Notas de la sesión 01

jueves, 25 de agosto de 2022

17:52

Comprobación de conocimientos

1. Su organización está considerando la posibilidad de adoptar la autenticación multifactor en Azure. El administrador le pregunta sobre los métodos de verificación secundarios. ¿Cuál de las siguientes opciones podría actuar como método de verificación secundario?

Una llamada de teléfono automatizada. Puede configurar una llamada telefónica automatizada para la verificación.

1. Su organización ha implementado la autenticación multifactor en Azure. El objetivo es proporcionar un informe de estado por cuenta de usuario. ¿Cuál de los siguientes valores se podría usar para proporcionar un estado de MFA válido?

Aplicado es un estado de MFA válido en la pantalla del informe.

1. ¿Cuál de las siguientes opciones se puede usar al configurar la autenticación multifactor en Azure?

Omisión por única vez de un usuario que está bloqueado. Permitir el acceso por única vez es una opción disponible.

1. Al configurar Azure AD, ¿cuál de los siguientes roles permitiría al usuario administrar todos los grupos de un inquilino y asignar otros roles de administrador?

Administrador global. Solo el administrador global puede administrar grupos entre inquilinos y asignar otros roles de administrador.

1. ¿Cuál de los métodos siguientes permite agregar o quitar automáticamente usuarios a grupos de seguridad o de Microsoft 365, de modo que no siempre tenga que hacerlo manualmente?

Usuario dinámico usa reglas para agregar y quitar miembros automáticamente.

Resumen

Azure AD ayuda a proporcionar acceso a los recursos de la organización al proporcionar derechos de acceso a un único usuario, a un grupo de Azure AD completo o a unidades administrativas específicas.

Ahora debería ser capaz de hacer lo siguiente:

* Comparación y contraste de Azure AD frente a los servicios de directorio locales con Azure AD Domain Services.
* Configure e implemente usuarios, grupos y unidades administrativas para acceder de forma segura a los recursos del inquilino.
* Implemente una solución de inicio de sesión sin contraseña para los usuarios y recursos de Azure.

Notas de la sesión 02

Comprobación de conocimientos

1. El departamento de soporte técnico de TI quiere reducir las incidencias de soporte técnico del restablecimiento de contraseña. Sugiere que los usuarios inicien sesión tanto en las aplicaciones locales como en las basadas en la nube utilizando la misma contraseña. Su organización no tiene previsto usar Azure AD Identity Protection; así pues, ¿qué característica sería más fácil de implementar dados estos requisitos?

Autenticación de paso a través. La autenticación transferida (PTA) permite a los usuarios iniciar sesión en aplicaciones basadas en la nube y en entornos locales con las mismas contraseñas. Con PTA, los usuarios inician sesión mediante la validación de sus contraseñas directamente en la instancia local de Active Directory. PTA no proporciona informes de credenciales filtradas de Azure AD Identity Protection.

1. ¿Qué herramienta puede usar para sincronizar las contraseñas de Azure AD con Active Directory local?

Azure AD Connect. La sincronización de Azure AD Connect es un componente principal de Azure AD Connect. Se encargan de todas las operaciones relacionadas con la sincronización de datos de identidad entre el entorno local y Azure AD.

1. ¿Cuál de los siguientes protocolos de seguridad admite Azure AD?

OAuth se usa para la autorización.

1. ¿Cuál de las siguientes es una opción de autenticación que se integra con Azure Active Directory, lo que requiere que use varios métodos diferentes, como el teléfono, para confirmar su identidad?

Azure Active Directory Multi-Factor Authentication (MFA) es una excelente manera de proteger la organización, pero los usuarios a menudo se frustran con la capa de seguridad adicional además de tener que recordar sus contraseñas. Los métodos de autenticación sin contraseña resultan más cómodos, ya que la contraseña se quita y se reemplaza por algo que se tiene más algo que se es o se sabe. Las otras opciones son las de autenticación sin contraseña que se integran con Azure AD. Azure AD DS permite el uso de cifrados como NTLM v1 y TLS v1.

Resumen

La identidad híbrida ayuda a conectar su instancia de Active Directory local con Azure AD para habilitar la autenticación y autorización compartidas a los recursos locales y en la nube.

Ahora debería ser capaz de hacer lo siguiente:

* Configuración e implementación de Azure AD Connect
* Configuración de la sincronización de hash de contraseña
* Implementación de la autenticación transferida
* Seleccione y configure el método de autenticación óptimo en función de su posición de seguridad.
* Implementación de la escritura diferida de contraseñas

Notas de la sesión 03

Comprobación de conocimientos

1. Los auditores de cumplimiento quieren asegurarse de que, a medida que los empleados cambian de trabajo o dejan la empresa, también se cambian o revocan sus privilegios. Les preocupa especialmente el grupo Administrador. Para abordar sus problemas, ¿cuál de las siguientes opciones implementaría?

Revisiones de acceso. Las revisiones de acceso permiten a las organizaciones administrar de forma eficiente la pertenencia a grupos, el acceso a las aplicaciones empresariales y la asignación de roles. El acceso de los usuarios se puede revisar de forma periódica para asegurarse de que solo las personas adecuadas tengan acceso continuado.

1. Identity Protection ha informado de que se han filtrado las credenciales de un usuario. Según la directiva, se debe restablecer la contraseña del usuario. ¿Qué rol de Azure AD puede restablecer la contraseña?

Administrador global. Para usar Identity Protection, un usuario debe estar en uno de estos roles. Cada rol tiene privilegios diferentes, pero solo el administrador global puede restablecer la contraseña de un usuario.

1. ¿En cuál de las siguientes clasificaciones identifica Identity Protection los riesgos?

Viaje atípico. Identity Protection puede reconocer inicios de sesión desde ubicaciones y horas inesperadas.

1. Ha implementado Identity Protection y está revisando el informe Usuarios de riesgo. Para cada evento notificado, ¿puede elegir cualquiera de las siguientes acciones?

Confirmar que un usuario se ha visto comprometido es una opción válida al revisar los informes de proyección de identidad.

1. ¿Para habilitar cuál de las acciones enumeradas a continuación puede usarse el acceso condicional?

Requerir autenticación multifactor. Es posible forzar a un usuario, a un grupo de usuarios o a todos los usuarios a utilizar MFA con una directiva de acceso condicional.

1. ¿Qué plan de licencias es compatible con Identity Protection?

Azure Active Directory Premium P2. Identity Protection facilita la configuración del acceso condicional en función del riesgo de las aplicaciones para protegerlas de riesgos basados en identidades.

Resumen

Las protecciones de Azure AD Identity Protection ayudan a mantener la seguridad de los usuarios mediante la realización de revisiones de acceso, la supervisión y la elaboración de informes sobre la forma en que cada identidad accede a los recursos en su sitio de Azure y la implementación del acceso condicional para controlar el acceso a los recursos.

Debería poder:

* Implementar y configurar Identity Protection
* Configurar MFA para usuarios, grupos y aplicaciones
* Crear directivas de acceso condicional para garantizar la seguridad
* Crear y seguir un proceso de revisión de acceso

Notas de la sesión 04

Comprobación de conocimientos

1. Si quiere habilitar Azure AD PIM para el directorio, ¿qué rol de Azure AD necesita para habilitarlo?

Administrador global. De las opciones enumeradas, solo el rol de administrador global tiene permiso para habilitar PIM.

1. Una empresa ha implementado Azure AD PIM. Es necesario asegurarse de que los nuevos empleados soliciten la elevación de privilegios antes de realizar cambios en Azure. ¿Qué debe hacer?

Asignar al nuevo empleado el tipo de pertenencia a rol Apto Cuando un usuario es Apto para la pertenencia a rol, debe solicitar la activación antes de poder usar el rol.

1. ¿Para administrar cuáles de los roles siguientes se usa Azure AD PIM?

Roles de Azure AD. Aunque no forma parte de esta pregunta, puede administrar todos los roles de recursos de Azure.

1. Una organización ha habilitado Azure AD PIM. El administrador de TI quiere configurar el rol para que no se requiera ninguna acción. ¿Qué debe hacer?

Haga que el administrador tenga las características de permanente y activo en el rol. Este tipo de asignación de roles no requiere que el usuario realice ninguna acción para usar el rol.

Resumen

Ha aprendido la forma en que PIM (Privileged Identity Management) va a proteger los recursos, roles y datos frente a riesgos mediante el control, la administración y la supervisión del acceso a los recursos con privilegios.

Debería poder:

* Describir la Confianza cero y cómo afecta a la seguridad
* Configurar e implementar roles con Privileged Identity Management (PIM)
* Evaluar la utilidad de cada configuración de PIM en relación con los objetivos de seguridad

Notas de la sesión 05

Comprobación de conocimientos

1. La empresa contrata a un nuevo administrador y necesita crear una nueva cuenta de usuario de Azure AD para él. El nuevo empleado debe ser capaz de: - Leer/escribir las implementaciones de los recursos de los que son responsables. - Leer los permisos de acceso a Azure AD No deberían poder ver la información de la suscripción a Azure. ¿Qué se debe configurar para que esto funcione?

Asigne al usuario el rol Colaborador en el nivel de grupo de recursos. Esto dará al nuevo contratado los mínimos privilegios necesarios para el rol.

1. ¿Cuál de las afirmaciones siguientes sería un buen ejemplo de cuándo usar un bloqueo de recurso?

Un circuito de ExpressRoute con conectividad a la red local. Los bloqueos de recursos impiden que otros usuarios de la organización eliminen o modifiquen accidentalmente los recursos críticos.

1. Una empresa tiene tres máquinas virtuales (VM1, VM2 y VM3) en un grupo de recursos. El departamento de soporte técnico contrata a un nuevo empleado. El nuevo empleado debe poder modificar la configuración en VM3, pero no en VM1 y VM2. La solución debe minimizar la sobrecarga administrativa. ¿Cómo se debe establecer la configuración?

Asignar el usuario al rol Colaborador en VM3. Esto significa que el usuario no tendrá acceso a VM1 o VM2. La asignación del rol Colaborador al grupo de recursos actual no es correcta, ya que la nueva contratación cambiaría la configuración de VM1 y VM2 y, por tanto, cumpliría los requisitos.

1. Es necesario orientar las directivas y revisar los presupuestos de gastos en varias suscripciones que administra. ¿Qué se debe crear para las suscripciones?

Un grupo de administración. Los grupos de administración se pueden usar para organizar y administrar suscripciones.

1. Un administrador pide una explicación de cómo utiliza Azure los grupos de recursos. ¿Cuál de las siguientes funcionalidades es una característica de cómo usa Azure los grupos de recursos?

Los recursos se pueden mover de un grupo de recursos a otro. Los recursos se pueden mover fácilmente entre grupos de recursos, por lo que es correcto.

Resumen

Nunca cree y olvide, debe implantar los controles y las estrategias de mantenimiento adecuados para las soluciones de Azure. La gobernanza empresarial proporciona el marco para proteger los sistemas y los datos.

Debería poder:

* Explicación del modelo de responsabilidad compartida y cómo afecta a la configuración de seguridad
* Creación de directivas de Azure para proteger las soluciones
* Configuración e implementación del acceso a servicios mediante RBAC