Налаштування автентифікації на основі SAML в Azure AD

Цей документ пояснює, як увімкнути **SAML-аутифікацію через Azure Active Directory (Azure AD)** у VMware vCloud Director для **єдиного входу (SSO)** користувачів Azure AD до вашого vCloud-тенанта. В данній статті розглянемо налаштування тестової організації **TestOrg** в Cloud Director.

□□ Попередні вимоги

Перед початком переконайтесь, що у вас є:

- Адміністративний доступ до **vCloud Director Tenant**.
- Адміністративний доступ до **Azure Active Directory Tenant**.

□□ Кроки налаштування

1) Отримання метаданих із vCloud Director

1. Увійдіть у свій **vCloud Director Tenant** (URL схожий на https://eurocloud.datagroup.ua/tenant/testorg).
2. Перейдіть у меню **Administration → Identity Providers → SAML**.
3. На сторінці конфігурації **SAML** натисніть посилання поруч із “Metadata” — це завантажить XML-файл метаданих, який потрібен для налаштування в Azure AD.

2) Конфігурація у Azure AD

1. Перейдіть на портал **https://portal.azure.com** і ввійдіть як адміністратор Azure.
2. У меню зліва оберіть **Microsoft Entra ID** (раніше Azure AD).
3. У розділі **Manage → Enterprise Applications** натисніть **New Application**.
4. Виберіть **Create your own application**, введіть назву (наприклад, *vCloud Director*) і підтвердьте.
5. У налаштуваннях додайте користувачів або групи, яким дозволено входити (через **Assign Users and Groups**).
6. Перейдіть до **2. Setup single sign on** і виберіть **SAML** як метод аутентифікації.
7. Завантажте раніше збережений XML-файл метаданих vCloud Director.
8. У полі **Sign On URL** введіть URL вашого тенанта (наприклад, https://eurocloud.datagroup.ua/tenant/testorg) і збережіть зміни.

3) Налаштування атрибутів та тверджень

Після базового налаштування SAML:

1. Перейдіть до розділу **Attributes & Claims** і натисніть **Edit**.
2. Додайте новий твердження (claim):

   - **Roles** — джерело: user.assignedroles
   - **UserName** — джерело: user.mail

3. Додайте груповий твердження **Groups**:

   - Оберіть **All groups**, джерело — **Group ID**
   - Увімкніть **Customize the name of the group claim** та введіть ім’я Groups.

4. Збережіть зміни.

4) Завантаження метаданих Azure AD у vCloud Director

1. Увійдіть назад у **vCloud Director SAML Configuration**.
2. Відкрийте **Edit**, перейдіть на вкладку **Identity Provider**.
3. Активуйте перемикач для ввімкнення **SAML Identity Provider**.
4. Завантажте **Federation Metadata XML** файл, який ви завантажили з Azure AD (розділ **SAML Signing Certificate → Federation Metadata XML**).
5. Натисніть **SAVE** для збереження конфігурації.

5) Імпорт користувачів та груп у vCloud Director

Після успішного налаштування SAML:

1. У меню vCloud Director перейдіть у **Users** або **Groups**.
2. Натисніть **Import Users** або **Import Groups**.
3. Введіть електронні адреси користувачів так, як вони визначені в Azure AD. Для груп — використовуйте **Group ID**, а не назву чи email.
4. Оберіть рівень доступу (ролі) для кожного — і збережіть.

6) Тестування

Відкрийте приватне/інкогніто вікно браузера та перейдіть до URL vCloud Director. При спробі входу оберіть SSO через Azure — ви повинні бути переадресовані на портал **Azure AD** для автентифікації.

□□ Важливі поради

- Імена атрибутів чутливі до регістру (case-sensitive).

- Переконайтеся, що у Azure AD додані саме ті користувачі/групи, які вам потрібні для доступу.
- Після внесення змін до SAML конфігурації може знадобитися кілька хвилин на поширення змін.

Версія #2
az створив 2026-01-29 08:08:06 UTC
az оновив 2026-01-30 08:58:58 UTC