerabilità ed esposizioni comuni (). CVEs Gli attacchi possono sfruttare le vulnerabilità non corrette tramite patch e compromettere la riservatezza, l'integrità e la disponibilità del servizio o dei dati. Il sistema CVE fornisce un metodo di riferimento per vulnerabilità ed esposizioni a livello di sicurezza delle informazioni pubblicamente note. Per ulteriori informazioni, consulta <https://cve.mitre.org/>.

Se un determinato CVE compare in un risultato prodotto da una valutazione di Amazon Inspector Classic, puoi [cercare](https://cve.mitre.org/) su <https://cve.mitre.org/> l'ID del CVE (ad esempio,). **CVE-2009-0021** I risultati della ricerca forniscono informazioni dettagliate sulla vulnerabilità CVE specifica, sulla sua gravità e sulla procedura di risoluzione.

Per il pacchetto di regole Common Vulnerabilities & Exploits (CVE), Amazon Inspector ha mappato i livelli di base CVSS Base Scoring e ALAS Severity forniti:

Severità di Amazon Inspector	Punteggio di base CVSS	Severità ALAS (se non viene assegnato un punteggio CVSS)
Elevata	$\geq 5$	Critico o importante
Media	$< 5$ and $> \text{Critico o importante}$ ----sep----- = 2.1	Media
Bassa	$< 2.1$ and $\geq 2.1$ ----set----- = 0,8	Bassa
Messaggio informativo	$< 0,8$	N/D

Le regole incluse in questo pacchetto consentono di valutare se le EC2 istanze sono esposte ai CVEs seguenti elenchi regionali:

- [Stati Uniti orientali \(Virginia settentrionale\)](#)
- [Stati Uniti orientali \(Ohio\)](#)
- [Stati Uniti occidentali \(California settentrionale\)](#)

- [Stati Uniti occidentali \(Oregon\)](#)
- [UE \(Irlanda\)](#)
- [UE \(Francoforte\)](#)
- [UE \(Londra\)](#)
- [UE \(Stoccolma\)](#)
- [Asia Pacifico \(Tokyo\)](#)
- [Asia Pacifico \(Seoul\)](#)
- [Asia Pacifico \(Mumbai\)](#)
- [Asia Pacifico \(Sydney\)](#)
- [AWS GovCloud West \(Stati Uniti\)](#)
- [AWS GovCloud East \(Stati Uniti\)](#)

Il pacchetto di regole CVE viene aggiornato regolarmente; questo elenco include le CVEs regole incluse nelle esecuzioni di valutazione che si verificano contemporaneamente al recupero di questo elenco.

Per ulteriori informazioni, consulta [Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati](#).

## Center for Internet Security (CIS) Benchmarks

Il programma CIS Security Benchmarks fornisce best practice di settore ben definite, imparziali e basate sul consenso per aiutare le organizzazioni a valutare e migliorare la propria sicurezza. AWS è una società membro di CIS Security Benchmarks. Per un elenco delle certificazioni Amazon Inspector Classic, consulta la [pagina Amazon Web Services sul sito Web](#) CIS.

Amazon Inspector Classic attualmente fornisce i seguenti pacchetti di regole CIS Certified per aiutare a stabilire posizioni di configurazione sicure per i seguenti sistemi operativi:

### Amazon Linux

- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1
- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1

- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2
- CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1

## CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

## Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

## Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

## Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)

- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

Se un benchmark CIS specifico compare in un risultato prodotto da un'esecuzione di valutazione di Amazon Inspector Classic, puoi scaricare una descrizione dettagliata in PDF del benchmark [da https://benchmarks.cisecurity.org/](https://benchmarks.cisecurity.org/) (è richiesta la registrazione gratuita). Nel documento relativo al benchmark sono incluse informazioni dettagliate sul CIS Benchmark corrente, sulla sua gravità e sulla procedura di risoluzione corrispondente.

Per ulteriori informazioni, consulta [Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati](#).

## Best practice di sicurezza per Amazon Inspector Classic

Utilizza le regole di Amazon Inspector Classic per determinare se i tuoi sistemi sono configurati in modo sicuro.

**⚠ Important**

Attualmente, puoi includere nei tuoi obiettivi di valutazione istanze EC2 che eseguono sistemi operativi basati su Linux o Windows.

Durante un'esecuzione di valutazione, le regole descritte in questa sezione generano risultati solo per le istanze EC2 che eseguono sistemi operativi basati su Linux. Le regole non generano risultati per le istanze EC2 che eseguono sistemi operativi basati su Windows.

Per ulteriori informazioni, consulta [Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati](#).

## Argomenti

- [Disabilita l'accesso root tramite SSH](#)
- [Supporta solo SSH versione 2](#)
- [Disabilita autenticazione password tramite SSH](#)
- [Configura età massima della password](#)
- [Configura lunghezza minima della password](#)
- [Configura complessità della password](#)
- [Enable ASLR](#)
- [Enable DEP](#)
- [Configura le autorizzazioni per le directory del sistema](#)

## Disabilita l'accesso root tramite SSH

Questa regola consente di determinare se il daemon SSH è configurato in modo da consentire l'accesso all'istanza EC2 come [root](#).

### Gravità

[Medio](#)

### Risultato

Nel target di valutazione è presente un'istanza EC2 configurata per consentire agli utenti di accedere con credenziali root tramite SSH. Questo scenario aumenta la probabilità di un attacco di forza bruta riuscito.

## Resolution (Risoluzione)

Ti consigliamo di configurare l'istanza EC2 per impedire l'accesso all'account root tramite SSH. Esegui invece l'accesso come utente non root e usa sudo per eseguire l'escalation dei privilegi quando necessario. Per disabilitare gli accessi di account root tramite SSH, imposta `PermitRootLogin` su `no` nel file `/etc/ssh/sshd_config`, quindi riavvia `sshd`.

## Supporta solo SSH versione 2

Questa regola aiuta a determinare se le istanze EC2 sono configurate per supportare il protocollo SSH versione 1.

Gravità

[Medio](#)

Risultato

Un'istanza EC2 inclusa nell'obiettivo di valutazione è configurata per supportare SSH-1, che contiene difetti di progettazione intrinseci che ne riducono notevolmente la sicurezza.

Resolution (Risoluzione)

Ti consigliamo di configurare le istanze EC2 nel tuo target di valutazione per supportare solo SSH-2 e versioni successive. Per ottenere questo risultato in OpenSSH, puoi impostare `Protocol 2` nel file `/etc/ssh/sshd_config`. Per ulteriori informazioni, consulta `man sshd_config`.

## Disabilita autenticazione password tramite SSH

Questa regola aiuta a determinare se le istanze EC2 sono configurate per supportare l'autenticazione tramite password tramite il protocollo SSH.

Gravità

[Medio](#)

Risultato

Un'istanza EC2 inclusa nell'obiettivo di valutazione è configurata per supportare l'autenticazione tramite password tramite SSH. L'autenticazione tramite password è soggetta ad attacchi di

forza bruta e deve essere disabilitata e sostituita dall'autenticazione basata su chiave, laddove possibile.

#### Resolution (Risoluzione)

Ti consigliamo di disabilitare l'autenticazione tramite password con il protocollo SSH sulle istanze EC2 e di abilitare invece il supporto dell'autenticazione basata su chiave. Ciò consente di ridurre sensibilmente la probabilità di un attacco di forza bruta riuscito. [Per ulteriori informazioni, consulta https://aws.amazon.com/articles/1233/](https://aws.amazon.com/articles/1233/). Se è supportata l'autenticazione tramite password, è importante consentire l'accesso al server SSH solo agli indirizzi IP affidabili.

## Configura età massima della password

Questa regola aiuta a determinare se l'età massima per le password è configurata sulle istanze EC2.

#### Gravità

[Medio](#)

#### Risultato

Un'istanza EC2 inclusa nel tuo obiettivo di valutazione non è configurata per un'età massima per le password.

#### Resolution (Risoluzione)

Se utilizzi password, ti consigliamo di configurare un'età massima per le password su tutte le istanze EC2 incluse nel tuo obiettivo di valutazione. Questo scenario prevede che gli utenti modifichino regolarmente la propria password in modo da ridurre la probabilità di un attacco basato sul tentativo di indovinare la password. Per risolvere questo problema per gli utenti esistenti, usa il comando `chage`. Per configurare la durata massima per le password per tutti gli utenti futuri, modifica il campo `PASS_MAX_DAYS` nel file `/etc/login.defs`.

## Configura lunghezza minima della password

Questa regola aiuta a determinare se è configurata una lunghezza minima per le password sulle istanze EC2.

#### Gravità

[Medio](#)

## Risultato

Un'istanza EC2 inclusa nel tuo obiettivo di valutazione non è configurata per una lunghezza minima per le password.

### Resolution (Risoluzione)

Se utilizzi password, ti consigliamo di configurare una lunghezza minima per le password su tutte le istanze EC2 incluse nel tuo obiettivo di valutazione. L'applicazione di una lunghezza minima delle password riduce il rischio di un attacco basato sul tentativo di indovinare la password. Puoi farlo utilizzando la seguente opzione nel file: `pwquality.conf minlen` Per ulteriori informazioni, vedere <https://linux.die.net/man/5/pwquality.conf>.

Se non `pwquality.conf` è disponibile sulla tua istanza, puoi impostare l'`minlen` opzione utilizzando il `pam_cracklib.so` modulo. Per ulteriori informazioni, consulta [man pam\\_cracklib](#).

L'`minlen` opzione deve essere impostata su 14 o superiore.

## Configura complessità della password

Questa regola aiuta a determinare se un meccanismo di complessità delle password è configurato sulle istanze EC2.

### Gravità

[Medio](#)

### Risultato

Nell'obiettivo di valutazione non è configurato alcun meccanismo o restrizione sulla complessità delle password sulle istanze EC2. Ciò consente agli utenti di impostare password poco complesse, aumentando la probabilità di accessi non autorizzati e usi impropri degli account da parte di utenti non autorizzati.

### Resolution (Risoluzione)

Se utilizzi password, ti consigliamo di configurare tutte le istanze EC2 nel tuo obiettivo di valutazione in modo da richiedere un livello di complessità delle password. A questo scopo, puoi utilizzare le opzioni seguenti nel file `pwquality.conf`: `lcredit`, `ucredit`, `dcredit` e `ocredit`. [Per ulteriori informazioni, consulta https://linux.die.net/man/5/pwquality.conf](https://linux.die.net/man/5/pwquality.conf).

Se `pwquality.conf` non è disponibile nell'istanza, puoi impostare le opzioni `lcredit`, `ucredit`, `dccredit` e `ocredit` usando il modulo `pam_cracklib.so`. Per ulteriori informazioni, consulta [man pam\\_cracklib](#).

Il valore previsto per ciascuna di queste opzioni è minore o uguale a -1, come illustrato di seguito:

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

Inoltre, l'opzione `remember` deve essere impostata su 12 o su un valore superiore. Per ulteriori informazioni, consulta [man pam\\_unix](#).

## Enable ASLR

Questa regola aiuta a determinare se la randomizzazione del layout dello spazio degli indirizzi (ASLR) è abilitata sui sistemi operativi delle istanze EC2 incluse nell'obiettivo di valutazione.

Gravità

[Medio](#)

Risultato

L'ASLR non è abilitato per un'istanza EC2 inclusa nel target di valutazione.

Resolution (Risoluzione)

Per migliorare la sicurezza del tuo obiettivo di valutazione, ti consigliamo di abilitare ASLR sui sistemi operativi di tutte le istanze EC2 del tuo target eseguendo l'esecuzione. `echo 2 | sudo tee /proc/sys/kernel/randomize_va_space`

## Enable DEP

Questa regola aiuta a determinare se la Data Execution Prevention (DEP) è abilitata sui sistemi operativi delle istanze EC2 che rientrano nell'obiettivo di valutazione.

### Note

Questa regola non è supportata per le istanze EC2 con processori ARM.

## Gravità

### Medio

## Risultato

Un'istanza EC2 inclusa nel tuo obiettivo di valutazione non ha il DEP abilitato.

## Resolution (Risoluzione)

Ti consigliamo di abilitare DEP sui sistemi operativi di tutte le istanze EC2 nel tuo obiettivo di valutazione. L'abilitazione della funzionalità Protezione esecuzione programmi consente di proteggere le istanze da possibili problemi di sicurezza mediante tecniche di overflow del buffer.

## Configura le autorizzazioni per le directory del sistema

Questa regola verifica le autorizzazioni delle directory di sistema che contengono file binari e informazioni sulla configurazione del sistema. Controlla che solo l'utente root (un utente che effettua l'accesso utilizzando le credenziali dell'account root) disponga delle autorizzazioni di scrittura per tali directory.

## Gravità

### Elevate

## Risultato

Un'istanza EC2 nel target di valutazione include una directory di sistema in cui gli utenti non root possono scrivere.

## Resolution (Risoluzione)

Per migliorare la sicurezza dell'obiettivo di valutazione e prevenire l'escalation dei privilegi da parte di utenti locali malintenzionati, configura tutte le directory di sistema su tutte le istanze EC2 della destinazione in modo che siano scrivibili solo dagli utenti che accedono utilizzando le credenziali dell'account root.

# Modelli di valutazione ed esecuzioni di valutazione di Amazon Inspector Classic

Amazon Inspector Classic ti aiuta a scoprire potenziali problemi di sicurezza utilizzando regole di sicurezza per analizzare le tue AWS risorse. Amazon Inspector Classic monitora e raccoglie dati comportamentali (telemetria) sulle tue risorse. I dati includono informazioni sull'uso di canali sicuri, sul traffico di rete tra i processi in esecuzione e dettagli sulla comunicazione con i servizi. AWS Successivamente, Amazon Inspector Classic analizza e confronta i dati con una serie di pacchetti di regole di sicurezza. Infine, Amazon Inspector Classic produce un elenco di risultati che identificano potenziali problemi di sicurezza di vari livelli di gravità.

Per iniziare, crei un obiettivo di valutazione (una raccolta di AWS risorse che desideri che Amazon Inspector Classic analizzi). Crea quindi un modello di valutazione (un modello usato per configurare la valutazione). Il modello consente di avviare un'esecuzione di valutazioni, ovvero il processo di monitoraggio e analisi che restituirà un set di risultati.

## Argomenti

- [Modelli di valutazione Amazon Inspector Classic](#)
- [Limiti dei modelli di valutazione Amazon Inspector Classic](#)
- [Creazione di un modello di valutazione](#)
- [Eliminazione di un modello di valutazione](#)
- [Esecuzioni di valutazioni](#)
- [Limiti dei cicli di valutazione di Amazon Inspector Classic](#)
- [L'impostazione della valutazione automatica avviene tramite una funzione Lambda](#)
- [Configurazione di un argomento SNS per le notifiche di Amazon Inspector Classic](#)

## Modelli di valutazione Amazon Inspector Classic

Un modello di valutazione consente di specificare una configurazione per le esecuzioni di valutazioni, inclusi i seguenti elementi:

- Pacchetti di regole utilizzati da Amazon Inspector Classic per valutare l'obiettivo di valutazione

- Durata dell'esecuzione della valutazione: puoi impostare la durata di un'esecuzione di valutazione compresa tra 3 minuti e 24 ore. Ti consigliamo di impostare la durata delle esecuzioni di valutazioni su 1 ora.
- Argomenti di Amazon SNS a cui Amazon Inspector Classic invia notifiche in merito agli stati e ai risultati dell'esecuzione della valutazione
- Attributi di Amazon Inspector Classic (coppie chiave-valore) che puoi assegnare ai risultati generati dall'esecuzione di valutazione che utilizza questo modello di valutazione

Dopo che Amazon Inspector Classic ha creato il modello di valutazione, puoi etichettarlo come qualsiasi altra AWS risorsa. Per ulteriori informazioni, consulta [Editor di tag](#). Il tagging dei modelli di valutazione consente di organizzarli e ottenere una panoramica più precisa sulla strategia di sicurezza adottata. Ad esempio, Amazon Inspector Classic offre un gran numero di regole in base alle quali puoi valutare i tuoi obiettivi di valutazione. Puoi decidere di includere vari sottoinsiemi di regole nei tuoi modelli di valutazione per gestire specifiche aree problematiche o per far emergere determinati problemi di sicurezza. Il tagging dei modelli di valutazione consente di individuare ed eseguire rapidamente i modelli in qualsiasi momento in modo conforme con le strategie e gli obiettivi di sicurezza correnti.

#### Important

Dopo aver creato un modello di valutazione, non puoi più modificarlo.

## Limiti dei modelli di valutazione Amazon Inspector Classic

Puoi creare fino a 500 modelli di valutazione per ogni AWS account.

Per ulteriori informazioni, consulta [Limiti del servizio Amazon Inspector Classic](#).

## Creazione di un modello di valutazione

Come creare un modello di valutazione

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo. <https://console.aws.amazon.com/inspector/>
2. Nel riquadro di navigazione selezionare Assessment templates (Modelli di valutazione), quindi Create (Crea).

3. In Name (Nome) immettere un nome per il modello di valutazione.
4. In Target name (Nome destinazione), scegliere il target di valutazione da analizzare.

#### Note

Quando crei un modello di valutazione, puoi utilizzare il pulsante Preview Target nella pagina Assessment Templates per esaminare tutte le istanze EC2 incluse nell'obiettivo di valutazione. Per ogni istanza EC2, puoi esaminare il nome host, l'ID dell'istanza, l'indirizzo IP e, se applicabile, lo stato dell'agente. Lo stato dell'agente può avere i seguenti valori: HEALTHY, UNHEALTHY e UNKNOWN. Amazon Inspector Classic mostra uno stato UNKNOWN quando non è in grado di determinare se c'è un agente in esecuzione sull'istanza EC2.

Puoi usare il pulsante Preview Target (Anteprima target) nella pagina Assessment Templates (Modelli di valutazione) anche per rivedere le istanze EC2 che compongono i target di valutazione inclusi nei modelli precedentemente creati.

5. In Rules packages (Pacchetti di regole), scegliere uno o più pacchetti di regole da includere nel modello di valutazione.
6. Nel campo Duration (Durata) specifica la durata del modello di valutazione.
7. (Facoltativo) Per gli argomenti relativi a SNS, specifica un argomento SNS a cui desideri che Amazon Inspector Classic invii notifiche sugli stati e sui risultati delle esecuzioni di valutazione. Amazon Inspector Classic può inviare notifiche SNS sui seguenti eventi:
  - Avvio di un'esecuzione di valutazioni
  - Completamento di un'esecuzione di valutazioni
  - Modifica dello stato di un'esecuzione di valutazioni
  - Generazione di un risultato

Per ulteriori informazioni sulla configurazione di un argomento SNS, consulta [Configurazione di un argomento SNS per le notifiche di Amazon Inspector Classic](#).

8. (Opzionale) In Tag inserire i valori per Key (Chiave) e Value (Valore). Al modello di valutazione puoi aggiungere più tag.
9. (Facoltativo) Per gli attributi aggiunti ai risultati, inserisci i valori per Chiave e Valore. Amazon Inspector Classic applica gli attributi a tutti i risultati generati dal modello di valutazione. Al

modello di valutazione puoi aggiungere più attributi. Per ulteriori informazioni sui risultati e sul relativo tagging, consulta [Risultati di Amazon Inspector Classic](#).

10. (Facoltativo) Per impostare una pianificazione per le esecuzioni di valutazioni utilizzando questo modello, selezionare la casella di controllo Set up recurring assessment runs once every <number\_of\_days>, starting now (Configura esecuzioni di valutazioni ricorrenti ogni <numero\_di\_giorni> a partire da adesso) e specificare la frequenza (numero di giorni) usando i tasti freccia su e freccia giù della tastiera.

#### Note

Quando utilizzi questa casella di controllo, Amazon Inspector Classic crea automaticamente una regola Amazon CloudWatch Events per la pianificazione delle esecuzioni di valutazione che stai configurando. Amazon Inspector Classic crea quindi automaticamente anche un ruolo IAM denominato `AWS_InspectorEvents_Invoke_Assessment_Template`. Questo ruolo consente a CloudWatch Events di effettuare chiamate API contro le risorse Amazon Inspector Classic. Per ulteriori informazioni, consulta [Che cos'è Amazon CloudWatch Events?](#) e [utilizzo di politiche basate sulle risorse](#) per gli eventi. CloudWatch

#### Note

È anche possibile configurare esecuzioni di valutazioni automatiche tramite una funzione AWS Lambda . Per ulteriori informazioni, consulta [L'impostazione della valutazione automatica avviene tramite una funzione Lambda](#).

11. Scegli Create and run (Crea ed esegui) o Create (Crea).

## Eliminazione di un modello di valutazione

Per eliminare un modello di valutazione, esegui questa procedura.

Come eliminare un modello di valutazione

- Nella pagina Assessment Templates (Modelli di valutazione) scegliere il modello da eliminare, quindi Delete (Elimina). Quando viene richiesta la conferma, scegli Sì.

**⚠ Important**

Quando elimini un modello di valutazione, verranno eliminati anche tutti i modelli di valutazione, tutte le valutazioni eseguite, tutti i risultati e tutte le versioni dei report associati al modello.

Puoi eliminare un modello di valutazione anche usando l'API [DeleteAssessmentTemplate](#).

## Esecuzioni di valutazioni

Dopo aver creato un modello di valutazione, puoi utilizzarlo per avviare le esecuzioni di valutazioni. Puoi avviare più esecuzioni utilizzando lo stesso modello purché rimanga entro il limite di esecuzioni per ogni account. AWS Per ulteriori informazioni, consulta [Limiti dei cicli di valutazione di Amazon Inspector Classic](#).

Se utilizzi la console Amazon Inspector Classic, devi avviare la prima esecuzione del nuovo modello di valutazione dalla pagina dei modelli di valutazione. Una volta avviata l'esecuzione, puoi usare la pagina Assessment runs (Esecuzioni di valutazioni) per monitorare l'avanzamento del processo. Usa i pulsanti Run (Esegui), Cancel (Annulla) e Delete (Elimina) per avviare, annullare o eliminare un'esecuzione. Puoi anche visualizzare i dettagli dell'esecuzione, tra cui l'ARN dell'esecuzione, i pacchetti di regole selezionati per l'esecuzione, i tag e gli attributi applicati all'esecuzione e così via.

Per le successive esecuzioni del modello di valutazione, puoi usare i pulsanti Run (Esegui), Cancel (Annulla) e Delete (Elimina) nella pagina Assessment templates (Modelli di valutazione) oppure nella pagina Assessment runs (Esecuzioni di valutazioni).

## Eliminazione di un'esecuzione di valutazioni

Per eliminare un'esecuzione di valutazioni, esegui questa procedura.

Per eliminare un'esecuzione

- Nella pagina Assessment runs (Esecuzioni di valutazioni) scegliere l'esecuzione da eliminare, quindi Delete (Elimina). Quando viene richiesta la conferma, scegli Sì.

**⚠ Important**

Quando elimini un'esecuzione, verranno eliminati anche tutti i risultati e tutte le versioni del report a essa associati.

Puoi anche eliminare un'esecuzione utilizzando l'API [DeleteAssessmentRun](#).

## Limiti dei cicli di valutazione di Amazon Inspector Classic

Puoi creare fino a 50.000 esecuzioni di valutazione per ogni AWS account.

Puoi eseguire più esecuzioni contemporaneamente purché i target utilizzati per le esecuzioni non contengano istanze EC2 sovrapposte.

Per ulteriori informazioni, consulta [Limiti del servizio Amazon Inspector Classic](#).

## L'impostazione della valutazione automatica avviene tramite una funzione Lambda

Se desideri impostare una pianificazione ricorrente per la tua valutazione, puoi configurare il modello di valutazione in modo che venga eseguito automaticamente creando una funzione Lambda utilizzando la console. AWS Lambda Per ulteriori informazioni, consulta la sezione relativa alle [funzioni Lambda](#).

Per configurare le esecuzioni di valutazione automatiche utilizzando la AWS Lambda console, esegui la procedura seguente.

Per configurare esecuzioni automatiche tramite una funzione Lambda

1. Accedi a e apri la [AWS Lambda console](#). Console di gestione AWS
2. Nel riquadro di navigazione, scegli Dashboard o Funzioni, quindi scegli Crea una funzione Lambda.
3. Nella pagina Crea funzione scegliere Sfoglia repository app serverless, quindi immettere **inspector** nel campo di ricerca.
4. Scegli il inspector-scheduled-runblueprint.

5. Nella pagina Rivedi, configura e distribuisci, imposta una pianificazione ricorrente per le esecuzioni automatiche specificando un CloudWatch evento che attiva la tua funzione. Per eseguire questa operazione, inserire un nome e una descrizione per la regola e quindi scegliere un'espressione di pianificazione. L'espressione di pianificazione determina la frequenza dell'esecuzione, ad esempio ogni 15 minuti o una volta al giorno. Per ulteriori informazioni su CloudWatch eventi e concetti, consulta [What is Amazon CloudWatch Events?](#)

Se si seleziona la casella di controllo Enable trigger (Abilita trigger), l'esecuzione viene avviata subito dopo aver creato la funzione. Le esecuzioni automatiche successive seguiranno il modello di ricorrenza specificato nel campo Schedule expression (Espressione di pianificazione). Se non selezioni la casella di controllo Enable trigger (Abilita trigger) durante la creazione della funzione, puoi modificare la funzione in un secondo momento per abilitare il trigger.

6. Nella pagina Configure function (Configura funzione) specifica le informazioni seguenti:
  - In Name (Nome) immettere un nome per la funzione.
  - (Facoltativo) In Description (Descrizione) immettere una descrizione per semplificare l'identificazione della funzione in un secondo momento.
  - Per il runtime, mantieni il valore predefinito di **Node.js 8.10**. AWS Lambda supporta il inspector-scheduled-runblueprint solo per il **Node.js 8.10** runtime.
  - Il modello di valutazione che desideri eseguire automaticamente usando questa funzione. A tale scopo, è necessario fornire il valore per la variabile di ambiente chiamata assessmentTemplateArn.
  - Per il set di gestori lascia invariato il valore predefinito **index.handler**.
  - Le autorizzazioni per la funzione mediante il campo Role (Ruolo). Per ulteriori informazioni, consulta la pagina relativa al [modello di autorizzazioni di AWS Lambda](#).

Per eseguire questa funzione, è necessario un ruolo IAM che AWS Lambda consenta di avviare le esecuzioni e scrivere messaggi di log sulle esecuzioni, inclusi eventuali errori, su Amazon CloudWatch Logs. AWS Lambda assume questo ruolo per ogni esecuzione automatica ricorrente. Ad esempio, puoi associare la seguente policy di esempio a questo ruolo IAM:

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  

```

```
{
  "Effect": "Allow",
  "Action": [
    "inspector:StartAssessmentRun",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource": "*"
}
]
```

7. Rivedere le selezioni effettuate, quindi scegliere Create function (Crea funzione).

## Configurazione di un argomento SNS per le notifiche di Amazon Inspector Classic

Amazon Simple Notification Service (Amazon SNS) è un servizio Web che invia messaggi a endpoint o client che hanno effettuato la sottoscrizione. Puoi utilizzare Amazon SNS per configurare le notifiche per Amazon Inspector Classic.

Per configurare un argomento SNS per le notifiche

1. Creare un argomento SNS. Consulta [Tutorial: creazione di un argomento Amazon SNS](#). Quando si crea l'argomento, espandere la sezione Access policy - optional (Policy di accesso - opzionale). Quindi, procedere come segue per consentire la valutazione per l'invio di messaggi all'argomento:
  - a. Per Choose method (Scegli metodo), selezionare Basic.
  - b. Per Definire chi può pubblicare messaggi sull'argomento, scegli Solo gli AWS account specificati, quindi inserisci l'ARN per l'account nella regione in cui stai creando l'argomento:
    - US East (Ohio) - arn:aws:iam::646659390643:root
    - US East (N. Virginia) - arn:aws:iam::316112463485:root
    - US West (N. California) - arn:aws:iam::166987590008:root
    - US West (Oregon) - arn:aws:iam::758058086616:root
    - Asia Pacific (Mumbai) - arn:aws:iam::162588757376:root

- Asia Pacific (Seoul) - arn:aws:iam::526946625049:root
  - Asia Pacific (Sydney) - arn:aws:iam::454640832652:root
  - Asia Pacific (Tokyo) - arn:aws:iam::406045910587:root
  - Europe (Frankfurt) - arn:aws:iam::537503971621:root
  - Europe (Ireland) - arn:aws:iam::357557129151:root
  - Europe (London) - arn:aws:iam::146838936955:root
  - Europe (Stockholm) - arn:aws:iam::453420244670:root
  - AWS GovCloud (US-East)- arn :iam: :206278770380:root aws-us-gov
  - AWS GovCloud (US-West)- arn: :iamaws-us-gov: :850862329162:root
- c. Per Definire chi può sottoscrivere questo argomento, scegli Solo gli AWS account specificati, quindi inserisci l'ARN per l'account nella regione in cui stai creando l'argomento.
- d. Per proteggerti dall'uso di Inspector come agente confuso, come descritto in dettaglio in [Confused vice problem](#) nella IAM User Guide, procedi come segue:
- i. Scegli Avanzato. In questo modo accederai all'editor JSON.
  - ii. Aggiungi la seguente condizione:

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": <your account Id here>,
    "aws:SourceArn": "arn:aws:inspector:*:*:*"
  }
}
```

- e. (Facoltativo) Per ulteriori informazioni su aws: SourceAccount e aws:SourceArn, consulta [Global condition context keys](#) nella IAM User Guide.
- f. Aggiornare altre impostazioni per l'argomento in base alle esigenze, quindi scegliere Create topic (Crea argomento).
2. (Facoltativo) Per creare un argomento SNS crittografato, consulta [Encryption at rest](#) nella SNS Developer Guide.
3. Per proteggerti dal fatto che Inspector venga usato come sostituto confuso della tua chiave KMS, segui i passaggi aggiuntivi seguenti:

**a. Accedi alla tua CMK nella console KMS.**

- b. Scegli Modifica.
- c. Aggiungi la seguente condizione:

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": <your account Id here>,
    "aws:SourceArn": "arn:aws:sns:*:*:*"
  }
}
```

4. Creare una sottoscrizione all'argomento creato. Per ulteriori informazioni, consulta [Tutorial: iscrizione di un endpoint a un argomento Amazon SNS](#).
5. Per confermare che l'abbonamento è configurato correttamente, pubblicare un messaggio nell'argomento. Per ulteriori informazioni, consulta [Tutorial: pubblicazione di un messaggio in un argomento Amazon SNS](#).

# Risultati di Amazon Inspector Classic

I risultati sono potenziali problemi di sicurezza che Amazon Inspector Classic rileva durante una valutazione dell'obiettivo di valutazione. I risultati vengono visualizzati sulla console Amazon Inspector Classic o tramite l'API. I risultati contengono le descrizioni dettagliate dei problemi di sicurezza e le raccomandazioni per risolverli.

Dopo che Amazon Inspector ha generato i risultati, puoi monitorarli assegnando loro gli attributi di Amazon Inspector Classic. Questi attributi sono composti da coppie chiave-valore.

Il monitoraggio dei risultati mediante gli attributi può essere utile per la gestione del flusso di lavoro della strategia di sicurezza. Ad esempio, dopo aver creato ed eseguito una valutazione, viene generato un elenco di risultati con vari gradi di gravità, priorità e rilevanza, a seconda degli obiettivi di sicurezza e dell'approccio utilizzato a riguardo. Potresti infatti decidere di implementare subito la procedura consigliata per un risultato specifico per risolvere una problematica di sicurezza particolarmente urgente. In alternativa potresti decidere di posticipare la risoluzione di un altro risultato fino al successivo aggiornamento del servizio. Ad esempio, per tenere traccia di un risultato che necessita di una risoluzione immediata, potresti creare e assegnare a un risultato un attributo con una coppia chiave-valore **Status/Urgent**. Potresti inoltre usare gli attributi per distribuire il carico di lavoro relativo alla risoluzione di potenziali problemi di sicurezza. Ad esempio, per assegnare a Bruno, il responsabile della sicurezza nel tuo team, l'attività di risoluzione di un risultato, puoi assegnare al risultato interessato un attributo con una coppia chiave-valore **Assigned Engineer/Bob**.


## Uso dei risultati

Completa la seguente procedura su uno qualsiasi dei risultati generati da Amazon Inspector Classic.

Per individuare, analizzare e assegnare attributi ai risultati

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo. <https://console.aws.amazon.com/inspector/>
2. Dopo aver eseguito una valutazione, vai alla pagina Findings nella console Amazon Inspector Classic per visualizzare i risultati.

Puoi anche visualizzare i risultati nella sezione Notable Findings della pagina Dashboard della console Amazon Inspector Classic.

 Note

Non puoi visualizzare i risultati generati da un'esecuzione di valutazioni in corso. Tuttavia, puoi visualizzare un sottoinsieme di risultati se interrompi la valutazione prima del suo completamento. In un ambiente di produzione, ti consigliamo di lasciar concludere tutte le esecuzioni di valutazioni in modo che vengano generati set di risultati completi.


3. Per visualizzare i dettagli di un risultato specifico, scegli il widget Expand (Espandi) accanto al risultato. I dettagli del risultato includono i seguenti elementi:
  - Nome dell'obiettivo di valutazione che include l' EC2 istanza in cui è stato registrato questo risultato.
  - Nome del modello di valutazione usato per generare questo risultato.
  - Ora di inizio dell'esecuzione di valutazioni.
  - Ora di fine dell'esecuzione di valutazioni.
  - Stato dell'esecuzione di valutazioni.
  - Nome del pacchetto di regole contenente la regola che ha attivato questo risultato.
  - Nome del risultato.
  - Gravità del risultato.
  - Dettagli sulla gravità nativa di Common Vulnerability Scoring System (CVSS). Questi includono i parametri relativi a vettori CVSS e punteggi CVSS (compreso CVSS versione 2.0 e 3.0) per i risultati attivati dalle regole nel pacchetto di regole Common Vulnerabilities and Exposures. Per dettagli su CVSS, consulta <https://www.first.org/cvss/>.
  - Dettagli nativi sulla gravità forniti dal Center for Internet Security (CIS). Questi includono i parametri relativi al peso CIS per i risultati attivati dalle regole nel pacchetto CIS Benchmarks. Per ulteriori informazioni sui parametri relativi al peso CIS, consulta <https://www.cisecurity.org/>.
  - Descrizione del risultato.
  - Procedure consigliate che puoi eseguire per correggere il potenziale problema di sicurezza descritto dal risultato.
4. Per assegnare attributi a un risultato, scegli un risultato, quindi Add/Edit Attributes (Aggiungi/Modifica attributi).

Puoi anche assegnare attributi ai risultati durante la creazione di un modello di valutazione. A tale scopo, configura il nuovo modello in modo che assegni automaticamente gli attributi a tutti i risultati generati dall'esecuzione di valutazioni. Puoi usare i campi Key (Chiave) e Value (Valore) del campo Tags for findings from this assessment (Tag per i risultati di questa valutazione). Per ulteriori informazioni, consulta [Modelli di valutazione ed esecuzioni di valutazione di Amazon Inspector Classic](#).

5. Per esportare i risultati in un foglio di calcolo, fare clic sul pulsante freccia giù nell'angolo in alto a destra della pagina Findings (Risultati). Nella finestra di dialogo, scegliere Export all columns (Esporta tutte le colonne) o Export visible columns (Esporta le colonne visibili).

Nel contenuto esportato tutti i valori datetime sono timestamp epoca (Unix epoch).

6. Per filtrare i risultati attuali, inserisci una singola stringa in base alla quale desideri filtrare, ad esempio un ID di istanza o un numero CVE, nella barra dei filtri sopra la tabella dei risultati. Per mostrare o nascondere colonne di informazioni aggiuntive, scegli l'icona delle impostazioni nell'angolo in alto a destra della pagina Findings.
7. Per eliminare i risultati, passare alla pagina Assessment runs (Esecuzioni di valutazioni) e selezionare l'esecuzione che ha generato i risultati che si desidera eliminare. Scegli Elimina. Quando viene richiesta la conferma, scegli Sì.

 Important

Non puoi eliminare singoli risultati in Amazon Inspector Classic. Quando elimini un'esecuzione di valutazioni, verranno eliminati anche tutti i risultati e tutte le versioni del report a essa associati.

Puoi eliminare un'esecuzione di valutazioni anche usando l'API [DeleteAssessmentRun](#).

# Rapporti di valutazione

Un rapporto di valutazione di Amazon Inspector Classic è un documento che descrive in dettaglio cosa viene testato durante l'esecuzione della valutazione e i risultati della valutazione. Puoi archiviare i report, condividerli con il tuo team per le operazioni correttive o usarli per migliorare i dati relativi all'audit della conformità. Un report per un'esecuzione di valutazioni può essere generato dopo che l'esecuzione è stata completata.

## Note

Puoi generare report solo per le esecuzioni di valutazione che si verificano dopo il 25 aprile 2017, data in cui i report di valutazione in Amazon Inspector Classic sono diventati disponibili.

Puoi visualizzare i seguenti tipi di report di valutazione:

- **Rapporto sui risultati:** questo rapporto contiene le seguenti informazioni:
  - La sintesi della valutazione
  - EC2 istanze valutate durante l'esecuzione della valutazione
  - I pacchetti di regole inclusi nell'esecuzione di valutazioni
  - Informazioni dettagliate su ogni risultato, inclusi tutti i EC2 casi in cui è stato riscontrato il risultato
- **Rapporto completo:** questo rapporto contiene tutte le informazioni incluse in un rapporto sui risultati e fornisce inoltre l'elenco delle regole che sono state verificate rispetto ai casi inclusi nell'obiettivo della valutazione.

Per generare un report di valutazione

1. Nella pagina Assessment runs (Esecuzioni di valutazioni) individuare l'esecuzione di valutazioni per cui si desidera generare un report. Assicurarsi che lo stato sia impostato su Analysis complete (Analisi completata).
2. Nella colonna Reports (Report) per l'esecuzione di valutazioni desiderata, scegliere l'icona dei report.

**⚠ Important**

A partire dal 24 marzo 2025, i rapporti di valutazione non includeranno più informazioni sulla gravità per i risultati della raggiungibilità della rete. Queste informazioni sono disponibili nella console Amazon Inspector.

3. Nella finestra di dialogo Assessment report (Report di valutazione) scegliere il tipo di report che si desidera visualizzare (un report dei risultati o un report completo) e il formato del report (HTML o PDF). Scegliere quindi Generate report (Genera report).

Puoi generare report di valutazioni anche tramite l'API [GetAssessmentReport](#).

Per eliminare un report di valutazione, esegui questa procedura.

Per eliminare un report

- Nella pagina Assessment runs (Esecuzioni di valutazioni) scegliere l'esecuzione su cui si basa il report da eliminare e quindi scegliere Delete (Elimina). Quando viene richiesta la conferma, scegli Sì.

**⚠ Important**

In Amazon Inspector Classic, non puoi eliminare singoli report. Quando elimini un'esecuzione di valutazioni, verranno eliminati anche tutti i risultati e tutte le versioni del report a essa associati.

Puoi eliminare un'esecuzione di valutazioni anche usando l'API [DeleteAssessmentRun](#).

# Esclusioni in Amazon Inspector Classic

Le esclusioni sono il risultato delle esecuzioni di valutazione di Amazon Inspector Classic. Le esclusioni mostrano quale dei controlli di sicurezza non può essere completato e come risolvere gli errori. Ad esempio, i problemi possono essere causati dall'assenza di un agente sulle EC2 istanze della destinazione specificata, dall'uso di un sistema operativo non supportato o da errori imprevisti.

Puoi visualizzare le esclusioni nella pagina Assessment runs (Esecuzioni di valutazioni) della console. Per ulteriori informazioni, consulta [Visualizzazione delle esclusioni post-valutazione](#).

Per evitare di incorrere in AWS commissioni inutili, Amazon Inspector Classic consente di visualizzare in anteprima le esclusioni prima di eseguire una valutazione. Puoi visualizzare le anteprime nella pagina Assessment templates (Modelli di valutazioni) della console. Per ulteriori informazioni, consulta [Anteprima delle esclusioni](#).

## Note

Puoi generare le esclusioni post-valutazione solo per le esecuzioni successive al 25 giugno 2018. È stato allora che sono diventate disponibili le esclusioni in Amazon Inspector Classic. Tuttavia, le anteprime delle esclusioni sono disponibili per tutti i modelli di valutazione a prescindere dalla data.

## Argomenti

- [Tipi di esclusione](#)
- [Anteprima delle esclusioni](#)
- [Visualizzazione delle esclusioni post-valutazione](#)

## Tipi di esclusione

Amazon Inspector Classic può produrre i seguenti tipi di esclusione.

Tipo di esclusione	Description	Raccomandazione									
Nessuna istanza in target	Non ci sono EC2 istanze con i tag specificati nell'obiettivo di valutazione.	Verifica che i tag nel tuo obiettivo di valutazione corrispondano ai tag dell' EC2 istanza di destinazione.									
L'agente è già in esecuzione	È già in corso un'esecuzione di valutazione sull' EC2 istanza di destinazione.	Attendi il completamento dell'esecuzione corrente della valutazione sull' EC2 istanza di destinazione.									
Agente non trovato	Non è stato trovato un agente Amazon Inspector Classic nell'istanza	Installa o reinstalla un agente Amazon Inspector Classic sull'istanza									

Tipo di esclusione	Description	Raccomandazione									
	di destinazione EC2 .	di destinazione. EC2 Per ulteriori informazioni, consulta <a href="#">Installazione degli agenti Amazon Inspector Classic.</a>									
L'agente non è integro	L'agente Amazon Inspector Classic sull' EC2 istanza di destinazione non è integro.	Verifica lo stato dell'agente Amazon Inspector Classic su questa istanza e intraprendi le azioni necessarie. Per ulteriori informazioni, consulta <a href="#">Agenti Inspector.</a>									

Tipo di esclusione	Description	Raccomandazione									
Versioni del sistema operativo dell'EC2 operanti non supportate	Il sistema operativo dell'EC2 istanza di destinazione non è supportato per le valutazioni di Amazon Inspector Classic.	Rimuovi l'EC2 istanza di destinazione dall'obiettivo di valutazione o crea una destinazione che non includa questa istanza. Per un elenco dei sistemi operativi supportati, consulta <a href="#">Regioni e sistemi operativi supportati da Amazon Inspector Classic</a> .									

Tipo di esclusione	Description	Raccomandazione									
Pacchetti di regole obsolete	Il modello di valutazione include un pacchetto di regole obsoleto.	Creare un modello di valutazione senza il pacchetto di regole obsoleto e utilizzarlo per l'esecuzione di valutazioni future.									

Tipo di esclusione	Description	Raccomandazione									
Pacchetti di regole non supportati dal sistema operativo	Il sistema operativo dell' EC2 istanza di destinazione non è supportato da un pacchetto di regole incluso nel modello di valutazione.	Crea un modello di valutazione senza i pacchetti di regole in conflitto o rimuovi l' EC2 istanza di destinazione dal modello di valutazione. Per un elenco di pacchetti di regole supportati dal sistema operativo , vedi <a href="#">Disponibilità di pacchetti di regole tra i sistemi operativi supportati.</a>									

Tipo di esclusione	Description	Raccomandazione									
Errore di valutazione delle regole per singole istanze	Un errore interno ha impedito il completamento della valutazione delle regole per questa istanza.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di valutazione delle regole	Un errore interno ha impedito il completamento della valutazione delle regole per questa valutazione.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di raggiungibilità della rete: intern	Si è verificato un errore interno per cui la valutazione di Network Reachability non è riuscita per le verifiche delle porte raggiungibili da Internet. È possibile ottenere risultati per altri tipi di Network Reachability.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di raggiungibilità della rete: Intern tramite un Applicon Load Balancer	Un errore interno ha causato il fallimento di una valutazione della raggiungibilità della rete durante il controllo delle porte raggiungibili da Internet tramite un Applicon Load Balancer. È possibile ottenere risultati per altri tipi di Network Reachability.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di raggiungibilità della rete: Internamente un sistema di bilanciamento del carico Elastic Load Balancing	Un errore interno ha causato il fallimento di una valutazione della raggiungibilità della rete durante il controllo delle porte raggiungibili da Internet tramite un sistema di bilanciamento del carico Elastic Load Balancing. È possibile ottenere risultati per altri tipi di Network Reachability.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di raggiungibilità della rete: VPN	Si è verificato un errore interno per cui la valutazione di Network Reachability non è riuscita per le verifiche delle porte raggiungibili da VPN. È possibile ottenere risultati per altri tipi di Network Reachability.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di raggiungibilità della rete — AWS Direct Connect	Un errore interno ha causato il fallimento di una valutazione della raggiungibilità della rete durante i controlli delle porte raggiungibili tramite AWS Direct Connect. È possibile ottenere risultati per altri tipi di Network Reachability.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

Tipo di esclusione	Description	Raccomandazione									
Errore di raggiungibilità della rete: peerir VPC	Si è verificato un errore interno per cui la valutazione di Network Reachability non è riuscita per le verifiche delle porte raggiungibili da VPC con peering. È possibile ottenere risultati per altri tipi di Network Reachability.	Provare a eseguire di nuovo la valutazione. Contattare il <a href="#">supporto</a> se l'esclusione persiste quando si esegue nuovamente la valutazione.									

## Anteprima delle esclusioni

Amazon Inspector Classic consente di visualizzare in anteprima le potenziali esclusioni prima di eseguire una valutazione.

Per visualizzare l'anteprima delle esclusioni della valutazione

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo.  
<https://console.aws.amazon.com/inspector/>
2. Nel riquadro di navigazione selezionare Assessment templates (Modelli di valutazione).
3. Espandere un modello e nella sezione Assessment templates (Modelli di valutazione) scegliere Preview exclusions (Anteprima delle esclusioni).
4. Esaminare le descrizioni di tutte le esclusioni rilevate e i suggerimenti per la loro risoluzione.

È inoltre possibile elencare e descrivere le esclusioni tramite le operazioni [ListExclusions](#) e [DescribeExclusions](#).

## Visualizzazione delle esclusioni post-valutazione

Dopo l'esecuzione di una valutazione, è possibile visualizzare i dettagli di qualsiasi esclusione.

Per visualizzare i dettagli delle esclusioni

1. Accedi a Console di gestione AWS e apri la console Amazon Inspector Classic all'indirizzo.  
<https://console.aws.amazon.com/inspector/>
2. Nel riquadro di navigazione selezionare Assessment runs (Esecuzioni di valutazione).
3. Nella colonna Exclusions (Esclusioni) scegliere il collegamento attivo associato a un'esecuzione di valutazioni.
4. Esaminare le descrizioni di tutte le esclusioni rilevate e i suggerimenti per la loro risoluzione.

È inoltre possibile elencare e descrivere le esclusioni tramite le operazioni [ListExclusions](#) e [DescribeExclusions](#).

# Pacchetti di regole Amazon Inspector Classic per i sistemi operativi supportati

Puoi eseguire pacchetti di regole Amazon Inspector Classic sulle istanze EC2 incluse nei tuoi obiettivi di valutazione. Nella tabella seguente sono indicati i pacchetti di regole disponibili per i sistemi operativi supportati.

## Important

Puoi eseguire una valutazione senza agenti con il pacchetto di regole di [raggiungibilità della rete](#) su qualsiasi istanza EC2 indipendentemente dal sistema operativo.

## Note

Per ulteriori informazioni sui sistemi operativi supportati, consulta [Regioni e sistemi operativi supportati da Amazon Inspector Classic](#).

Sistema operativo supportato	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Best practice di sicurezza	Runtime Behavior Analysis
Amazon Linux 2	Supportato	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2018.	Supportato	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2017.	Supportato	Supportato	Supportato	Supportata	Deprecated

Sistema operativo supportato	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Best practice di sicurezza	Runtime Behavior Analysis
Amazon Linux 2017.	Supportata	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2016.	Supportata	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2016.	Supportata	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2015.	Supportata	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2015.	Supportata	Supportato	Supportato	Supportata	Deprecated
Amazon Linux 2014.	Supportata		Supportato	Supportata	
Amazon Linux 2014.	Supportata		Supportato	Supportata	
Amazon Linux 2013.	Supportata		Supportato	Supportata	

Sistema operativo	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Best practice di sicurezza	Runtime Behavior Analysis
Amazon Linux 2013.	Supportata		Supportato	Supportata	
Amazon Linux 2012.	Supportata		Supportato	Supportata	
Amazon Linux 2012.	Supportata		Supportato	Supportata	
Amazon Linux 2012.	Supportata		Supportato	Supportata	
Ubuntu 20.04 LTS	Supportata		Supportato	Supportata	
Ubuntu 18.04 LTS	Supportata	Supportato	Supportato	Supportata	Deprecated
Ubuntu 16.04 LTS	Supportata	Supportato	Supportato	Supportata	Deprecated
Ubuntu 14.04 LTS	Supportata	Supportato	Supportato	Supportata	Deprecated

Sistema operativo	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Best practice di sicurezza	Runtime Behavior Analysis
Debian 10.x, 9.0 - 9.5, 8.0 - 8.7	Supportata		Supportato	Supportata	
RHEL 8.x	Supportata		Supportato	Supportata	
RHEL 7.6 - 7.x	Supportata	Supportato	Supportato	Supportata	
RHEL 6.2 - 6.9, 7.2 - 7.5	Supportata	Supportato	Supportato	Supportata	Deprecated
CentOS 7.6 - 7.X	Supportata	Supportato	Supportato	Supportata	

Sistemi operativi supportati	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Best practice di sicurezza	Runtime Behavior Analysis
CentOS 6.2 – 6.9, 7.2 – 7.5	Supportata	Supportato	Supportato	Supportata	Deprecated
Windows Server 2019 Base	Supportata		Supportata		
Windows Server 2016 Standard	Supportata	Supportato	Supportata		Deprecated
Windows Server 2012 R2	Supportata	Supportato	Supportata		Deprecated
Windows Server 2012	Supportata	Supportato	Supportata		Deprecated
Windows Server 2008 R2	Supportata	Supportato	Supportata		Deprecated

# Registrazione delle chiamate API Amazon Inspector Classic con AWS CloudTrail

Amazon Inspector Classic è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon Inspector Classic. CloudTrail acquisisce tutte le chiamate API per Amazon Inspector Classic come eventi, incluse le chiamate dalla console Amazon Inspector Classic e le chiamate in codice alle operazioni dell'API Amazon Inspector Classic. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon Inspector Classic. Se non configuri un trail, puoi comunque visualizzare gli eventi più recenti nella console CloudTrail in Event history (Cronologia eventi). Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon Inspector Classic, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e altro ancora.

Per ulteriori informazioni CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#). Per un elenco completo delle operazioni dell'API Amazon Inspector Classic, consulta [Azioni](#) nel riferimento all'API Amazon Inspector Classic.

## Informazioni su Amazon Inspector Classic in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon Inspector Classic, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS . Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon Inspector Classic, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail si applica a tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un trail](#)
- [CloudTrail Servizi e integrazioni supportati](#)

- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

CloudTrail registra tutte le operazioni di Amazon Inspector Classic, incluse le operazioni di sola lettura, `ListAssessmentRuns` come `DescribeAssessmentTargets` and, e le operazioni di gestione, come e. `AddAttributesToFindings` `CreateAssessmentTemplate`

#### Note

CloudTrail registra solo le informazioni di richiesta relative alle operazioni di sola lettura di Amazon Inspector Classic. Le informazioni relative alla richiesta e alla risposta vengono registrate per tutte le altre operazioni di Amazon Inspector Classic.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM)
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

## Informazioni sulle voci dei file di log di Amazon Inspector Classic

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione e altri parametri della richiesta. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra il funzionamento di Amazon Inspector Classic `CreateResourceGroup`:

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2016-04-14T17:05:54Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "userName": "Alice"
      }
    }
  },
  "eventTime": "2016-04-14T17:12:34Z",
  "eventSource": "inspector.amazonaws.com",
  "eventName": "CreateResourceGroup",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.179",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "resourceGroupTags": [
      {
        "key": "Name",
        "value": "ExampleEC2Instance"
      }
    ]
  },
  "responseElements": {
    "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-oc1RMp8B"
  },
  "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
  "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
  "eventType": "AwsApiCall",
}
```

```
"apiVersion": "v20160216",  
"recipientAccountId": "444455556666"  
}
```

# Monitoraggio di Amazon Inspector Classic tramite Amazon CloudWatch

Puoi monitorare Amazon Inspector Classic utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi in metriche leggibili quasi in tempo reale. Per impostazione predefinita, Amazon Inspector Classic invia dati metrici CloudWatch in periodi di 5 minuti. Puoi utilizzare il Console di gestione AWS, AWS CLI, il o un'API per visualizzare i parametri a cui invia Amazon Inspector Classic. CloudWatch

Per ulteriori informazioni su Amazon CloudWatch, consulta la [Amazon CloudWatch User Guide](#).

## Metriche di Amazon Inspector Classic CloudWatch

Lo spazio dei nomi Amazon Inspector Classic include i seguenti parametri.

### Parametri di **AssessmentTargetARN**

Metrica	Description
TotalMatchingAgents	Numero di agenti che corrispondono a questo target
TotalHealthyAgents	Numero di agenti integri che corrispondono a questo target
TotalAssessmentRuns	Numero di esecuzioni di valutazioni per questo target
TotalAssessmentRun Findings	Numero di risultati per questo target

### Parametri di **AssessmentTemplateARN**

Metrica	Description
TotalMatchingAgents	Numero di agenti che corrispondono a questo modello
TotalHealthyAgents	Numero di agenti integri che corrispondono a questo modello
TotalAssessmentRuns	Numero di esecuzioni di valutazioni per questo modello

Metrica	Description
TotalAssessmentRun Findings	Numero di risultati per questo modello

### Parametro Aggregate

Metrica	Description
TotalAssessmentRuns	Numero di valutazioni eseguite in questo account AWS

# Configurazione di Amazon Inspector Classic tramite AWS CloudFormation

Per informazioni di riferimento sulle risorse di Amazon Inspector Classic supportate da AWS CloudFormation, consulta i seguenti argomenti:

- [AWS::Inspector::AssessmentTarget](#)
- [AWS::Inspector::AssessmentTemplate](#)
- [AWS::Inspector::ResourceGroup](#)

## Important

Per gli elenchi dei pacchetti ARNs di regole di Amazon Inspector Classic AWS nelle regioni supportate, consulta. [Amazon Inspector Classic ARNS per pacchetti di regole](#)

# Integrazione con AWS Security Hub CSPM

[AWS Security Hub CSPM](#) ti offre una visione completa del tuo stato di sicurezza AWS e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Security Hub CSPM raccoglie dati sulla sicurezza da AWS account, servizi e prodotti partner di terze parti supportati e ti aiuta ad analizzare le tendenze della sicurezza e identificare i problemi di sicurezza con la massima priorità.

L'integrazione di Amazon Inspector con Security Hub CSPM consente di inviare i risultati da Amazon Inspector a Security Hub CSPM. Security Hub CSPM può quindi includere tali risultati nell'analisi del livello di sicurezza dell'utente.

## Indice

- [In che modo Amazon Inspector invia i risultati al Security Hub CSPM](#)
  - [Tipi di risultati inviati da Amazon Inspector](#)
  - [Latenza per l'invio degli esiti](#)
  - [Riprova quando Security Hub CSPM non è disponibile](#)
  - [Aggiornamento degli esiti esistenti CSPM Security Hub](#)
- [Risultati tipici di Amazon Inspector](#)
- [Abilitazione e configurazione dell'integrazione](#)
- [Come interrompere l'invio degli esiti](#)

## In che modo Amazon Inspector invia i risultati al Security Hub CSPM

In CSPM Security Hub, i problemi di sicurezza vengono monitorati come esiti. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub CSPM dispone anche di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

CSPM Security Hub fornisce strumenti per gestire gli esiti da tutte queste origini. È possibile visualizzare e filtrare gli elenchi di esiti e visualizzare i dettagli per un riscontro. Consulta [Visualizzazione dei risultati](#) nella Guida per l'utente di AWS Security Hub . È inoltre possibile monitorare lo stato di un'indagine in un esito. Consulta [Operazioni sui risultati](#) nella Guida per l'utente di AWS Security Hub .

Tutti i risultati in Security Hub CSPM utilizzano un formato JSON standard chiamato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato corrente dell'esito. Consulta [AWS Security Finding Format \(ASFF\)](#) nella Guida per l'AWS Security Hub utente.

Amazon Inspector è uno dei AWS servizi che invia i risultati al Security Hub CSPM.

## Tipi di risultati inviati da Amazon Inspector

Amazon Inspector invia tutti i risultati generati a Security Hub CSPM.

Amazon Inspector invia i risultati a Security Hub CSPM utilizzando il Security [Finding Format \(AWS ASFF\)](#). In ASFF, il Types campo fornisce il tipo di esito. I risultati di Amazon Inspector possono avere i seguenti valori per. Types

- Software e configurazione Checks/Vulnerabilities/CVE
- Checks/AWS Sicurezza del software e della configurazione Migliore Practices/Network raggiungibilità
- Software e configurazione Checks/Industry e benchmark normativi per il rafforzamento degli Standards/CIS host

## Latenza per l'invio degli esiti

Quando Amazon Inspector crea una nuova scoperta, di solito viene inviata al Security Hub CSPM entro cinque minuti.

## Riprovare quando Security Hub CSPM non è disponibile

Se Security Hub CSPM non è disponibile, Amazon Inspector riprova a inviare i risultati finché non vengono ricevuti.

## Aggiornamento degli esiti esistenti CSPM Security Hub

Dopo aver inviato un risultato a Security Hub CSPM, Amazon Inspector lo aggiorna per riflettere ulteriori osservazioni sull'attività di ricerca. Ciò comporterà un minor numero di risultati di Amazon Inspector in Security Hub CSPM rispetto ad Amazon Inspector.

## Risultati tipici di Amazon Inspector

Amazon Inspector invia i risultati a Security Hub CSPM utilizzando il [AWS Security Finding Format \(ASFF\)](#).

Ecco un esempio di una tipica scoperta di Amazon Inspector.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
reachable from the internet. You can install the Inspector agent on this instance
and re-run the assessment to check for any process listening on this port. The
instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
  }
}
```

```

    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubect1"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IPv4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ]
},

```

```
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE"
}
```

## Abilitazione e configurazione dell'integrazione

Per utilizzare l'integrazione con Security Hub CSPM, è necessario abilitare Security Hub CSPM. Per informazioni su come abilitare Security Hub CSPM, vedere [Configurazione di Security Hub nella Guida](#) per l'AWS Security Hub utente.

Quando abiliti sia Amazon Inspector che Security Hub CSPM, l'integrazione viene abilitata automaticamente. Amazon Inspector inizia a inviare i risultati al Security Hub CSPM.

## Come interrompere l'invio degli esiti

Per interrompere l'invio degli esiti a CSPM Security Hub, è possibile utilizzare la console CSPM Security Hub o l'API.

Consulta [Disabilitazione e abilitazione del flusso di risultati da un'integrazione \(console\)](#) o [Disabilitazione del flusso di risultati da un'integrazione \(API Security Hub, AWS CLI\)](#) nella Guida per l'utente.AWS Security Hub

# Amazon Inspector Classic ARNs

A ogni tipo di risorsa e pacchetto di regole in Amazon Inspector Classic è associato un Amazon Resource Name (ARN) univoco.

## Indice

- [ARNs per le risorse di Amazon Inspector Classic](#)
- [Amazon Inspector Classic ARNs per pacchetti di regole](#)
  - [Stati Uniti orientali \(Ohio\)](#)
  - [Stati Uniti orientali \(Virginia settentrionale\)](#)
  - [Stati Uniti occidentali \(California settentrionale\)](#)
  - [Stati Uniti occidentali \(Oregon\)](#)
  - [Asia Pacifico \(Mumbai\)](#)
  - [Asia Pacifico \(Seul\)](#)
  - [Asia Pacifico \(Sydney\)](#)
  - [Asia Pacifico \(Tokyo\)](#)
  - [Europa \(Francoforte\)](#)
  - [Europa \(Irlanda\)](#)
  - [Europa \(Londra\)](#)
  - [Europa \(Stoccolma\)](#)
  - [AWS GovCloud \(Stati Uniti orientali\)](#)
  - [AWS GovCloud \(Stati Uniti occidentali\)](#)

## ARNs per le risorse di Amazon Inspector Classic

In Amazon Inspector Classic, le risorse principali sono gruppi di risorse, obiettivi di valutazione, modelli di valutazione, esecuzioni di valutazione e risultati. A queste risorse sono associati Amazon Resource Names (ARNs) univoci, come illustrato nella tabella seguente.

Tipo di risorsa	Formato ARN
Gruppo di risorse	arn:aws:inspector: <i>region:account-id</i> :resource group/ <i>ID</i>
Target di valutazione	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i>
Modello di valutazione	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i> :template: <i>ID</i>
Esecuzione di valutazioni	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i> /template/ <i>ID</i> /run/ <i>ID</i>
Risultato	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i> /template/ <i>ID</i> /run/ <i>ID</i> /finding/ <i>ID</i>

## Amazon Inspector Classic ARNS per pacchetti di regole

Le tabelle seguenti mostrano i pacchetti ARNs di regole di Amazon Inspector Classic in tutte le regioni supportate.

### Argomenti

- [Stati Uniti orientali \(Ohio\)](#)
- [Stati Uniti orientali \(Virginia settentrionale\)](#)
- [Stati Uniti occidentali \(California settentrionale\)](#)
- [Stati Uniti occidentali \(Oregon\)](#)
- [Asia Pacifico \(Mumbai\)](#)
- [Asia Pacifico \(Seul\)](#)
- [Asia Pacifico \(Sydney\)](#)
- [Asia Pacifico \(Tokyo\)](#)
- [Europa \(Francoforte\)](#)
- [Europa \(Irlanda\)](#)
- [Europa \(Londra\)](#)
- [Europa \(Stoccolma\)](#)

- [AWS GovCloud \(Stati Uniti orientali\)](#)
- [AWS GovCloud \(Stati Uniti occidentali\)](#)

## Stati Uniti orientali (Ohio)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-JnA8Zp85</code>
CIS Operating System Security Configuration Benchmarks	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-m8r61nnh</code>
Network Reachability	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-cE4kTR30</code>
Best practice di sicurezza	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-AxKmMHPX</code>

## Stati Uniti orientali (Virginia settentrionale)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	<code>arn:aws:inspector:us-east-1:31611246:3485:rulespackage/0-gEjTy7T7</code>

Nome del pacchetto di regole	ARN
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8
Network Reachability	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd
Best practice di sicurezza	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q

## Stati Uniti occidentali (California settentrionale)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoV0a
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX
Network Reachability	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF

Nome del pacchetto di regole	ARN
Best practice di sicurezza	arn:aws:inspector: us-west-1:16698759 0008:rulespackage/ 0-byoQRFYm

## Stati Uniti occidentali (Oregon)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-9hgA516p
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-H5hpSawc
Network Reachability	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-rD1z6dp1
Best practice di sicurezza	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-JJ0tZiqQ

## Asia Pacifico (Mumbai)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9d0</code>
CIS Operating System Security Configuration Benchmarks	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSU1X14m</code>
Network Reachability	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1</code>
Best practice di sicurezza	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj</code>

## Asia Pacifico (Seul)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	<code>arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc</code>
CIS Operating System Security Configuration Benchmarks	<code>arn:aws:inspector:ap-northeast-2:526</code>

Nome del pacchetto di regole	ARN
	946625049:rulespackage/0-T9srhg1z
Network Reachability	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-s30mLzhL
Best practice di sicurezza	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-2WRpmi4n

## Asia Pacifico (Sydney)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-D5TGAXiR
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-Vkd2Vxjq
Network Reachability	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-FLcuV4Gz
Best practice di sicurezza	arn:aws:inspector:ap-southeast-2:454

Nome del pacchetto di regole	ARN
	640832652:rulespackage/0-asL6HRgN

## Asia Pacifico (Tokyo)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-gHP9oWNT
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-7WNjqgGu
Network Reachability	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-YI95DVd7
Best practice di sicurezza	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-bBUQnxMq

## Europa (Francoforte)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-central-1:53750

Nome del pacchetto di regole	ARN
	3971621:rulespackage/0-wNqHa8M9
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8
Network Reachability	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
Best practice di sicurezza	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

## Europa (Irlanda)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
Network Reachability	arn:aws:inspector:eu-west-1:35755712

Nome del pacchetto di regole	ARN
	9151:rulespackage/ 0-SPzU33xe
Best practice di sicurezza	arn:aws:inspector: eu-west-1:35755712 9151:rulespackage/ 0-SnojL3Z6

## Europa (Londra)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-kZGCqcE1
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-IeCjwf1W
Network Reachability	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-AizSYyNq
Best practice di sicurezza	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-XApUiSaP

## Europa (Stoccolma)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	<code>arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd</code>
CIS Operating System Security Configuration Benchmarks	<code>arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f</code>
Network Reachability	<code>arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu</code>
Best practice di sicurezza	<code>arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQsSf</code>

## AWS GovCloud (Stati Uniti orientali)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	<code>arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFu0b</code>
CIS Operating System Security Configuration Benchmarks	<code>arn:aws-us-gov:inspector:us-gov-east</code>

Nome del pacchetto di regole	ARN
	-1:206278770380:rulespackage/0-pTLCdIww
Best practice di sicurezza	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

## AWS GovCloud (Stati Uniti occidentali)

Nome del pacchetto di regole	ARN
Common Vulnerabilities and Exposures	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
CIS Operating System Security Configuration Benchmarks	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CF0uc
Best practice di sicurezza	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-r0TGqe5G

# Cronologia dei documenti

La tabella seguente descrive la cronologia dei rilasci della documentazione di Amazon Inspector Classic dopo maggio 2018.

Modifica	Descrizione	Data
<a href="#">Avviso di fine del supporto</a>	Avviso di fine del supporto: il 20 maggio 2026, AWS terminerà il supporto per Amazon Inspector Classic. Dopo il 20 maggio 2026, non potrai più accedere alla console Amazon Inspector Classic o alle risorse di Amazon Inspector Classic. Per ulteriori informazioni, consulta la pagina relativa <a href="#">alla fine del supporto di Amazon Inspector Classic</a> .	20 maggio 2025
<a href="#">Best practice di sicurezza aggiornate per le password</a>	I requisiti delle best practice di sicurezza di Amazon Inspector Classic per la lunghezza e la complessità delle password delle istanze EC2 sono stati aggiornati. Vedi <a href="#">Configurazione della lunghezza minima della password</a> e <a href="#">Configurazione della complessità della password</a>	8 marzo 2021
<a href="#">È stato aggiunto il supporto per le versioni più recenti del sistema operativo</a>	Amazon Inspector Classic ora supporta le seguenti versioni del sistema operativo: Ubuntu 20.4 LTS, Debian 10.x, RHEL	15 ottobre 2020

8.x e Windows Server 2019  
Base.

[Informazioni sulla sicurezza consolidate in un nuovo capitolo sulla sicurezza](#)

Le informazioni sulla sicurezza per Amazon Inspector Classic, incluse le informazioni sulla gestione delle identità e degli accessi, sono consolidate in un capitolo sulla sicurezza. Consulta [la sezione Sicurezza in Amazon Inspector Classic](#).

7 aprile 2020

[Documentazione aggiornata per rimuovere il supporto per il pacchetto di regole di Runtime Behavior Analysis.](#)

Sono stati aggiornati più argomenti per rimuovere informazioni sul pacchetto di regole Runtime Behavior Analysis, che non è più supportato.

5 settembre 2019

[Supporto per il sistema operativo aggiunto](#)

È stato aggiunto il supporto Amazon Inspector Classic per CentOS 7.6. Per ulteriori informazioni, consulta le [aree geografiche e i sistemi operativi supportati da Amazon Inspector Classic e la disponibilità dei pacchetti di regole tra i sistemi operativi supportati](#).

3 dicembre 2018

<a href="#">Nuovo contenuto</a>	È stato aggiunto il pacchetto di regole di raggiungibilità della rete Amazon Inspector Classic, che consente agli utenti di eseguire valutazioni senza agenti che analizzano la configurazione della rete alla ricerca di vulnerabilità di sicurezza. Per ulteriori informazioni, consulta la sezione relativa alla <a href="#">raggiungibilità della rete</a> .	9 novembre 2018
<a href="#">Supporto per il sistema operativo aggiunto</a>	È stato aggiunto il supporto Amazon Inspector Classic per RHEL 7.6. Per ulteriori informazioni, consulta le <a href="#">aree geografiche e i sistemi operativi supportati da Amazon Inspector Classic e la disponibilità dei pacchetti di regole tra i sistemi operativi supportati</a> .	30 ottobre 2018
<a href="#">Aggiunto il supporto del sistema operativo</a>	Aggiunta del supporto per vari sistemi operativi al pacchetto di regole CIS Benchmark. Per ulteriori informazioni, consulta <a href="#">Center for Internet Security (CIS) Benchmarks</a> e <a href="#">Disponibilità dei pacchetti di regole nei sistemi operativi supportati</a> .	13 agosto 2018
<a href="#">È stato aggiunto il supporto per una regione</a>	È stato aggiunto il supporto delle regioni per AWS GovCloud (US).	13 giugno 2018

La tabella seguente descrive la cronologia dei rilasci della documentazione di Amazon Inspector Classic prima di giugno 2018.

Modifica	Descrizione	Data
Nuovo contenuto	È stata aggiunta la possibilità di indirizzare tutte le istanze Amazon EC2 in un account. Per ulteriori informazioni, consulta <a href="#">Obiettivi di valutazione di Amazon Inspector Classic</a> .	24 maggio 2018
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto Amazon Inspector Classic per Amazon Linux 2018.03 e Ubuntu 18.04.	15 maggio 2018
Nuovo contenuto	È stata aggiunta la possibilità di configurare valutazioni ricorrenti di Amazon Inspector Classic.	30 Aprile 2018
Nuovo contenuto	È stata aggiunta la possibilità di installare un agente Amazon Inspector Classic tramite la console.	30 Aprile 2018
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto Amazon Inspector Classic per Amazon Linux 2.	13 marzo 2018
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto di valutazione Amazon Inspector Classic per Windows Server 2016 Base.	20 febbraio 2018

Modifica	Descrizione	Data
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto Amazon Inspector Classic per la US East (Ohio) regione.	7 febbraio 2018
Nuovo contenuto	Le valutazioni di Amazon Inspector Classic ora possono essere eseguite quando il modulo kernel non è disponibile.	11 gennaio 2018
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto Amazon Inspector Classic per la EU (Frankfurt) regione.	19 dicembre 2017
Nuovo contenuto	È stata aggiunta la possibilità di controllare lo stato degli agenti di Amazon Inspector Classic con l'API e la console Amazon Inspector Classic.	15 dicembre 2017
Nuovo contenuto	Sono state aggiunte le seguenti caratteristiche: <ul style="list-style-type: none"><li>• Utilizzo del ruolo collegato al servizio</li><li>• L'AMI dell'agente Amazon Inspector Classic è disponibile nel Marketplace AWS</li><li>• Modelli Amazon Inspector Classic CloudFormation</li></ul>	5 dicembre 2017
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto di valutazione Amazon Inspector Classic per CentOS 7.4.	9 novembre 2017

Modifica	Descrizione	Data
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto di valutazione Amazon Inspector Classic per Amazon Linux 2017.09.	11 ottobre 2017
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto di valutazione Amazon Inspector Classic per RHEL 7.4.	20 febbraio 2018
Aggiunta dell'idoneità HIPAA	Amazon Inspector Classic è ora idoneo alla normativa HIPAA.	31 luglio 2017
Nuovo contenuto	È stata aggiunta la possibilità di attivare automaticamente la valutazione della sicurezza di Amazon Inspector Classic con Amazon CloudWatch Events.	27 luglio 2017
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto Amazon Inspector Classic per la US West (N. California) regione.	06 giugno 2018
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto di valutazione Amazon Inspector Classic per RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9 e CentOS 7.2-7.3.	23 maggio 2017
Aggiunto il supporto del sistema operativo	È stato aggiunto il supporto di valutazione Amazon Inspector Classic per Amazon Linux 2017.03.	25 Aprile 2017

Modifica	Descrizione	Data
Nuovi contenuti e aggiunto il supporto del sistema operativo	Aggiunto: <ul style="list-style-type: none"><li>• Supporto di Amazon Inspector Classic per Ubuntu 16.04.</li><li>• Disponibilità del modello Lambda per automatizzare le operazioni di Amazon Inspector Classic.</li></ul>	5 gennaio 2017
Nuovo supporto dei sistemi operativi	È stato aggiunto il supporto di Amazon Inspector Classic per Microsoft Windows.	26 agosto 2016
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto Amazon Inspector Classic per la Asia Pacific (Seoul) regione.	26 agosto 2016
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto Amazon Inspector Classic per la Asia Pacific (Mumbai) regione.	25 Aprile 2016
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto Amazon Inspector Classic per la Asia Pacific (Sydney) regione.	25 Aprile 2016
Avvio del servizio	Lancio dei servizi Amazon Inspector Classic.	7 ottobre 2015

# AWS Glossario

Per la AWS terminologia più recente, consultate il [AWS glossario](#) nella sezione Reference. Glossario AWS