Setup non-admin user to query Domain Controller Event Log for Windows 2008 and Windows 2012

Introduction

In a UserFW AD integration solution, the SRX queries the Domain Controller event log to obtain the user-to-IP mapping. The easiest way to accomplish this is to configure the SRX to query the Domain Controller with a user who is part of the Domain Administrator group.

This is restrictive and potentially risky to administrators, so we need to provide a way for the firewall to query the Domain Controller via a user with non-admin privileges.

In our solution, SRX uses Windows Management Instrumentation (WMI) to query the Active Directory Domain Controllers for the Security Event logs. To handle the remote call to DC, we also use Distributed COM (DCOM) technology.

After the user connects to DC, it should have event log reading permission. For a non-admin user, it should have the following permissions to query DC:

- DCOM Permission
- WMI Permission
- Event log reading permission

Instructions

**Step 1:** Create a domain user. It’s better to create a group, and apply the following steps to the group; then all the group members will have appropriate permissions to query the event log.

**Step 2:** Add this user/group to domain Builtin group: ‘Distributed COM Users’, ‘Event Log Readers’, and ‘Server Operators’

In Windows 2008 and Windows 2012, after we add user/group into “Event Log Readers” group, the user and group will have event log reading permission, but in Windows 2003, an additional configuration for event log reading is needed.
Step 3: Give the user/group DCOM remote launch, activation permission, and remote access permission.

**Step 3.1** To grant DCOM Remote Launch and Activation permissions for a user/group:

1. Select **Start**, click **Run**, and then type: `DCOMCNFG`
2. Click **OK**.
3. In the Component Services dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer**. Click **Properties**.
4. In the My Computer Properties dialog box, click the **COM Security** tab.
5. Under Launch and Activation Permissions, click **Edit Limits**.
6. In the Launch Permission dialog box, follow these steps if your name or your group does not appear in the Groups or user names list; otherwise skip to step 7.
   
   A. In the Launch Permission dialog box, click **Add**.
      
   B. In the Select Users, Computers, or Groups dialog box, add your name and the group in the “Enter the object names to select” box, and then click **OK**.

7. In the Launch Permission dialog box, select **your user and group** in the “Group or user names” box. In the Allow column under “Permissions for User”, select **Remote Launch** and **Remote Activation**; and then click **OK**.
**Grant DCOM Remote Launch and Activation**

**Step 3.2 To grant DCOM Remote Access permissions for user/group**

1. Select **Start**, click **Run**, and then type: `DCOMCNFG`
2. Click **OK**.
3. In the Component Services dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer**. Click **Properties**.
4. In the My Computer Properties dialog box, click the **COM Security** tab.
5. Under Access Permissions, click **Edit Limits**.
6. In the Access Permission dialog box, select **ANONYMOUS LOGON** name in the “Group or user names” box. In the Allow column under “Permissions for User”, select **Remote Access**, and then click **OK**.
Step 4: Give the User/Group WMI permissions

1. Run Windows Management Instrumentation (WMI) console. Select Start, click Run, and then type: `wmimgmt.msc`
2. Click OK and press Enter.
3. Right-click "WMI Control" and select "Properties".
4. Select the Security tab, and then expand "Root".
5. Select "CIMV2" and then click "Security".
6. Add the domain user that you’ve created to work with AD Query. Give the user the “Enable Account” and “Remote Enable” permissions.

7. Click “Advanced”. Select the domain user and check that “Apply to” is set to “this namespace and subnamespaces”.

© Juniper Networks, Inc. 5
8. Select **OK** to save changes.

**Step 5: Restart WMI Service**

1. Run the Windows Services Manager (WMI): Select **Start**, click **Run**, and then type: `services.msc`
2. Click **OK** and press enter.
3. Locate the *"Windows Management Instrumentation"* service, right-click the service, and then select *"Restart"* option.

![WMI Service Manager](image)

**Step 6: Configure the non_admin user in SRX**

Enter the following CLI commands:

```bash
set services user-identification active-directory-access domain juniper.net user [username]
set services user-identification active-directory-access domain juniper.net user password "[user password]"
```

*Note: Replace [username] and [user password] with the correct user information, do not include the square brackets.*