Oppsett av user-id med integrert agent

Oppskriften er basert på dokumentasjon fra Palo Alto Networks, men strippet ned til kun relevant informasjon.

Om oppsett

WinRM over HTTP with Kerberos brukes for å slippe å vedlikeholde sertifikat. Kerberos-protokollen gir alene høy nok sikkerhet.

Det er antagelig mulig å stramme inn enda litt til, men det krever mer labbing.

Merk at alt er forslag fra Palo Alto, og i enkelte miljø kan det hende lokale tilpasninger må gjøres av AD-administrator. Prinsippene bør likevel værel ike.

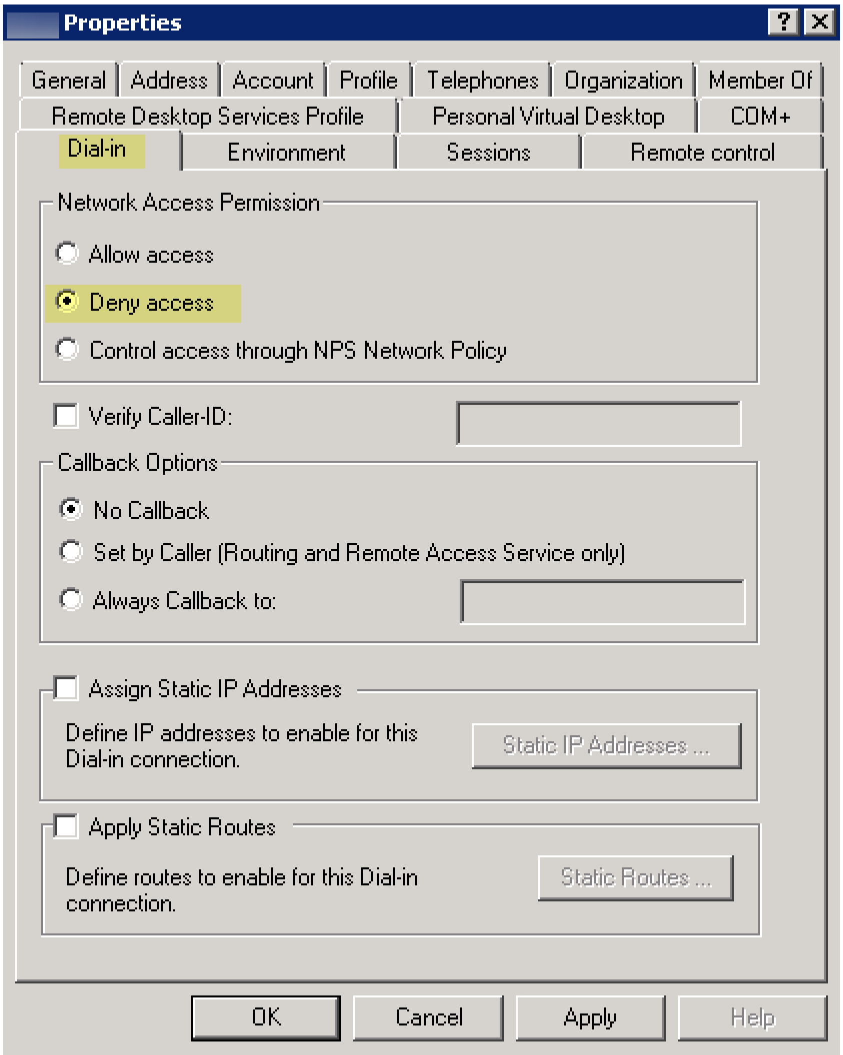
Opprett service-bruker

Gjøres av Windows-administrator

I Active Directory Users and Computers, lag ny user vha. New > User. Plasseres enten i Managed Service Accounts, eller i annen dedikert OU for slike kontoer. Sørg for at passord er never expire.

Fjern remote access

Åpne Properties på den opprettede kontoen, velg Dial-In og merk av Deny Access under Network Access Permission



Network Access Permission

○ Allow access

● Deny access

○ Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

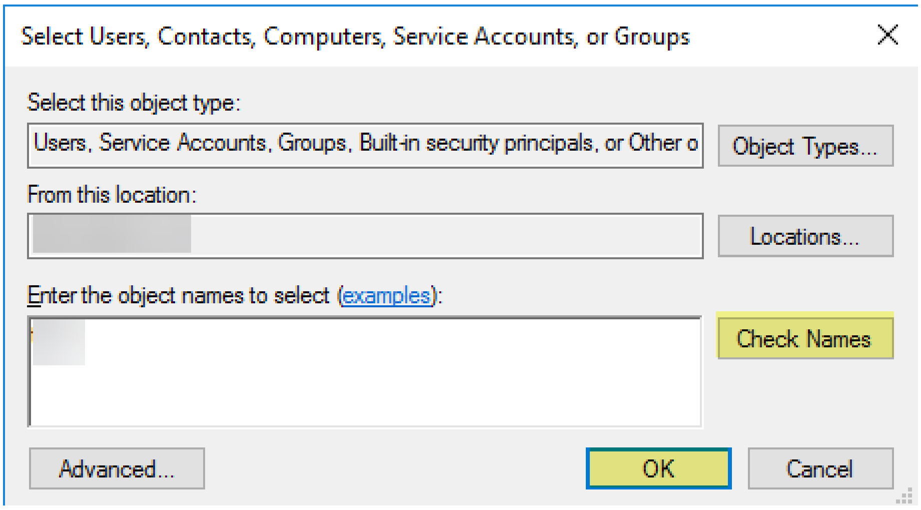
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Gruppemedlemskap

Systembrukeren må legges inn følgende to grupper under Bultin

- Event Log Reader
- Distributed COM Users
- Remote Management Users

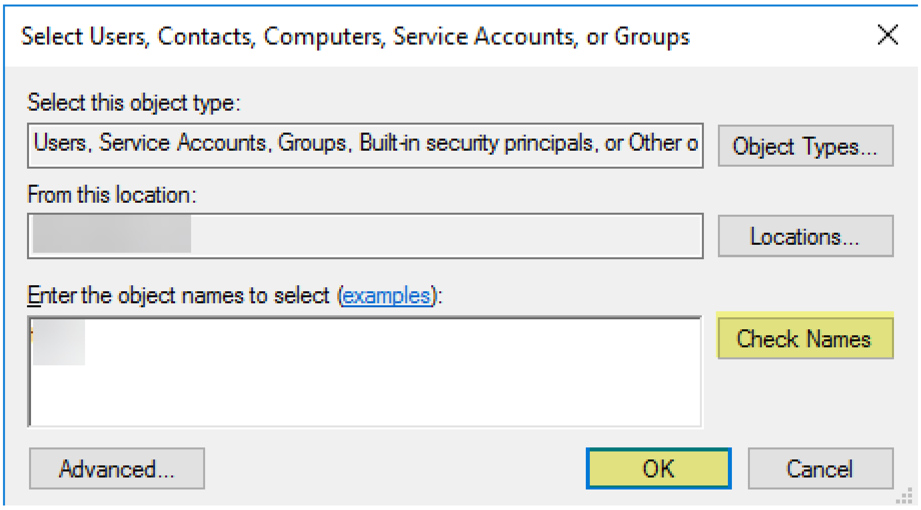

Select Users, Contacts, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

Select this object type:

Users, Service Accounts, Groups, Built-in security principals, or Other o

From this location:

Enter the object names to select (examples):


Select Users, Contacts, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

Select this object type:
Users, Service Accounts, Groups, Built-in security principals, or Other o

From this location:
[redacted]

Enter the object names to select (examples):
[redacted]

WMI Namespace

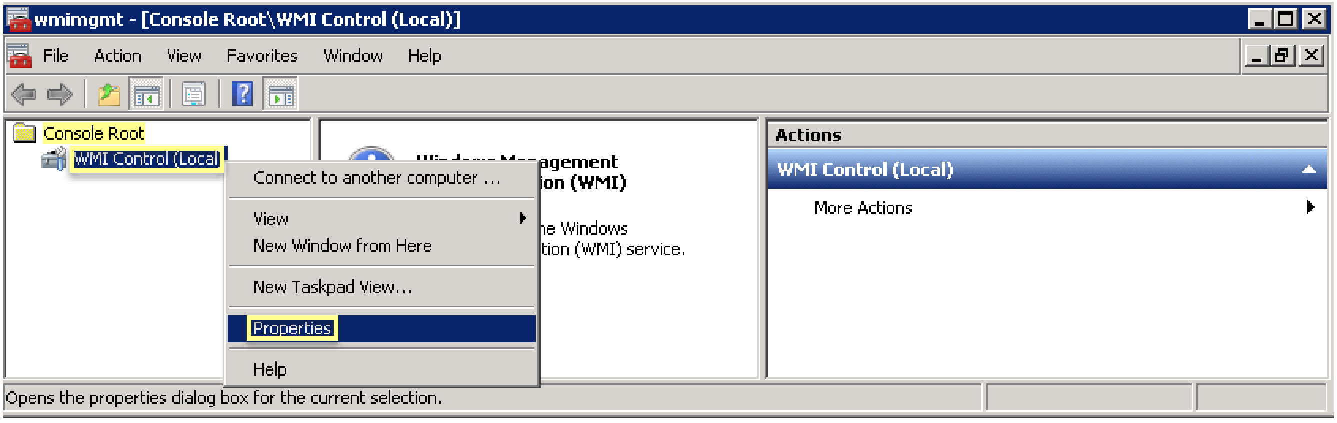
På en DC, utfør følgende

1. Åpne MMC-konsoll

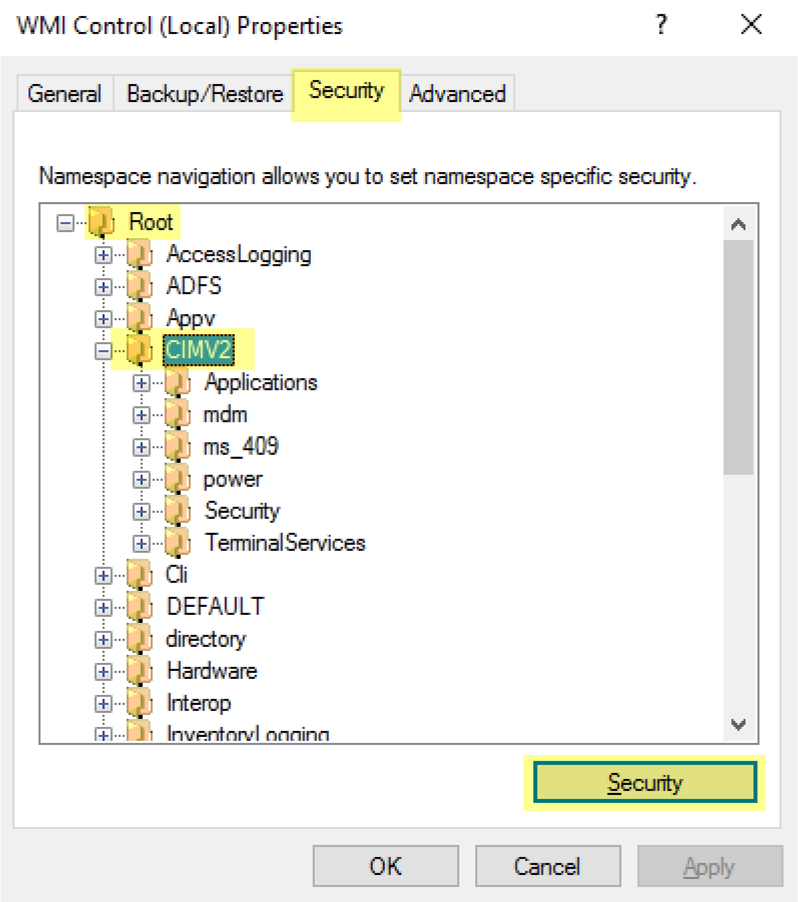
```
wmimgmt.msc
```

1. Høyreklikk WMI Control og velg Properties
2. Velg Security tab
3. Merk CIMV2 i treet, og klikk på knappen Security
4. Legg til servicekonto
5. Servicekonto må gis følgende rettigheter
    - Enable Account
    - Remote Enable

Verifiser at endringen trår i kraft på samtlige DC-er som brukes til pålogging i domenet.



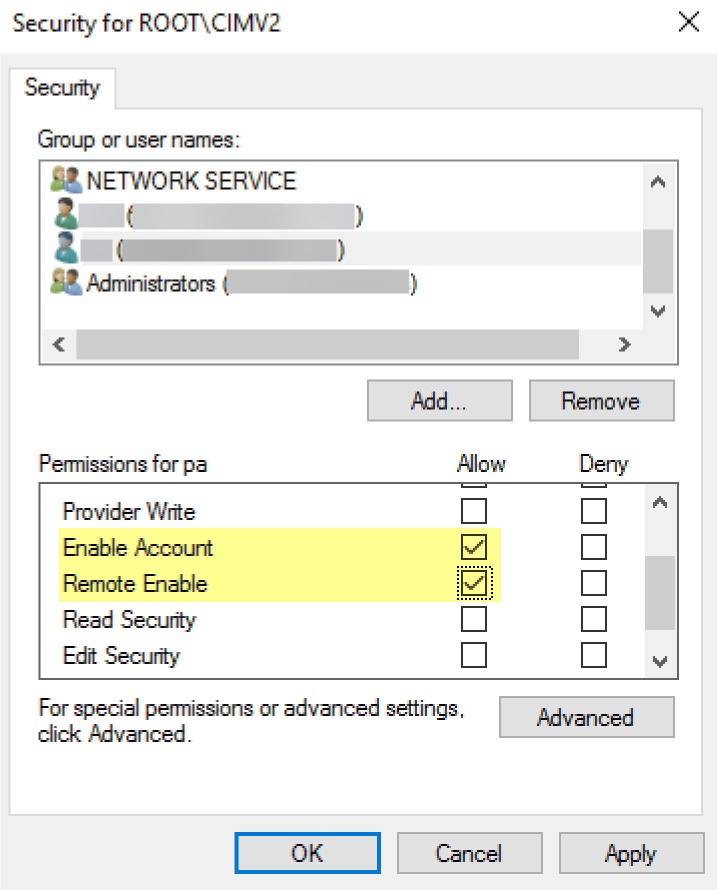
Opens the properties dialog box for the current selection.



WMI Control (Local) Properties

Namespace navigation allows you to set namespace specific security.

- Root
  - AccessLogging
  - ADFS
  - Appv
  - CIMV2
    - Applications
    - mdm
    - ms_409
    - power
    - Security
    - TerminalServices
  - Cli
  - DEFAULT
  - directory
  - Hardware
  - Interop
  - InventoryLogging



Security for ROOT\CIMV2

Group or user names:

- NETWORK SERVICE
- [redacted]
- [redacted]
- Administrators ([redacted])

Permissions for pa

	Allow	Deny
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□
Read Security	□	□
Edit Security	□	□

For special permissions or advanced settings, click Advanced.

Stripp unødvendige rettigheter

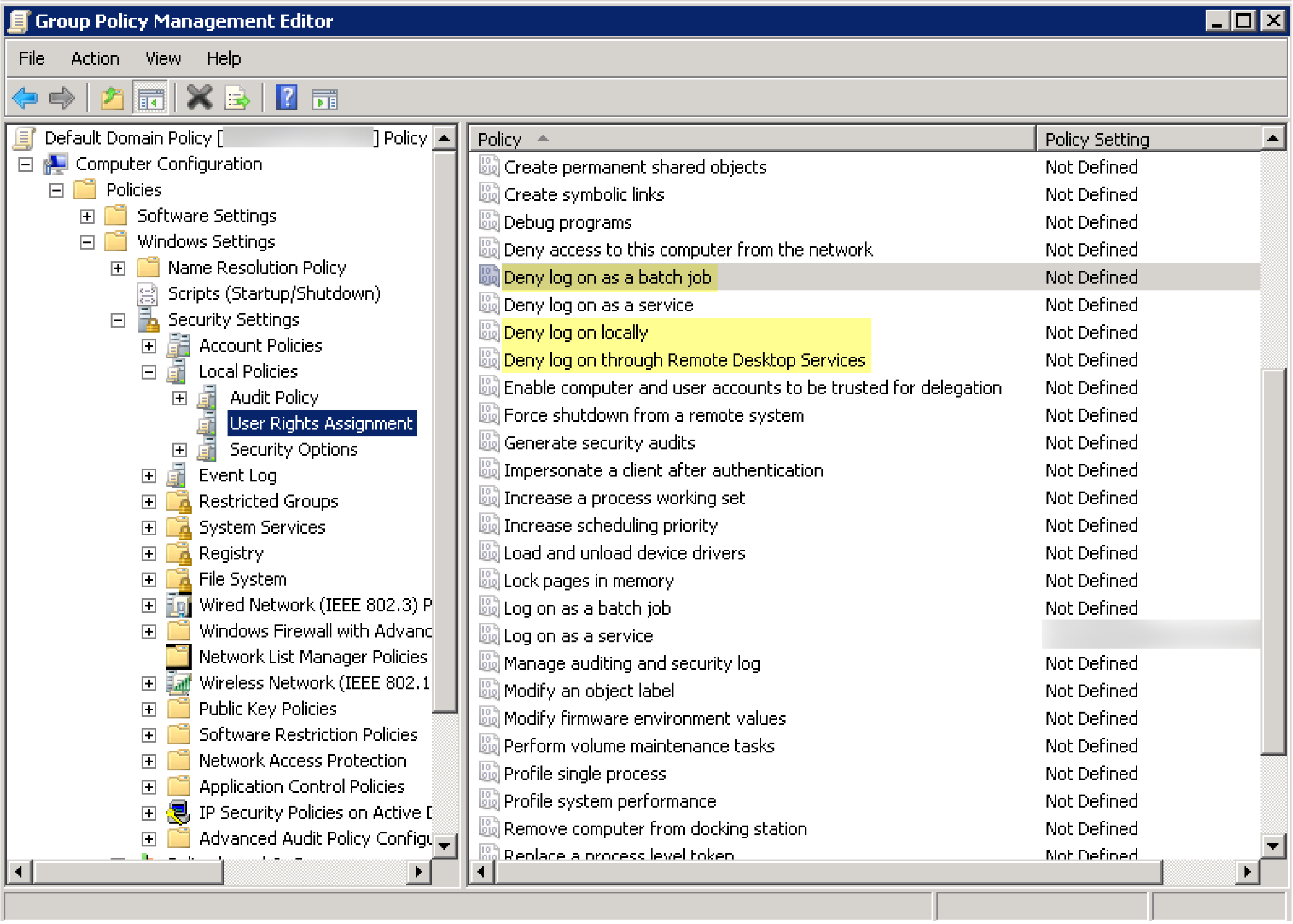
Ved hjelp av Group Policy Management Editor, legg servicekonto inn i følgende deny-policies.

- Deny log on as a batch job
- Deny log on locally
- Deny log on through Remote Desktop Services

For hver policy

- Høyreklikk
- Velg Properties
- Velg Define these policy settings
- Add User or Group.

Som default ligger disse under **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **User Rights Assignment**



- Default Domain Policy [[redacted]] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) P
          - Windows Firewall with Advanc
          - Network List Manager Policies
          - Wireless Network (IEEE 802.1
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active D
          - Advanced Audit Policy Configu

Policy	Policy Setting
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	[redacted]
Manage auditing and security log	Not Defined
Modify an object label	Not Defined
Modify firmware environment values	Not Defined
Perform volume maintenance tasks	Not Defined
Profile single process	Not Defined
Profile system performance	Not Defined
Remove computer from docking station	Not Defined
Replace a process level token	Not Defined

Verifiser at WinRM kjører på domenekontrollere

Logg inn med administrator-konto.

- For å starte WinRM og åpne lokal brannmur, kjør kommandoen `winrm quickconfig`
  - Om WinRM allerede kjørte, bekreft og gå videre

- For å sette opp transport over HTTP, kjør kommandoen `winrm enumerate winrm/config/listener`
  - Verifiser at den viser Transport = HTTP
- Kjør `winrm get winrm/config/service/Auth`
  - Verifiser at Kerberos = True

Sett opp server monitor på brannmur

Konfigurer User-ID

- Verifiser at NTP er konfigurert og fungerer både på domenekontrollere og brannmurer. Korrekt klokke er kritisk for Kerberos.
- Sett opp Kerberos-profiler mot alle domenekontrollere som brukes til autentisering
- Åpne **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Server Monitor Account**
- Fyll inn brukernavn, domenets DNS-navn (ikke det samme som NETBIOS-navnet), passord og velg Kerberos-profil

Legg til domenekontrollere

Alle domenekontrollere som brukes til autentisering legges inn.

- **Type:** *Active Directory*
- **Transport Protocol:** *WinRM-HTTP*
- **Network Address:** *<Fully Qualified Domain Name (FQDN)> til domenekontroller*

Kjør commit

Referanser

- Create a Dedicated Service Account for the User-ID Agent
- Configure Server Monitoring Using WinRM