1 JUNE 2022

Certificate Auto Enrollment

Automatic Certificate Enrollment from Active Directory Certificate Services

What is Certificate Auto Enrollment?

New in Samba since 4.16

What is Certificate Auto Enrollment?

Overview

ADCS

Certificate Auto Enrollment is a function of Active Directory Certificate Services. It's enabled by Group Policy, and allows users and devices to enroll for certificates. There is generally no user interaction required.

Monitoring Certificates

Ordinarily, IT teams would manually monitor and manage certificates. However, manual monitoring of certificates can cause disruptive outages and security gaps. Certificate Auto Enrollment eliminates manual monitoring.

Certificate Expiration

Certificates expire. Monitoring certificates manually means finding which certificates will soon expire and renewing them early. This can be like finding a needle in a haystack. Certificate Auto Enrollment eliminates manual renewals.

What about certmonger?

Some here might point out that certmonger already accomplishes these things

- Exactly the point!
  - Samba is utilizing certmonger to monitor Active Directory Certificate Services (via the cepces plugin)
- certmonger is missing the Group Policy piece of the puzzle
  - certmonger alone requires manual interaction
  - Cannot automatically configure servers

(DRAFT) [MS-CAESO]: Certificate Autoenrollment System Overview

The Certificate Autoenrollment System Overview (CAESO) describes the task of automatically enrolling and re-enrolling digital certificates that systems and protocols require to operate. System administrators usually perform this task manually, and as demand for certificates increases, they can become overwhelmed. Autoenrollment automatically handles certificate enrollment and the re-enrollment of expired certificates, which relieves the administrator from this task.

Autoenrollment serves a central role in client and server relationships that rely on certificate enrollment. By instituting autoenrollment, the system administrator can concentrate on other tasks. Autoenrollment determines what policies are available for certificate enrollment, the set of certificates specified through these policies, and what certificates can be issued based on the templates in these policies.

Proprietary Implementations

There are a number of proprietary implementations of Certificate Auto Enrollment for Linux

- Vintela Group Policy
- Centrify Group Policy
- BeyondTrust AD Bridge Group Policy
- Others?

How it Works in Samba

Dependencies

- samba-gpupdate
- certmonger
- cepces

How it Works in Samba (samba-gpupdate)

Determing whether to run

- Check if Auto Enrollment is enabled (SYSVOL AEPolicy)
- Choose between advanced SYSVOL config and simple LDAP config
- Fetch endpoints from SYSVOL, or from LDAP
- Enroll each endpoint (via certmonger's `getcert add-ca`)

How it Works in Samba

Enrolling endpoints

- Install the CA root certificate
- Add the CA to certmonger
- Fetch the list of certificate templates
- Enroll each template and monitor via cepces

Basic LDAP Configuration

Endpoints stored in LDAP

Basic LDAP Configuration

Endpoints stored in LDAP

- Endpoint server information stored in LDAP
- "CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=…"
  - CN
  - dNSHostName
  - certificateTemplates
  - cACertificate

Advanced SYSVOL Configuration

Endpoints stored on the SYSVOL in a Registry.pol file

Advanced SYSVOL Configuration

Endpoints stored on the SYSVOL in a Registry.pol file

- KEY: Software/Policies/Microsoft/Cryptography/PolicyServers
  - URL
  - PolicyID
  - Flags
  - AuthFlags
  - Cost

Endpoint URL

- In the form of: https://<server>/ADPolicyProvider_CEP_<auth_type>/service.svc/CEP

Endpoint AuthFlags

- Specifies the type of authentication
  - Anonymous
  - Kerberos
  - Password
  - Certificate

Lack of Certificate

Advanced configuration does not provide a root certificate for the server

- Easy work around is to fetch the certificate via NDES (if enabled)
- Possible to fetch the certificate via LDAP, if present

Improvements Since Samba 4.16

Improvements since Samba 4.16

- Enhanced logging capabilities
- Certificate and Anonymous enrollment authentication
- CA Initialization and template fetching follows spec
- Support Cert Auto Enroll Advanced Configuration
- Remove sscep dependency
- Make NDES optional with simple config
- Various bug fixes

Certificate Auto Enrollment TODO

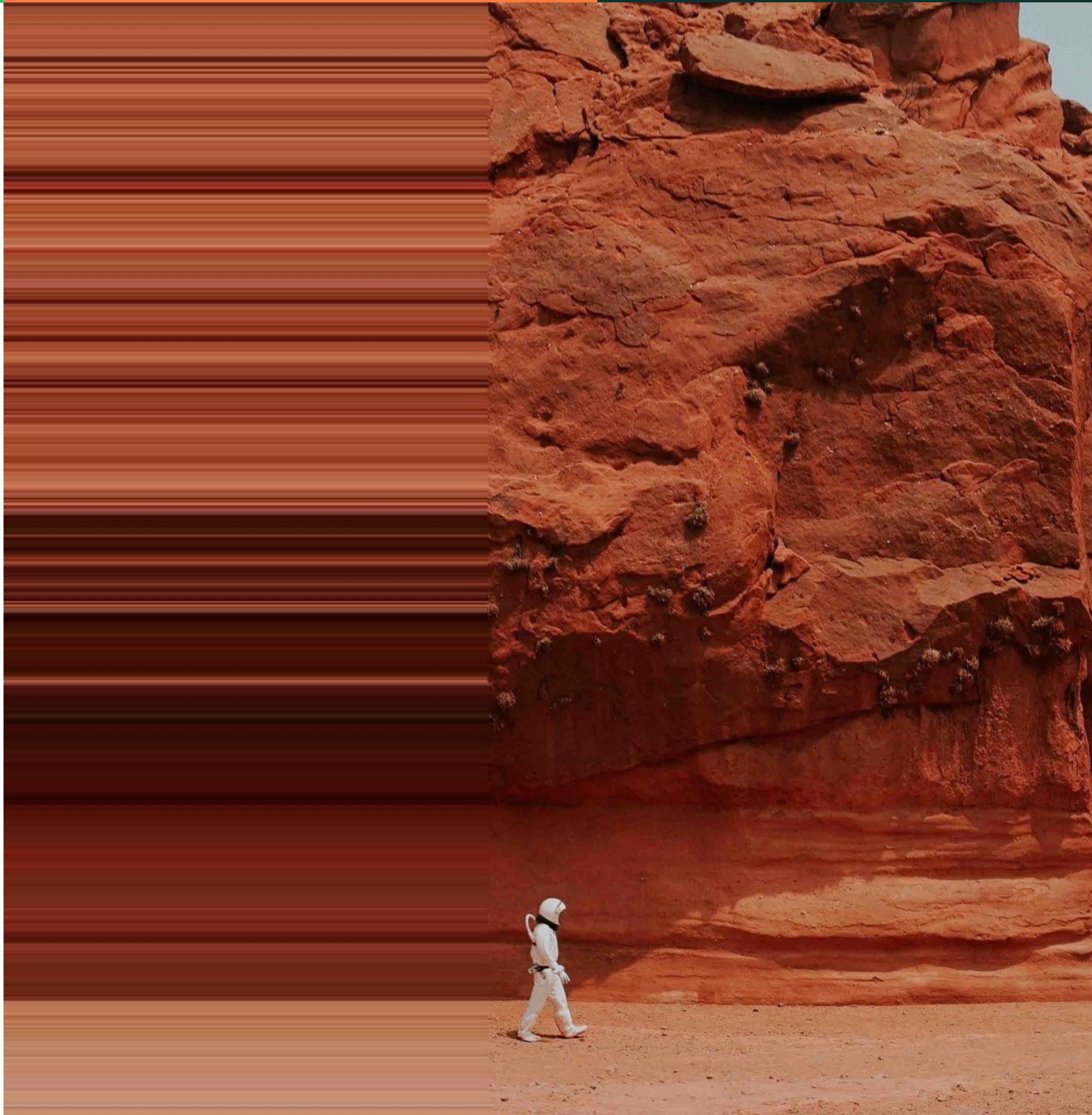
Work still needing done

TODO

Projects needing attention

- cepces
  - More testing/better testing
  - Command line configurable certificate authentication
  - Password authentication (safe?)
- samba-gpupdate
  - Certificate chain loading without NDES

DEMO



Samba
Group Policy

General update on Samba Group Policy

Extensions Added Since SambaXP 2021

These extensions have been added to Samba since my Group Policy update last year

- Certificate Auto Enrollment
- Centrify Compatible Crontab Extension
- Centrify Compatible Sudoers Extension
- Chrome/Chromium Extension
- Firefox Extension
- Scripts User Extension
- Firewalld Extension

ALT Linux Group Policy Integrations

Group Policy features merged from ALT Linux gpupdate

- User Policies
- Enhanced logging
- Firefox/Chrome Policies (rewritten)
- Firewall Policies (rewritten)
- oddjob-gpupdate

samba-tool gpo load/remove

In coordination with Kees van Vloten, not yet merged into master

This adds commands for adding/removing/displaying any Registry.pol Group Policy.

- Useful for both Windows and Linux GPO management

How to follow the Group Policy progress

https://wiki.samba.org/index.php/Group_Policy

Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Maxfeldstrasse 5
90409 Nuremberg
www.suse.com