



Forest Druid

Version: 3.1 (and later)

Cohesity Cluster Integration Guide

December 2024 (2)

Legal Notice

Copyright © 2024 Semperis. All rights reserved.

All information included in this document, such as text, graphics, photos, logos, and images, is the exclusive property and contains confidential information of Semperis or its licensors and is protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions and international conventions. The information included in this document regarding processes, systems, and technological mechanisms is proprietary to Semperis and constitutes trade secrets of Semperis. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, translated into any language or computer language, distributed, or made available to others, in any form or by any means, whether electronic, mechanical, or otherwise, without prior written permission of Semperis.

Semperis is a registered trademark of Semperis Inc. All other company or product names are trademarks or registered trademarks of their respective holders.

This document is provided strictly on an "AS IS" basis without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Semperis and its staff assume no responsibility for any errors that may have been included in this document and reserve the right to make changes to the document without notice. Semperis and its staff disclaim any responsibility for incidental or consequential damages in connection with the furnishing, performance, use of, or reliance on this document or its content.

Contents

Preface	4
Document Revisions	4
Styles and Conventions used in this Document	5
Contacting Semperis	5
Forest Druid Cohesity Partnership Overview	6
Prerequisites	6
Integration Setups	7
Step 1: Run Forest Druid	7
Step 2: Collector Setup and Configuration	8
Step 3: Review Cohesity Cluster Results	12

Preface

Welcome to the *Cohesity Cluster Integration Guide for Forest Druid*. This document is intended for Security and IT professionals interested in including custom Cohesity Cluster security zones in the attack path analysis performed by Forest Druid.

The procedures in this integration guide are written with the presumption that you are already running Forest Druid and are familiar with the user interface. If this is the first time you are using Forest Druid, please review the *Forest Druid User Guide* to ensure the Forest Druid system requirements are met and that you have successfully unblocked the zip file to run the tool. The *Forest Druid User Guide* also explains the user interface in more detail so please refer to that guide if you are looking for more information about the Forest Druid screens and controls. The *Forest Druid User Guide* can be found in the Forest Druid download package or can be accessed from the [Semperis Community Documentation Portal](#).

Document Revisions

Table 1: Document Revisions

Product Version	Date	Document Revision	Comments
Forest Druid 3.1 (and later)	November 2024	1	Initial release
Forest Druid 3.1 (and later)	December 2024	2	Updated download information

Styles and Conventions used in this Document

The following styles are used in this document.

Table 2: Document conventions and styles

Typeface	Description
Bold	Used for names of UI elements, such as buttons, pages, menus, options, fields, and columns.
<i>Italics</i>	Used for references to documents that are not hyperlinks to other documents or topics. Also used for dialog names and to introduce new terms.
Monospace	Used for command-line input and code examples.
<PLACE HOLDER>	Brackets denote place holder text that is to be replaced with a user-specified value.

The following styles are used for notices:



NOTE:

This notice style is used to provide additional information and background overview.



IMPORTANT!

This notice style is used to present additional important information or warnings.

Contacting Semperis

Thank you for your interest in Semperis and Forest Druid. We are here to answer any questions you may have.

For product inquiries or feature requests, contact pk-community@semperis.com.

CHAPTER 1

Forest Druid Cohesity Partnership Overview

Forest Druid allows you to visualize the critical connection between Active Directory and Cohesity. This visibility is vital because if an attacker compromises the Active Directory environment, they could potentially compromise key identities in the Cohesity platform as well, gaining the ability to delete backups, alter policies, or disrupt data protection strategies.

Prerequisites

The Forest Druid-Cohesity collector uses specific API calls to the Cohesity Cluster's REST API and Forest Druid's backend engine; therefore, the following requirements must be met.

Table 3: Forest Druid requirements

Component	Requirement
Forest Druid	Minimum version: Version 3.1
PowerShell	Minimum version: Version 7.4

Table 4: Cohesity DataProtect requirements

Component	Requirement
Cohesity DataProtect	Minimum version: Version 7.1 (using V1 APIs)

CHAPTER 2

Integration Setups

The following procedures are written with the presumption that Forest Druid and Cohesity DataProtect are both successfully deployed.

The Forest Druid-Cohesity collector is only available upon request. Please request to download the package from the [Cohesity Solutions](#) page on the Semperis website.

**NOTE:**

After the initial synchronization of the Forest Druid-Cohesity collector, please keep the following in mind when making changes to Active Directory or Cohesity identities.

- *Changes made to Active Directory identities are captured by Forest Druid when you click **RESYNC DATA** in Forest Druid.*
- *Changes made to Cohesity identities (users/groups) require you to delete the existing Cohesity security zones from Forest Druid and rerun the `FD_CohesityCollectorGUI PowerShell` script to capture those changes. Use the **Delete** function on the **Configure Security Zones** page in Forest Druid to delete a security zone.*

Step 1: Run Forest Druid

Forest Druid must be run on an Active Directory domain-joined machine.

**NOTE:**

For convenience, we suggest that you rename the folder where the Forest Druid files were extracted to 'ForestDruid-Community'. This is because, the default import module path is set to 'C:\Users\$currentUser\Desktop\ForestDruid-Community\Backend\ApiTools\DruidApi\DruidApi.psd1'.

*You can use a different folder name; however, you must then edit the value in the **Import Module Path** field in the Cohesity Cluster interface when setting up the collector.*

1. Double-click the **ForestDruid.exe** file to run Forest Druid and generate a new access token, which you must provide during the Forest Druid-Cohesity collector setup.

If this is the first time you are using Forest Druid, please review the *Forest Druid User Guide* to ensure the Forest Druid system requirements are met and that you have successfully unblocked the zip file and extracted the contents of the ForestDruid-Community.zip file to a folder with write permissions on a domain-joined computer (Windows workstation or server).

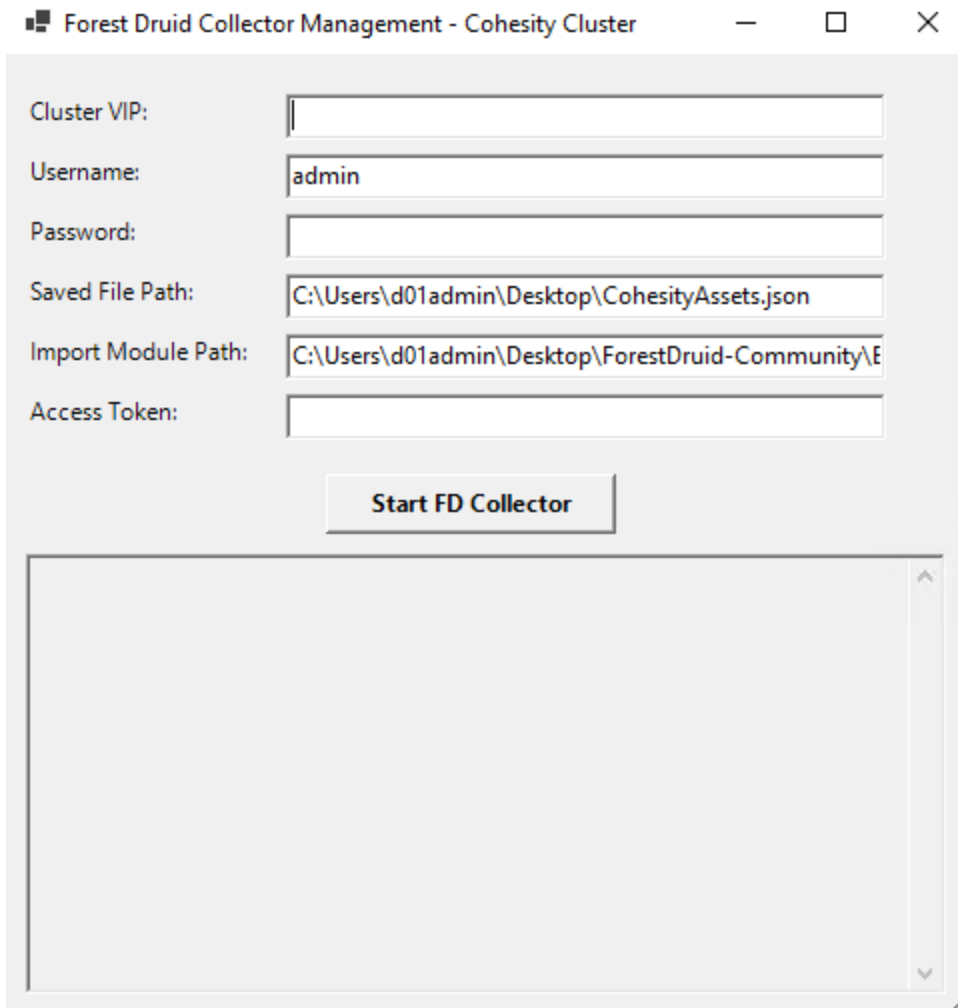
2. When prompted to select the data to be collected, select **Active Directory** and click **CONTINUE**.

At least one Forest Druid scan must be completed before adding the Forest Druid-Cohesity collector. Leave the Forest Druid interface running and proceed to [Step 2: Collector Setup and Configuration](#).

Step 2: Collector Setup and Configuration

1. Download the Forest Druid-Cohesity collector script (FDCohesityCollectorGUI.ps1).
2. Launch PowerShell 7 (pwsh.exe) and run the collector script, `FDCohesityCollectorGUI.ps1`.

The Cohesity Cluster interface displays.



Forest Druid Collector Management - Cohesity Cluster

Cluster VIP:

Username:

Password:

Saved File Path:

Import Module Path:

Access Token:

Start FD Collector

3. In the Cohesity Cluster interface, enter the following information:

- **Cluster VIP:** Enter the hostname or virtual IP (VIP) address of the Cohesity cluster. This VIP is assigned to the cluster when it was created.
- **Username:** Enter the name of the user who has permissions to view data on the Cohesity cluster. The current user will be populated in this field, but can be changed to any user with the View rule in Cohesity.
- **Password:** Enter the password associated with the specified user.
- **Saved File Path:** Optionally, enter the target location where data from the Cohesity machine (CohesityAssets.json) is to be saved on the local machine. This field is populated with the default file path, but can be changed as required.

- **Import Module Path:** Enter the path where the Forest Druid API that is used to import data from Cohesity resides. This field is populated with the default import module path, which is

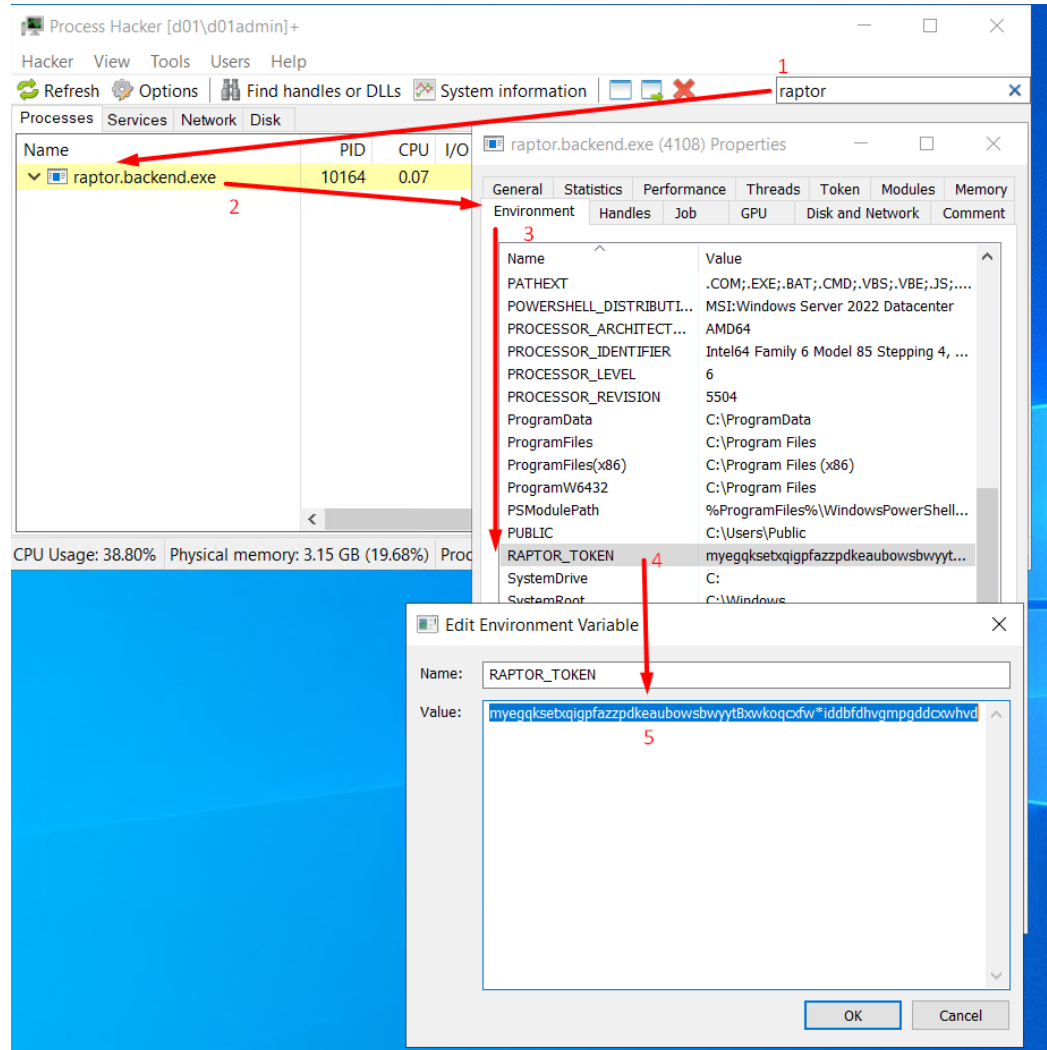
'C:\Users\$currentUser\Desktop\ForestDruid-Community\Backend\ApiTools\DruidApi\DruidApi.psd1'.

If you extracted the files to a different folder (other than 'ForestDruid-Community'), be sure to change the path to reflect the correct folder name.

- **Access Token:** Paste the Forest Druid access token.

This is a dynamic token that is created each time Forest Druid runs. It can be accessed by reading the RAPTOR_TOKEN environment variable of Forest Druid's backend engine (raptor.backend.exe). You can obtain the token using software applications such as Process Explorer (by Sysinternals) and Process Hacker 2.

The following example illustrates how to obtain the access token using Process Hacker.



1. In the **Search Processes** field, enter **raptor** to locate Forest Druid's backend engine (raptor.backend.exe).
2. In the **Processes** tab (left pane), select **raptor.backend.exe**. Right-click and select **Properties** to display the environment variables for the backend process.
3. In the **Environment** tab on the *Properties* dialog, scroll down to locate the **RAPTOR_TOKEN**. Select the **RAPTOR_TOKEN** variable and click **Edit**.
4. On the *Edit Environment Variable* dialog, copy the value and click **OK**.

This is the value you will paste into the **Access Token** field on the Cohesity Cluster interface.

4. After entering all the required information, click **Start FD Collector**.

The progress pane at the bottom of the Cohesity Cluster interface allows you to view the steps being performed, including any errors that may be encountered.

**NOTE:**

If an error is encountered, you may be asked to copy the events posted in the progress pane to assist us with troubleshooting the issue. If you encounter an error, ensure you copy the contents of the progress page before you close the Cohesity Cluster interface.

5. Wait for the collector to finish running. The duration may vary based on the size of the Cohesity cluster.

You will see a **Process completed! Please click the 'RESYNC DATA' button on Forest Druid** message.


6. Back in Forest Druid, click the **RESYNC DATA** button in the upper right corner of the application header.

Step 3: Review Cohesity Cluster Results

Once the collection process has completed and has been synchronized in Forest Druid, the following custom security zones are displayed in Forest Druid:

- **Cohesity AD Sources:** This security zone provides a comprehensive inventory of all client machines and servers protected by Cohesity DataProtect. This zone gives you a clear view of the assets that are included in the backup ecosystem, ensuring that no critical systems are inadvertently left unprotected. By maintaining this security zone you can more effectively manage your data protection strategy, facilitate compliance efforts, and optimize resource allocation for your backup infrastructure.
- **Cohesity Control Plane:** This security zone encompasses all user accounts, group accounts, and machine identities with elevated privileges and roles to the Cohesity ecosystem. This zone is critical for protecting the integrity of the backup system itself. By isolating these high-privileged accounts, you can apply stricter security controls and monitoring, reducing the risk of unauthorized access to critical backup functions. By clearly defining and monitoring this security zone, you can better defend against threats and safeguard your ability to recover from disasters or cyberattacks.

Verify that the Cohesity cluster results (custom security zones listed above) are being displayed in the following screens within Forest Druid:

- **Defense Parameter:** After the scan completes, the **Defense Perimeter** screen displays privilege escalation relationships to assets in security zones, including the Cohesity security zones that rely on Active Directory to change and control backup activities. From this screen, you can classify objects as part of a security zone or identify objects that are in violation of the security model that need to be addressed.
- **Attack Paths:** Open the **Attack Paths** screen to view risky attack paths within your environment leading to Cohesity clusters. Using the list and graph in the **Attack Paths** screen you can quickly see identities with escalation relationships with objects in a security zone.
- **Configure Security Zones:** Click the  button in the application header to access the **Configure Security Zones** page. From this page you can view all security zones and a list of the objects that are being protected in each zone.

Once you have identified any dangerous access points, you can start to remediate the security risks by removing excessive privileges, closing off paths to threat actors that target sensitive business data stored in Cohesity clusters.