Saviynt – HomeDirectory Design & Integration Guide

February 2023

Table of Contents

[Document Control 3](#_Toc126849449)

[Introduction 3](#_Toc126849450)

[Prerequisites 3](#_Toc126849451)

[Process of Invoking HomeDirectory Creation PowerShell Script through Saviynt 3](#_Toc126849452)

[Architecture 4](#_Toc126849453)

[Rest Connector 4](#_Toc126849454)

[Create Connection in Saviynt 4](#_Toc126849455)

[Create Security System in Saviynt 5](#_Toc126849456)

[Create Endpoint in Saviynt 5](#_Toc126849457)

[Operations 6](#_Toc126849458)

[Create Operation 6](#_Toc126849459)

[Enable Operation 6](#_Toc126849460)

[Delete 7](#_Toc126849461)

[HomeDirectory Creation Flow 7](#_Toc126849462)

[Appendix 9](#_Toc126849463)

[Technical Rules 9](#_Toc126849464)

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version control** | | | |
| **Version** | **Name** | **Role** | **Date** |
| V1 | Gaurav Khandelwal | Author | 01/15/2023 |
| V2 | Vineet Gupta | Author | 02/01/2023 |

Introduction

The purpose of this document is to capture the design and integration details for Saviynt integration with HomeDirectory for provisioning.

Once user is on-boarded and new Active Directory account is created based on [Birthright Rule](#_Technical_Rules), Saviynt will invoke PowerShell script, which resides on the ADSI Windows server to create the HomeDirectory and assign HomeDirectory permissions to the user. After the process is completed, the user has full control access to their HomeDirectory.

Prerequisites

* Windows Server is set up
* SaviyntApp is deployed on the Windows Server
* Service Account has privileges to invoke PowerShell script on the ADSI server and to create/update directory on all NAS Shares

For Windows Server setup and SaviyntApp deployment, please refer the Active Directory Design Integration Guide for detailed steps.

Process of Invoking HomeDirectory Creation PowerShell Script through Saviynt

1. Configure Windows Server to Execute PowerShell Scripts
2. Installation of Windows Internet Information Services Server
3. Deploy PowerShell Script on Windows Server
4. Setup REST connector to invoke HomeDirectory Creation PowerShell Script

Architecture

The figure below shows the communication between Saviynt and PowerShell Script on Windows Server.

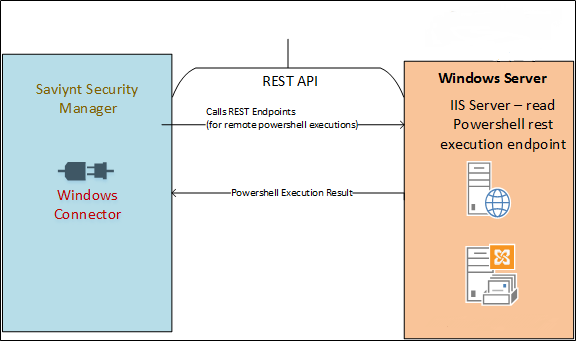


Figure 1 HomeDirectory Integration Architecture

Rest Connector

For executing PowerShell scripts, we either need a REST or Windows connector. Hence, we need to create a REST Connection, a Security System and an Endpoint.

### Create Connection in Saviynt

1. Login to Saviynt with administrator user role.
2. Click on “Admin” on the top right corner and then on “Identity Repository”. Under the “Identity Repository” select “Connections”.
3. Click on “Actions” and then “Create Connections”.
4. Fill the details of the connections in the page as below.

|  |  |
| --- | --- |
| Attribute Name | **Attribute Value** |
| Connection Name | HomeDirectory Endpoint |
| Connection Description | This connection is used to create Home Directory |
| Connection Type | REST |
| ConnectionJSON | Specify the JSON to authenticate the .NET API |

Similarly, create and configure connection for the HomeDirectory with following name.

**HomeDirectory Connection Name**: HomeDirectory endpoint

### Create Security System in Saviynt

General configuration parameter for security systems:

|  |  |
| --- | --- |
| **Attribute Name** | **Attribute Value** |
| System Name | HomeDirectory Endpoint |
| Display Name | HomeDirectory Endpoint |
| Connections | HomeDirectory Endpoint |
| Provisioning Connection | HomeDirectory Endpoint |
| Access Add Workflow | NA |
| Access Remove Workflow | NA |
| Number of tries for provisioning | 1 |
| Default System | No |
| Automated Provisioning | Enable |
| Manage Entity | No |
| Persistent Data | No |
| Use open connector | No |
| Recon HomeDirectory | Yes |
| Instant Provisioning | Enable |

Similarly, create and configure security system for the HomeDirectory with following name.

**HomeDirectory Security System Name**: Security Endpoint

### Create Endpoint in Saviynt

General configuration parameter for security systems:

|  |  |
| --- | --- |
| **Attribute Name** | **Attribute Value** |
| Endpoint Name | HomeDirectory Endpoint |
| Display Name | HomeDirectory Endpoint |
| Security System | HomeDirectory Endpoint |
| Add Email Template | Provide any email templates for specific provisioning operation if any |
| Description | HomeDirectory Provisioning |

Along with the above attributes, provide additional information like owners etc.

Similarly, create and configure endpoint for the HomeDirectory with following name.

**HomeDirectory Endpoint Name:** HomeDirectory Endpoint

Operations

### Create Operation

When a new user is created in Saviynt from the HR services trusted reconciliation, a configured technical rule will be evaluated to trigger Active Directory account provisioning. HomeDirectory provisioning will be triggered after the user is successfully provisioned to AD.

**Description:**

The following actions take place when a new HomeDirectory Account is created in Saviynt

1. Once the AD account is provisioned, Saviynt will trigger HomeDirectory account provisioning.
2. For all the users having AD account, HomeDirectory account will be provisioned.
3. For the Company and HomeDirectory users, respective HomeDirectory endpoint will be provisioned. The ‘User Origin Path’ of HR Service will be used to identify the users origin.
4. Saviynt will invoke the PowerShell script for HomeDirectory creation.

**Connection Configuration:**

|  |  |
| --- | --- |
| **Attribute Name** | **Attribute Value** |
| Connection Name | HomeDirectory Endpoint |
| ConnectionJSON | Provide the JSON to connect to the Windows connector server setup in Prerequisites |
| CreateAccountJSON | JSON to invoke the rest API to execute the PowerShell script with input parameters as   * HomeDirectory location * SamAccountName * Domain |

**PowerShell:**

The KPMG team will provide the PowerShell script for the following:

1. Get input variables passed by Saviynt as stated int the above section
2. Commands to create HomeDirectory on NAS share location
3. Commands to set permissions to HomeDirectory folder

### Enable Operation

When a user is enabled in Saviynt by re-hire process in HR Service, Saviynt will take no action if user is re-hired within X days. Saviynt will provision the HomeDirectory if rehired after X days.

**Description:**

The following actions take place for rehire in Saviynt

* + 1. User is rehired in HR Service
    2. If user is rehired within X day, no action.
    3. If user is rehired after X days, birthright rules will trigger HomeDirectory account provisioning after AD account is provisioned.
    4. Saviynt will create the HomeDirectory by invoking the PowerShell script. Refer Section Create Operation.

**Connection Configuration:**

|  |  |
| --- | --- |
| **Attribute Name** | **Attribute Value** |
| Connection Name | HomeDirectory Endpoint |
| EnableAccountJSON | JSON to invoke the rest API to execute the PowerShell script with input parameters as   * HomeDirectory Locaition * SamAccountName * Domain |

**PowerShell:**

**The KPMG team will provide the PowerShell script for the following:**

1. Get input variables passed by Saviynt as stated in the above section
2. Commands to create HomeDirectory on NAS share location
3. Commands to set permissions to the HomeDirectory folder

### Delete

Saviynt will not take any action for deletion. The deletion of HomeDirectory directory will be addressed by the company.

Hence legal hold will not be accountable for HomeDirectory de-provisioning operations.

HomeDirectory Creation Flow

The diagram below explains the end to end flow for home directory creation.



Figure2. HomeDirectory Creation Flow

Appendix

### Technical Rules

Technical rules can be configured to grant birthright access to HomeDirectory based on specified user attribute criteria.

|  |  |
| --- | --- |
| **Rule Name** | **Function** |
| Birthright Provisioning for HomeDirectory | This rule is used for Birthright Provisioning of HomeDirectory for company users |