Advanced Guide: LDAP Authentication on Ruckus vSZ via Azure AD Domain Services (Azure AD DS)

Since **Ruckus Virtual SmartZone (vSZ) does not support SAML authentication** for admin logins, you must use **Azure AD Domain Services (Azure AD DS)** to provide an LDAP interface that vSZ can authenticate against.

Below is a more detailed breakdown, including user group mappings and troubleshooting.

---

1. Configure Azure AD Domain Services (Azure AD DS) for LDAP

Step 1: Enable Azure AD DS

1. **Log in to Azure Portal**.
2. **Go to "Azure AD Domain Services" (AAD DS)** and create a **managed domain**:
   - Set the **DNS domain name** (e.g., `corp.yourcompany.local`).
   - Choose a **resource group** and **region**.
   - Select an **Azure Virtual Network (VNet)** (Ensure vSZ can reach this network).
3. **Synchronize Users from Azure AD to Azure AD DS**:
   - Azure AD DS automatically synchronizes users and groups from Azure AD.
   - Users must have **Kerberos and NTLM authentication enabled** (this is automatic for synced users).

Step 2: Enable Secure LDAP (LDAPS)

1. **Enable Secure LDAP** under **Azure AD DS > Properties**.
2. **Download and install the SSL certificate** for LDAPS.
3. **Allow LDAP over SSL (TCP 636)** through your **Network Security Group (NSG)**.

Step 3: Verify LDAP Access

1. Run the following command from a machine that can reach Azure AD DS: `ldp.exe`
2. Connect to **`yourdomain.local`** on **port 636**.
3. Bind using an Azure AD DS **admin account**.
4. If successful, LDAP is ready.

---

2. Configure LDAP Authentication on Ruckus vSZ

Step 1: Add an LDAP Server

1. **Log in to vSZ Web UI**.
2. Navigate to **Administration > AAA Servers**.
3. Click **Create** and select **LDAP**.
4. Fill in the LDAP server details:
   - **Server Address**: Enter the **IP Address of Azure AD DS**.
   - **Port**: `636` (for LDAPS).
   - **Bind DN**: A service account in Azure AD DS, e.g.: `cn=admin,ou=Users,dc=yourcompany,dc=local`
   - **Password**: The service account's password.
   - **Base DN**: The starting point for LDAP searches, e.g.: `dc=yourcompany,dc=local`
   - **User Attribute**: `sAMAccountName`
   - **SSL**: **Enable LDAPS**
   - **Certificate**: Upload the LDAPS certificate from Azure AD DS.
5. **Click Test Connection** to verify authentication.

---

3. Configure User Group Mappings

Since Azure AD DS syncs groups from Azure AD, you can **map LDAP groups to Ruckus admin roles**.

Step 1: Find LDAP Group DNs

1. Run **`ldp.exe`** and connect to Azure AD DS.
2. Browse to **OU=Groups** to locate the full **Distinguished Name (DN)** of groups, e.g.: `cn=WiFiAdmins,ou=Groups,dc=yourcompany,dc=local`

Step 2: Assign LDAP Groups in vSZ

1. **Go to "Administration > Users & Roles"**.
2. **Create a new User Group**.
3. **Select "Authentication Type: LDAP"**.
4. **Enter Group DN**, e.g.:
   `cn=WiFiAdmins,ou=Groups,dc=yourcompany,dc=local`
5. Assign appropriate **permissions (e.g., System Admin, Read-Only Admin, etc.)**.
6. **Save and Apply**.

---

4. Troubleshooting LDAP Authentication on vSZ

Issue 1: LDAP Connection Fails

- **Check firewall rules:** Allow **TCP 636** from vSZ to **Azure AD DS**.
- **Verify LDAPS certificate:** Upload it again if necessary.
- **Ensure service account has permissions** to query LDAP.

Issue 2: Users Cannot Log In

- **Confirm correct Base DN:** Run `ldp.exe` to verify the correct structure.
- **Ensure correct user attribute (`sAMAccountName`)** in vSZ settings.
- **Try logging in with UPN (`user@yourdomain.com`)** instead of the username.

Issue 3: Group Mappings Do Not Work

- Use **full group DN** (not just the group name).
- Ensure users are in the **correct group** in Azure AD DS.
- Run `ldapsearch` to manually verify group membership.

Final Thoughts

Using **Azure AD DS with LDAPS** is the best way to integrate Azure authentication with **Ruckus Virtual SmartZone (vSZ)**. With proper **LDAP configuration and group mappings**, you can ensure **secure authentication** and centralized management.

Revision #1
Created 14 March 2025 11:30:50 by Jarryd

Updated 14 March 2025 11:36:29 by Jarryd