Guía de Seguridad de las TIC
CCN-STIC 1308

Procedimiento de Empleo Seguro
Azure Activity Log

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:26:45 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. Azure Activity Log es un servicio incluido en Microsoft Azure que captura un registro de las actividades y eventos que ocurren en una suscripción de Azure.
2. Proporciona información sobre acciones administrativas, interacciones con recursos y modificaciones de configuración de los recursos de Azure.
3. Azure Activity Log forma parte de Azure Monitor, que incluye un conjunto más amplio de capacidades de monitorización, análisis, visualización y respuesta.
4. Azure Activity Log permite a los usuarios monitorizar, solucionar problemas y auditar su entorno de Azure. Entre sus funcionalidades se incluyen: la visualización de eventos en Azure Portal, la descarga de registros en formato CSV, la consulta del historial de cambios y la configuración de diagnósticos para redirigir los registros a otros destinos cuando se requiere una retención superior.
5. Para más información sobre el funcionamiento de Azure Activity Log, consultar la guía **Registro de actividad de Azure** [REF1].

2 OBJETO Y ALCANCE

6. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Azure Activity Log.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Al tratarse de un servicio en la nube, se darán de alta los datos del cliente en la plataforma de **Microsoft Azure Portal** [REF2] y se enviarán de forma segura los accesos pertinentes a la plataforma.
8. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
9. Una vez dado el alta en la plataforma se podrá activar las licencias por cada usuario dentro de la plataforma.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.
11. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.
12. Sólo los usuarios autorizados y con la licencia activa podrán acceder al producto.

4.3 REGISTRO Y LICENCIAS

13. Los servicios prestados son mediante contratación y no es necesario la instalación. Las licencias se activan por cada usuario dentro de la suscripción contratada.

4.4 CONSIDERACIONES PREVIAS

14. Al tratarse de un servicio alojado en la nube, la principal consideración previa es tener conexión a Internet y estar dado de alta en la plataforma para hacer uso del producto.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

15. El producto consta de los siguientes componentes principales:
    - Azure Activity Log: Servicio de Azure accesible y administrable mediante Azure Portal y la capa de gestión de Azure, que proporciona información sobre eventos a nivel de suscripción.
    - API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
16. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
    - Azure Portal: acceso al portal de gestión.
    - Microsoft Entra ID: autenticación de usuarios, acceso condicional, políticas.
    - Tipo de fuente de datos (alcance): Azure Platform
    - Azure Storage: Solución de almacenamiento en la nube.
    - Log Analytics workspace: área de trabajo utilizada para consultar y analizar los registros redirigidos.
    - Azure Event Hubs: servicio utilizado para la transmisión de eventos.

- Azure Key Vault Managed HSM: claves criptográficas y secretos.
- Power BI: solución analítica empresarial.

17. Los componentes anteriores se interrelacionan a través del plano de administración de Azure. El acceso de los administradores se realiza mediante Azure Portal, previa autenticación con Microsoft Entra ID. Azure Activity Log, como servicio integrado en Azure Monitor, registra los eventos de la suscripción y puede redirigirlos hacia Azure Storage, Azure Event Hubs o Log Analytics workspace, según la configuración establecida.

5 FASE DE INSTALACIÓN

18. En este apartado se describe la implementación del producto.

5.1 ALTA DEL SERVICIO EN LA NUBE

19. Al tratarse de un servicio en la nube, se requiere el alta en **Microsoft Azure Portal** [REF2] mediante la suscripción correspondiente para que el usuario pueda hacer uso del servicio.
20. Una vez que se encuentre dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

5.2 ACTIVACIÓN AZURE ACTIVITY LOG

21. El proveedor proporciona documentación acerca de Azure Activity Log en la guía **Registro de actividad de Azure** [REF1]**.**

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

22. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. Para más información sobre el producto se debe consultar la guía **Azure Monitor Overview** [REF3]**.**
23. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al producto. Todos los usuarios deben ser autenticados por Microsoft Entra ID antes de cual interacción con el producto.
24. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft Entra ID. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

6.2 AUTENTICACIÓN

25. El producto usa la infraestructura de Azure vinculado a Microsoft Entra ID, para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.
26. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC).
27. Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación. Se exige el uso de MFA a las cuentas privilegiadas.
28. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure [REF4].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

29. Al ser un producto en la nube que forma parte de la infraestructura de Microsoft Azure, la administración se realiza de forma remota utilizando el protocolo seguro HTTPS con TLS 1.2 o superior para el establecimiento de las comunicaciones seguras.
30. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

31. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure, la administración del producto se realiza de forma remota.
32. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft Entra ID. Sólo los usuarios con el rol

de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

33. El producto utiliza Azure RBAC (Control de Acceso Basado en Roles) para acceder a los recursos. A continuación, se enumeran cuatro roles fundamentales integrados. Los primeros tres se aplican a todos los tipos de recursos:

    - Propietario (Owner): Tiene acceso completo a todos los recursos, incluyendo el derecho para delegar el acceso a otros.
    - Colaborador (Contributor): Puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
    - Lector (Reader): Puede ver los recursos existentes de Azure.
    - Administrador de Acceso de Usuario (User Access Administrator): Le permite gestionar el acceso de los usuarios a los recursos de Azure.

34. Estos roles son esenciales para controlar quién tiene permiso para realizar acciones específicas en los recursos de Azure, asegurando una gestión segura y eficiente del acceso.

35. El producto utiliza Microsoft Entra ID para las cuentas, y se aplican diferentes mecanismos de seguridad haciendo uso de la tecnología Smart Lockout. El bloqueo inteligente protege las cuentas de usuario de los ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar. Los valores predeterminados de bloqueo inteligente son los siguientes:

    - Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 3 intentos fallidos
    - Duración del bloqueo: 5 minutos.
    - Tiempo de inactividad de las sesiones: 5 minutos.

36. Para más información sobre los diferentes mecanismos de seguridad de la tecnología Smart Lockout y cómo modificar los valores establecidos, se puede consultar la siguiente guía, **Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra [REF5]**.

37. El producto utiliza la infraestructura de Azure y puede administrar la directiva de contraseñas mediante las directivas de Microsoft Entra ID. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Microsoft Entra ID. Los siguientes requisitos de directiva de contraseñas de Microsoft Entra ID se aplican a todas las contraseñas que se crean, cambian o restablecen en Microsoft Entra ID:

Propiedad	Requisitos
Caracteres permitidos	Mayúsculas (A - Z) Minúsculas (a - z) Números (0 - 9) Símbolos: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > Espacio en blanco

Caracteres no permitidos	Caracteres unicode
Longitud de la contraseña	Un mínimo de 12 caracteres y un máximo de 256.
Complejidad de contraseñas	Las contraseñas requieren 3 categorías de las 4 siguientes: - Mayúsculas - Minúsculas - Números - Símbolos
Contraseña no utilizada recientemente	La nueva contraseña no puede ser la misma que la contraseña actual ni reutilizarse dentro de un periodo mínimo de 10 días.
Tiempo de validez en días de las contraseñas tras el cual expiran	La contraseña tendrá una validez máxima de 730 días.

Tabla 1. Política de contraseñas

38. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra ID**[REF6].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

39. Todo acceso al producto se realiza mediante el uso de HTTPS con TLS1.2 o superior.

6.5 GESTIÓN DE CERTIFICADOS

40. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure los certificados usan RSA con longitud de clave de 2048 bits. Este cifrado es suficientemente robusto y, aunque se considera seguro para las comunicaciones en el momento de creación de este documento, se recomienda la utilización de RSA con longitud de clave de 3072 bits.

41. Para la gestión y configuración de la longitud de clave ver la subsección “Creación de claves” de la sección “3.1.2.2 Protección de claves criptográficas” de la guía **CCN-STIC-884A** [REF4]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

42. El producto usa Microsoft Entra ID para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.

6.7 SINCRONIZACIÓN

43. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

44. Las actualizaciones se realizan automáticamente cuando están disponibles. Este proceso está completamente controlado por el CSP (Proveedor de Servicios en la Nube) porque el servicio es parte de la infraestructura de Azure.
45. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

46. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube realiza los auto-chequeos (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas del producto de manera automatizada.

6.10 ALTA DISPONIBILIDAD

47. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

48. El producto es parte de la infraestructura de Azure y también forma parte de Azure Activity Monitor para auditar todos los eventos que se generan por parte del producto y otros servicios de Azure.
49. Para más información, se puede consultar la guía oficial de Uso del registro de actividad de Azure Monitor y la información del registro de actividad [REF7].
50. El servicio genera registros de auditoría clasificados por actividades que se auditan en la infraestructura de Azure, para más información se puede consultar la guía **Esquema de eventos del registro de actividad de Azure** [REF8]**.** Se pueden buscar estos eventos buscando el Activity Log en el portal de seguridad y cumplimiento, seleccionando las siguientes categorías:

    - Proceso de inicio de sesión del personal autorizado (estos eventos proceden de la integración con Entra ID). Debido a la arquitectura y modo de operación de la infraestructura Azure, la plataforma utiliza la capacidad de sesiones y no hay eventos de cierre de sesión. Los inicios de sesión (sing-ins) se registran con los siguientes estados descritos:
        - Éxito: inicio de sesión exitoso.
        - Fallo: Error al validar las credenciales debido a que el nombre de usuario o la contraseña no son válidos.

- Interrumpido: La contraseña del usuario ha caducado, por lo que su login o sesión ha sido finalizado. Cuando se pregunta al usuario si desea seguir conectado a este navegador para facilitar el inicio de sesión en el futuro.

- Eventos relacionados con la suscripción:
  - Administrativo: contiene el registro de todas las operaciones de creación, actualización, eliminación y acción realizadas a través del Resource Manager.
  - Salud del servicio: contiene el registro de cualquier incidente de salud de los servicios que ocurrió en Azure.
  - Salud de los recursos: contiene el registro de cualquier incidente relacionado con la salud de los recursos en tu suscripción de Azure.
  - Alerta: contiene el registro de las activaciones de alertas de Azure.
  - Autoscale: contiene el registro de cualquier evento relacionado con el funcionamiento del motor de escalado automático, basado en cualquier configuración de autoscale que hayas definido en tu suscripción.
  - Recomendación: contiene eventos de recomendación de Azure Advisor.
  - Seguridad: contiene el registro de cualquier alerta generada por Microsoft Defender for Cloud.
  - Política: contiene registros de todas las operaciones de acción efectivas realizadas por Azure Policy.

51. El Activity Log se muestra dentro del menú de Monitor Log, en el portal de Azure.

52. Los resultados de una búsqueda en el Activity Log se muestran con la siguiente información:

    - El tipo de evento identificado corresponde a “Autorización:acción” y “Autorización:ámbito”: La acción realizada por el usuario (crear asignación de funciones, eliminar asignación de funciones, crear o actualizar definición de rol...) y el ámbito de la acción.
    - El usuario que produce el evento corresponde a la propiedad “Caller”: Quién inició la acción.
    - Fecha y hora del evento corresponde a la propiedad “EventTimestamp”: Hora en que ocurrió la acción.
    - Resultado del evento corresponde a la propiedad “Status:value”: Estado de la acción.

6.11.2 ALMACENAMIENTO LOCAL

53. Al tratarse de un servicio en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada.

6.11.3 ALMACENAMIENTO REMOTO

54. La opción de enviar eventos de registros a un servidor no está disponible. Únicamente se pueden enviar los registros a los siguientes recursos de Azure: Azure Storage, Azure Event Hubs y Azure Log Analytics workspace.

55. Para más información sobre cómo realizar el envío de registros a los recursos de Azure mencionados, se puede consultar la siguiente guía, **Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage** [REF9].

6.12 BACKUP

56. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.

7 FASE DE OPERACIÓN

57. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta por el proveedor del servicio.

58. No obstante, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del producto:

    - Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.
    - Los administradores deben estar correctamente formados en el uso y la correcta operación del producto.
    - Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
    - Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.

59. Azure Activity Log ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.

60. En las siguientes subsecciones de la fase de operación, se analizarán dichas funcionalidades en detalle, haciendo referencia, cuando corresponda, a la documentación oficial proporcionada por el proveedor para garantizar su uso de manera segura, eficiente y conforme a las directrices establecidas.

7.1 MONITOREO PASIVO DE TRÁFICO DE RED

61. El producto permite el monitoreo pasivo de todo el tráfico de red detectado a través de sus propias interfaces utilizando Azure Network Watcher, que proporciona un conjunto de herramientas para realizar dicha tarea.

62. Azure Network Watcher ofrece una suite de herramientas para monitorear, diagnosticar, visualizar métricas y habilitar o deshabilitar registros para los recursos de IaaS (Infraestructura como Servicio) en Azure.

63. Azure Network Watcher permite supervisar y reparar la salud de la red de productos IaaS como máquinas virtuales (VMs), redes virtuales (VNets), puertas de enlace de aplicaciones, balanceadores de carga, entre otros.

64. Es importante destacar que Azure Network Watcher no está diseñado ni destinado para el monitoreo de PaaS ni para el análisis web.

65. Azure Network Watcher se compone de tres conjuntos principales de herramientas y capacidades:

    - Monitoreo
    - Herramientas de diagnóstico de red
    - Tráfico

66. Para obtener más información sobre cómo utilizar Azure Network Watcher para el monitoreo de redes, consultar la guía **Documentación de Network Watcher** [REF11].

7.2 DESCARGA DE REGISTROS EN FORMATO CSV

67. El producto permite la descarga de registros desde Azure Monitor en formato CSV.
68. Los registros de actividad pueden ser descargados en este formato para su análisis y posterior procesamiento.
69. Esta funcionalidad facilita la exportación de datos de actividades para realizar auditorías, análisis o integrarlos en otros sistemas para su revisión.
70. Para obtener más información sobre cómo descargar el registro de actividad en formato CSV, consultar la guía **Supervisión de recursos mediante información del registro de actividad** [REF12].

7.3 VISUALIZACIÓN DEL HISTORIAL DE CAMBIOS

71. El producto permite visualizar el historial de cambios para ciertos eventos, mostrando qué cambios ocurrieron durante el tiempo de ese evento, hasta 30 minutos antes y después de la operación.
72. Esta funcionalidad proporciona una visión detallada de las modificaciones realizadas en los recursos, ayudando a comprender el contexto de los eventos y las acciones tomadas.
73. Además, el producto ofrece una opción para un conjunto específico de eventos, permitiendo al usuario autorizado acceder al historial de cambios de dichos eventos.
74. Para obtener más información sobre cómo ver el historial de cambios en el registro de actividad, consultar la guía **Supervisión de recursos mediante información del registro de actividad** [REF12].

7.4 ALMACENAMIENTO Y TRANSMISIÓN DE REGISTROS DE ACTIVIDAD

75. El producto es capaz de almacenar la información de auditoría generada durante un período de 90 días, garantizando que los registros de actividad estén disponibles para su análisis y revisión dentro de este plazo.
76. Además, el producto permite transmitir la información de auditoría generada a una entidad externa utilizando Azure Storage y Azure Event Hub, asegurando que todas las conexiones se realicen a través de un canal seguro (TLS 1.2).
77. El registro de actividad de Azure Monitor es un registro de plataforma que proporciona información sobre los eventos a nivel de suscripción. Este registro incluye detalles como cuándo se modifica un recurso o cuándo se inicia una máquina virtual.
78. Los registros de actividad se pueden visualizar en el portal de Azure o recuperar utilizando PowerShell y Azure CLI. Además, los registros pueden enviarse a los siguientes destinos:
    - Enviar a Azure Monitor Logs para consultas más complejas, alertas y retención prolongada de hasta 12 años.
    - Enviar a Azure Event Hubs para su envío fuera de Azure.
    - Enviar a Azure Storage para archivado a largo plazo y más económico.
79. Para obtener más información sobre cómo almacenar y exportar los registros de actividad, consultar la guía **Enviar datos del registro de actividad de Azure Monitor** [REF13].

8 REFERENCIAS

[REF1] Registro de actividad Azure
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log

[REF2] Microsoft Azure Portal
https://portal.azure.com

[REF3] Azure Monitor Overview
https://learn.microsoft.com/es-es/azure/azure-monitor/fundamentals/overview

[REF4] CCN-STIC-884A Guía de configuración segura para Azure
https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/4253-ccn-stic-884a-guia-de-configuracion-segura-para-azure/file.html

[REF5] Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra
https://learn.microsoft.com/es-es/entra/identity/authentication/howto-password-smart-lockout

[REF6] Roles Integrados de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/role-based-access-control/permissions-reference

[REF7] Uso del registro de actividad de Azure Monitor y la información del registro de actividad
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-insights

[REF8] Esquema de eventos del registro de actividad de Azure
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-schema

[REF9] Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/resource-logs

[REF10] Introducción a Azure Monitor
https://learn.microsoft.com/es-es/azure/azure-monitor/getting-started

[REF11] Documentación de Network Watcher
https://learn.microsoft.com/es-es/azure/network-watcher/

[REF12] Supervisión de recursos mediante información del registro de actividad
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-insights

[REF13] Enviar datos del registro de actividad de Azure Monitor
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log?tabs=powershell

9 ABREVIATURAS

API	Interfaz de Programación de Aplicaciones
CCN	Centro Criptográfico Nacional.
CLI	Command Line Interface
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CSP	Cloud Service Provider
CSV	Comma-Separated Values
ENS	Esquema Nacional de Seguridad.
HSM	Hardware Security Module
HTTPS	Secure Hyper Text Transfer Protocol.
IaaS	Infrastructure as a Service
ID	Identity Directory (en el contexto de Microsoft Entra ID)
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
OMS	Operations Management Suite
PaaS	Platform as a Service
RBAC	Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman (algoritmo de cifrado)
TLS	Transport Layer Security.
VM	Virtual Machine
VNet	Virtual Network