[Publish] - 13. Las instancias de EC2 no deben estar asociadas con una Dirección IP Elástica o Pública

El hallazgo de seguridad **"Las instancias de EC2 no deben estar asociadas con una Dirección IP Elástica o Pública"** se enfoca en un riesgo de seguridad común pero significativo. Asignar una dirección IP pública a una instancia EC2 la conecta directamente a internet, haciéndola accesible desde cualquier parte del mundo. Esto efectivamente pone una "puerta principal" en tu servidor, exponiéndolo a:

- **Escaneos Automatizados:** Actores maliciosos escanean constantemente rangos de IP públicas en busca de puertos abiertos y vulnerabilidades conocidas.
- **Ataques de Fuerza Bruta:** Servicios expuestos como SSH (puerto 22) o RDP (puerto 3389) son objetivos principales para ataques automatizados de adivinación de contraseñas.
- **Explotación de Vulnerabilidades (Zero-Day):** Si se descubre una vulnerabilidad en el software que se ejecuta en la instancia, los atacantes pueden explotarla directamente.
- **Ataques de Denegación de Servicio (DoS):** La instancia puede ser el objetivo de inundaciones de tráfico, lo que podría sobrecargarla y causar una interrupción del servicio.

La mejor práctica es colocar las instancias en subredes privadas y utilizar un servicio gestionado de AWS, como un Application Load Balancer o un NAT Gateway, para manejar el tráfico de internet. Esto crea una capa protectora, reduciendo la superficie de ataque directa de la instancia.

Análisis de las Instancias EC2 Reportadas

Las siguientes instancias de EC2 han sido identificadas por tener direcciones IP públicas. Es necesario investigar su propósito para determinar la remediación adecuada.

Tipo	Nombre	Número de cuenta
Instance	i-000fbf2a79f92c3ab	002670977573
Instance	i-00248cdd12c9ceb94	002670977573
Instance	i-0097dc2f5bc287109	002670977573
Instance	i-009e9de48650cfbfe	002670977573
Instance	i-0102bd635a284e84e	398984081329
Instance	i-0118ff93c3766f93b	002670977573

Instance	i-014ba36b999dfa791	613703092215
Instance	i-017853c6643601641	002670977573
Instance	i-0195867f8c0aa2c79	002670977573
Instance	i-01bcd4c331a68a6a2	002670977573
Instance	i-0201d025e251cce12	002670977573
Instance	i-020ef317b525398a2	002670977573
Instance	i-02107fa019533cfc9	002670977573
Instance	i-025714965e3a949f0	002670977573
Instance	i-028c3fe2a5fe47e16	613703092215
Instance	i-0361d9073c0b9d8da	002670977573
Instance	i-0370e6a66e2bb202e	398984081329
Instance	i-0375aeb0c2e4d3607	002670977573
Instance	i-0375b08b8377e65f4	002670977573
Instance	i-03851a61748e27931	002670977573
Instance	i-03c171fa80e8824ff	002670977573
Instance	i-03ea3bdeea26ae150	398984081329
Instance	i-03ee29b7c46530ef3	002670977573
Instance	i-03f9ade49d4949e8f	613703092215
Instance	i-044ed9556b72bf573	002670977573
Instance	i-046ceefd81c10686e	890342916428
Instance	i-04aa2e5982c74273f	890342916428
Instance	i-04ce7e0f7ee914dad	002670977573
Instance	i-0549f3dd66e271055	890342916428
Instance	i-054f00812fab2a4f9	002670977573
Instance	i-05545802b22afd142	002670977573

Instance	i-057082e3663b766a9	890342916428
Instance	i-05786c8888262fa7a	002670977573
Instance	i-05de17ee861eb96ab	174771279728
Instance	i-05fbfb9d8a620ecc7	613703092215
Instance	i-060952b97ecbb5ea3	890342916428
Instance	i-06915e3e672b0a8cf	002670977573
Instance	i-06ad74674e8a48f89	002670977573
Instance	i-06af34899b8ab0913	002670977573
Instance	i-06cd40cf562734ae7	002670977573
Instance	i-06fe4642fc9338d60	398984081329
Instance	i-07554df176f70b0d2	002670977573
Instance	i-0773a446fabab9981	890342916428
Instance	i-07980ac58766e24b4	002670977573
Instance	i-079e7eb2666f902c6	002670977573
Instance	i-07d79434b4e803164	002670977573
Instance	i-08249aa35510d0c6f	890342916428
Instance	i-083b8a90b48de6e49	398984081329
Instance	i-085224b6e33b24fad	002670977573
Instance	i-0855a67c9803befd4	002670977573
Instance	i-087fb602b20252e59	890342916428
Instance	i-08c363b3afa916266	002670977573
Instance	i-08e561cb0648b48e7	002670977573
Instance	i-08e60134966ec5a6b	002670977573
Instance	i-08f0c6ec87a595923	002670977573
Instance	i-092ac23d761c67be1	002670977573

Instance	i-095bb40653ef2d7e0	890342916428
Instance	i-09c8ea427f61934c0	002670977573
Instance	i-09d82919d2e96e71b	002670977573
Instance	i-09e67761338c6c937	002670977573
Instance	i-0a1306b1d2e1d2d86	613703092215
Instance	i-0a3dc851efc9b9949	890342916428
Instance	i-0a4d4b0cac465d090	398984081329
Instance	i-0a59a83c85bb62e27	890342916428
Instance	i-0a70ed56f594c86c6	890342916428
Instance	i-0a7a3dc890bae02d6	002670977573
Instance	i-0a7aaf6a2b4078899	002670977573
Instance	i-0ab7c03cebd52828e	002670977573
Instance	i-0abedd6fed83f63da	613703092215
Instance	i-0acf4b80216e0bbf8	002670977573
Instance	i-0aea114ebcc9fe154	613703092215
Instance	i-0af65d815395fb91a	002670977573
Instance	i-0be60800aa1e9d9a5	613703092215
Instance	i-0c0189f0c6f1e66db	398984081329
Instance	i-0c44bb9dfa5f0cff5	002670977573
Instance	i-0c4730320e45e503d	002670977573
Instance	i-0c636e4458f00b74d	398984081329
Instance	i-0c93846849a4a1ed6	890342916428
Instance	i-0c9842f8d11cf184a	002670977573
Instance	i-0c9c0b6ef36d57332	002670977573
Instance	i-0cdd21e9bd5de13e1	002670977573

Instance	i-0ce94d3dabf70e6f7	890342916428
Instance	i-0cf943ec1228fe4b8	002670977573
Instance	i-0d2eb8da875d4814b	398984081329
Instance	i-0d3a5cc895c2290c6	613703092215
Instance	i-0d5b8488b12a9b4a4	002670977573
Instance	i-0d87d5b6342e8e4cb	002670977573
Instance	i-0d99b7287573033fd	002670977573
Instance	i-0ddb2c8b93ac9d4f9	002670977573
Instance	i-0df3ee6bae187f599	398984081329
Instance	i-0e28cafe31926d286	002670977573
Instance	i-0e31a36f1fd1a0b9d	398984081329
Instance	i-0e3d8c08fe0f3e007	002670977573
Instance	i-0ea2685bcc302483c	613703092215
Instance	i-0eca0290b4de12fb5	002670977573
Instance	i-0f1df26d17b3a3ac0	890342916428
Instance	i-0f7a69726e8f1c81c	002670977573
Instance	i-0f7c3273e8aaeaf50	002670977573
Instance	i-0fce67638c6fa20fb	890342916428

Preguntas para tu Equipo (Acción Requerida)

Para determinar la ruta de remediación correcta, por favor, haz que los dueños de las instancias respondan estas preguntas críticas para cada recurso:

1. **¿Cuál es la función de esta instancia EC2?** (ej. servidor web, servidor de aplicaciones, base de datos, bastion host, etc.)
2. **¿Necesita esta instancia *recibir* tráfico entrante no solicitado desde internet?**
   - Si la respuesta es **sí** (ej. es un servidor web), debe colocarse detrás de un **Application Load Balancer (ALB)**. El ALB tendrá la IP pública, y la instancia en sí estará en una subred privada.

- Si la respuesta es **no**, procede a la siguiente pregunta.

3. **¿Necesita esta instancia solo *iniciar* conexiones salientes a internet?** (ej. para descargar actualizaciones de software, llamar a APIs externas).
   - Si la respuesta es **sí**, debe colocarse en una subred privada y enrutar su tráfico saliente a través de un **NAT Gateway**. El NAT Gateway reside en una subred pública y maneja la comunicación con internet en nombre de las instancias privadas.
   - Si la respuesta es **no** (no necesita acceso a internet en absoluto), debe estar en una subred privada sin ruta a internet.

Consideraciones de Costo

Eliminar una IP pública y adoptar una arquitectura más segura implica un balance de costos.

Componente	Costo con IP Pública (Mensual)	Costo con Alternativa Segura (Mensual)	Explicación de la Diferencia
Dirección IPv4 Pública	~$3.65 USD (a $0.005/hr)	$0.00 USD	Ya no pagarías por la dirección IP adjunta a la instancia.
Alternativa Segura	$0.00 USD	**ALB:** ~$18.25 USD/mes **NAT Gateway:** ~$32.85 USD/mes	**Este es el principal costo nuevo.** Ahora estarías pagando por un servicio gestionado (ALB o NAT Gateway) para manejar el tráfico de internet de forma segura.
Procesamiento de Datos	Incluido en la transferencia de datos de EC2	**ALB:** ~$0.008 USD por LCU-hora **NAT Gateway:**	Ambas alternativas tienen una tarifa de procesamiento

		$0.045 USD por GB	de datos que es independiente de los costos estándar de transferencia de datos salientes de EC2.

Conclusión sobre Costos:

Aunque adjuntar directamente una IP pública parece más barato inicialmente, conlleva un alto riesgo de seguridad. Adoptar una arquitectura segura con un Load Balancer o un NAT Gateway introduce un costo mensual fijo por el servicio gestionado, pero este costo se traduce en una reducción significativa del riesgo de seguridad y de la carga operativa.

Cómo Solucionarlo: Eliminar una IP Pública

El proceso implica desasociar la IP Elástica y asegurarse de que la instancia esté en una subred privada.

1. **Desasociar la Dirección IP Elástica:**
   - Navega a la consola de **EC2**.
   - En el panel de navegación izquierdo, en **Red y Seguridad**, elige **IPs Elásticas**.
   - Selecciona la IP Elástica asociada con la instancia.
   - Haz clic en el botón **Acciones** y selecciona **Desasociar dirección IP elástica**. Confirma la desasociación.
2. **Modificar la Configuración de Asignación Automática de IP de la Subred (si aplica):**
   - Si la instancia está recibiendo una IP pública automáticamente de su subred, necesitas deshabilitar esto.
   - Navega a la consola de **VPC**, selecciona **Subredes** y encuentra la subred en la que se encuentra la instancia.
   - Selecciona la subred, haz clic en **Acciones** y elige **Modificar la configuración de asignación automática de IP**.
   - Desmarca la casilla **Habilitar la asignación automática de direcciones IPv4 públicas** y guarda.
   - Es posible que necesites detener e iniciar la instancia para que pierda su IP pública autoasignada.

Después de eliminar la IP pública, debes implementar la alternativa apropiada (ALB o NAT Gateway) para restaurar la conectividad a internet necesaria.

Recomendación

Se recomienda que investiguen el propósito de cada instancia listada y las muevan a una arquitectura privada por defecto.

- **Para servidores web:** Usar un Application Load Balancer.
- **Para todas las demás instancias que necesiten acceso saliente:** Usar un NAT Gateway.

La exposición directa de instancias EC2 a internet debe evitarse en todos los casos, excepto en los más específicos y bien justificados.

Referencias

Elastic IP addresses - Amazon Elastic Compute Cloud

Manage the IPv4 addresses for your EC2 instances - Amazon Elastic Compute Cloud