Microsoft

AZ-140

Tag 4

Configuring and Operating Azure Virtual Desktop

Guten Morgen!

AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Monitor and manage performance and health
14. Plan and implement updates, backups, and disaster recovery

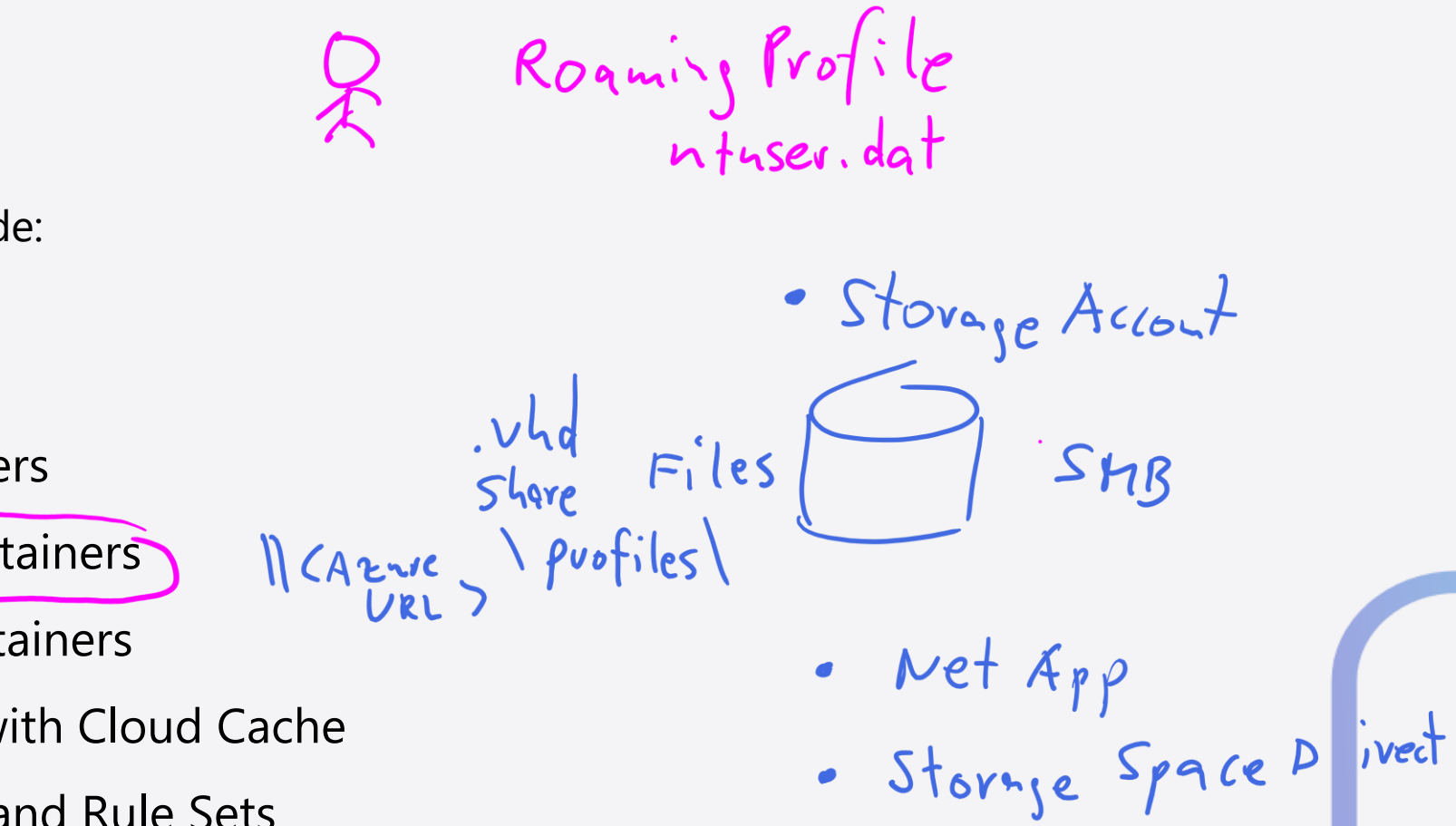
Microsoft

Implement and manage FSLogix

Introduction

The topics covered in this module include:

- Understanding FSLogix
- Understanding FSLogix containers
- Configuring FSLogix Profile Containers
- Configuring FSLogix Office Containers
- Configuring profile containers with Cloud Cache
- Using FSLogix Apps RuleEditor and Rule Sets
- Creating and implementing Rule Sets for application masking



Overview of FSLogix

Overview of FSLogix

FSLogix enhances and enables a consistent experience for Windows user profiles in virtual desktop computing environments.

FSLogix isn't limited to virtual desktop environments and could be used on physical desktops where a more portable user experience is desired.

Here are a few things that FSLogix provides:

- Roam user data between remote computing session hosts.
- Minimize sign in times for virtual desktop environments.
- Optimize file I/O between host/client and remote profile store.
- Provide a local profile experience, eliminating the need for roaming profiles.
- Simplify the management of applications and 'Gold Images'.

Key Capabilities

Redirect user profiles to a storage provider. Mounting and using the profile from a storage provider eliminates delays often associated with solutions that copy profiles to and from a network location.

Redirect only the portion of the profile that contains Office data by using an ODFCcontainer. The ODFC container allows an organization already using an alternate profile solution to enable Microsoft 365 applications in multi-session desktop environments.

Applications use the user's profile as if it were on the local disk. FSLogix uses a filter driver to virtualize and redirect the profile at the file system level. Applications are unaware the profile is on the network. Obscuring the redirection is important because many applications can't work properly with a profile stored remotely.

Profile containers used with Cloud Cache to provide high availability and disaster recovery profile solutions.

Application Rule Sets manage access to an application, font, printer, or other items. Access can be controlled using users, groups, IP Addresses, and other criteria. Application Rule Sets significantly decrease the complexity of managing large numbers of gold images.

Understanding FSLogix containers

Understanding FSLogix containers

FSLogix has two primary container types for profile management:

- Profile containers store user profile data in VHD files.
- ODFC containers focus on Office-related profile content.

A profile container is the most common container used in an FSLogix solution. A profile container is all the data related to a user's profile, which is directly stored in the VHD(x).

- A Windows user profile is typically stored in C:\Users\%username%. Nearly all the files and folders found under this location would be included in an FSLogix profile container.
- Some data in a user's profile shouldn't or can't be roamed which can be found in the exclusion list.

When to use Profile and ODFC containers

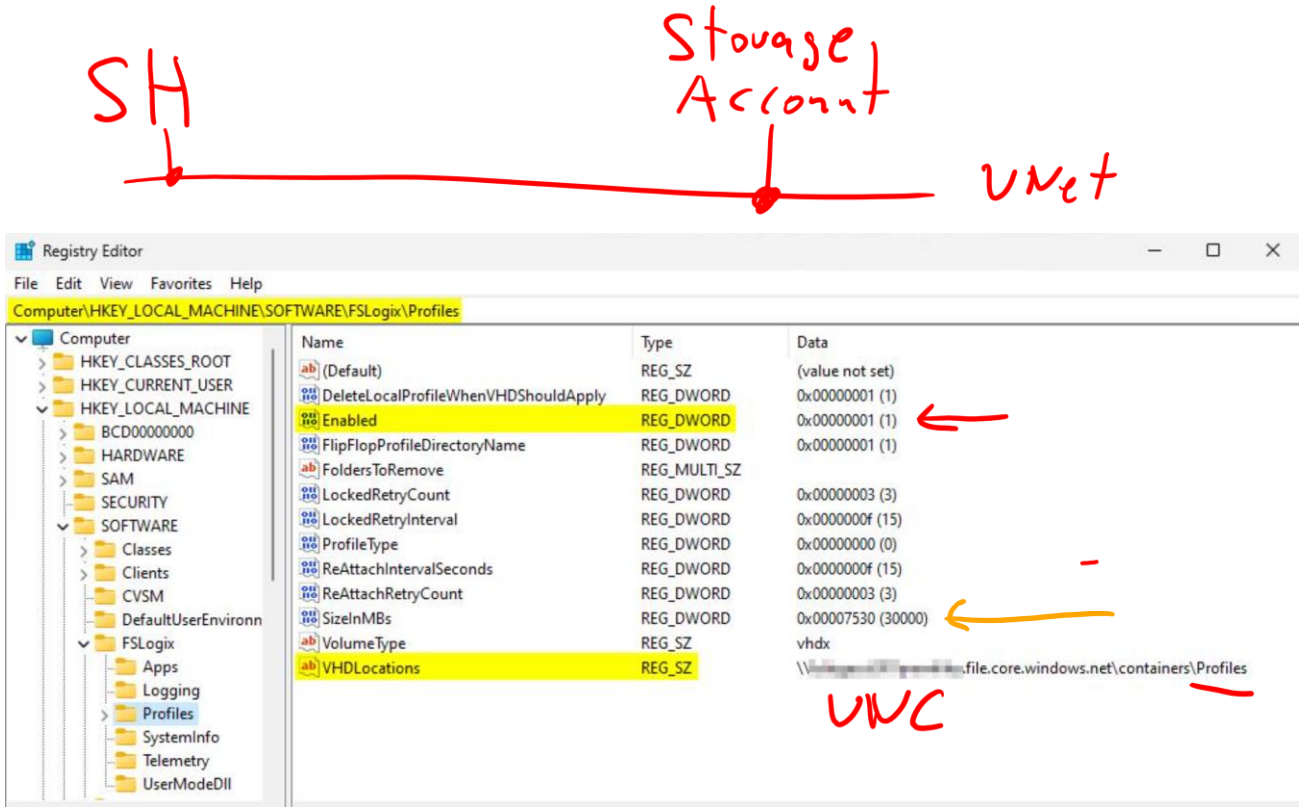
Profile and ODFC containers should be used together when:

- Discretion is wanted in the storage location for Office data vs. other profile data.
- Provides isolation from data loss or corruption in one of the containers.
- Used as a mechanism to specify which Office components have their data included in the container.
- Allows organizations to have different container sizes to accommodate specific workloads or data synced from OneDrive.

Configuring FSLogix Profile Containers

Configuring FSLogix Profile Containers

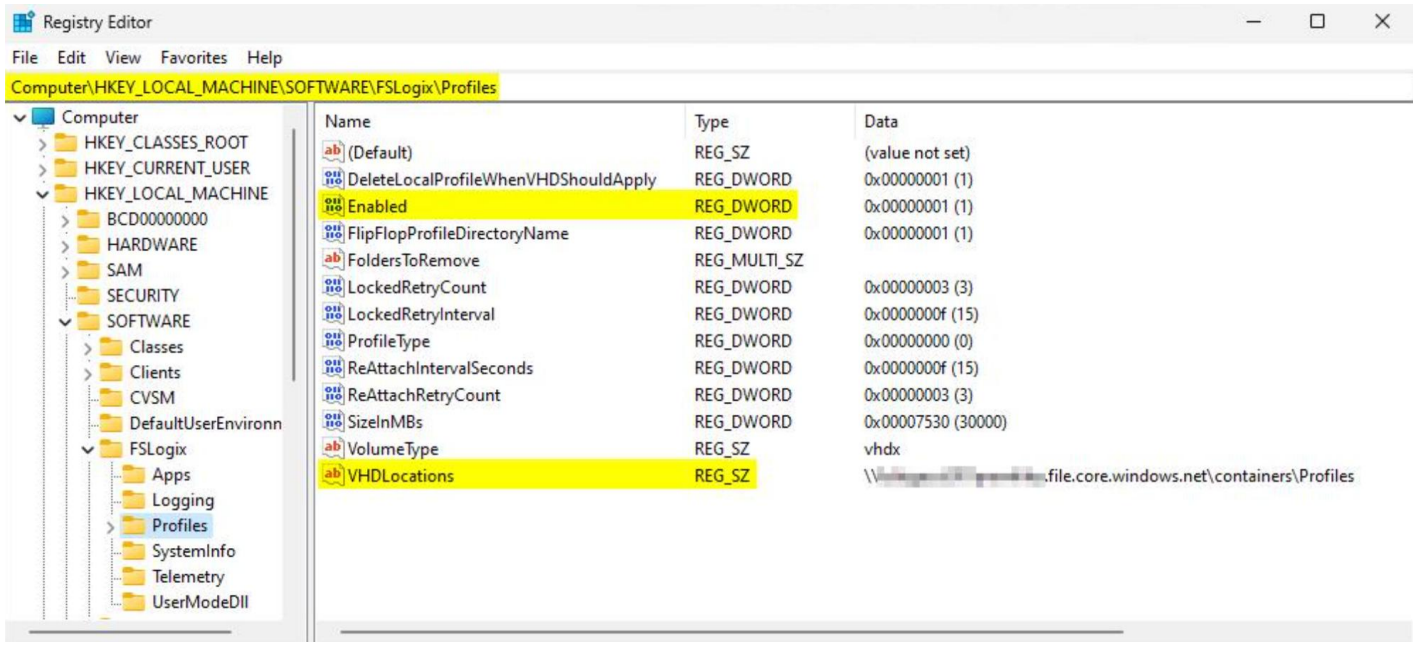
- FSLogix profile containers are a complete roaming profile solution for virtual environments.
- The profile container (single container), redirects the entire Windows user profile into a VHD stored on a storage provider. The most common storage provider is an SMB file share.
- The profile container is inclusive of all the benefits and uses found in the ODFC container.



Configuring FSLogix Office Containers

Configuring FSLogix Office Containers

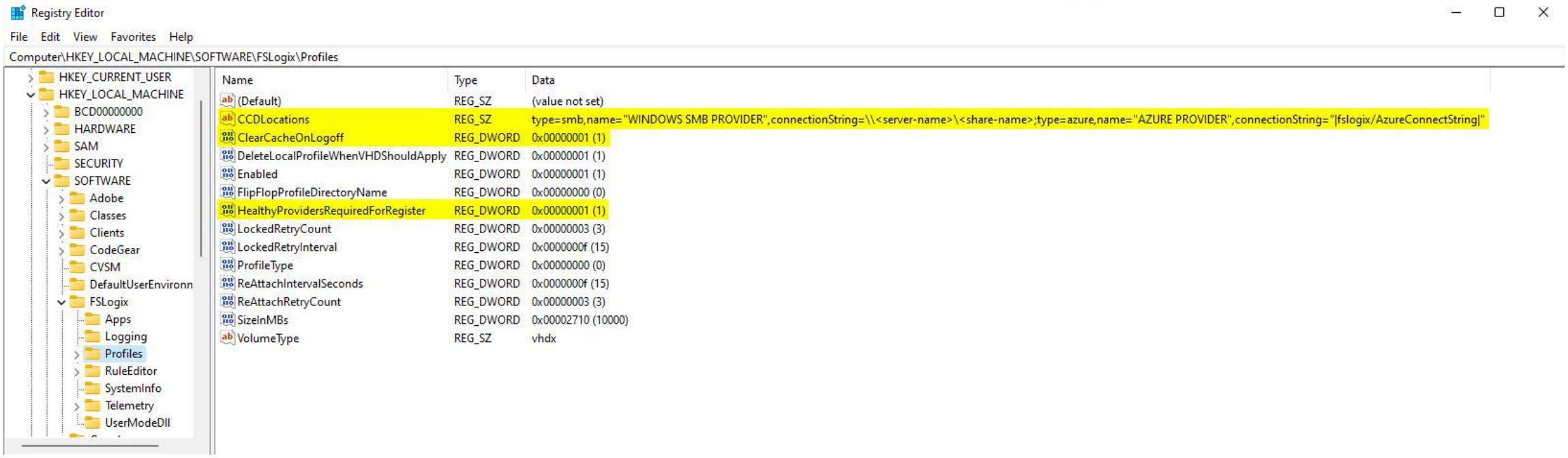
- FSLogix ODFC containers are a subset to the profile container and are used to redirect-specific Microsoft 365 app data into a VHD stored on a storage provider.
- All benefits of the ODFC Container are automatic when using profile containers in a single container configuration.
- ODFC containers can optionally be used in with profile containers in a dual container configuration, to place Microsoft 365 app data in a different VHD from the rest of the profile data.



Configuring profile containers with Cloud Cache

Configuring profile containers with Cloud Cache

Cloud Cache is an optional type of configuration to profile or ODFC containers. The primary function of Cloud Cache is to mitigate short-term or intermittent connectivity problems with the remote storage providers.



Using FSLogix Apps RuleEditor and Rule Sets

The FSLogix Apps RuleEditor is a standalone application that creates FSLogix Rule Set files.

FSLogix Apps Services (frxsvc) processes Rule Set files and can perform various actions that manage the end-user experience in virtual desktop environments.

Rule Set files are a collection of rules that show, hide, redirect, or customize specific aspects of the registry, file system, applications or printers.

A single Rule Set file can support any number of rules of varying types.

You can create four types of rules:

- Hiding rule
- Redirection rule
- App container (VHD) rule
- Specify value rule

Types of Rules

Hiding rule

Hides specific items from users. Applies to files, folders, registry keys, values, printers, or fonts.

Redirection rule

Redirects non-profile data into user profile container for consistency across virtual machines.

App container VHD rule

Contains applications with read-only data in a VHD, automatically mounts for specific users.

Rule Assignments and Assignment Types

Assignment order

Order affects Rule Set application. Managed with Move Up/Down buttons.

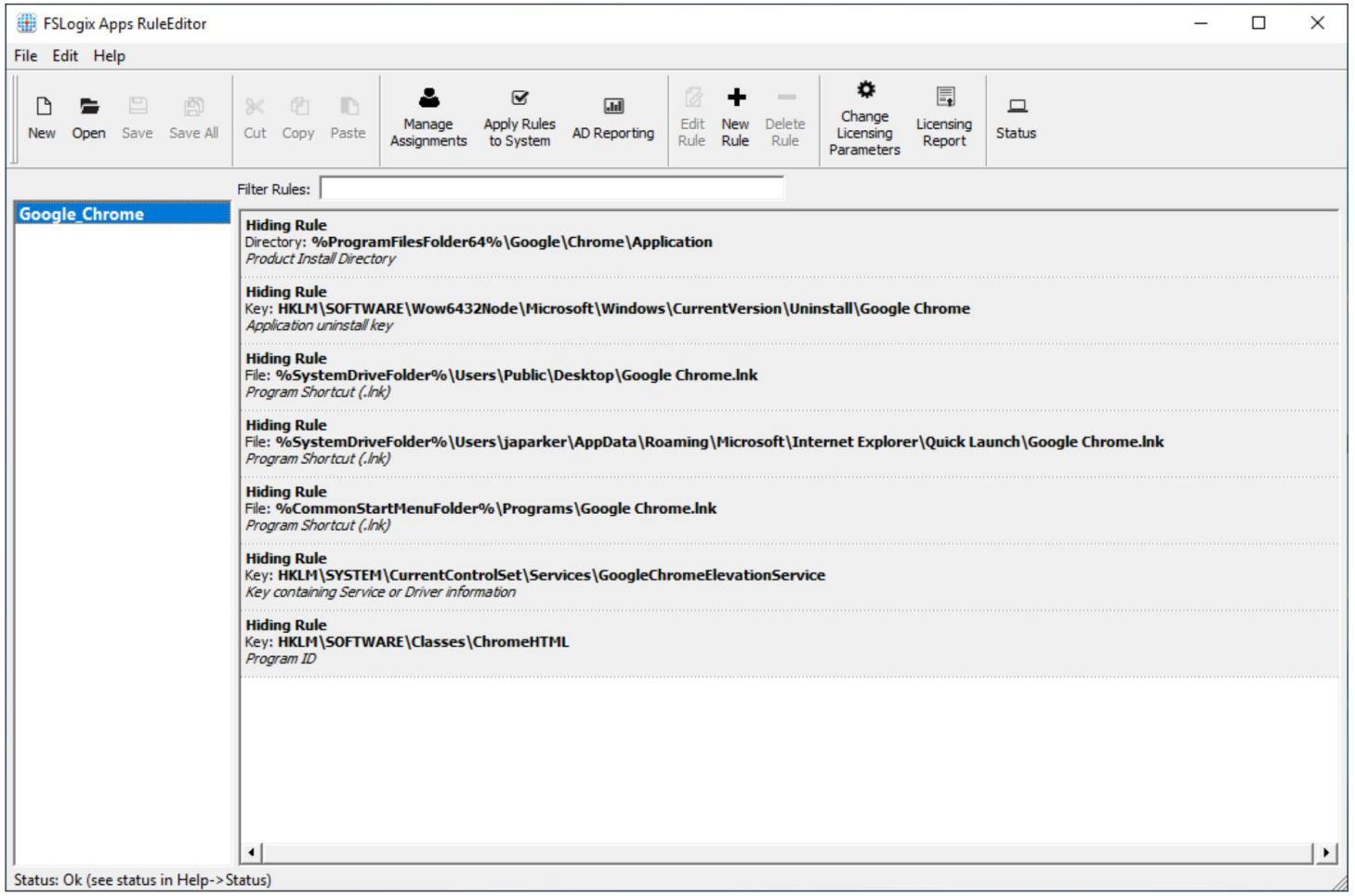
Assignment types

Assign Rule Sets to users, groups, processes, network locations, IP addresses, etc.

Creating and Implementing Rule Sets for Application Masking

Creating and Implementing Rule Sets for Application Masking

This unit provides step-by-step instructions for creating and implementing an application hiding Rule Set, which "hides" the Google Chrome browser for specific users.



Knowledge check

Knowledge check

A system administrator is tasked with optimizing file I/O between host client and remote profile store in a virtual desktop environment. Which solution would be most effective for this task?

Choices:

1. Using an alternate profile solution to enable Microsoft 365 applications
2. Redirecting only the portion of the profile that contains Office data by using an ODFC container
3. Implementing FSLogix to provide a local profile experience, eliminating the need for roaming profiles

Knowledge check

A team is planning to host a general purpose file share for less than 200 users. Which performance tier should they use?

Choices:

1. Standard with multiple file shares
2. Premium file shares
3. Standard file shares

Knowledge check

An IT administrator is managing the end user experience in a virtual desktop environment using FSLogix Apps RuleEditor. They need to set a registry value for a specific user group at sign in. Which type of rule should they create?

Choices:

1. Hiding rule
2. Redirection rule
3. Specify value rule

Knowledge check

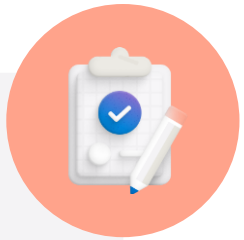
A system administrator is configuring Cloud Cache for FSLogix profiles. They have followed the steps to configure the registry settings and now need to verify the configuration. What should they do to confirm that the Cloud Cache has been correctly set up?

Choices:

1. Reboot the system and check for any error messages during startup
2. Check the system's task manager for any FSLogix related processes
3. Review the Windows Event Viewer, File Explorer or the FSLogix profile logs

Summary

Summary



What you learned:

- Configure FSLogix Profile Containers
- Configure FSLogix Office Containers
- Configure profile containers with Cloud Cache
- Using FSLogix Apps RuleEditor and Rule Sets
- Create and Implement Rule Sets for Application Masking