Servicio de autenticación adaptable

Machine translated content

Disclaimer

Contents

Notas de la versión

June 19, 2024

La nota de versión de autenticación adaptable es un subconjunto de las notas de la versión de NetScaler. Los clientes de autenticación adaptativa deben usar las notas de la versión de NetScaler para obtener información sobre las mejoras, los problemas solucionados y los problemas que se sabe que existen en el servicio de autenticación adaptativa.

> **Nota:**
>
> La fecha de este documento hace referencia a la fecha de la última actualización del servicio.

16 Jan 2024

Novedades

- **Actualización automática de las instancias de autenticación adaptativa**

Las instancias de autenticación adaptativa se actualizan automáticamente a las compilaciones 14.1—12.35 y posteriores para solucionar las vulnerabilidades de seguridad descritas en CTX584986.

26 Sep 2023

Novedades

- **Actualización automática de las instancias de autenticación adaptativa**

Las instancias de autenticación adaptativa se actualizan automáticamente a las compilaciones 14.1—8.50 y posteriores para solucionar las vulnerabilidades de seguridad descritas en CTX579459.

18 de julio de 2023

Novedades

- **Actualización automática de las instancias de autenticación adaptativa**

Las instancias de autenticación adaptativa se actualizan automáticamente a las compilaciones 13.1—49.101 y versiones posteriores, lo que corrige las vulnerabilidades de seguridad descritas en CTX561482.

28 April 2023

Novedades

- **Compatibilidad con LDAP y LDAPS con equilibrio de carga**

  La instancia de autenticación adaptable de Citrix proporciona soporte para LDAP y LDAPS mediante un servidor virtual de equilibrio de carga. Para obtener más información, consulte Ejemplo de configuración de equilibrio de carga de LDAP y LDAPS.

  [AAUTH-2067]

- **Mapear subredes de servidores AD o RADIUS del backend con ubicaciones de recursos**

  Los administradores pueden elegir los conectores a través de los cuales se debe acceder a los servidores AD y RADIUS de fondo. Para obtener más información, consulte Provisión de autenticación adaptable.

Problemas resueltos

- Las directivas de acceso inteligente y las directivas de autenticación de OAuth configuradas para la autenticación adaptable faltan en la GUI de NetScaler.

  [AAUTH-68]

Problemas conocidos

- En una instancia de autenticación adaptativa, cuando utiliza la opción **Probar conexión** en el perfil LDAP (GUI de administrador de NetScaler) para comprobar la conectividad, el servidor LDAP aparece incorrectamente como accesible aunque no esté accesible.

  [AAUTH-2111]

Configurar el servicio de autenticación adaptable

June 19, 2024

La configuración del servicio de autenticación adaptable implica los siguientes pasos de alto nivel.

1. Autenticación adaptable de provisión
2. Configurar directivas de autenticación adaptable
3. Habilitar la autenticación adaptable para Workspace

Requisitos previos

- Reserve un FQDN para la instancia de Autenticación adaptable. Por ejemplo `aauth.xyz.com` , suponiendo que `xyz.com` es el dominio de su empresa. En este documento, este FQDN se denomina FQDN del servicio de autenticación adaptable y se utiliza al aprovisionar la instancia. Asigne el FQDN a la dirección IP pública del servidor virtual del IdP. Esta dirección IP se obtiene tras el aprovisionamiento en el paso **Cargar certificado**.
- Adquiera un certificado para aauth.xyz.com. Los certificados deben contener el atributo SAN. De lo contrario, no se aceptarán los certificados.
- La interfaz de usuario de autenticación adaptable no admite la carga de paquetes de certificados. Para vincular un certificado intermedio, consulte Configurar certificados intermedios.
- Elija el tipo de conectividad para la conectividad AD/RADIUS local. Están disponibles las dos opciones siguientes. Si no desea tener acceso al centro de datos, utilice el tipo de conectividad de conector.
  - **Citrix Cloud Connector** : para obtener más información, consulte Citrix Cloud Connector.
  - **Interconexión de redes virtuales de Azure**: Para obtener más información, consulte Configurar la conectividad con los servidores de autenticación locales mediante la interconexión de redes virtuales de Azure.
- Configure un servidor de protocolo de tiempo de red (NTP) para evitar sesgos de tiempo. Para obtener más información, consulte Cómo sincronizar el reloj del sistema con los servidores de la red.

Puntos que tener en cuenta

- Citrix recomienda no ejecutar clear config para ninguna instancia de autenticación adaptable ni modificar ninguna configuración con el prefijo `AA` (por ejemplo, AAuthAutoConfig), incluidos los certificados. Esto interrumpe la administración de la autenticación adaptable y el acceso de los usuarios se ve afectado. La única forma de recuperarse es mediante el reaprovisionamiento.
- No agregue SNIP ni ninguna ruta adicional en la instancia de Autenticación adaptable.
- La autenticación del usuario falla si el ID del cliente no está en minúsculas. Puede convertir su ID a minúsculas y configurarlo en la instancia de NetScaler mediante el comando `set cloud parameter -customerID <all_lowercase_customerid>`.
- La configuración de nFactor necesaria para Citrix Workspace o el servicio Citrix Secure Private Access es la única configuración que los clientes deben crear directamente en las instancias. Actualmente, no hay comprobaciones ni advertencias en NetScaler que impidan que los administradores realicen estos cambios.
- Se recomienda que todas las configuraciones personalizadas se realicen en la interfaz de usuario y no directamente en las instancias de autenticación adaptativa. Esto se debe a que

los cambios realizados en las instancias no se sincronizan automáticamente con la interfaz de usuario y, por lo tanto, los cambios se pierden.

- No actualice las instancias de autenticación adaptable a compilaciones RTM aleatorias. Citrix Cloud administra todas las actualizaciones.
- Solo se admite un conector en la nube basado en Windows. El dispositivo Connector no es compatible con esta versión.
- Si ya es cliente de Citrix Cloud y ya ha configurado Azure AD (u otros métodos de autenticación), para cambiar a la autenticación adaptativa (por ejemplo, la verificación de postura del dispositivo), debe configurar la autenticación adaptativa como método de autenticación y configurar las directivas de autenticación en la instancia de autenticación adaptativa. Para obtener más información, consulte Conectar Citrix Cloud a Azure AD.
- Para la implementación del servidor RADIUS, agregue todas las direcciones IP privadas del conector como clientes RADIUS en el servidor RADIUS.
- En la versión actual, el agente ADM externo no está permitido y, por lo tanto, no se admite Citrix Analytics (CAS).
- El servicio NetScaler Application Delivery Management recopila la copia de seguridad de la instancia de autenticación adaptable. Para extraer la copia de seguridad de ADM, incorpore el servicio ADM. Para obtener más información, consulte Configurar copia de seguridad y restauración. Citrix no toma las copias de seguridad de forma explícita del servicio de autenticación adaptable. Los clientes deben tomar la copia de seguridad de sus configuraciones del servicio de administración de entrega de aplicaciones si es necesario.
- Las instancias de autenticación adaptativa no pueden establecer el túnel si hay un proxy configurado en la configuración del cliente. Por lo tanto, se recomienda deshabilitar la configuración del proxy para la autenticación adaptativa.
- Si utiliza servicios de autenticación de terceros, como SAML, la autenticación puede fallar si no se encuentran todas las notificaciones. Por lo tanto, se recomienda que los clientes agreguen un factor adicional, como NOAUTH, en la configuración de autenticación multifactor para aprobar todas las solicitudes.
- Se recomienda mantener el nivel de registro de depuración desactivado durante las operaciones normales y habilitarlo solo cuando sea necesario. Si el nivel de registro de depuración está siempre activado, se produce una enorme carga en la CPU de administración. Esto puede provocar bloqueos del sistema durante cargas de tráfico elevadas. Para obtener más información, consulte CTX222945.

Cómo configurar el servicio de autenticación adaptable

Acceso a la interfaz de usuario de la autenticación

Puede acceder a la interfaz de usuario de la autenticación adaptable mediante uno de los métodos siguientes.

- Escriba la URL manualmente https://adaptive-authentication.cloud.com.
- Inicie sesión con sus credenciales y seleccione un cliente.

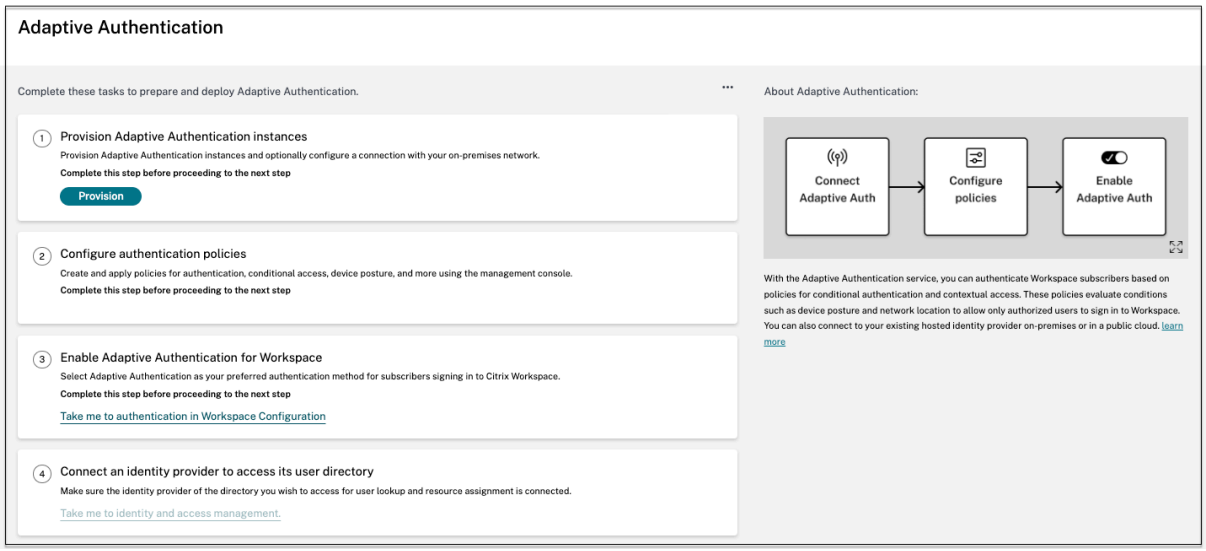
  Una vez que se haya autenticado correctamente, se le redirigirá a la interfaz de usuario de la autenticación adaptativa.

O BIEN:

- Vaya a **Citrix Cloud > Administración de identidades y accesos**.
- En la pestaña Autenticación, en **Autenticación adaptativa**, haga clic en el menú de puntos suspensivos y seleccione **Administrar**.

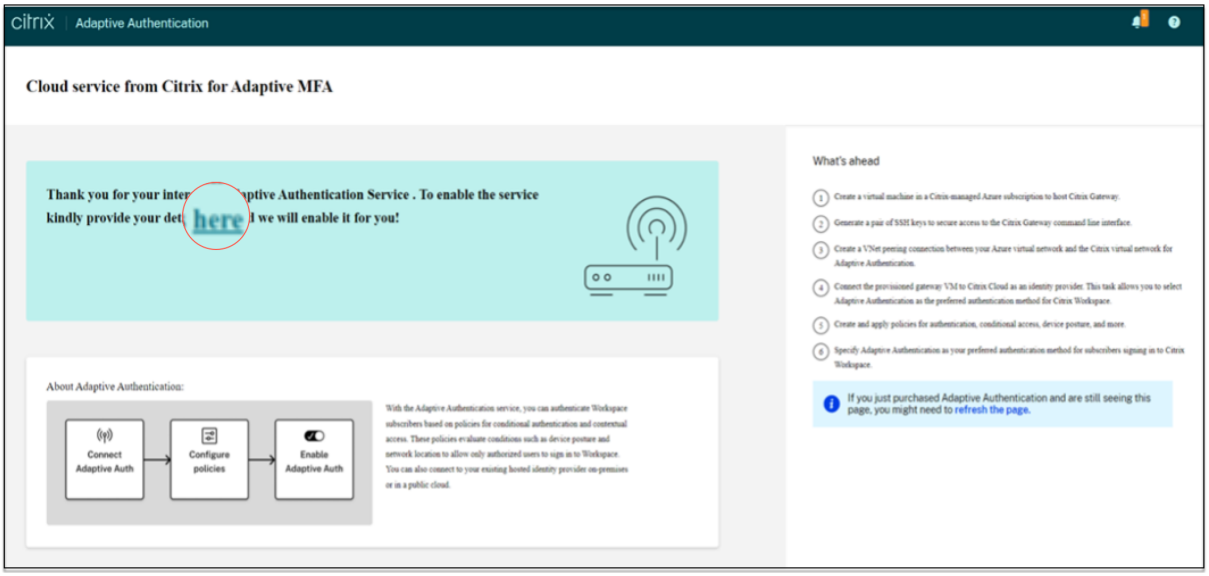
Aparece la interfaz de usuario de la autenticación adaptable.

Esta ilustración muestra los pasos necesarios para configurar la autenticación adaptable.



Paso 1: Provisión de la autenticación adaptable

> **Importante:**
>
> Los clientes interesados en el servicio de autenticación adaptativa deben hacer clic en el enlace que se muestra en la siguiente captura de pantalla y completar el formulario de Podio. A continuación, el equipo de Citrix Adaptive Authentication habilita el aprovisionamiento de instancias de Adaptive Authentication.



Realice los siguientes pasos para aprovisionar la instancia de autenticación adaptable:

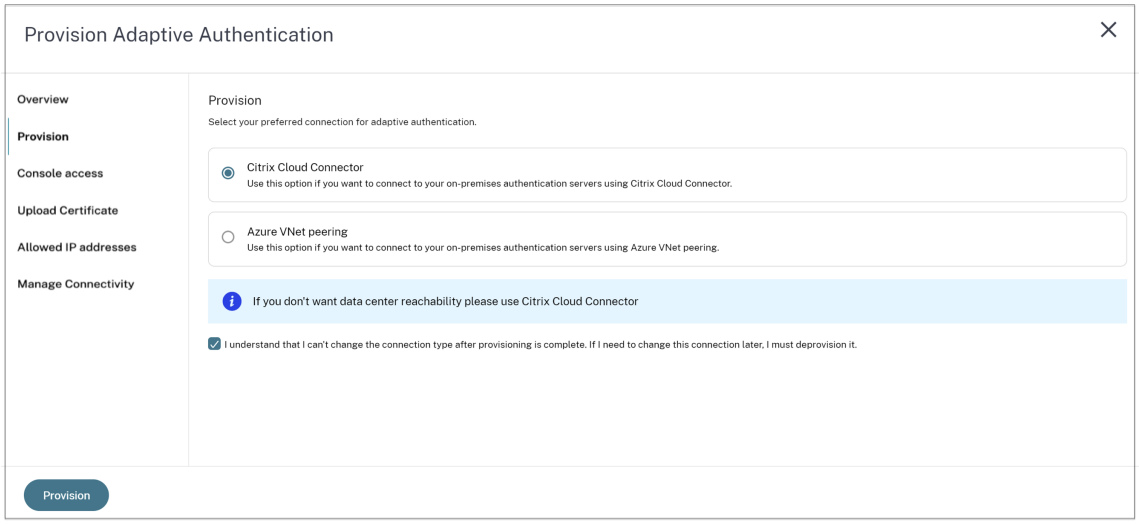
1. En la interfaz de usuario de **Autenticación adaptable,**haga clic
2. Seleccione la conexión que prefiera para la autenticación adaptable.

   - **Citrix Cloud Connector:** Para este tipo de conexión, debe configurar un conector en la red local. Citrix recomienda implementar al menos dos Citrix Cloud Connectors en su entorno para configurar la conexión a Citrix Gateway alojado en Azure. Debe permitir que Citrix Cloud Connector acceda al dominio/URL que ha reservado para la instancia de autenticación adaptativa. Por ejemplo, permita https://aauth.xyz.com/*.

     Para obtener más información sobre Citrix Cloud Connector, consulte Citrix Cloud Connector.

   - **Emparejamiento de VNet de Azure**: Debe configurar la conectividad entre los servidores mediante el emparejamiento de VNet de Azure.

     - Asegúrese de tener una cuenta de suscripción de Azure para configurar la conectividad.
     - La VNet del cliente que se está emparejando ya debe tener una puerta de enlace VPN de Azure aprovisionada. Para obtener información detallada, consulte https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal.



Para agregar un Citrix Cloud Connector como su conexión preferida:

Realice los siguientes pasos.

- Seleccione la opción **Citrix Cloud Connector** y, a continuación, active la casilla de verificación del acuerdo de usuario final.
- Haga clic en **Aprovisionar**. La configuración del aprovisionamiento puede tardar hasta 30 minutos.

> **Nota:**
>
> Para el tipo de conectividad del conector, asegúrese de que se pueda acceder al FQDN de autenticación adaptable desde la máquina virtual del conector después del aprovisionamiento.

Para configurar la interconexión de Azure VNet:

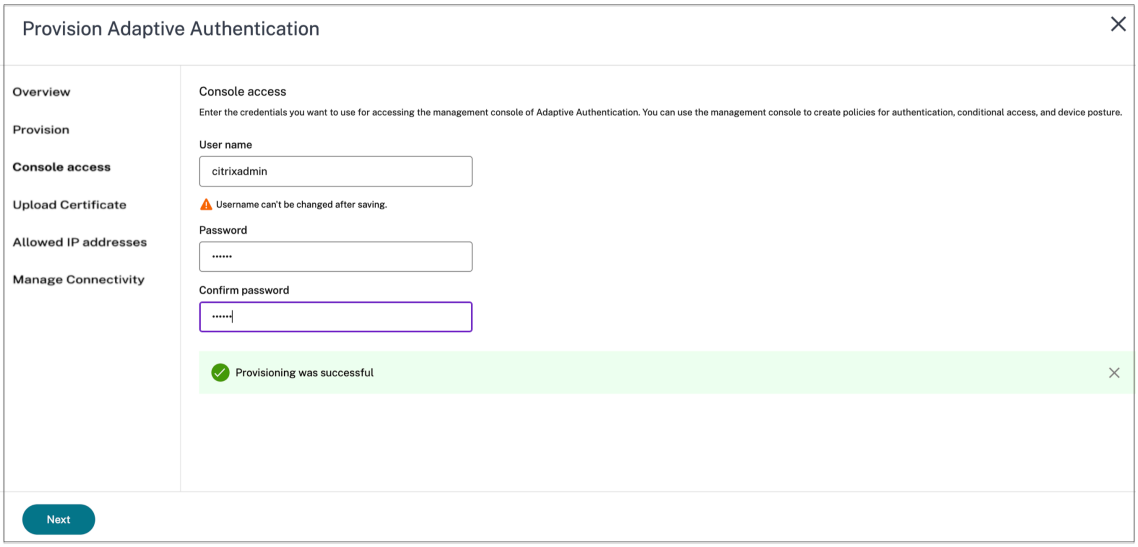
Si selecciona la **interconexión de Azure VNet** como conexión, debe agregar un bloque CIDR de subred que se debe usar para aprovisionar la instancia de Autenticación adaptable. También debe asegurarse de que el bloque CIDR no se superponga con otros rangos de redes de su organización.

Para obtener más información, consulte Configurar la conectividad a los servidores de autenticación locales mediante la interconexión de Azure VNet.

3. Configura las credenciales para acceder a las instancias que has habilitado para la autenticación adaptativa. Necesita el acceso a la consola de administración para crear directivas de autenticación, acceso condicional, etc.

   a) En la pantalla **Acceso a la consola**, introduzca el nombre de usuario y la contraseña.
   b) Haga clic en **Siguiente**.

> **Nota:**
>
> Los usuarios creados desde la pantalla **Acceso a la consola** cuentan con privilegios de "superusuario"que tienen acceso a la consola.



4. Agregue el FQDN del servicio de autenticación adaptable y cargue el par de claves de certificado. Debe introducir el FQDN del servicio de autenticación adaptable de su elección para el servidor de autenticación de acceso público. Este FQDN debe poder resolverse públicamente.

   a) En la pantalla **Cargar certificado**, introduzca el FQDN que ha reservado para la autenticación adaptativa.

   b) Seleccione el tipo de certificado.

      - El servicio de autenticación adaptable admite certificados de tipo PFX, PEM o DER para el aprovisionamiento de instancias.
      - El paquete de certificados solo es compatible con los certificados de tipo PEM. Para otros tipos de paquetes, Citrix recomienda instalar los certificados raíz e intermedio y vincularlos al certificado del servidor.

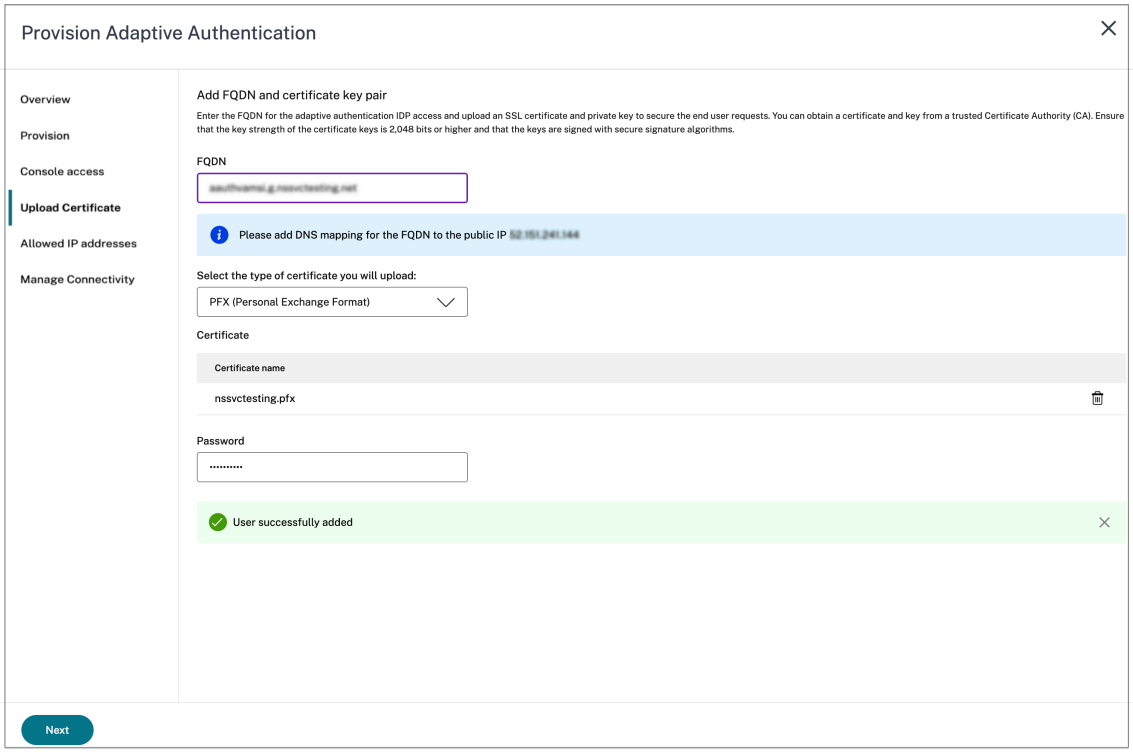
   c) Cargue el certificado y la clave.

> **Nota:**
>
> - Instale el certificado intermedio en la instancia de Autenticación adaptable y vincúlelo con el certificado del servidor.
>
> ```
> 1. Inicie sesión en la instancia de Autenticación adaptable. 1. Diríjase a **Administración del tráfico > SSL**. Para obtener más información, consulte [Configurar certificados intermedios](/en-us/citrix-
> ```



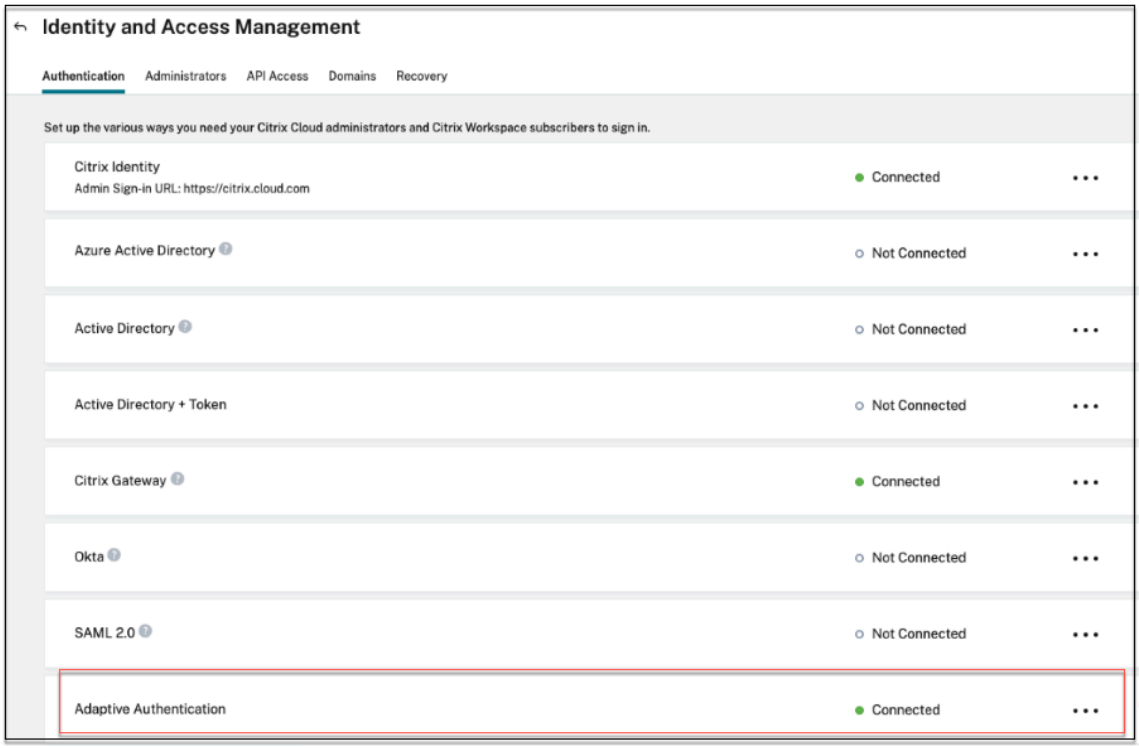
```
gateway/current-release/install-citrix-gateway/
certificate-management-on-citrix-gateway/configure-
intermediate-certificate.html).
```

- Solo se aceptan certificados públicos. No se aceptan certificados firmados por entidades certificadoras privadas o desconocidas.
- La configuración o las actualizaciones de los certificados deben realizarse únicamente mediante la interfaz de usuario de autenticación adaptable. No lo cambie directamente en la instancia, ya que esto podría provocar inconsistencias.



5. Cargue el certificado y la clave.

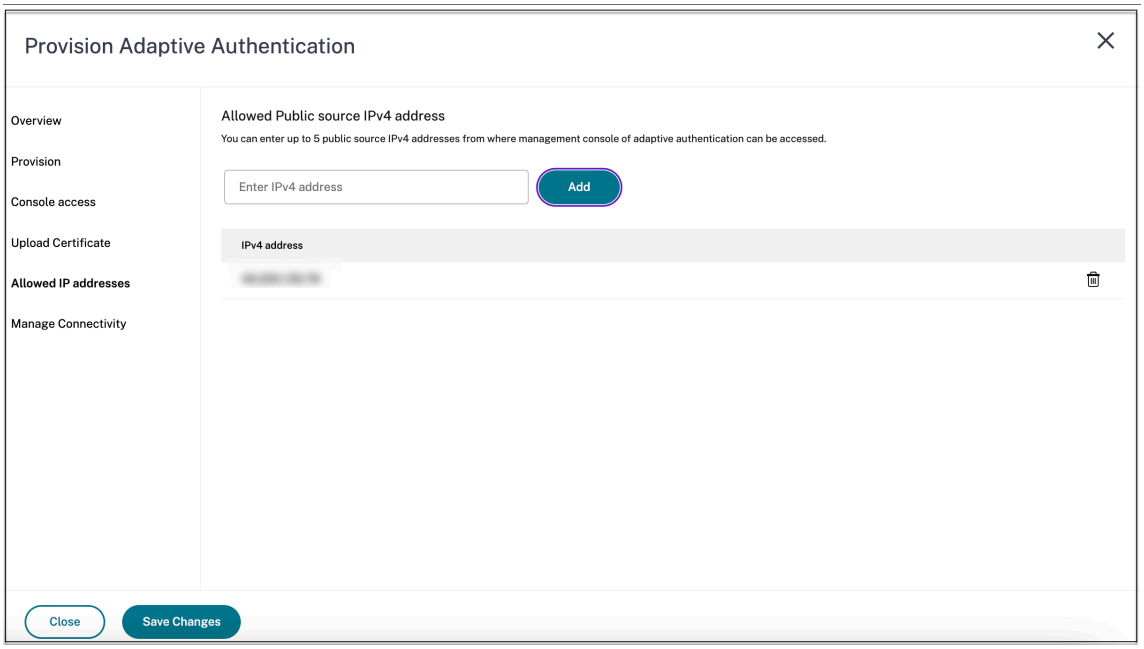
   La instancia de Autenticación adaptable ahora está conectada al servicio Administración de acceso e identidad. El estado del método de **autenticación adaptable** se muestra como **Conectado**.



6. Configure una dirección IP a través de la cual se pueda acceder a la consola de administración de Adaptive Authentication.

    a) En la pantalla **Direcciones IP permitidas**, para cada instancia, introduzca una dirección IP pública como dirección IP de administración. Para restringir el acceso a la dirección IP de administración, puede agregar varias direcciones IP que tengan permiso para acceder a la consola de administración.

    b) Para agregar varias direcciones IP, debe hacer clic en **Agregar**, escribir la dirección IP y, a continuación, **hacer clic en Listo**. Esto debe hacerse para cada dirección IP. Si no hace clic en el botón **Listo**, las direcciones IP no se agregan a la base de datos, sino que solo se agregan a la interfaz de usuario.



7. Si utiliza el tipo de conectividad de conector, especifique un conjunto de ubicaciones de recursos (conectores) a través de las cuales se pueda acceder a los servidores AD o RADIUS. Si utiliza el tipo de conectividad de interconexión de redes virtuales, puede omitir este paso.

   Los administradores pueden elegir los conectores a través de los cuales se debe acceder a los servidores AD y RADIUS de fondo. Para habilitar esta función, los clientes pueden configurar un mapeo entre las subredes de sus servidores AD/RADIUS de fondo de modo que, si el tráfico de autenticación se encuentra en una subred específica, ese tráfico se dirija a la ubicación de recursos específica. Sin embargo, si una ubicación de recursos no está asignada a una subred, los administradores pueden especificar el uso de la ubicación de recursos comodín para esas subredes.

   Anteriormente, el tráfico de autenticación adaptable para el AD/RADIUS local se dirigía a cualquier ubicación de recursos disponible mediante el método de todos contra todos. Esto causó problemas a los clientes con varias ubicaciones de recursos.

   a) En la interfaz de usuario de autenticación adaptable, haga clic en **Administrar conectividad**.

   b) Introduzca los detalles de la subred y seleccione la ubicación del recurso correspondiente.

      > **Nota:**
      >
      > Si desactiva la casilla **Usar cualquier ubicación de recursos disponible para las subredes restantes**, solo se tunelizará el tráfico dirigido hacia las subredes configuradas.

   c) Haga clic en **Agregar** y, a continuación, en **Guardar cambios**.

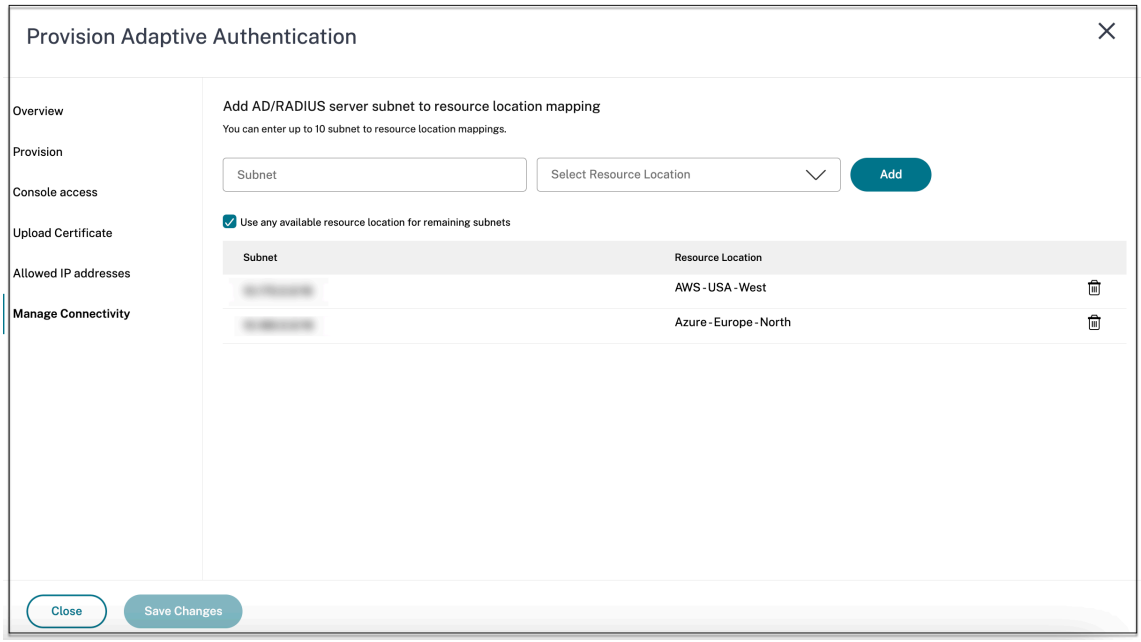
Nota:

- Solo se permiten las subredes de direcciones IP RFC1918.
- El número de asignaciones de ubicación de recursos de subred por cliente está limitado a 10.
- Se pueden asignar varias subredes a una sola ubicación de recursos.
- No se permiten entradas duplicadas para la misma subred.
- Para actualizar la entrada de subred, elimine la entrada existente y, a continuación, actualícela.
- Si cambia el nombre de la ubicación del recurso o la elimina, asegúrese de eliminar la entrada de la pantalla **Administrar conectividad** de la interfaz de usuario de Autenticación adaptable.
- Todos los cambios realizados en la asignación de ubicaciones de los recursos mediante los siguientes comandos de la CLI se sobrescriben con los cambios introducidos desde la interfaz de usuario (**Provisioning de autenticación adaptable > Gestionar**la conectividad).

```
- set cloudtunnel parameter -subnetResourceLocationMappings


- set policy expression aauth_allow_rfc1918_subnets
   <>

- set policy expression aauth_listen_policy_exp <>
```

> El Provisioning de la autenticación adaptable ya está completo.

Paso 2: Configurar las directivas de autenticación adaptable

Cómo conectarse a su instancia de autenticación adaptable:

Tras el aprovisionamiento, puede acceder directamente a la dirección IP de administración de la autenticación adaptable. Puede acceder a la consola de administración de Autenticación adaptable mediante el FQDN o su dirección IP principal.

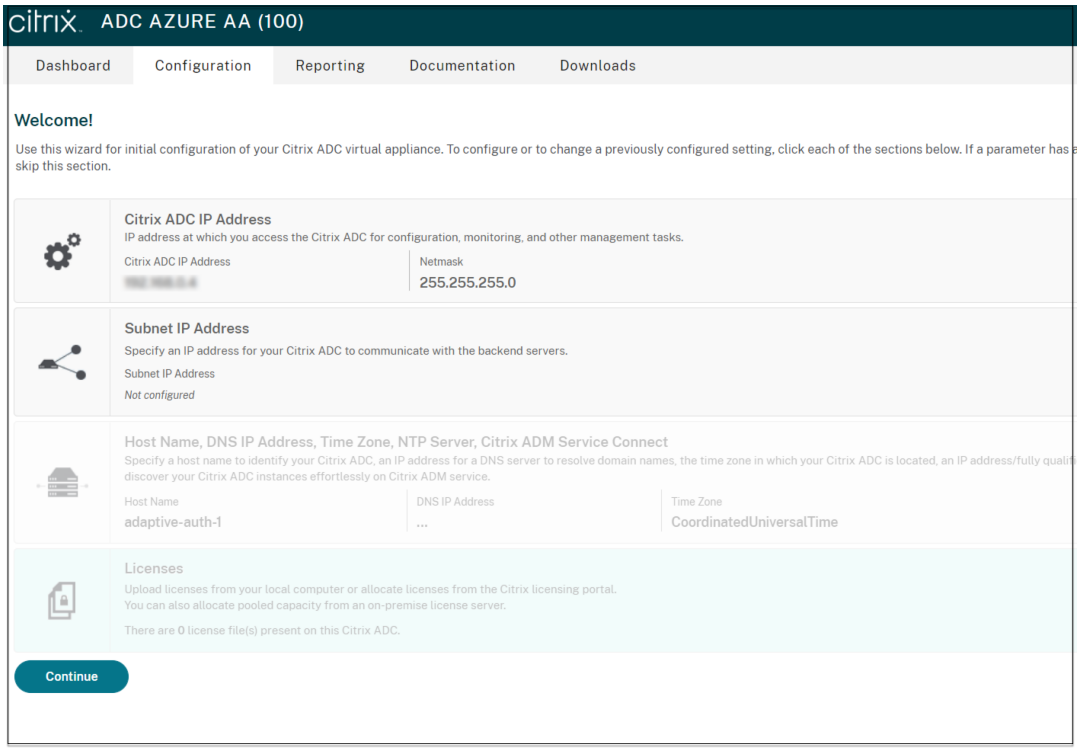
> **Importante:**
>
> - En una configuración de alta disponibilidad, como parte del proceso de sincronización, los certificados también se sincronizan. Por lo tanto, asegúrese de usar el certificado comodín.
> - Si necesita un certificado único para cada nodo, cargue los archivos y claves del certificado en cualquier carpeta que no se sincronice (por ejemplo, cree una carpeta independiente (nosync_cert) en el directorio NSconfig/SSL) y, a continuación, cargue el certificado de forma exclusiva en cada nodo.

Acceda a la consola de administración de autenticación adaptable:

- Para acceder a la consola de administración de autenticación adaptable mediante el FQDN, consulte Configurar SSL para el acceso a la interfaz de usuario de administración de ADC.
- Para acceder a la autenticación adaptable mediante su dirección principal, haga lo siguiente:

  1. Copie la dirección IP principal de la sección **Configurar políticas de autenticación** de la GUI y acceda a la dirección IP en su navegador.

2. Inicie sesión con las credenciales que introdujo durante el aprovisionamiento.
3. Haga clic en **Continuar**.

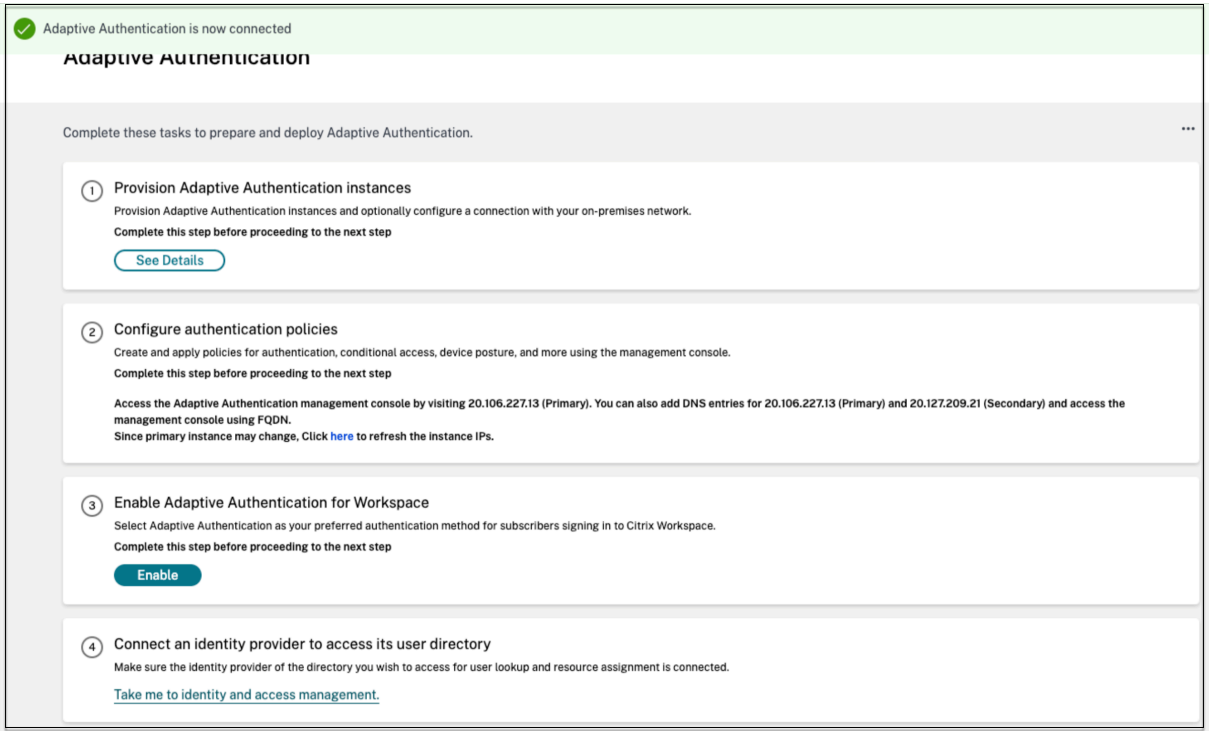


4. Vaya a **Configuración > Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**.
5. Agregue las directivas de autenticación. Para ver varios casos de uso, consulte Configuraciones de autenticación de ejemplo.

> **Nota:**
>
> El acceso a la instancia de autenticación adaptativa mediante la dirección IP no es confiable y muchos navegadores bloquean el acceso con advertencias. Le recomendamos que acceda a la consola de administración de autenticación adaptable con FQDN para evitar cualquier barrera de seguridad. Debe reservar el FQDN para la consola de administración de Autenticación adaptable y asignarlo con las direcciones IP de administración principal y secundaria.
>
> Por ejemplo, si la IP de la instancia de autenticación adaptativa es 192.0.2.0 y la secundaria: 192.2.2.2, entonces:
>
> - primary.domain.com se puede asignar a 192.0.2.0
> - secondary.domain.com se puede asignar a 192.2.2.2

Paso 3: Habilitar la autenticación adaptable para Workspace

Una vez finalizado el aprovisionamiento, puede habilitar la autenticación para Workspace haciendo clic en **Habilitar** en la sección **Habilitar la autenticación adaptable para Workspace**.



> **Nota:**
>
> Con esto, se completa la configuración de autenticación adaptable. Cuando accedas a la URL de su espacio de trabajo, debes redirigirte al FQDN de autenticación adaptable.

Referencias relacionadas

- Modificar un FQDN
- Programar la actualización de las instancias de autenticación adaptable
- Desaprovisionar las instancias de autenticación adaptable
- Permitir el acceso seguro a la puerta de enlace
- Configurar la conectividad con los servidores de autenticación locales mediante la interconexión de Azure VNet
- URL personalizada del espacio de trabajo o URL personalizada
- Configurar el respaldo y la restauración
- Ejemplo de configuración LDAPS con equilibrio de carga
- Migrar el método de autenticación a la autenticación adaptable
- Ejemplos de configuraciones de autenticación

Configuraciones de autenticación adaptable relacionadas

June 19, 2024

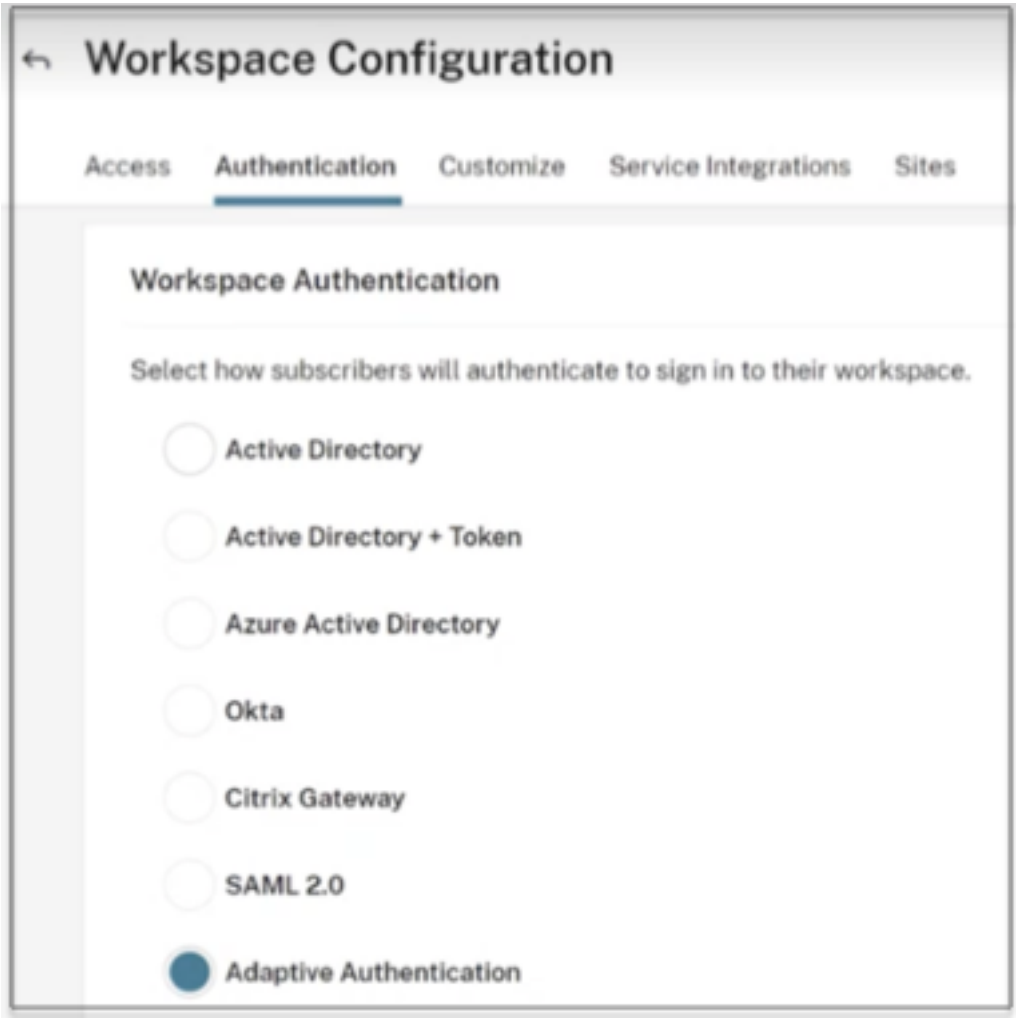
Modificar un FQDN

No puede modificar un FQDN si se ha seleccionado **Autenticación adaptable** como método de autenticación en la configuración de Workspace. Debe cambiar a un método de autenticación diferente para modificar el FQDN. Sin embargo, puede modificar el certificado si es necesario.

> **Importante:**
>
> - Antes de modificar el FQDN, asegúrese de que el nuevo FQDN esté asignado a la dirección IP pública del servidor virtual del IdP.
> - Los usuarios existentes que estén conectados a **Citrix Gateway** mediante directivas de OAuth deben migrar el método de autenticación a la **autenticación adaptable**. Para obtener más información, consulte Migrar el método de autenticación a la autenticación adaptable.

Para modificar un FQDN, realice lo siguiente:

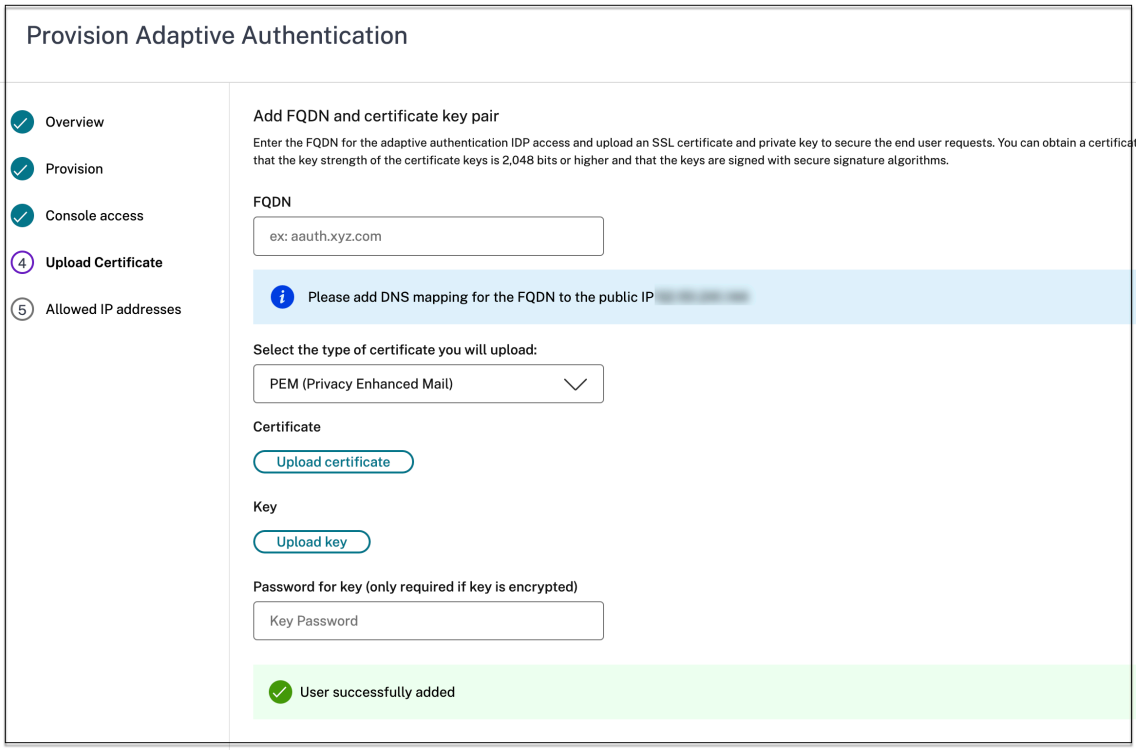
1. Cambie a un método de autenticación diferente de la **Autenticación adaptable**.



2. Selecciona **Comprendo el impacto en la experiencia del suscriptor y, a continuación,** haz clic en **Confirmar** .

   Al hacer clic en **Confirmar**, el inicio de sesión del espacio de trabajo para los usuarios finales se ve afectado y la Autenticación adaptable no se usa para la autenticación hasta que la autenticación adaptable vuelva Por lo tanto, se recomienda modificar el FQDN durante un período de mantenimiento.

3. En la pantalla **Cargar certificado**, modifique el FQDN.



4. Haga clic en **Guardar cambios**.

> **Importante:**
>
> Si modifica un FQDN, también debe volver a cargar el certificado.

5. Vuelva a habilitar el método de autenticación adaptable haciendo clic en **Habilitar** (paso 3) en la página de inicio de la autenticación adaptable.

6. Haga clic en **Actualizar**.

URL personalizada del espacio de trabajo o URL personalizada

Una URL de espacio de trabajo personalizada le permite usar un dominio de su elección para acceder a su almacén de Citrix Workspace. Los usuarios pueden acceder a Workspace mediante la URL predeterminada del espacio de trabajo, la URL del espacio de trabajo personalizada o ambas.

Para configurar una URL de espacio de trabajo personalizada o una URL personalizada, debes realizar lo siguiente:

1. Configura tu dominio personalizado. Para obtener más información, consulta Cómo configurar tu dominio personalizado.
2. Configure un nuevo perfil de OAuthIDP con el mismo ID de cliente, secreto y público que su perfil actual o predeterminado (AAuthAutoConfig_oauthIdpProf) pero con una URL de redireccionamiento diferente. Para obtener más información, consulte Configuración de directivas y perfiles de OAuth.

   Ejemplo:

   Perfil actual:

   ```
   -add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf
    -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
   ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https
   ://accounts-internal.cloud.com/core/login-cip"-audience zzzz -
   sendPassword ON

   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol -
   rule true -action AAuthAutoConfig_oauthIdpProf

   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol
    -priority 100 -gotoPriorityExpression NEXT
   ```

   Nuevo perfil:

   ```
   add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf_Custom1
    -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
   ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://
   custom_domain/core/login-cip"-audience zzzz -sendPassword ON

   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol_Custom1
    -rule true -action AAuthAutoConfig_oauthIdpProf_Custom1

   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol_Cu
    -priority 101 -gotoPriorityExpression NEXT
   ```

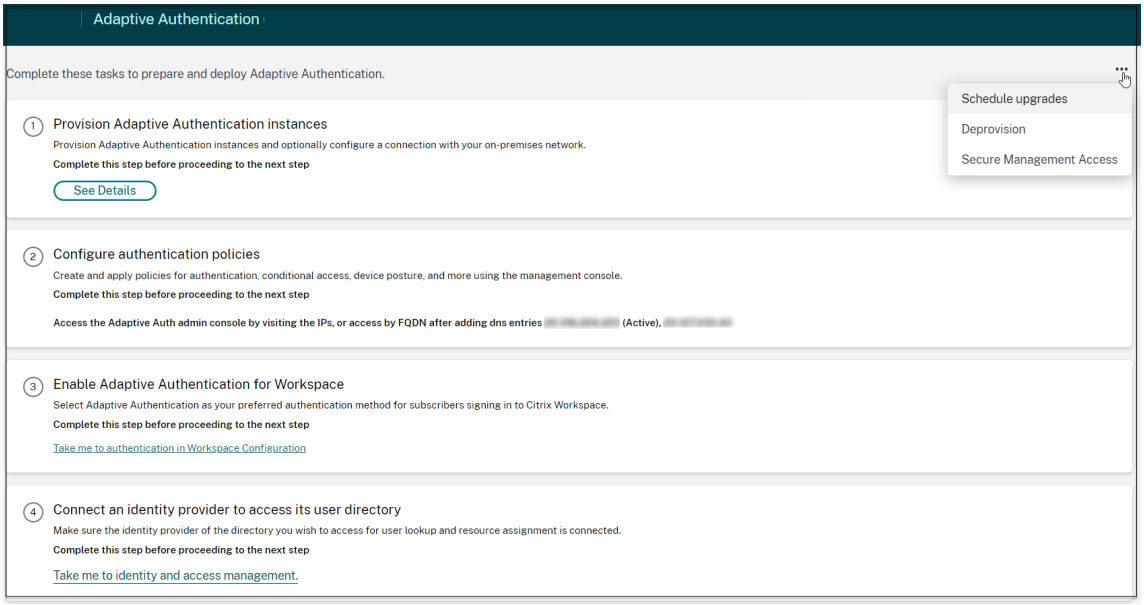
> **Importante:**
>
> - El servicio de autenticación adaptativa crea la directiva y el perfil de OAuth durante la fase de aprovisionamiento. Como resultado, el administrador de Citrix Cloud no tiene acceso al secreto de cliente no cifrado. Puede obtener el secreto cifrado en el archivo ns.conf. Para crear un perfil de OAuth, debe usar el secreto cifrado y crear el perfil solo con los comandos de la CLI.
> - No puede crear un perfil de OAuth mediante la interfaz de usuario de NetScaler.

Programar la actualización de las instancias de autenticación adaptable

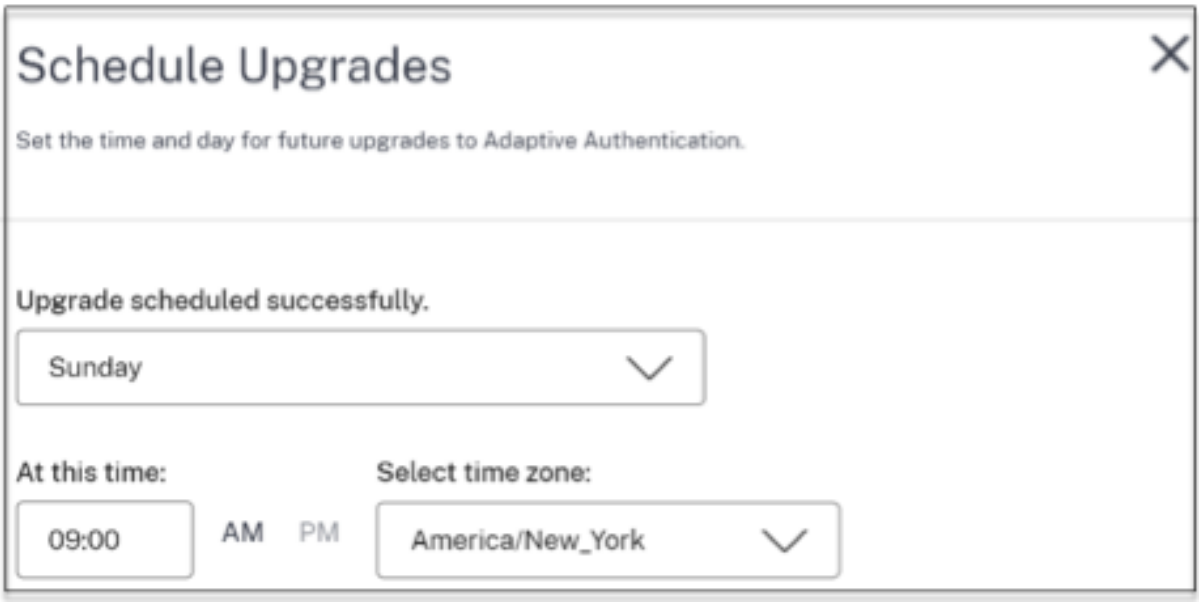
Para el sitio o la implementación actual, puede seleccionar el período de mantenimiento para la actualización.

> **Importante:**
>
> No actualice las instancias de autenticación adaptable a compilaciones RTM aleatorias. Citrix Cloud administra todas las actualizaciones.

1. En la interfaz de usuario de **Autenticación adaptable**, en la sección **Aprovisionar instancias de autenticación adaptable**, haga clic en el botón



2. Haga clic en **Programar actualizaciones**.
3. Seleccione el día y la hora de la actualización.



Desaprovisionar las instancias de autenticación adaptable

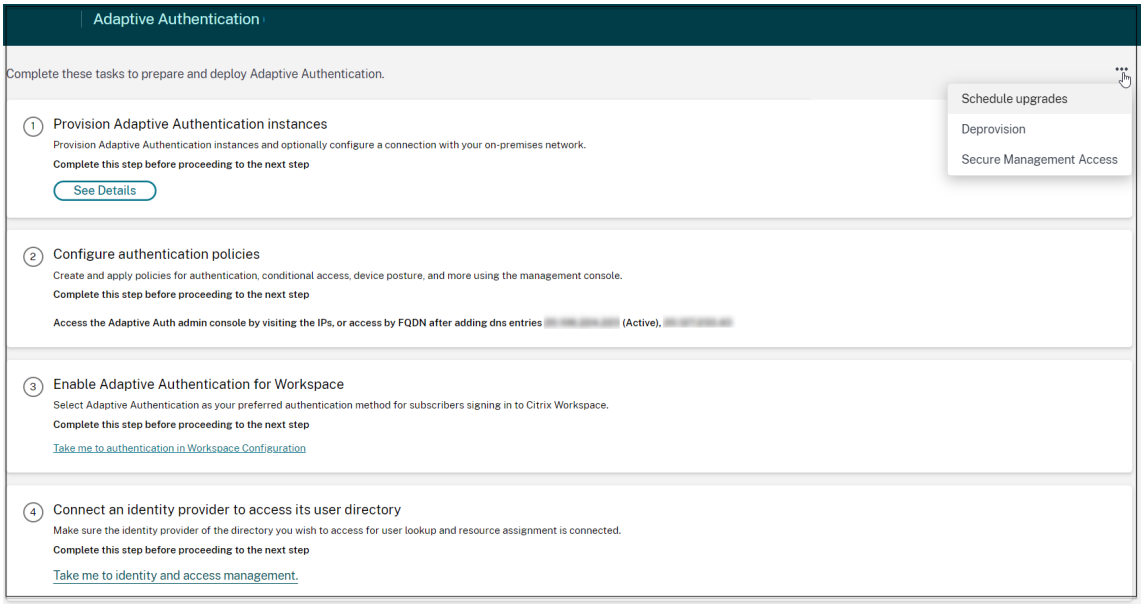
Los clientes pueden anular el aprovisionamiento de las instancias de Autenticación adaptable en los siguientes casos y según la sugerencia del soporte de Citrix.

- No se puede acceder a las instancias de Autenticación adaptable (especialmente después de una actualización programada), aunque es posible que este caso no se produzca.
- Si el cliente tiene que cambiar del modo de emparejamiento de VNet al modo de conector o viceversa.
- Si el cliente seleccionó una subred incorrecta en el momento de aprovisionar el modo de emparejamiento de VNet (la subred entra en conflicto con otras subredes de su centro de datos o VNet de Azure).

> **Nota: Al**
>
> desaprovisionar, también se elimina la copia de seguridad de la configuración de las instancias. Por lo tanto, debe descargar los archivos de copia de seguridad y guardarlos antes de anular el aprovisionamiento de las instancias de autenticación adaptable

Realice lo siguiente para anular el aprovisionamiento de una instancia de autenticación adaptable:

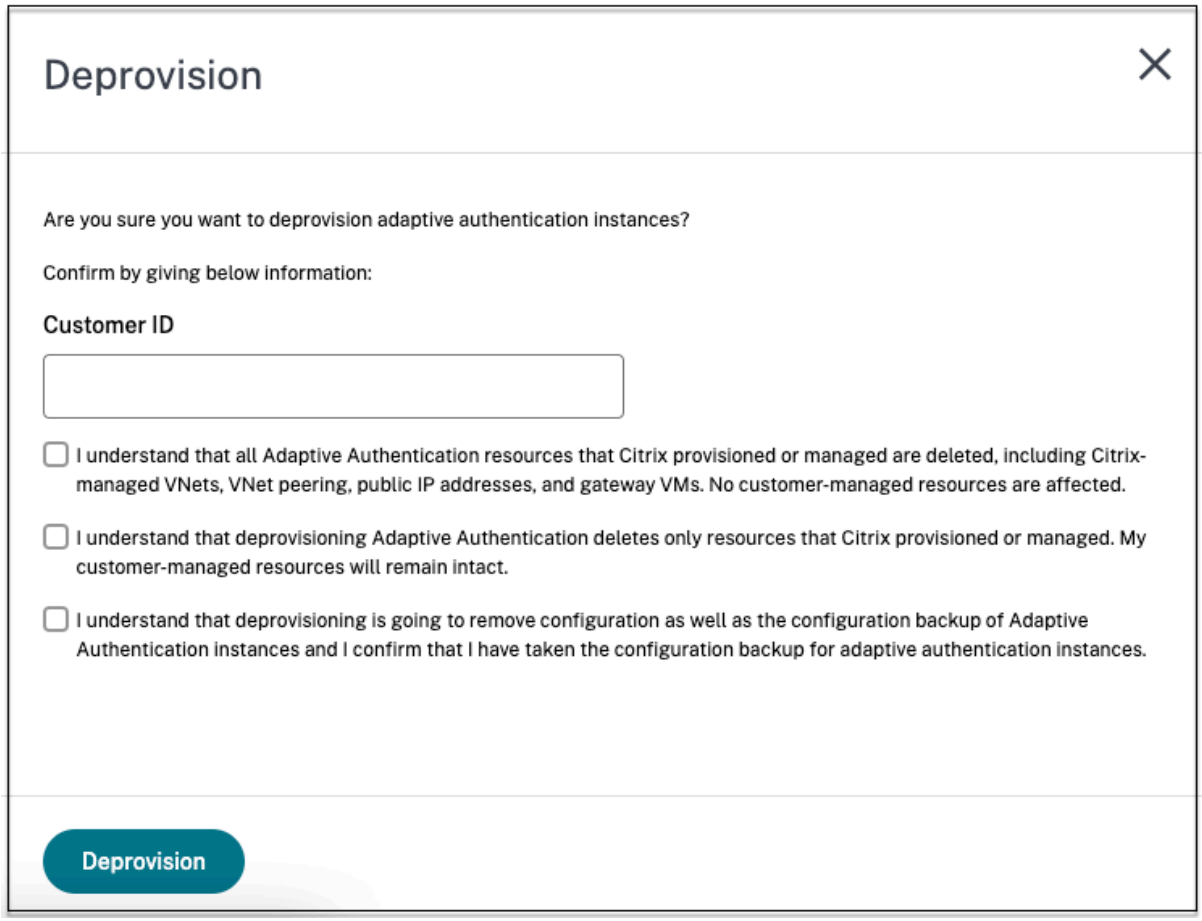
1. En la interfaz de usuario de **Autenticación adaptable**, en la sección **Aprovisionar instancias de autenticación adaptable**, haga clic en el botón



2. Haga clic en **Desaprovisionar**.

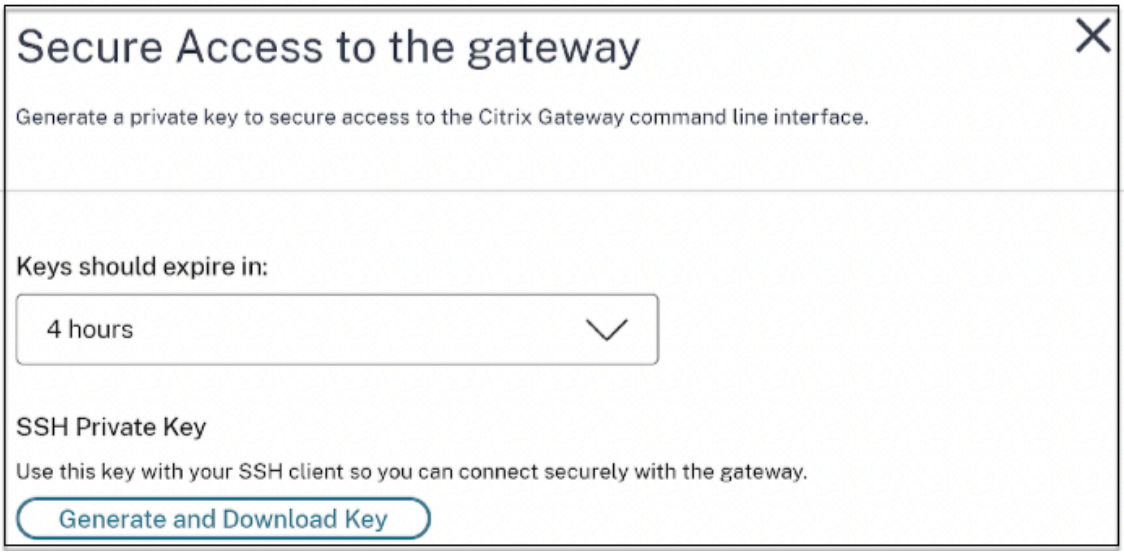
> **Nota:**
>
> Antes de desaprovisionar, debe desconectar **Citrix Gateway** de Configuración de Workspace.

3. Introduzca el ID de cliente para anular el aprovisionamiento de las instancias de autenticación adaptable.



Permitir el acceso seguro a la puerta de enlace

1. En la interfaz de usuario de **Autenticación adaptable**, en la sección **Aprovisionar instancias de autenticación adaptable**, haga clic en el botón
2. Haga clic en **Acceso seguro a la administración**.



3. En **Las claves deben caducar en**, selecciona una duración de caducidad para la nueva clave SSH.
4. Haga clic en **Generar y descargar claves**.
   Copie o descargue la clave privada SSH para usarla más adelante, ya que no se muestra después de cerrar la página. Esta clave se puede usar para iniciar sesión en las instancias de Autenticación adaptable con el nombre de usuario `authadmin`.

   Puede hacer clic en **Generar y descargar claves** para crear un nuevo par de claves si el par de claves anterior caduca. Sin embargo, solo puede haber un par de claves activo.
5. Haga clic en **Listo**.

Importante:

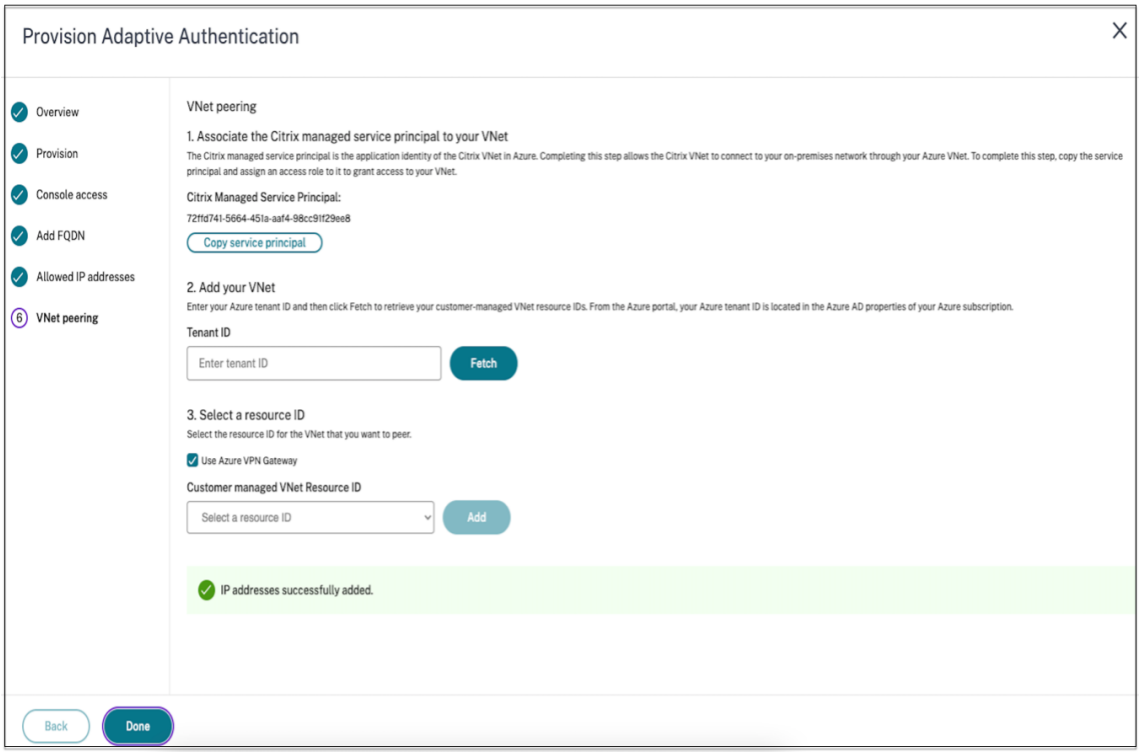
- Si usa PuTTY en Windows para conectarse a instancias de Autenticación adaptable, debe convertir la clave privada descargada a PEM. Para obtener información detallada, consulte https://www.puttygen.com/convert-pem-to-ppk.
- Se recomienda usar el siguiente comando para conectarse a las instancias de Autenticación adaptable a través del terminal desde el MAC o PowerShell/símbolo del sistema desde Windows (versión 10).
  `ssh -i <path-to-private-key> authadmin@<ip address of ADC>`
- Si quiere que los usuarios de AD accedan a la GUI de autenticación adaptable, debe agregarlos como nuevos administradores al grupo LDAP. Para obtener información detallada, consulte.https://support.citrix.com/article/CTX123782
  Para todas las demás configuraciones, Citrix recomienda usar la GUI de autenticación adaptable y no los comandos de la CLI.

Configurar la conectividad con los servidores de autenticación locales mediante la interconexión de Azure VNet

Debe configurar esta configuración solo si ha seleccionado el tipo de conectividad como interconexión de Azure VNet.

> **Nota:**
>
> Si utiliza IDP de terceros como Okta, Azure AD o Ping, este paso no es obligatorio.

1. En la interfaz de usuario de Connect autenticación adaptable, haga clic en **Aprovisionar** y, a continuación, haga clic en **Emparejamiento de redes virtuales de Azure**.



El campo **Citrix Managed Service Principal** contiene el ID de aplicación de una entidad de servicio de Azure creada por Citrix para su cliente. Esta entidad de servicio es necesaria para permitir que Citrix agregue una interconexión de VNet a una VNet en la suscripción y el arrendatario.

Para permitir que esta entidad de servicio inicie sesión en el arrendatario del cliente, el administrador del sitio del cliente (administrador global del arrendatario) debe ejecutar los siguientes comandos de PowerShell para agregar el SPN al arrendatario. También se puede usar Cloud-Shell.

```
Connect-AzureAD
New-AzureADServicePrincipal -AppId $App_ID
```

Donde `$App_ID` es un ID de aplicación de SPN compartido por Citrix.

> **Nota:**
>
> - El comando mencionado anteriormente genera un nombre principal de servicio que debe usarse para las asignaciones de roles.
> - Para permitir que esta entidad de servicio agregue una interconexión de VNet de Azure, el administrador del sitio del cliente (no limitado al administrador global) debe agregar una función de "Colaborador de red"a la VNet que debe estar vinculada a la VNet administrada por Citrix.
> - SPN es un identificador único que se utiliza para asociar la red virtual de Citrix en Azure. La asociación del SPN con la VNet permite que la red virtual de Citrix se conecte a la red local de los clientes a través de la VNet de Azure.

2. Cree un emparejamiento de VNet.

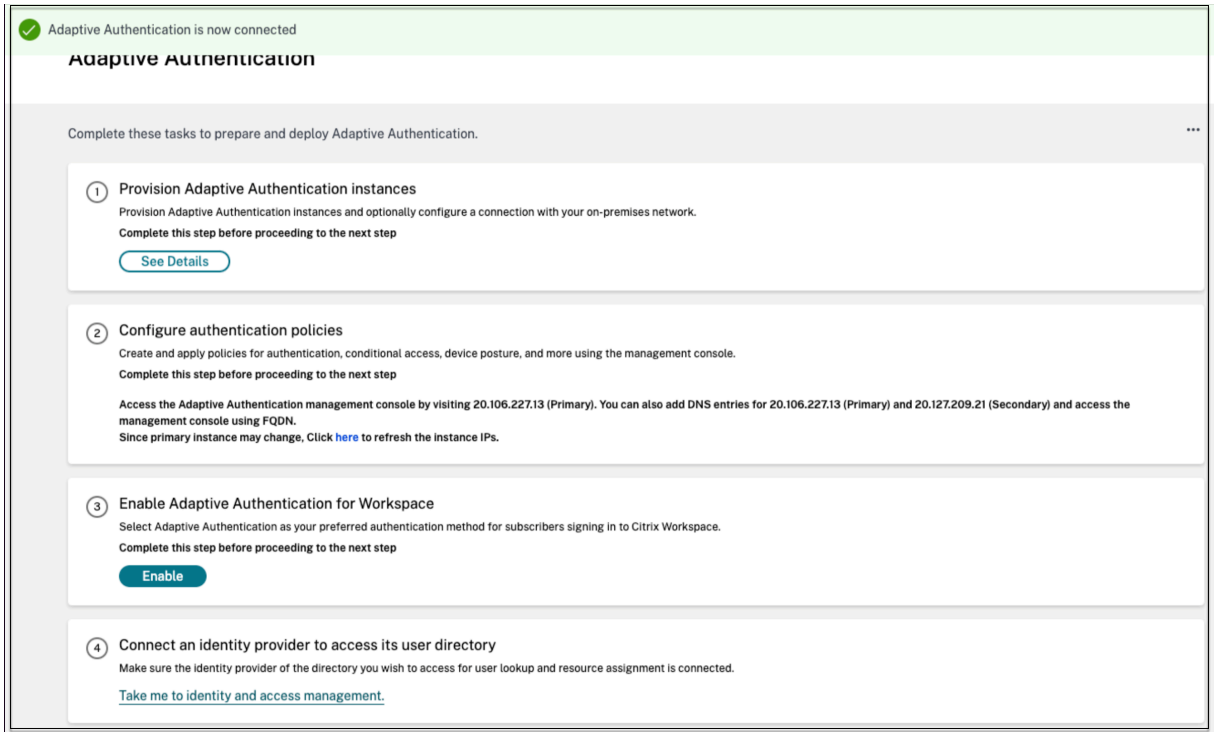
   - Introduzca el ID de arrendatario para el que se realizaron los pasos anteriores y haga clic en **Obtener**.

   Esto completa el ID de recurso de VNet administrado por el cliente con las VNet candidatas para las que se agrega la función de colaborador de red para el SPN. Si no ve la VNet, asegúrese de que los pasos anteriores se ejecutan correctamente o repita los pasos.

   > **Nota:**
   >
   > Para obtener más información sobre cómo encontrar su ID de arrendatario, consulte https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant.

3. Seleccione **Usar Azure VPN Gateway** para conectar las redes locales a Azure.
4. En **Customer managed VNet Resource ID**, seleccione la VNet identificada para la interconexión y haga clic en **Add**.
   La VNet se agrega a la tabla con el estado inicial de **En curso**. Una vez que el emparejamiento se haya completado correctamente, el estado cambia a **Hecho**.
5. Haga clic en **Listo**.
6. Continúe con la configuración, consulte Paso 1: Provisión de la autenticación adaptable.

   > **Importante:**
   >
   > - Para que el tráfico fluya entre la VNet administrada por Citrix y la red local, es posible que se cambien las reglas de firewall y enrutamiento en las instalaciones para dirigir el tráfico a la VNet administrada por Citrix.
   > - Solo puede agregar un par de VNet a la vez. Actualmente, no se permiten varios pares de VNet. Puede eliminar una interconexión de VNet o crear una según sea necesario.



Configurar el respaldo y la restauración

El servicio Administración de entrega de aplicaciones lleva a cabo la administración de copias de seguridad para las instancias Para obtener más información, consulte Realizar copias de seguridad y restaurar instancias de NetScaler.

1. En el mosaico Administración de entrega de aplicaciones, haga clic en **Administrar** .
2. Vaya a **Infraestructura > Instancias** y acceda a las copias de seguridad.

> **Nota:**
>
> Si no ve el servicio incorporado, incorpore el servicio de administración de entrega de aplicaciones. Para obtener más información, consulte Primeros pasos.

Ejemplo de configuración de equilibrio de carga de LDAP y LDAPS

La instancia de autenticación adaptable de Citrix proporciona soporte para LDAP/LDAPS mediante un servidor virtual de equilibrio de carga.

> **Nota:**
>
> - Si no utiliza el equilibrio de carga para LDAP/LDAPS, evite crear un servicio o un servidor para un servidor LDAP, ya que esto podría interrumpir el túnel de autenticación adaptable.

> - Si utiliza el equilibrio de carga para LDAP, cree un grupo de servicios y vincúlelo al servicio de equilibrio de carga y no a un servicio independiente.
> - Cuando utilice un servidor virtual de equilibrio de carga para la autenticación, asegúrese de agregar la dirección IP del servidor virtual de equilibrio de carga en lugar de la dirección IP real del servidor LDAP en la acción LDAP.
> - De forma predeterminada, un monitor TCP está enlazado al servicio que se crea. En las instancias de NetScaler de Autenticación adaptable, el servicio se marca como ACTIVO de forma predeterminada si se utiliza un monitor TCP.
> - Para la monitorización, se recomienda utilizar monitores personalizados.

Requisitos previos

Dirección IP privada (dirección RFC1918) del servidor virtual de equilibrio de carga. Puede ser una dirección IP ficticia, ya que se utiliza para la configuración interna.

Servidores LDAP de equilibrio de carga

Para los servidores LDAP de equilibrio de carga, cree un grupo de servicios y vincúlelo al servidor virtual de equilibrio de carga. No cree un servicio para equilibrar la carga de los servidores LDAP.

Configure LDAP mediante la CLI de NetScaler:

Puede utilizar los siguientes comandos de CLI como referencia para configurar LDAP.

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>)<port>`
3. `add lb vserver <name> <serviceType> <ip> <port>` - El puerto debe ser 389. Este puerto se usa para la comunicación interna y la conexión a un servidor local se realiza a través de SSL según el puerto configurado para el grupo de servicios.
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
6. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
7. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Configure LDAP mediante la interfaz gráfica de usuario de NetScaler:

1. Vaya a **Administración del tráfico > Equilibrio de carga** y, a continuación, haga clic en **Servidores virtuales**.

2. Cree un servidor virtual de tipo TCP y puerto 389.

   No cree un servidor virtual de equilibrio de carga de tipo SSL/SSL_TCP.

3. Vaya a **Administración del tráfico > Equilibrio de carga** y, a continuación, haga clic en **Grupos de servicios**.
4. Cree un grupo de servicios de tipo TCP y puerto 389.
5. Enlazar el grupo de servicios al servidor virtual que ha creado en el paso 1.

Para obtener más información sobre los procedimientos, consulte Configurar el equilibrio de carga básico.

Servidores LDAPS de equilibrio de carga

Para los servidores LDAPS de equilibrio de carga, debe crear un servidor virtual de equilibrio de carga de tipo TCP para evitar el cifrado SSL interno o el descifrado en la instancia de autenticación adaptable. El servidor virtual de equilibrio de carga gestiona el cifrado/descifrado de TLS en este caso. No cree un servidor virtual de equilibrio de carga de tipo SSL.

Configure LDAPS mediante la CLI de NetScaler:

Puede utilizar los siguientes comandos de CLI como referencia para configurar LDAPS.

1. `add lb vserver <name> <serviceType> <ip> <port>` - El puerto debe ser el 636.
2. `bind lb vserver <name> <serviceGroupName>`
3. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
4. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
5. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Configure LDAPS mediante la interfaz gráfica de usuario de NetScaler:

1. Vaya a **Administración del tráfico > Equilibrio de carga** y, a continuación, haga clic en **Servidores virtuales**.
2. Cree un servidor virtual de tipo TCP y puerto 636.

   No cree un servidor virtual de equilibrio de carga de tipo SSL/SSL_TCP.

3. Vaya a **Administración del tráfico > Equilibrio de carga** y, a continuación, haga clic en **Servicio**.
4. Cree un servicio de tipo SSL_TCP y el puerto 636.

5. Enlazar el servicio al servidor virtual que ha creado en el paso 1.

Para obtener más información sobre los procedimientos, consulte Configurar el equilibrio de carga básico.

Crea monitores personalizados

Cree monitores personalizados mediante la interfaz gráfica de usuario de NetScaler:

1. Vaya a **Administración del Tráfico > Equilibrio de carga > Monitores**.
2. Cree un monitor de tipo LDAP. Asegúrese de configurar el intervalo de sondeo del monitor en 15 segundos y el tiempo de espera de respuesta en 10 segundos.
3. Enlaza este monitor a tu servicio.

Para obtener más información, consulte Monitores personalizados.

Disposición para agregar hasta 15 direcciones IP de administrador

El servicio de autenticación adaptable le permite introducir hasta 15 subredes IP públicas y direcciones IP individuales para acceder a la consola de administración de Autenticación adaptable.

Puntos a tener en cuenta al introducir las direcciones IP o subredes:

- Asegúrese de que los CIDR de las subredes IP públicas estén entre /20 y /32.B.
- Asegúrese de que no haya superposición entre las entradas.

Ejemplos:

- No se aceptan 192.0.2.0/24 y 192.0.2.8 porque 192.0.2.8 se encuentra dentro de 192.0.5.0/24.
- Subredes superpuestas: 192.0.2.0/24 y 192.0.0.0/20 no se aceptan porque las subredes se superponen.
- Al introducir un valor de subred de red, introduzca la dirección IP de la red como el valor de la dirección IP.

  Ejemplo:

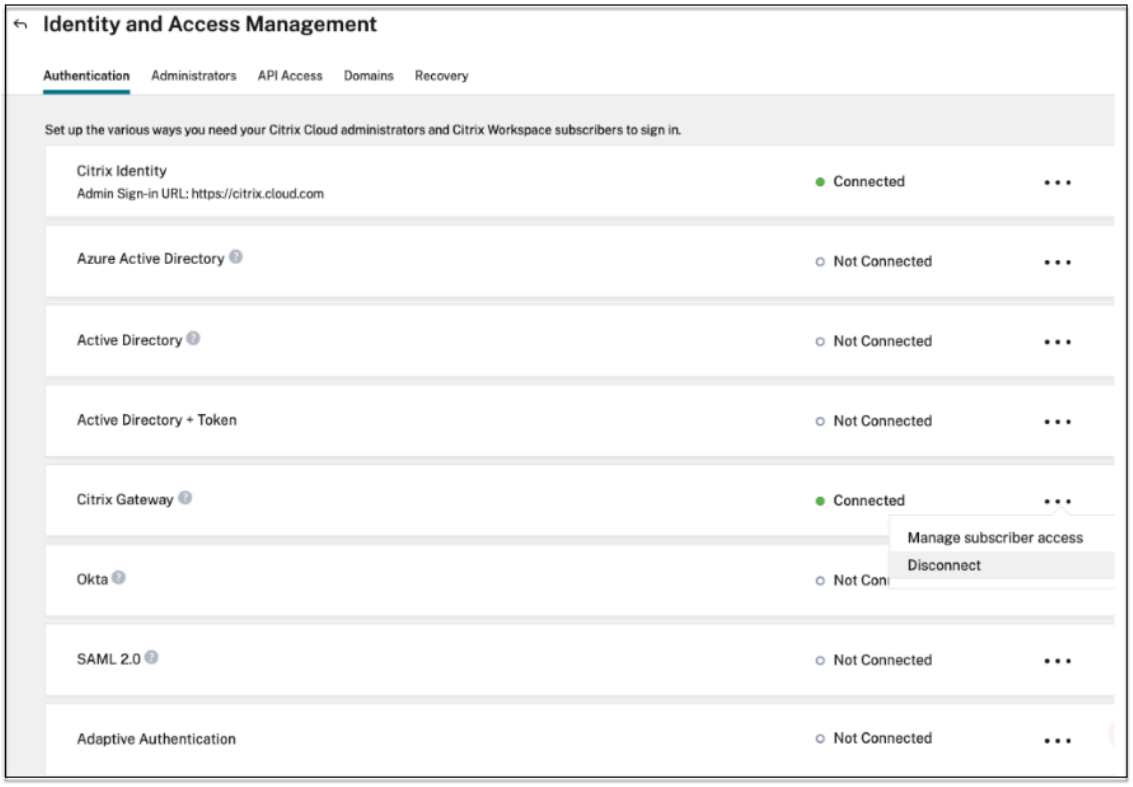
  - 192.0.2.2/24 es incorrecto, en su lugar utilice 191.0.2.0/24
  - 192.0.2.0/20 es incorrecto, en su lugar utilice 192.0.0.0/20

Para habilitar esta función, póngase en contacto con el soporte de Citrix.

Migrar el método de autenticación a la autenticación adaptable

Los clientes que ya utilizan la autenticación adaptable con el método de autenticación como **Citrix Gateway** deben migrar la **autenticación adaptable** y, a continuación, eliminar la configuración de OAuth de la instancia de autenticación adaptable.

1. Cambie a un método de autenticación diferente que no sea Citrix Gateway.
2. En **Citrix Cloud > Administración de acceso e identidad**, haga clic en el botón de puntos suspensivos correspondiente a Citrix Gateway y, a continuación, haga clic en **Desconectar**.



3. Seleccione **Comprendo el impacto en la experiencia del suscriptor** y, a continuación, haga clic en **Confirmar**.

   Al hacer clic en **Confirmar**, el inicio de sesión del espacio de trabajo para los usuarios finales se ve afectado y la Autenticación adaptable no se usa para la autenticación hasta que la autenticación adaptable vuelva

4. En la consola de administración de instancias de autenticación adaptable, elimina la configuración relacionada con OAuth.

   Mediante la CLI:

```
unbind authentication vs <authvsName> -policy <oauthIdpPolName>
rm authentication oauthIdpPolicy <oauthIdpPolName>
rm authentication oauthIdpProfile <oauthIdpProfName>
```



```
<!--NeedCopy-->
```

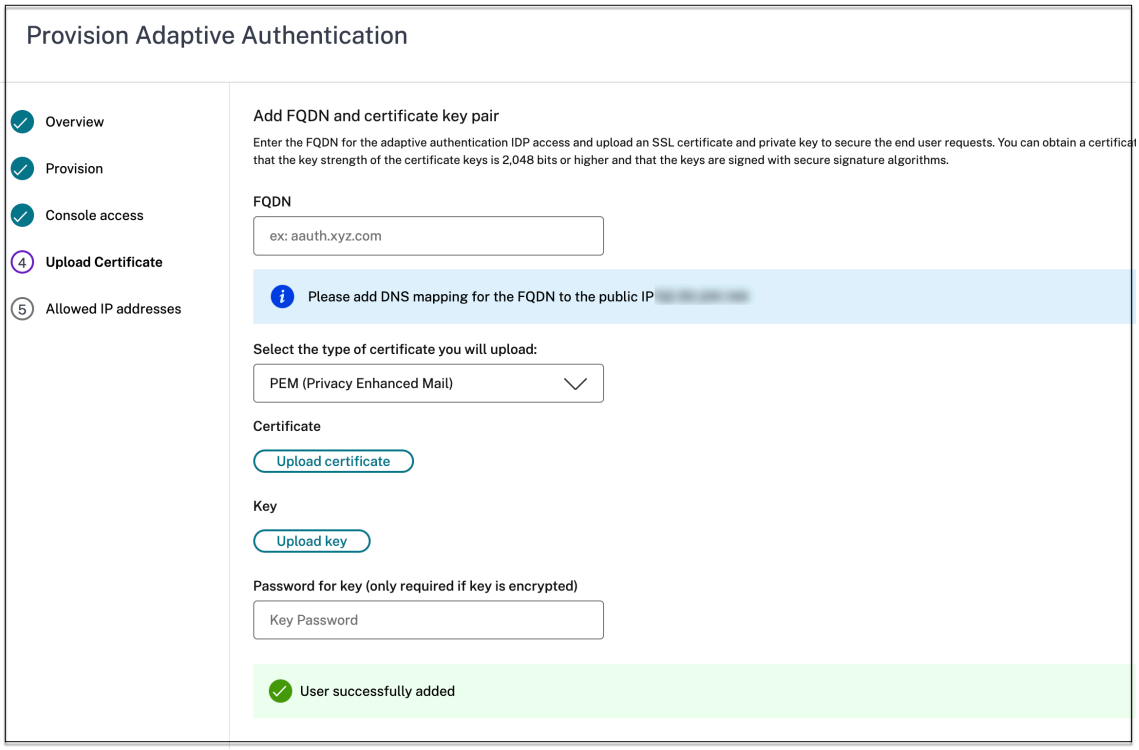
Mediante la interfaz gráfica de usuario:

a) Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Servidores virtuales**.
b) Desvincula la directiva de OAuth.
c) Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > OAuth IDP**.
d) Elimine la directiva y el perfil de OAuth.

5. Vaya a **Citrix Cloud > Administración de identidades y accesos**.
   En la pestaña Autenticación, en Autenticación adaptativa, haga clic en el menú de puntos suspensivos y seleccione **Administrar** .

   O acceso https://adaptive-authentication.cloud.com
6. Haga clic en **Ver detalles**.
7. En la pantalla **Cargar certificado**, haga lo siguiente:

   - Agregue el FQDN de autenticación adaptable.
   - Elimine los certificados y los archivos de claves y cárguelos de nuevo.



> **Importante:**
>
> Si modifica un FQDN o el par de claves de certificado directamente sin migrar a la **Autenti-**

> **cación adaptable**, se produce un error en la conexión a Identity and Access Management y se muestran los siguientes errores. Debe migrar al método de autenticación adaptable para corregir estos errores.
>
> - Error en el comando ADC. Una directiva ya está vinculada a la prioridad especificada.
> - Error en el comando ADC. No se puede desvincular una directiva que no está vinculada.

8. Haga clic en **Guardar cambios**.

   En este punto, Administración de acceso e identidad muestra **Autenticación adaptable** como **Conectada** y la instancia de Autenticación adaptable tiene el perfil de OAuth configurado automáticamente.

   Puede validarlo desde la GUI.

   a) Acceda a su instancia de autenticación adaptable e inicie sesión con sus credenciales.
   b) Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Servidores virtuales**. Debe ver que se creó el perfil del IdP de OAuth.
   c) Vaya a **Citrix Cloud > Administración de identidades y accesos**. La autenticación adaptable está en estado **Conectado**.

9. Vuelva a habilitar el método de autenticación adaptable haciendo clic en **Habilitar** (paso 3) en la página de inicio de la autenticación adaptable.

   Este paso habilita el método de autenticación como Autenticación adaptable en la configuración del espacio de trabajo

10. Haga clic en el enlace del espacio de trabajo en el paso 3 después **de**hacer clic Debe ver que el método de autenticación se ha cambiado a Autenticación adaptable.

> **Nota:**
>
> Los nuevos usuarios deben seguir los mismos pasos, excepto el paso para eliminar la configuración relacionada con OAuth.

Ejemplos de configuraciones de autenticación

Los clientes pueden configurar una directiva de autenticación de su elección y vincularla al servidor virtual de autenticación. Los enlaces de perfil de autenticación no son necesarios para el servidor

virtual de autenticación. Solo se pueden configurar las directivas de autenticación. Los siguientes son algunos de los casos de uso.

> **Importante:**
>
> La configuración de autenticación debe realizarse solo en los nodos principales.

Autenticación multifactor con autenticación condicional

- Autenticación de doble factor con LDAP y RADIUS mediante el esquema de doble factor (toma la entrada del usuario solo una vez)
- Método de inicio de sesión de autenticación según los departamentos del usuario (empleado, socio, proveedor) en la organización con menú desplegable para seleccionar el departamento
- Método de inicio de sesión de autenticación según los dominios de usuario con menú desplegable
- Configure la entrada de ID de correo electrónico (o nombre de usuario) como primer factor con acceso condicional basado en la extracción de grupos con el ID de correo electrónico en el primer factor y proporcione diferentes tipos de inicio de sesión para cada grupo
- Autenticación multifactor mediante autenticación de certificados para usuarios con certificados de usuario y registro OTP nativo para usuarios sin certificado
- Tipo de autenticación diferente con autenticación condicional según las entradas del nombre de host del usuario
- Autenticación de doble factor con autenticación OTP nativa
- Re-CAPTCHA de Google

Integración de terceros con autenticación multifactor

- Configurar Azure AD como proveedor de identidades SAML (configurar el siguiente factor como directiva LDAP: NO_AUTH para completar la confianza de OAuth)
- Autenticación condicional con el primer factor como SAML y, a continuación, el inicio de sesión personalizado en el certificado o LDAP según los atributos
- Primer factor como inicio de sesión de webauth seguido de LDAP

Escaneos de postura del dispositivo (EPA)

- Comprobación de la postura del dispositivo para la comprobación de la versión seguida de un inicio de sesión personalizado para usuarios que cumplen con las normas (RADIUS) y no las cumplen
- Autenticación LDAP seguida de un análisis obligatorio de posición

- Comprobación de la postura del dispositivo antes y después de la autenticación de AD: un factor previo y posterior a la EPA
- Certificado de dispositivo como factor EPA

Casos diversos

- Agregar CLUF con autenticación
- Personalizar etiquetas de directivas de nFactor, esquema de inicio

Administración del espacio en disco para instancias

June 19, 2024

El equipo de autenticación adaptativa administra todas las actualizaciones y el mantenimiento de las instancias de autenticación adaptativa. Por lo tanto, se recomienda no actualizar ni degradar las instancias de autenticación adaptativa a compilaciones RTM aleatorias. Citrix administra las instancias de autenticación adaptativa de forma predeterminada.

Para las actualizaciones de las instancias, se requiere un espacio mínimo de 7 GB en el directorio VAR. Por lo tanto, el equipo del servicio de autenticación adaptativa limpia el espacio en disco de las instancias antes de aplicar las actualizaciones. Se recomienda que no guarde ninguna información confidencial, privada o personal en los siguientes directorios:

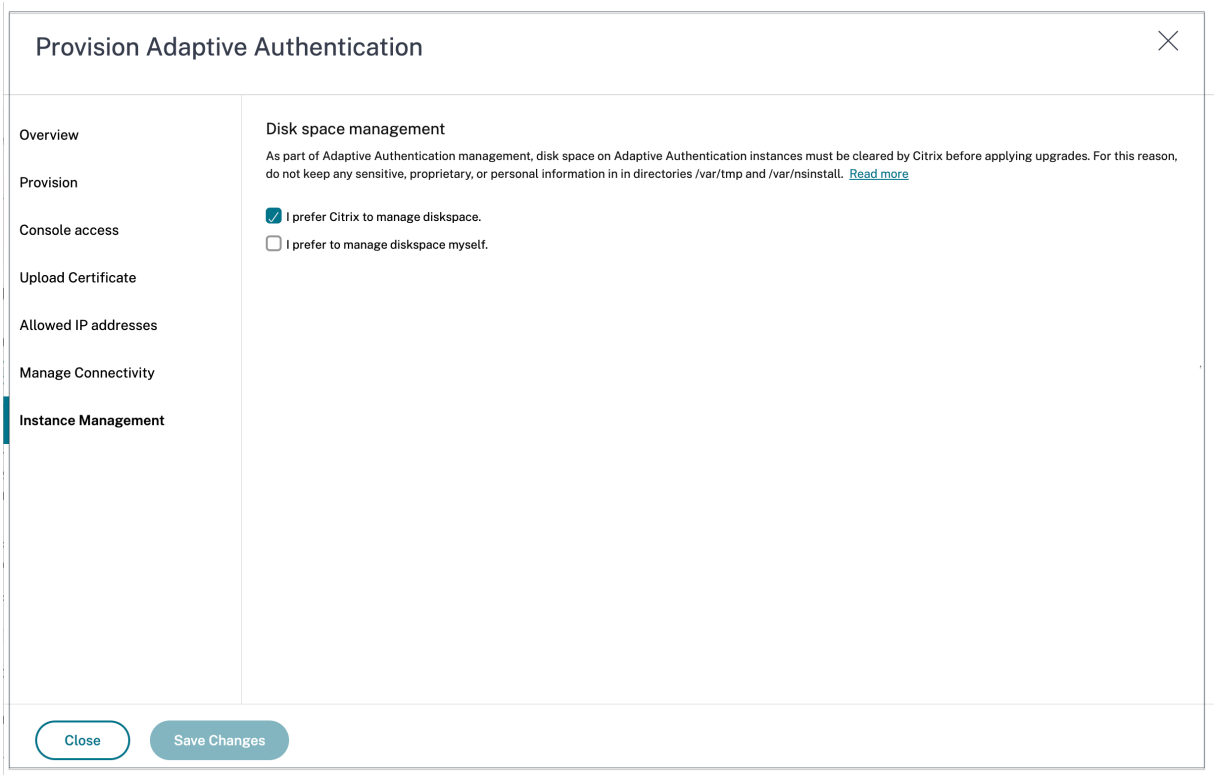
- /var/núcleo
- /var/bloquear
- /var/tmp
- /var/nsinstall
- /var/nstrace
- /var/nslog

> **Nota:**
>
> - El directorio /var/nsinstall se borra primero durante la actualización, seguido del directorio /var/tmp. Si aún no se cumple el requisito de espacio mínimo, también se borran los demás directorios (/var/core, /var/crash, /var/nstracem y /var/nslog).
> - El cliente es responsable de administrar y mantener el espacio en disco de NetScaler y la limpieza del disco.

Opción de administrar el espacio en disco usted mismo

Aunque Citrix administra las instancias de autenticación adaptativa, de forma predeterminada, puede preferir limpiar el espacio en disco de las instancias usted mismo. Puede optar por no utilizar el método predeterminado de la siguiente manera:

1. En el panel de navegación de Autenticación adaptativa, haga clic en **Administración de instancias**.
2. Seleccione **Prefiero administrar el espacio en disco yo mismo y después** haga clic en **Confirmar** en el cuadro de diálogo del mensaje de confirmación.
3. Haga clic en **Guardar cambios**.



Nota:

También puede programar las actualizaciones de acuerdo con el tráfico de sus clientes. A continuación, el equipo de Citrix Cloud actualiza las instancias en consecuencia.
Para obtener información sobre la programación de actualizaciones, consulte Programar la actualización de las instancias de Adaptive Authentication.

Solucionar problemas de autenticación adaptable

June 19, 2024

Los problemas se clasifican según las diferentes etapas de la configuración:

- Provisioning
- Problema de accesibilidad de
- Problema de conectividad y autenticación de AD/RADIUS
- Problemas de autenticación
- Problemas relacionados con la postura del dispositivo y la EPA
- Problemas relacionados con las etiquetas inteligentes
- Recopilación de registros

También puede solucionar los problemas mediante la CLI de Autenticación adaptable. Para conectarse a la CLI, haga lo siguiente:

- Descargue el cliente SSH como putty/securecrt en su máquina.
- Acceda a la instancia de Autenticación adaptable mediante la dirección IP (principal) de administración.
- Inicie sesión con sus credenciales.

Para obtener más información, consulte Acceso a un dispositivo NetScaler.

Habilitar el registro de registros de autenticación adaptable

Asegúrese de habilitar los niveles de registro para capturar los registros de autenticación adaptable.

Habilite los registros mediante la CLI:

1. Inicie sesión en la CLI de la instancia de autenticación adaptable.
2. Con PuTTY, introduzca las credenciales de administración.
3. Ejecute el comando `set audit syslogParams logLevel ALL`

Habilitar los registros mediante la GUI:

1. Inicie sesión en la instancia de autenticación adaptable mediante un explorador web.
2. Vaya a **Configuración > Sistema > Auditoría**.
3. En la página Auditoría, en **Configuración**, haga clic en **Cambiar la configuración de syslog de auditoría**.
4. En **Niveles de registro**, seleccione **TODOS.**

Problemas de aprovisionamiento

- **No se puede acceder a la IU de autenticación adaptable**

  Compruebe si el derecho está habilitado para su ID de cliente/arrendatario.

- **Estancado en la página de aprovisionamiento durante más de 45 minutos**

  Recopile la captura de pantalla del error, si existe, y luego póngase en contacto con el Soporte de Citrix para obtener ayuda.

- **El par de VNet está inactivo**

  - Compruebe si hay alertas en Azure Portal correspondientes a este emparejamiento y tome las medidas recomendadas.
  - Elimine el emparejamiento y vuelva a agregarlo desde la interfaz de usuario de Autenticación adaptable.

- **El desaprovisionamiento no está completo**

  Contacte con Citrix Support para obtener ayuda.

Problema de accesibilidad de

- **No se puede acceder a la dirección IP de administración para la instancia**

  - Compruebe si la dirección IP pública del cliente utilizada para el acceso se encuentra entre las direcciones IP de origen permitidas.
  - Valide si hay algún proxy que cambie la dirección IP de origen del cliente.

- **No se puede iniciar sesión en la instancia**

  Asegúrese de que el acceso de administrador funcione correctamente con las credenciales que introdujo durante el aprovisionamiento.

- **Los usuarios finales no tienen derechos completos**

  Asegúrese de que, al agregar el usuario, haya vinculado la directiva de comandos adecuada para el acceso. Para obtener más información, consulte Directivas de usuario, grupos de usuarios y comandos.

Problema de conectividad AD o RADIUS

Problema con el tipo de conectividad de pares de Azure Vnet:

- Compruebe si se puede acceder a la Azure VNet administrada por el cliente desde las instancias de autenticación adaptable.

- Compruebe si funciona la conectividad/accesibilidad de Azure VNet administrada por el cliente a AD.
- Asegúrese de que se agreguen las rutas adecuadas para dirigir el tráfico desde las instalaciones a las VNet de Azure.

Conector basado en Windows:

- Todos los registros están disponibles en el directorio /var/log/ns.log y cada registro lleva el prefijo [NS_AAUTH_TUNNEL].
- ConnectionID de los registros se puede usar para correlacionar diferentes transacciones.
- Asegúrese de que la dirección IP privada de la máquina virtual del conector se agregue como uno de los clientes RADIUS en el servidor RADIUS, ya que esa dirección IP es la dirección IP de origen del conector.

  Para cada solicitud de autenticación, se establece el túnel entre la instancia de autenticación adaptable (proceso NS - AAAD) y el servidor de autenticación. Una vez que el túnel se ha establecido correctamente, se produce la autenticación.

  Asegúrese de que la máquina virtual del conector pueda resolver el FQDN de autenticación adaptable.

- El conector está instalado, pero la conectividad local falla.

  Valide si NSAUTH-TUNNEL se está estableciendo.

  ```
  cat ns.log | grep -I “tunnel”
  ```

  Si el siguiente registro de ejemplo no se imprime en el archivo ns.log para la solicitud de autenticación, es posible que haya un problema al establecer un túnel o algún problema desde el lado del conector.

  ```
  1  LDAP:
  2  [NS_AAUTH_TUNNEL] Entering bitpump for
  3  Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636 ,
         Connection2 => Src : 10.106.103.70:2271, Dst :
        10.106.103.80:443"
  4  RADIUS:
  5  [NS_AAUTH_UDP_TUNNEL] MUX channel established"
  6  <!--NeedCopy-->
  ```

  Compruebe los detalles del registro y tome las medidas oportunas.

Detalles del registro	Acción correctiva
No se incluyen registros con prefijo `[NS_AAUTH_TUNNEL]` en el archivo de registros	Ejecute el comando `show cloudtunnel vserver`. Este comando debe incluir ambos servidores virtuales de túnel en la nube (TCP y UDP) con el estado “UP”.
`[NS_AAUTH_TUNNEL] Waiting for outbound from connector` Para este registro, si no se recibe la siguiente respuesta: `[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"`	Compruebe si la máquina conectora puede acceder al FQDN de autenticación adaptable **O** compruebe si hay conexiones salientes al FQDN de autenticación adaptable en el firewall del lado del conector.
`[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0` y`[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"`	Contacto con Citrix Support.

No hay respuesta del conector:

- Asegúrese de que se pueda acceder al FQDN de autenticación adaptable desde la máquina virtual del conector.
- Asegúrese de tener un certificado intermedio enlazado y vinculado al certificado del servidor en la instancia de Autenticación adaptable.

Configuración LDAP/RADIUS incorrecta:

Si la dirección IP de su servidor AD/RADIUS es una dirección IP pública, debe agregar la subred o la dirección IP a las expresiones en NetScaler. No modifique los rangos existentes.

- Para agregar una subred o una dirección IP mediante la CLI:

```
1  set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST
       .BETWEEN(10.0.0.0,10.255.255.255) || CLIENT.IP.DST.BETWEEN
       (172.16.0.0,172.31.255.255) || CLIENT.IP.DST.BETWEEN
       (192.168.0.0, 192.168.255.255) || CLIENT.IP.DST.BETWEEN
       (13.14.0.0, 13.14.255.255)||CLIENT.IP.DST.EQ(1.2.5.4))"
2  <!--NeedCopy-->
```

- Para agregar una subred o dirección IP mediante la GUI:

1. Vaya a **Appexpert > Expresiones**.
2. Agregue la expresión **aauth_allow_rfc1918_subnets**.

Si se establece el túnel pero la autenticación sigue fallando, siga estos pasos para solucionar el problema.

LDAP:

- Valide los detalles de Bind DN.
- Utilice la prueba de conectividad para confirmar el error.
- Valide los errores mediante la depuración `aaad`.
- Inicie sesión en la instancia de Autenticación adaptable mediante la CLI.

```
shell
cd /tmp
cat aaad.debug
<!--NeedCopy-->
```

Errores LDAP comunes:

- Tiempo de espera del servidor: no hay respuesta del conector para la consulta LDAP.
- Otros errores de LDAP, consulte https://support.citrix.com/article/CTX138663.

Radio:

- La dirección IP del conector debe agregarse como la dirección IP de origen del cliente RADIUS en la configuración del servidor RADIUS.

Problemas de autenticación

- **Errores de afirmación de publicaciones para OAuth**
  - Asegúrese de que AD proporcione todos los reclamos. Necesitas 7 reclamos para que esto tenga éxito.
  - Valide los registros en /var/log/ns.log para localizar el error de los errores de OAuth.

```
cat /var/log/ns.log
<!--NeedCopy-->
```

  - Valide los parámetros del perfil de OAuth.

- **Autenticación de Azure AD bloqueada después de la afirmación**

  Agregue la autenticación de AD como el siguiente factor con la autenticación desactivada. Esto es para obtener todos los reclamos necesarios para una autenticación correcta.

Asuntos relacionados con la EPA

- **El complemento ya está presente, pero el usuario recibe una solicitud para descargarlo.**

  Posibles causas: No coinciden las versiones o archivos corruptos

  - Ejecute las herramientas para desarrolladores y compruebe si el archivo de lista de complementos contiene la misma versión que la de NetScaler y la máquina cliente.
  - Asegúrese de que la versión del cliente en el NetScaler sea la misma que en la máquina cliente.

    Actualice el cliente en NetScaler.

    En la instancia de Autenticación adaptable, vaya a **Citrix Gateway > Configuración global > Actualizar bibliotecas cliente**.

    La página de bibliotecas de complementos de la EPA en Descargas de Citrix le proporciona información detallada.
  - En ocasiones, la solicitud se puede almacenar en caché en NetScaler incluso si se actualiza la versión.

    `show cache object` muestra los detalles del complemento en caché. Puede eliminarlo mediante el comando;

    ```
    flush cache object -locator 0x00000023345600000007
    ```

  Para obtener detalles sobre la recopilación de registros de la EPA, consulte https://support.citrix.com/article/CTX209148.

- **¿Hay alguna manera de revertir la configuración de EPA (Siempre, Sí, No) después de que el usuario haya seleccionado una opción?**

  Actualmente, la reversión de la configuración de la EPA se realiza manualmente.

  - En el equipo cliente, vaya a C:\Users<user_name>\AppData\Local\Citrix\AGEE.
  - Abra el archivo `config.js` y establezca trustAlways en null - `"trustAlways":null`

Problemas con las etiquetas de acceso inteligente

- **Después de configurar el acceso inteligente, las aplicaciones no están disponibles**

  Asegúrese de que las etiquetas estén definidas tanto en la instancia de autenticación adaptable como en los grupos de entrega de Citrix VDA.

  Compruebe que las etiquetas se agreguen en el grupo de entrega de Workspace en todas las mayúsculas.

Puede recopilar el archivo ns.log y ponerse en contacto con el Soporte de Citrix si esto no funciona.

Recopilación de registros general para la instancia de autenticación adaptable

- Paquete de soporte técnico: para obtener más información, consulte Cómo recopilar el paquete de soporte técnico de los dispositivos SDX y VPX para el análisis de información.
- Archivos de rastreo. Para obtener más información, consulte Cómo grabar un seguimiento de paquetes en NetScaler.

Póngase en contacto con el Soporte de Citrix para

Acceso inteligente mediante autenticación adaptable

June 19, 2024

Los clientes de Citrix Cloud pueden proporcionar acceso inteligente (acceso adaptable) a los recursos de Citrix DaaS (aplicaciones y escritorios virtuales) o al servicio Secure Private Access mediante la autenticación adaptativa como IdP para Citrix Workspace.

La función Smart Access permite que el servicio de autenticación adaptable muestre toda la información de directiva sobre el usuario a Citrix Workspace o Citrix DaaS. El servicio de autenticación adaptativa puede proporcionar la posición del dispositivo (EPA), la ubicación de la red (dentro o fuera de la red corporativa, geolocalización), los atributos de usuario, como los grupos de usuarios, la hora del día o una combinación de estos parámetros como parte de la información de la directiva. A continuación, el administrador de Citrix DaaS puede usar esta información de directiva para configurar el acceso contextual a las aplicaciones y escritorios virtuales. Las aplicaciones y escritorios virtuales se pueden enumerar o no en función de los parámetros anteriores (directiva de acceso). También se pueden controlar algunas acciones del usuario, como el acceso al portapapeles, la redirección de la impresora, la unidad cliente o la asignación de USB.

Ejemplo de casos de uso:

- El administrador puede configurar el grupo de aplicaciones para que solo se muestre o se acceda a él desde ubicaciones de red específicas, como la red corporativa.
- El administrador puede configurar el grupo de aplicaciones para que solo se muestre o se acceda a él desde dispositivos administrados por la empresa. Por ejemplo, los análisis de EPA pueden verificar si el dispositivo es administrado por la empresa o BYOD. Según el resultado del análisis de EPA, se pueden enumerar las aplicaciones relevantes para el usuario.

Requisitos previos

- La autenticación adaptable como proveedor de identidad debe estar configurada para Citrix Workspace. Para obtener más información, consulte Servicio de autenticación adaptable.
- El servicio de autenticación adaptable con Citrix DaaS está en funcionamiento.
- La función Adaptive Access está habilitada. Para obtener más información, consulte Habilitar el acceso adaptable.

Comprender el flujo de eventos para un acceso inteligente

1. El usuario inicia sesión en Citrix Workspace.
2. Se redirige al usuario al servicio de autenticación adaptativa configurado como IdP.
3. Se solicita al usuario la autenticación previa (EPA) o la autenticación.
4. El usuario se ha autenticado correctamente.
5. Las directivas de acceso inteligente se evalúan de acuerdo con la configuración y las etiquetas están asociadas a la sesión del usuario.
6. El servicio de autenticación adaptativa envía las etiquetas al servicio Citrix Graph. Se redirige al usuario a la página de inicio de Citrix Workspace.
7. Citrix Workspace obtiene la información de la directiva de esta sesión de usuario, coincide con el filtro y evalúa las aplicaciones o escritorios que se deben enumerar.
8. El administrador configura la directiva de acceso en Citrix DaaS para restringir el acceso ICA a los usuarios.

Configuración de directivas de acceso inteligente en instancias de autenticación adaptativa

La configuración de directivas de acceso inteligente en una instancia de autenticación adaptativa es un proceso de dos pasos:

1. Defina directivas de acceso inteligentes con etiquetas de acceso inteligentes en instancias de autenticación adaptativa. Por ejemplo, consulte el *paso 1*.
2. Defina las mismas etiquetas en su DaaS/Secure Private Access para el acceso a los recursos. Por ejemplo, consulte el *paso 2*.

Caso de uso 1: configurar una directiva de acceso inteligente para permitir el acceso a los usuarios que inician sesión desde el explorador Chrome y bloquearles el acceso al portapapeles

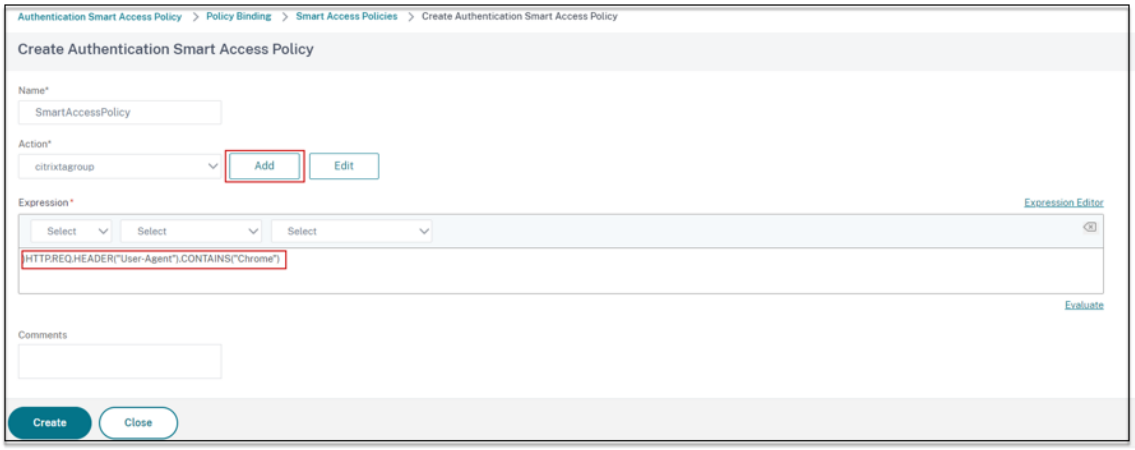
Paso 1: Configurar directivas de acceso inteligentes con etiquetas inteligentes en la instancia de autenticación adaptativa

1. Inicie sesión en la instancia de Autenticación adaptable.
2. Navegue hasta el servidor virtual de autenticación adaptativa (**Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**).
3. Seleccione el servidor virtual de autenticación y después haga clic en **Editar**.
4. Haga clic en **Directivas de acceso inteligentes**.
5. Defina la expresión de la directiva según sus necesidades.

    a) Haga clic en **Add Binding**.
    b) En **Seleccionar directiva**, haga clic en **Agregar**.
    c) Introduzca un nombre para la directiva de acceso inteligente.
    d) Defina la expresión.

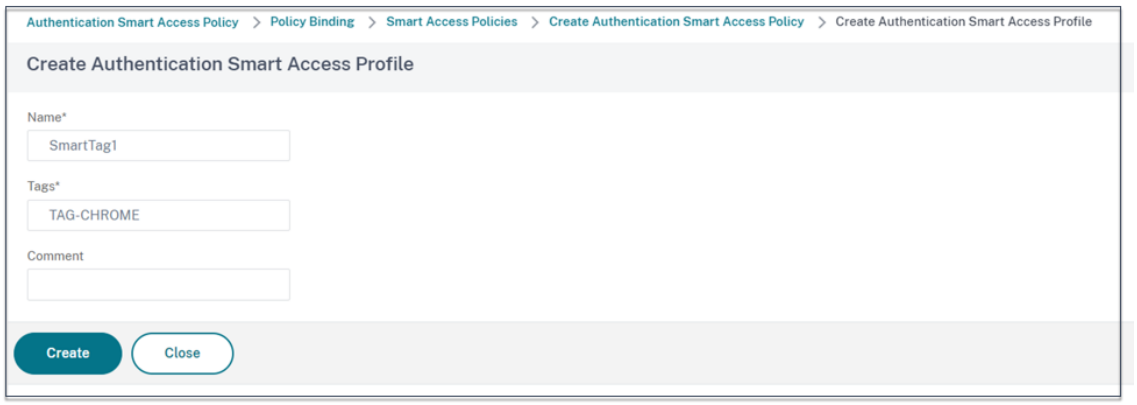
    Para ver el ejemplo de cómo permitir el acceso a los usuarios que inician sesión desde un explorador Chrome, introduzca la expresión `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")`

    Del mismo modo, puede crear expresiones basadas en la hora, el inicio de sesión del usuario, el grupo de autenticación y autorización y otras opciones.

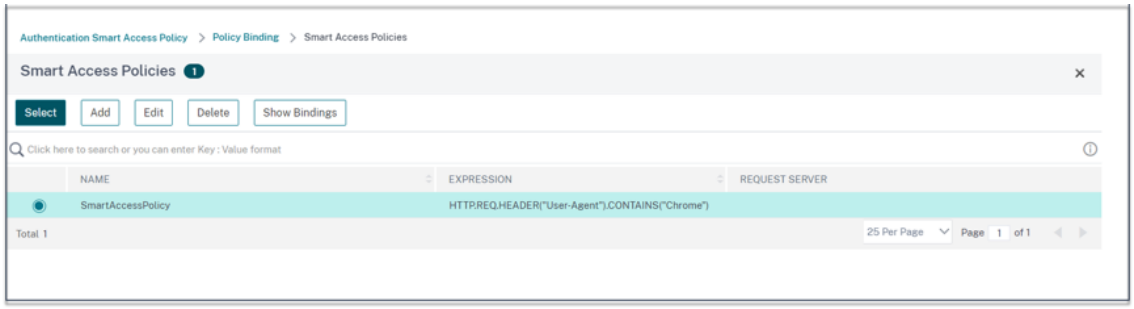


6. Ahora, cree etiquetas inteligentes y vincule estas etiquetas a la directiva de acceso inteligente.

    a) En **Acción**, haga clic en **Agregar**.
    b) En **Nombre**, escriba un nombre para el perfil de acceso inteligente.
    c) En **Etiquetas**, defina las etiquetas de acceso inteligente. Por ejemplo, TAG-CHROME.



a) Haga clic en **Crear**.
b) Seleccione la directiva de acceso inteligente y haga clic en **Agregar vinculación**.
c) Enlace esta etiqueta de acceso inteligente a la directiva de acceso inteligente creada anteriormente.



> **Nota:**
>
> También puede crear una directiva de acceso inteligente desde **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Acceso inteligente > Directivas** y después vincularla al servidor virtual de autenticación.

Paso 2: Definir etiquetas de acceso inteligentes en DaaS Studio

1. Agregue las directivas con la etiqueta inteligente “TAG-CHROME”. Para obtener más información, consulte Definir etiquetas en Citrix Studio.

Caso de uso 2: configurar directivas de acceso inteligentes basadas en los resultados de EPA, para la autenticación posterior

Paso 1: Configurar directivas de acceso inteligentes con etiquetas inteligentes en la instancia de autenticación adaptativa Para un acceso inteligente basado en condiciones como el análisis de puntos finales, configure nFactor flow, defina una acción EPA y después agregue el grupo predeterminado.

Para configurar el EPA como un factor en el flujo de nFactor, consulte Configurar el EPA como un factor.

Flujo lógico

1. El usuario accede a la URL del espacio de trabajo.
2. Se redirige al usuario a la autenticación adaptativa para la autenticación/EPA.
3. El análisis del punto final se realiza en el usuario final y los resultados se almacenan agregando al usuario al grupo predeterminado definido.
4. Se solicita al usuario el siguiente flujo de autenticación.
5. Se evalúan las directivas de acceso inteligente y se asignan al usuario las etiquetas de acceso inteligente.

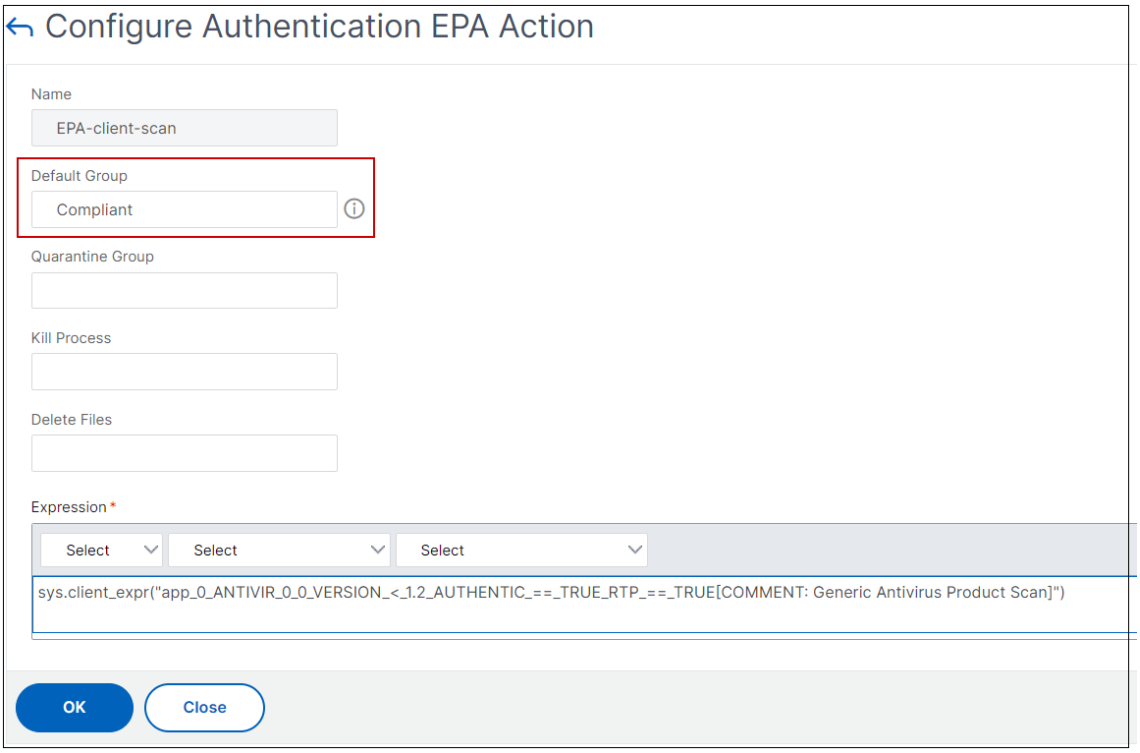
Configuración

Los usuarios que accedan desde un equipo con un antivirus instalado deben marcarse como compatibles y tener acceso completo. Sin embargo, los equipos de usuario sin antivirus deben marcarse como no conformes y tener acceso limitado.

1. Cree una directiva de nFactor para EPA. Para obtener más información, consulte Configurar EPA como factor.

   En el flujo nFactor, asegúrese de que el primero sea un factor de autenticación de usuario.

2. Seleccione la expresión EPA para comprobar si el antivirus está presente o no.
3. En la acción de EPA, defina el grupo predeterminado.



El usuario se agrega a este grupo predeterminado si EPA se ejecuta correctamente.

4. Ahora, cree directivas de acceso inteligentes

   a) Inicie sesión en la instancia de Autenticación adaptable.

   b) Navegue hasta el servidor virtual de autenticación adaptativa (**Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales**).

   c) Seleccione el servidor virtual de autenticación adaptativa y haga clic en **Editar**.

   d) Haga clic en **Directivas de acceso inteligentes**.

   e) Cree dos directivas de acceso inteligentes con las siguientes expresiones.

      - AAA.USER.IS_MEMBER_OF (“Conforme”): Para el usuario, condición de pase de EPA
      - !AAA.USER.IS_MEMBER_OF (“Conforme”): Para el usuario, condición de error de EPA

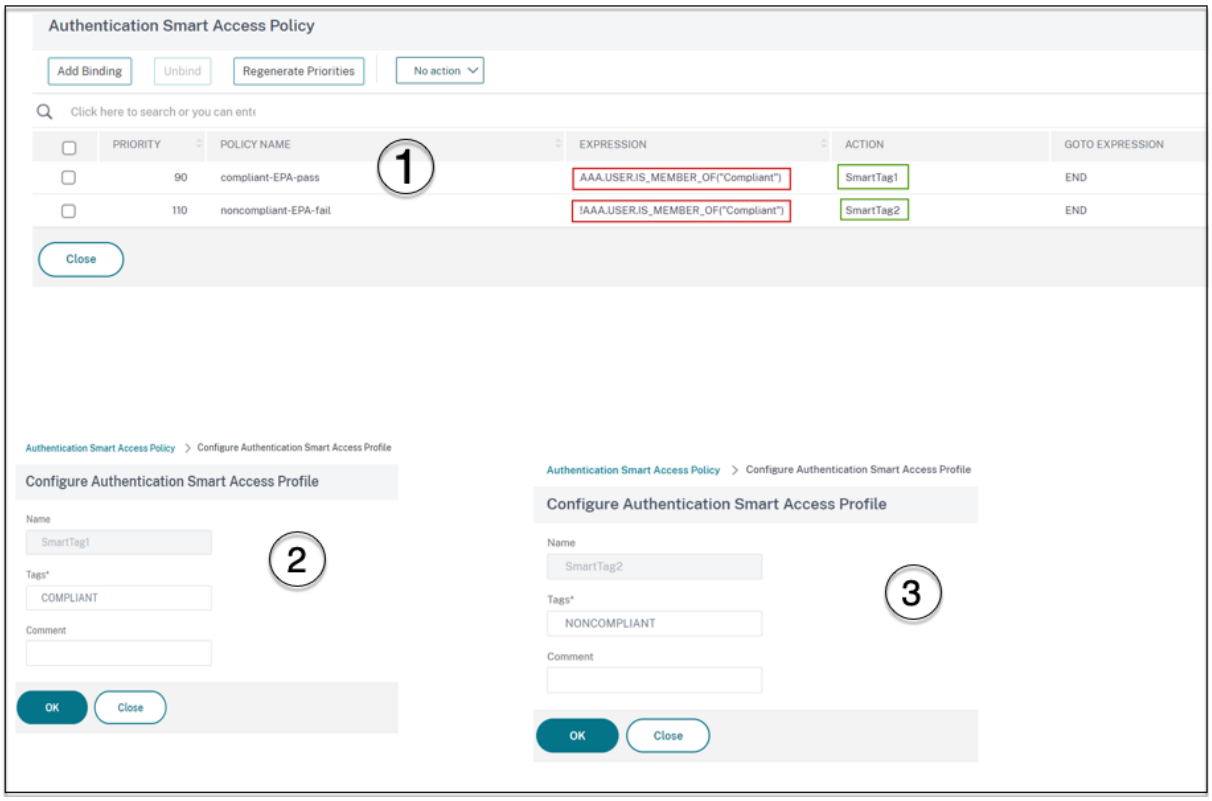
   f) Defina etiquetas de acceso inteligentes para ambas directivas.

      Ejemplo:

      - Nombre de la etiqueta `SmartTag1` con la etiqueta COMPLIANT para `AAA.USER.IS_MEMBER_OF (“Compliant”)`
      - Nombre de la etiqueta `SmartTag2` con la etiqueta NONCOMPLIANT para `!AAA.USER.IS_MEMBER_OF (“Compliant”)`

La configuración de la instancia de autenticación adaptativa con condiciones como EPA para el acceso inteligente ya está completa.

Puede configurar las etiquetas y la expresión según sus necesidades.



Paso 2: Configurar las etiquetas de acceso inteligentes en DaaS Studio Agregue las directivas con las etiquetas inteligentes “COMPLIANT”y “NONCOMPLIANT”en los grupos de entrega respectivos. Para obtener más información, consulte Definir etiquetas en Citrix Studio.

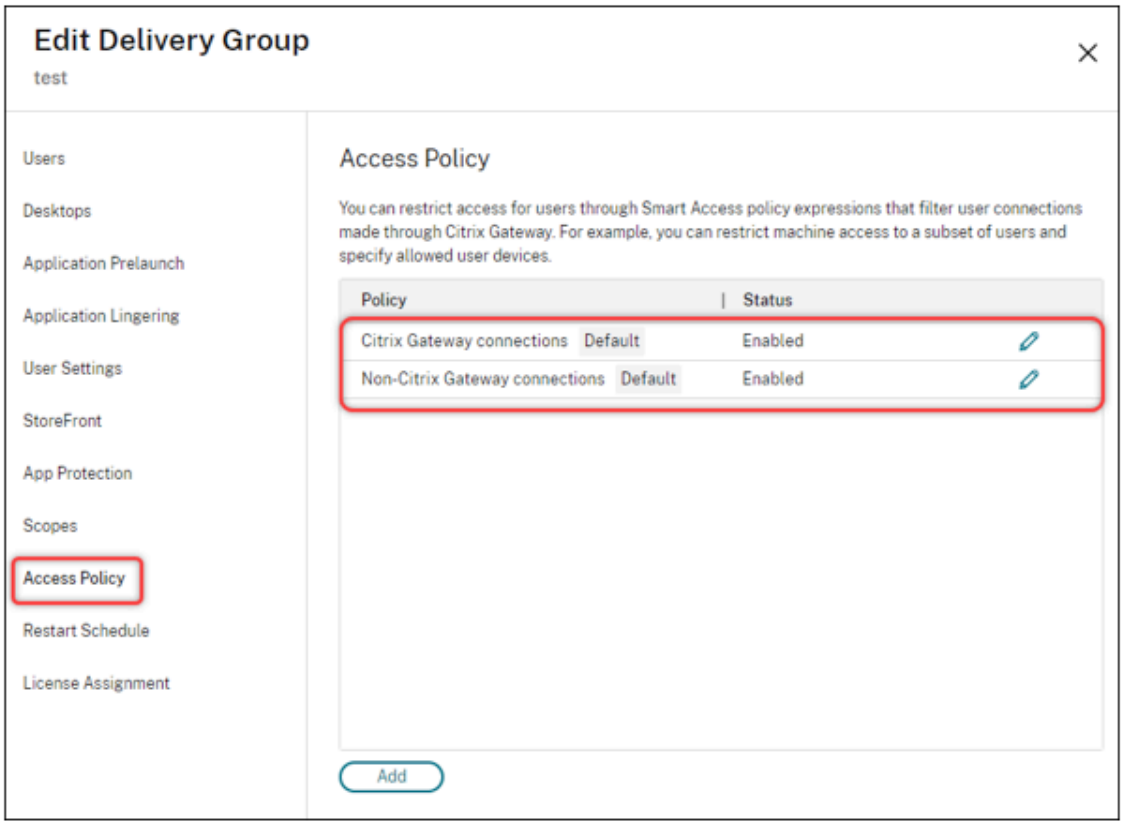
Definir etiquetas en DaaS studio

Defina etiquetas en los grupos de entrega para restringir la enumeración de aplicaciones para los usuarios.

Ejemplo: los usuarios de BranchOffice deben ver las aplicaciones del **grupo de entrega de Adaptive Access**, que contiene todas las aplicaciones.
Mientras que los usuarios de WorkFromHome deben ver las aplicaciones de **WFH**Delivery Group.

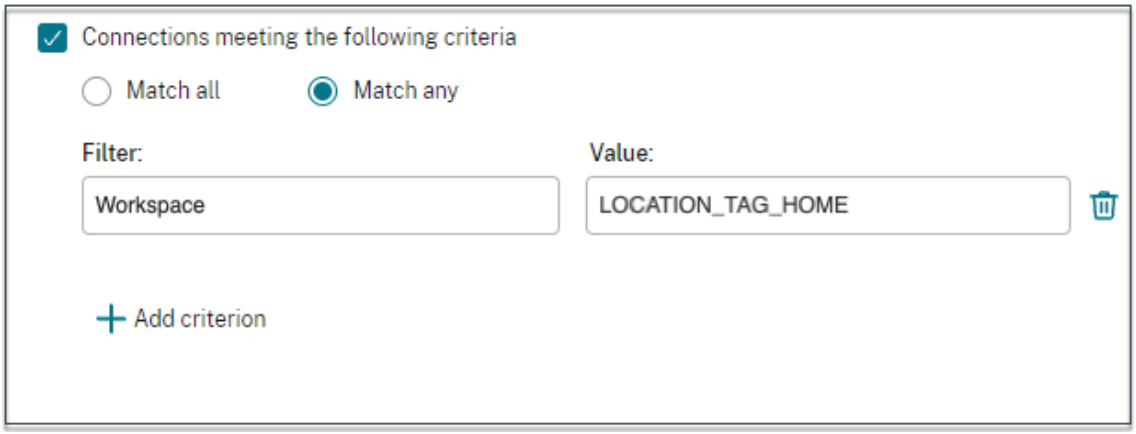
1. Inicie sesión en Citrix Cloud.
2. Seleccione **Mis servicios > DaaS**.
3. Haga clic en **Administrar**.
4. Cree los grupos de entrega necesarios. Para obtener información detallada, consulte Crear grupos de entrega.

5. Seleccione el grupo de entrega que ha creado y haga clic en **Modificar grupo de entrega**.



6. Haga clic en **Directiva de acceso**.
7. Para los clientes que usan el acceso adaptable en la plataforma de Citrix Workspace, siga estos pasos para restringir el acceso de un grupo de entrega a las redes internas solamente:

   a) Haga clic con el botón derecho en el grupo de entrega y seleccione **Modificar**.
   b) Seleccione la directiva de acceso en el panel de la izquierda.
   c) Haga clic en el icono de edición para modificar la directiva de conexiones predeterminada de Citrix Gateway.
   d) En la página Editar directiva, seleccione **Conexiones que cumplan los siguientes criterios**, seleccione Coincidir con **cualquiera** y después añada los criterios.



Para los usuarios de WorkFromHome, introduzca los siguientes valores en el Delivery Controller correspondiente.

Comunidad: Workspace

Filtro: LOCATION_TAG_HOME

Para los usuarios de BranchOffice, introduzca los siguientes valores en el Delivery Controller correspondiente.

Filtro: Workspace

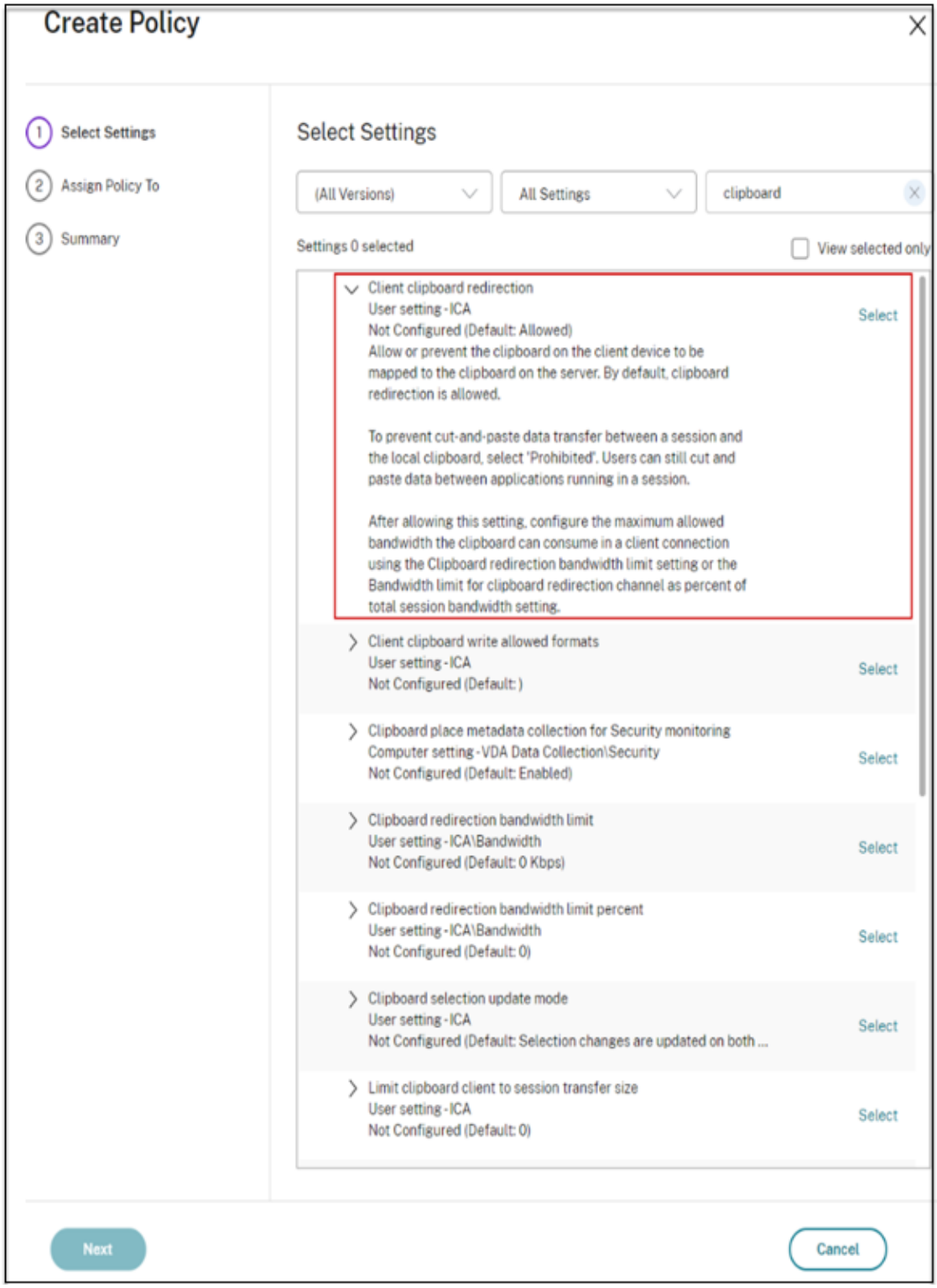
Valor: LOCATION_TAG_BRANCHOFFICE

Ahora puede usar estas etiquetas para restringir el acceso a sus aplicaciones.

Restringir el tipo de acceso para las aplicaciones proporcionadas

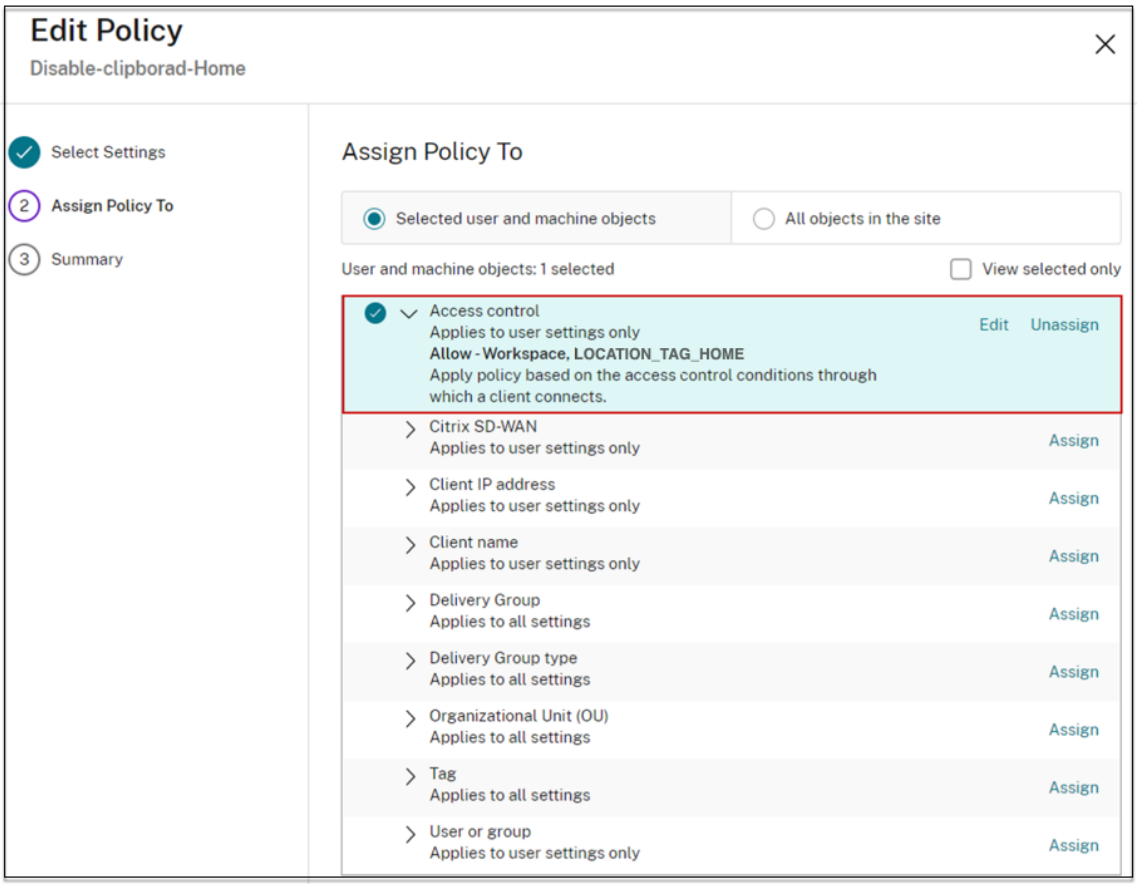
Ejemplo: los usuarios que trabajan desde casa no deben tener derechos de portapapeles.

1. En DaaS Studio, vaya a **Directivas** y haga clic en **Crear**directiva.
2. En la página **Crear directiva**, seleccione la configuración para la que desea permitir o prohibir el acceso.
3. haga clic en **Seleccionar**.



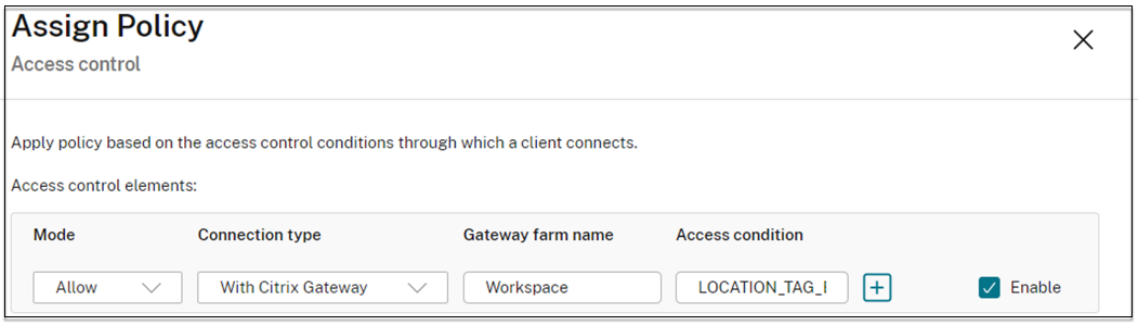
4. En la página **Editar configuración**, haga clic en **Permitido** o **Prohibido** y después haga clic en **Guardar.**
5. Haga clic en **Siguiente**.

6. En la página **Asignar directiva a**, seleccione **Control de acceso** y después haga clic en **Siguiente**.

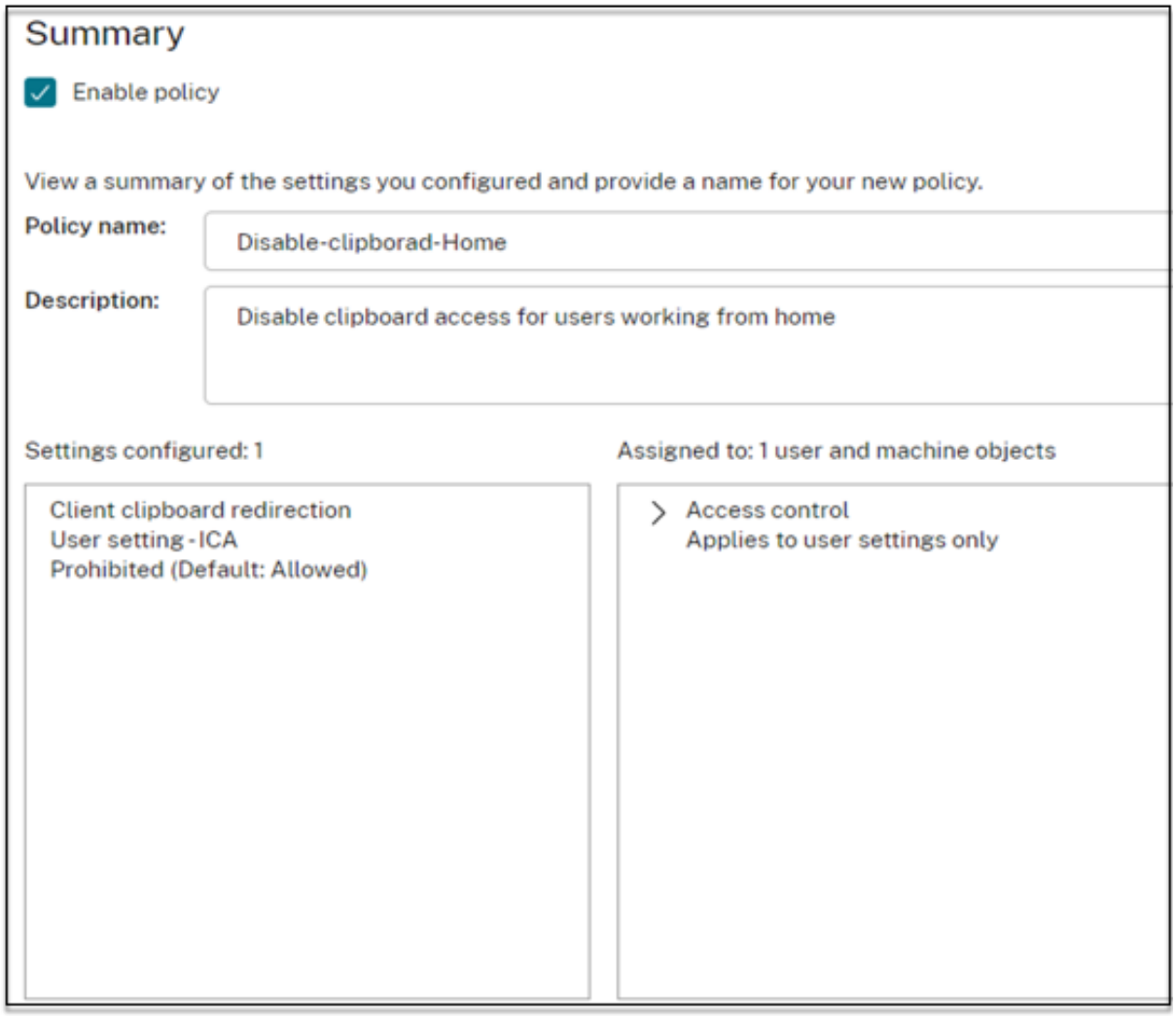


7. Defina una directiva con los siguientes detalles:

   - **Modo**: - Permitir
   - **Tipo de conexión**: - Con Citrix Gateway
   - **Nombre de la comunidad**: - Workspace
   - **Estado de acceso**: LOCATION_TAG_HOME (todo en mayúsculas)



8. Haga clic en **Siguiente** e introduzca un nombre para la directiva.
9. Haga clic en **Finalizar**.



Ya puede probar su acceso.

Solución de errores comunes

- **Problema:** aparece el mensaje "No se puede completar la solicitud".

  La resolución

  1. Asegúrese de que el acceso adaptable esté habilitado. Para obtener más información, consulte Habilitar el acceso adaptable.
  2. Si la función no está habilitada, contacte con Citrix Support.

- **Problema:** no se publican aplicaciones ni escritorios.

  Este problema puede producirse si las etiquetas inteligentes no se envían desde la autenticación adaptativa al espacio de trabajo o si no se reciben en DaaS o Secure Private Access.

  Solución:

- Compruebe si las directivas de acceso inteligente se están viendo afectadas. Para obtener información detallada, consulte https://support.citrix.com/article/CTX138840.
- Compruebe si la instancia de Citrix Adaptive Authentication puede conectarse a `cas.citrix.com`.
- Consulte la instancia de autenticación adaptativa para obtener más información sobre las etiquetas inteligentes.
  * Asegúrese de que, en el comando `set audit syslogParams`, el parámetro LogLevel esté establecido en `ALL` en todas las instancias.
  * Inicie sesión en la instancia principal de Adaptive Authentication mediante putty.

    Escriba shell

    ```
    cd /var/log
    cat ns.log | more or cat ns.log | grep -I “smartaccess”
    ```
- Si estos pasos no resuelven el problema, contacte con Citrix Support.

Cambios de configuración para una configuración de alta disponibilidad

En algún momento, puede producirse un retraso en la sincronización de archivos en una configuración de alta disponibilidad en los siguientes directorios. Como resultado, las claves creadas durante el registro de Citrix ADM no se leen a tiempo.

- /var/mastools/conf/agent.conf
- /var/mastools/trust/.ssh/private.pem
- /var/mastools/trust/.ssh/public.pem

Para solucionar el problema de sincronización de archivos, lleve a cabo los pasos siguientes para volver a ejecutar el comando `set cloud` en el secundario.

```
1  > shell cat /var/mastools/conf/agent.conf
2  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3  <mps_agent>
4  <uuid>temp_str</uuid>
5  <url>fuji.agent.adm.cloud.com</url>
6  <customerid>customer_id</customerid>
7  <instanceid>instance_id</instanceid>
8  <servicename>MAS</servicename>
9  <download_service_url>download.citrixnetworkapistaging.net</
       download_service_url>
10 <abdp_url>fuji.agent.adm.cloud.com</abdp_url>
11 <msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>
12 </mps_agent> Done
13 > set cloud param -CustomerID customer_id -InstanceID instance_id -
       Deployment Production
```



```
<!--NeedCopy-->
```

Pautas de tamaño y rendimiento

June 19, 2024

La autenticación adaptativa brinda a los clientes acceso a sus servidores de autenticación locales mediante Cloud Connectors implementados en sus centros de datos o Azure VNet Peering en caso de que la accesibilidad al centro de datos ya esté establecida desde la VNet administrada por el cliente. Este tema contiene información sobre las cifras de rendimiento de las implementaciones de Citrix Cloud Connector y Azure VNet Peering, así como las configuraciones de escala y tamaño recomendadas para las máquinas de Citrix Cloud Connector.

Tasa de autenticación de usuarios

Una máquina virtual con conector de 2 vCPU y 7 GB de RAM puede autenticar 14 usuarios por segundo.

De forma predeterminada, el servicio de conectores está configurado para reiniciarse automáticamente dos veces si se produce un error o un bloqueo. En caso de fallo o caída posterior, el servicio se detiene. Además, actualmente, el servicio del conector falla si la velocidad de autenticación aumenta más allá de 4 autenticaciones por segundo. Esta velocidad se puede lograr configurando el servicio de conectores para que se reinicie después de cualquier número de errores (**Citrix Netscaler Cloud Gateway > Recuperación > Reiniciar el servicio**). Si esta configuración no está configurada, la velocidad se reduce a 4 autenticaciones por segundo.

Latencia del tráfico y tasa de autenticación de usuarios al usar Citrix Cloud Connectors

En la siguiente tabla se muestran la latencia del tráfico y la tasa de autenticación de usuarios cuando se utilizan Citrix Cloud Connectors:

Tipo de autenticación	Latencia de autenticación (p95) en ms	Tasa de autenticación o inicio de sesión de usuario por segundo
LDAP	5.99	14
RADIUS	3.17	14
LDAP+RADIUS	4.59	14

Tipo de autenticación	Latencia de autenticación (p95) en ms	Tasa de autenticación o inicio de sesión de usuario por segundo
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

Latencia del tráfico y tasa de autenticación de usuarios al usar Azure vNet Peering

En la siguiente tabla se muestran la latencia del tráfico y la tasa de autenticación de usuarios cuando se usa el peering de redes virtuales de Azure:

Tipo de autenticación	Latencia de solicitud (p95) en ms	Tasa de autenticación o inicio de sesión de usuario por segundo
LDAP	6.95	17.54
LDAPS	7.19	16.98

Reglamentación de datos

June 19, 2024

Este tema proporciona información sobre la recopilación, el almacenamiento y la retención de registros por parte del servicio Citrix Adaptive Authentication y las instancias de Adaptive Authentication. Todos los términos en mayúscula no definidos en Definiciones tienen el significado especificado en el Acuerdo de servicios para el usuario final de Citrix.

- Servicios de autenticación adaptable: servicio de Citrix Cloud en el que los administradores pueden iniciar sesión para implementar y administrar instancias de autenticación adaptable.
- Instancias de autenticación adaptable: máquinas virtuales NetScaler implementadas por el servicio de autenticación adaptable para permitir a los administradores administrar la autenticación de usuarios.

Residencia de datos

Servicios de autenticación adaptable

Los datos de contenido del cliente del servicio Citrix Adaptive Authentication residen en la región Este de Azure Cloud Services. Se replican en las siguientes regiones de Azure para obtener disponibilidad y redundancia:

- Oeste de EE. UU.
- Norte de Europa

Los siguientes son los diferentes destinos para los registros de configuración y tiempo de ejecución del servicio.

- Servicio Splunk para la monitorización del sistema y los registros de depuración, solo en las ubicaciones de EE. UU. y la UE (Unión Europea).
- Servicio NetScaler Application Delivery Management para los registros de acceso de usuarios agregados. Para obtener más información, consulte NetScaler ADM Data Governance.
- Servicio de registros del sistema de Citrix Cloud para registros de auditoría de administradores. Para obtener más información, consulte Consideraciones geográficas y manejo de registros y contenido del cliente de Citrix Cloud Services.

Instancias de autenticación adaptable

Servicio NetScaler Application Delivery Management para realizar copias de seguridad de todas las configuraciones, artefactos específicos de la instancia. Para obtener más información, consulte NetScaler ADM Data Governance.

Recopilación de datos

El servicio Citrix Adaptive Authentication permite a los administradores del cliente configurar el servicio a través de la interfaz de usuario de autenticación adaptable y los Connector Appliances complementarios a través de Se recopila el siguiente contenido del cliente:

- Servicio de autenticación adaptable
  - FQDN (nombre de dominio completo) y dirección IP del punto final de IdP (proveedor de identidad).
  - Direcciones/rangos IP, puertos y protocolos
  - Certificados utilizados para acceder al servidor virtual de autenticación de IdP
  - Dirección IP pública del punto final de administración

  - Para la interconexión de Azure VNet, entidad de servicio con función de colaborador de red. Para obtener más información, consulte Configurar la conectividad a los servidores de autenticación locales mediante la interconexión de Azure VNet.

- Identificadores de usuario para los derechos de aplicaciones
- Detalles relacionados con Citrix Cloud Connector. Para obtener más información, consulte Citrix Cloud Connector.

  - Direcciones IP o nombres de dominio completo (FQDN)
  - Identificadores de ubicación de usuarios, dispositivos y recursos
  - Configuración de proxy interno

Para los registros de tiempo de ejecución recopilados por los componentes del servicio, la información clave consiste en lo siguiente:

- Puerto y dirección IP del cliente
- FQDN/dirección y puerto de destino
- Agente de usuario de cliente
- Ruta URL de la aplicación
- Tiempo y duración del acceso a las aplicaciones
- Solicitar recuento de bytes
- recuento de bytes de respuesta
- ID de transacción HTTP
- Modo de implementación (emparejamiento de Connector o Azure VNet)
- Recursos de Azure

  - Nombres de grupos de recursos
  - VNet (direcciones IP, CIDR)
  - Subredes (direcciones IP, CIDR)
  - Nombres de máquinas virtuales

Transmisión de datos

El servicio Citrix Adaptive Authentication envía registros a los destinos (Splunk) protegidos por la seguridad de la capa de transporte.

Control de datos

El servicio Citrix Adaptive Authentication actualmente no ofrece opciones para que los clientes desactiven el envío de registros o impidan que el contenido del cliente se replique globalmente.

Retención de datos

Según la directiva de retención de datos de Citrix Cloud, los datos de configuración del cliente se purgan del servicio 90 días (aproximadamente 3 meses) después de que caduque la suscripción.

Los destinos de registro mantienen su directiva de retención de datos específica del servicio.

- Para los eventos almacenados en Citrix Application Delivery Management. Consulte Gobernanza de datos de Citrix ADM.
- Los registros de Splunk se archivan y, finalmente, se eliminan después de 90 días (aproximadamente 3 meses).
- Las instancias de Autenticación adaptable se desasignan 30 días (aproximadamente cuatro semanas y media) después del vencimiento de la suscripción.

Exportación de datos

Hay diferentes opciones de exportación de datos para varios tipos de registros.

- Se puede acceder a los registros de auditoría del administrador desde la consola Registro del sistema de Citrix Cloud.
- Los registros de Splunk no son para que los clientes los consuman. Estos eventos también se pueden exportar desde Splunk como un archivo CSV.

Definiciones

- Contenido del cliente se refiere a cualquier dato cargado en una cuenta de cliente para su almacenamiento o datos en un entorno de cliente al que Citrix tenga acceso para prestar los servicios.
- Registro significa un registro de eventos relacionados con los servicios, incluidos los registros que miden el rendimiento, la estabilidad, el uso, la seguridad y el soporte.
- Los servicios significan los servicios de Citrix Cloud descritos anteriormente con el fin de facilitar los casos de uso de los clientes.