Service operations

Service operations for Windows resources

The following service operations are performed at Windows resources on behalf of the domain or local service account:

- Checking of connection to resources
- Synchronization of local accounts
- Checking of local account passwords
- Changing of local account passwords
- Getting data about operating system
- Getting list of security groups

Configuring a domain account as service one

1. Log in to resource
2. Run the **Computer management** snap-in
3. Switch to **System tools** - **Local Users and Groups** - **Groups section**
4. Open the context menu of **Administrators** group
5. Select **Properties** item
6. Click **Add**
7. Select the domain account to be used as service one for the resource and click **OK**

Configuring a local account as service one

If you plan to use local built-in administrator account as service account, then no additional configuration is required. Otherwise, proceed as follows:

1. Log in to resource
2. Run the **Computer management** snap-in
3. Switch to **System tools** - **Local Users and Groups** - **Groups** section
4. Open the context menu of **Administrators** group
5. Select **Properties** item
6. Click **Add**
7. Select the local account to be used as service one for the resource and click **Ок**
8. Run **Windows registry editor** (RegEdit)
9. Expand the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch
10. Open the context menu of **System** section
11. Select **Create** - **DWORD (32-bit) Value**
12. Specify the parameter name - **LocalAccountTokenFilterPolicy**
13. Open the context menu of **LocalAccountTokenFilterPolicy** parameter
14. Select **Modify** item and set the **Value data:** equal to **1**

Registry editing is required due to restrictions on remote WinRM management for all local accounts except for built-in administrator account.

Configuring PAM Core to perform service operations on behalf of local resource accounts

Service operations are performed using WinRM. To use local resource accounts as service one, you need to add the resource to the **TrustedHosts** list of trusted ones on PAM Core server.

Configuring the TrustedHosts list

1. Log in to the server on which PAM Core will be installed
2. Run **Command line** (CMD) as Administrator
3. Execute the following command:

```
C:\>winrm s winrm/config/client @{TrustedHosts="Resource1.domain.local,
Resource2.domain.local"}
```

The specified resources shall be added to the TrustedHosts list.

When adding new resources to the trusted list, you must specify previously added resources and new ones, since the new value overwrites the old one.

```
@{TrustedHosts="Resource1.domain.local, Resource2.domain.local,
Resource3.domain.local"}
```

Service operations in Active Directory

Account for service operations in Active Directory

1. Start the **Active Directory Users and Computers** snap-in
2. Open the context menu of the Container or Organization Unit
3. Select **Create** - **User** item
4. Enter the name, for example, **IPAMADServiceOps**
5. Fill in the required fields and complete the creation of the account
6. Open the context menu of the container, organizational unit, or domain root and select the **Properties** item
7. Go to the **Security** tab
8. Click **Add**
9. Select **IPAMADServiceOps** account and click **Ок**
10. Click **Advanced**
11. Select **IPAMADServiceOps** and click **Edit**
12. For the field **Applies to:** set value **Descendant User objects**
13. In the **Permissions:** section check **Reset password**
14. Save all changes

Service operations for *nix resources

The following service operations are performed at *nix resources on behalf of the local service account:

- Checking of connection to resource
- Searching for local accounts
- Checking of local account passwords
- Changing of local account passwords
- Getting data about operating system
- Getting list of security groups

Creating and configuring a service account

1. Log in to resource.
2. Run **Terminal**.
3. Create a user, for example **IPAMService**:

   ```
   adduser IPAMService
   ```

4. Add the user to **SUDO** group

   ```
   usermod -aG sudo IPAMService
   ```

Configuring a group of privileged accounts

Automatic searching and adding of Access accounts to Indeed Identity PAM is performed based on their permission to execute a SUDO command. To grant the permission to execute SUDO command, you need to edit the **/etc/sudoers** file.