AWS Marketplace RidgeShield Smart Center Deployment Guide

Smart Center Version V1.1.9

Contact Information:

Ridge Security Technology Inc.

1900 McCarthy Blvd STE 112

Milpitas, CA 95035
United States

www.ridgesecurity.ai

Table of Contents

Chapter 1. Introduction

Overview

This installation guide describes how to install and deploy of the RidgeShield instance via AWS Marketplace.

Applicable Products

The RidgeShield Smart Center is your first line of defense, providing zero-trust micro-segmentation technology to protect cloud workloads, regardless of whether they are deployed on-premises, in hybrid cloud, or multi-cloud environments. With RidgeShield, organizations can ensure the security posture of their network against sophisticated security threats.

This manual describes the installation and initial deployment of the RidgeShield Smart Center product of Ridge Security Technology via AWS marketplace, hereafter referred to as "Ridgeshield", or "the Ridgeshield system".

Audience

This document is directed at the administrator responsible for installing, deploying and upgrading the RidgeShield system. The content assumes a working knowledge of server operating systems , scripts and AWS operation permission.

Product Version

RidgeShield product versions covered by this document are listed below.

Product Name	Product Version
RidgeShield Smart Center	V1.1.9.x.x
RidgeShield Agent	V2.1.2

Additional Resources

Companion documents used with this manual include:

- RidgeShield Smart Center User Manual

All software images mentioned in this document (Agents) are downloadable from https://ridgesecurity-public.s3.us-west-1.amazonaws.com/sagent-2.1.2.5.357/sagent-2.1.2.5.357.zip (No credential required)

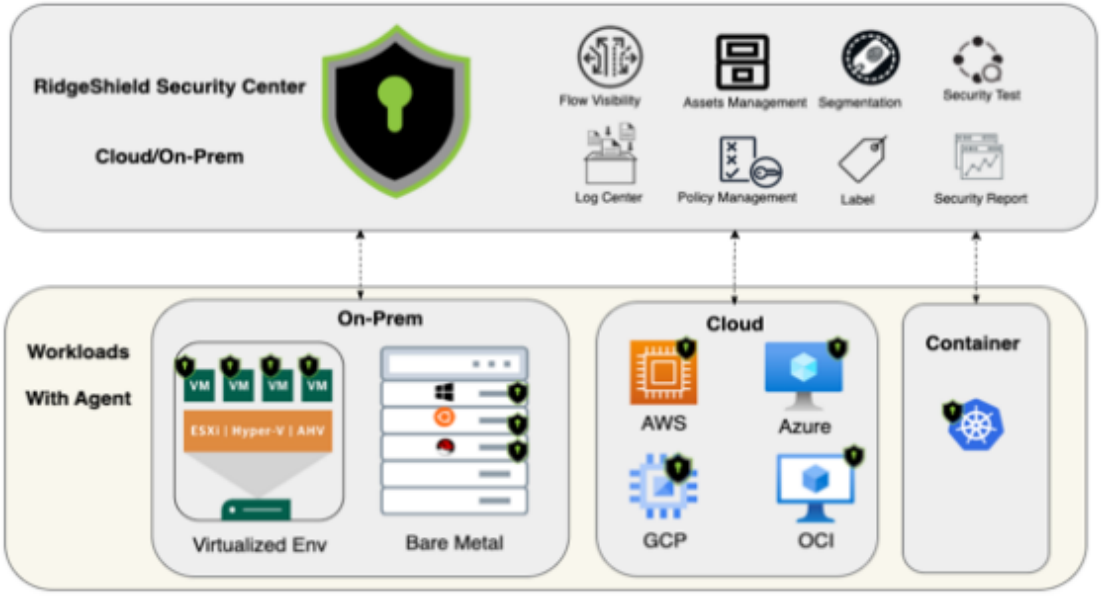
Chapter 2. Product Overview

RidgeSecurity RidgeShield enables zero-trust micro-segmentation cloud workload protection with an adaptive, unified security architecture and innovative host protection technologies, including integrated security testing. This approach integrates prediction, defense, monitoring and response to help customers with diverse business environments such as public, private and/or hybrid clouds to implement comprehensive security protection for digital enterprise assets.

Product Architecture

RidgeShield is a Smart Center that manages and monitors cloud workloads and traffic. An Agent is associated with each workload. The Agent registers with the RidgeShield Smart Center and monitors the workload at all times. Traffic flows between workloads are constantly monitored allowing you to view all sources and destinations of workload traffic.

Agents are installed by running a script on the workload, creating an association between the Agent and the workload referred to as a pairing. The same Agent can be paired with multiple workloads. Agents are OS and OS-version dependent. Linux and Windows OS variations are supported by RidgeShield.



Label-based Micro-Segmentation

At the core of any successful zero-trust strategic initiative lies ensuring that least-privilege access is achieved for every device, endpoint, workload and identity, whether human or machine. A micro-segmentation design isolates identities into small segments. By treating every identity as a separate segment, granular context-based policy enforcement is achieved for every attack surface, protecting against lateral movement through the network.

RidgeShield characterizes workloads by four attributes used as labels. These labels must be created during the RidgeShield installation process.

- The **Location** label is the *site* associated with the workload. It can be a geographic location, such as SanJose, NewYork, LosAngeles, or it can be a virtual cloud site such as AWS, Azure or GCP.
- The **Environment** label is the *operational environment* associated with the workload. It can denote the department or the business view of the workload. Examples include Engineering, Production, Development, and Human Resources.
- The **Role** label is the *function* associated with the workload, such as web service, database or authentication server.
- The **Application** label is the *service* associated with the workload, such as ERP, Billing, or Office Automation (OA).

Scope and Grouping

Three of the attributes, or labels, associated with each workload—Location, Environment, and Application—together form the scope of the workload or policy. Workloads (or policies) with the same scope—in other words, workloads (or policies) with the same set of these three labels—form a group or segment. Traffic policies are constructed separately for traffic **within** the group (segment), and traffic **between** groups (segments).

Chapter 3. Getting Started from AWS marketplace

Deployment Requirements

Operator should have at least EC2 admin permission and also be able to reach out to AWS marketplace to deploy 3rd party vendor's cloud offerings.

RidgeShield Cloud Offering

There are two types of offering in AWS marketplace,

- **RidgeShield SmartCenter (free trial):** Free Monitoring Licenses by default (support 5 workloads, can request to support up to 20 workloads)
- RidgeShield SmartCenter (BYOL): Need to bring customer own license to activate the RidgeShield services.

RidgeShield License

RidgeShield SmartCenter (Free trial) does not need to request license. By default, 5 monitoring licenses embedded.

License request process is just applicable to for RidgeShield SmartCenter (BYOL).
Purchasing a license is based on the machine code of the server you want to use to install the RidgeShield Smart Center.

- Find and copy down the machine code of your server. (Setting→License→Device info)
  - Device info is the machine code.
- Provide the machine code to Ridge Security (support@ridgesecurity.ai) and indicate a request of RidgeShield license.
- After license request is approved, Ridge Security issues a License Key that you use during the installation steps to activate RidgeShield software functionality on your server.

Available license types include *Monitor* and *Full Control*, and these include system functionality as shown below.

The *Monitor* licenses enable your system to monitor traffic and to see the potential effect of configured policies, but these licenses do not enable active control (permit, deny) of traffic. The *Full Control* license allows active control of traffic with policies. All licenses have an expiry date and must be renewed upon expiry to continue system operation. The *Free Trial* license includes only 5 workloads as assets with Monitor mode.

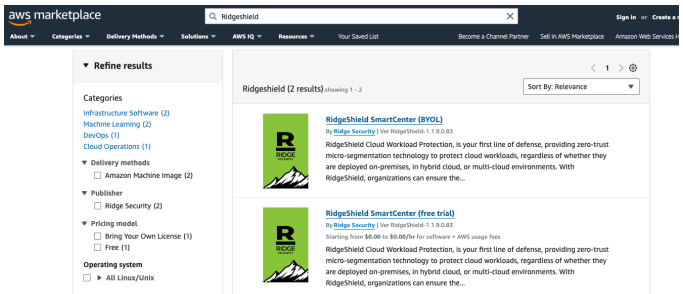
Chapter 4. SmartCenter Server Deployment Steps

Installing the RidgeShield Smart Center software includes the steps detailed in this chapter. All software images mentioned in this document (RidgeShield Agents) are downloadable from https://ridgesecurity-public.s3.us-west-1.amazonaws.com/sagent-2.1.2.5.357/sagent-2.1.2.5.357.zip

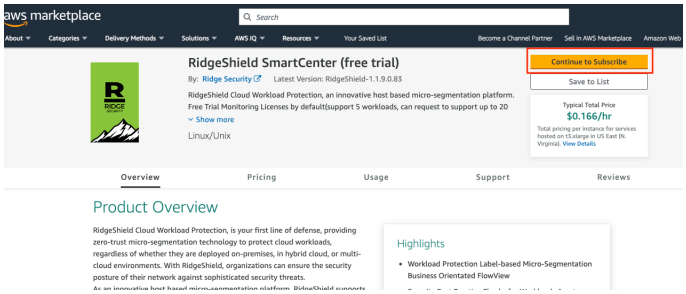
For RidgeShield SmartCenter (BYOL), you must purchase a license from Ridge Security to activate the software images.

Step 1: Find RidgeShield Smart Center in AWS marketplace

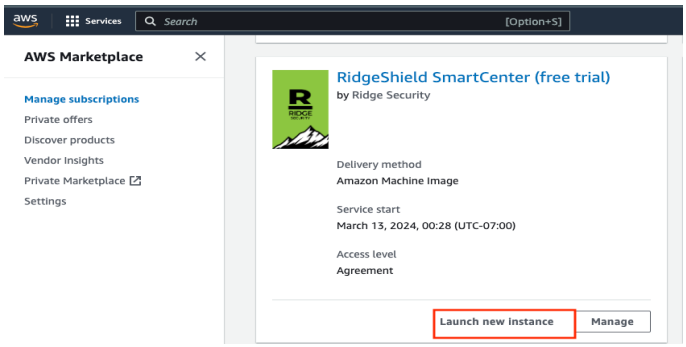
- ☐ Open web browser and visit https://aws.amazon.com/marketplace
- ☐ Use "RidgeShield" in the search bar to navigate to RidgeShield Cloud offerings.



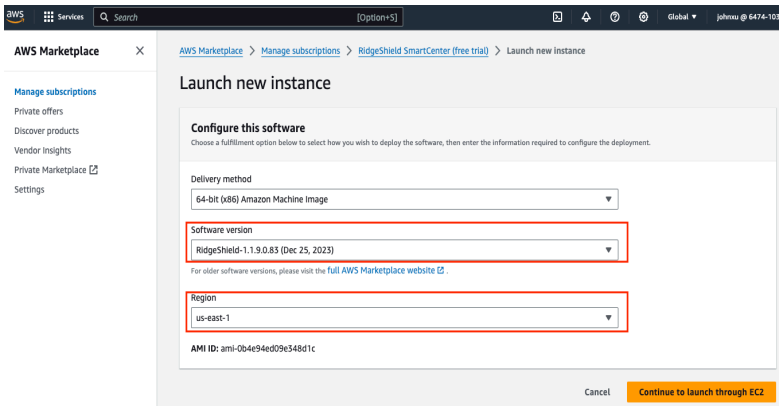
- ☐ Select RidgeShield SmartCenter and subscribe



- ☐ Launch the new instance



- Select the Version and Region to deploy RidgeShield



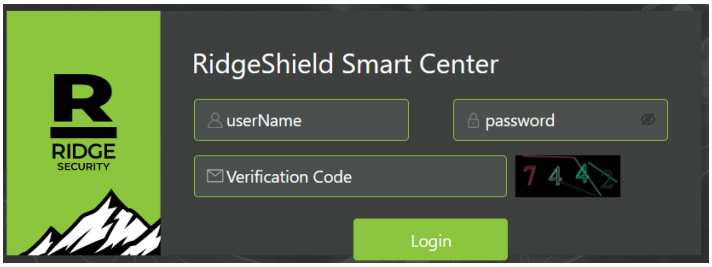
- Launch through EC2.
  - EC2 instance type is t3.xlarge or t3.2xlarge.
  - Disk space, at least 100G
  - Security group, by default, need to allow SSH (troubleshooting purpose) and Https (Access requirement).

Step 2: Login to RidgeShield

After deployment is done via AWS, a new instance will be shown up in EC2. Following a successful RidgeShield installation, note down the IP address of the server and enter it into your browser's address bar using the format:

https://192.168.100.100

After pressing **Enter**, you are presented with the RidgeShield login page. When logging in for the first time, the page may take a few moments to load.



> **Note**: When logging into the system for the first time, and there is not yet any data in the system, the **Dashboard** display is empty.

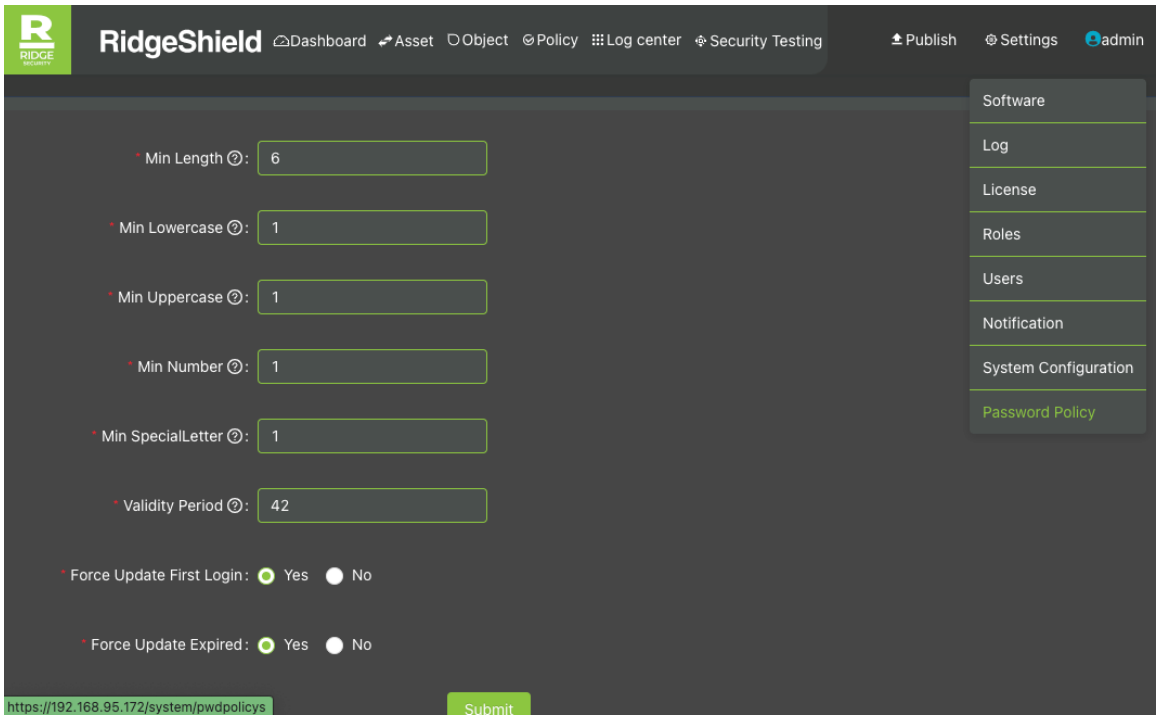
If you are login into RidgeShield for the first time, use the default credentials given below.

- Default login username: **admin**
- Default login password: **RidgeShield@666**

Step 3: Change admin Password

Navigate to **Settings -> Password Policy** in the top-right toolbar to see a display of the currently defined password policy—applicable to all users—in the system.

1. Review the default system password policy and make any changes you wish to comply with your organization's password policy.



The password strength demanded by user accounts is based on the system's password policy. Parameters related to password strength that you can configure include:

- **Min length:** The minimum length of the current password. The default is 6.
- **Min Lowercase:** The minimum number of lowercase letters that must be included in the password. The default is 1.
- **Min Uppercase:** The minimum number of uppercase letters that must be included in the password. The default is 1
- **Min Numbers:** The minimum number of numeric characters that must be included in the password. The default is 1.
- **Min Special Letter:** The minimum number of special characters that must be included in the password. The default is 1. Special characters allowed are shown by clicking on the ? icon next to the field label.
- **Validity period:** The number of days that the password is valid for.
- **Force Update First Login**: Yes or No.
- **Force Update Expired**: Yes or No.

Note: Overall, the password must conform to the following formula:

Minimum length ≥ (lowercase letters + uppercase letters + numbers + special characters)

If a password entered does not meet all the requirements, an error message is displayed. Modify the password to comply with all the rules then click **Submit** again.

2. Change the password for the **admin** username.

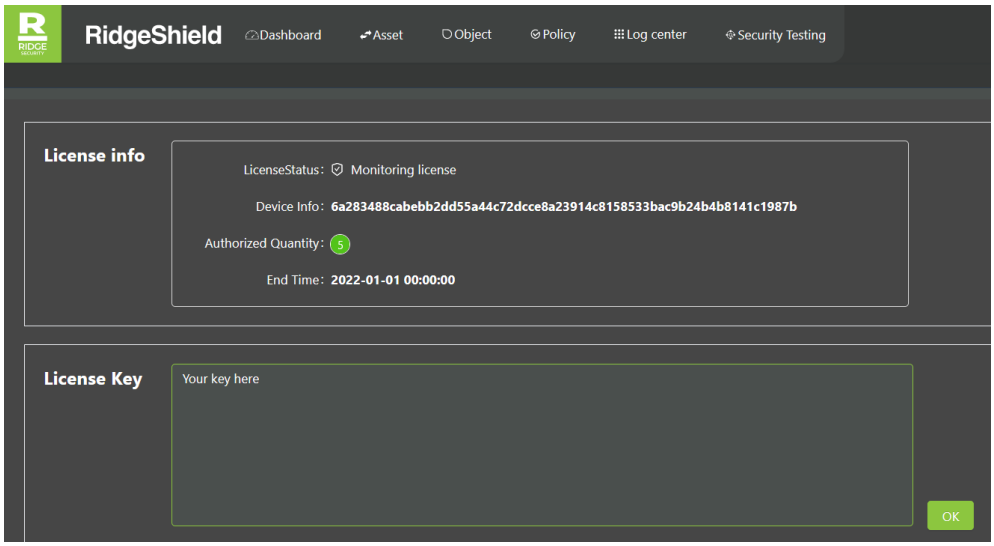
Navigate to **Settings -> Users** in the top-right toolbar to see a display of the currently defined users (login accounts) in the system.

Step 4: Install RidgeShield License (Just for BYOL)

Note: this step is only appliable to RidgeShield SmartCenter (BYOL). For RidgeShield SmartCenter (Free), please skip this step.

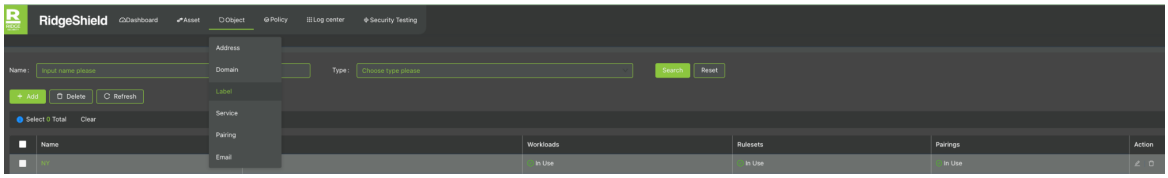
To enable functionality on your RidgeShield system, it must have a license installed.

When you have received your license key from Ridge Security, navigate to **Settings -> License**, enter your key in the **License Key** field and click **OK** as shown below. The device ID (shown below as Device Info) must match the one you provided to Ridge Security before the license key was issued.



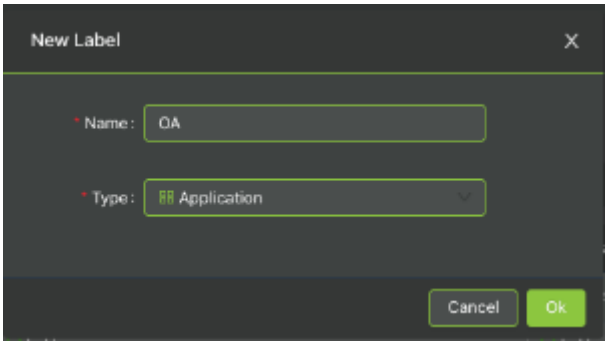
Step 5: Define Labels

Navigate to **Object -> Label**, as shown below, to define the appropriate *Location*, *Environment*, *Role* and *Application* labels for your organization. See Chapter 2 Label-based Micro-Segmentation for an explanation of the use and meaning of labels.

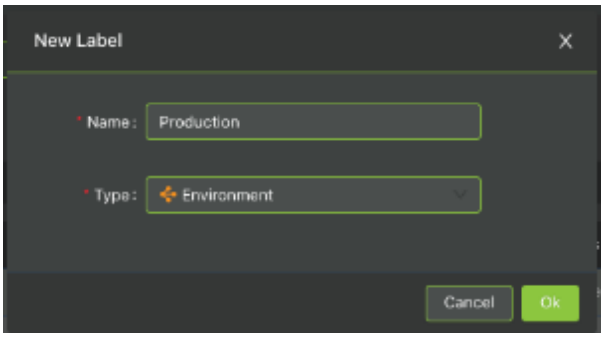


In the example scenario in this step, we want to set up a configuration with three labels: **Location** NY, **Environment** Production, and **Application** OA.

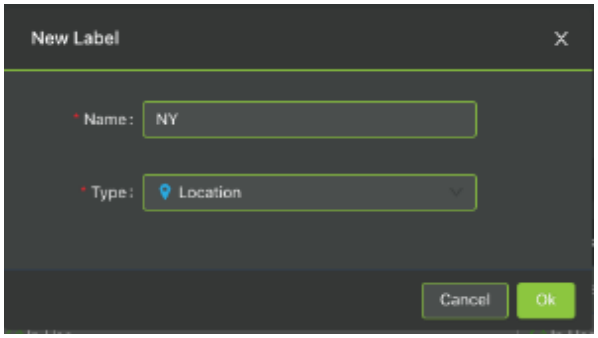
Click the **Add** button, and in the pop-up window, enter *OA* as the label **name**, and select *Application* as the label **type** as shown below. Then click **OK**.



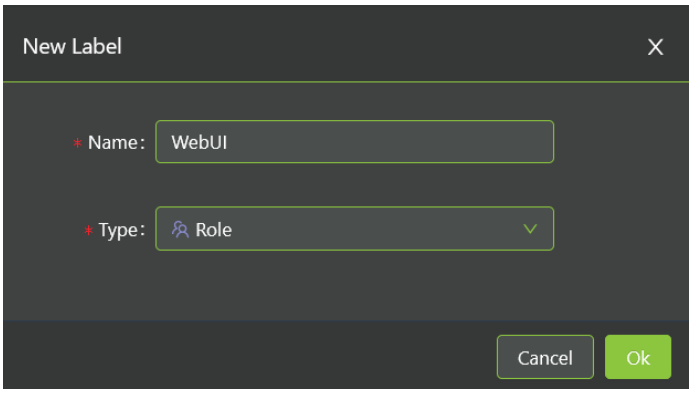
Click the **Add** button again, and in the pop-up window, enter *Production* as the label **name**, and select *Environment* as the label **type** as shown below. Then click **OK**.



Click the **Add** button again, and in the pop-up window, enter *NY* as the label **name**, and select *Location* as the label **type** as shown below. Then click **OK**.



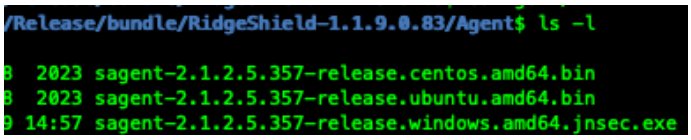
Click the **Add** button again, and in the pop-up window, enter *WebUI* as the label **name**, and select *Role* as the label **type** as shown below. Then click **OK**.



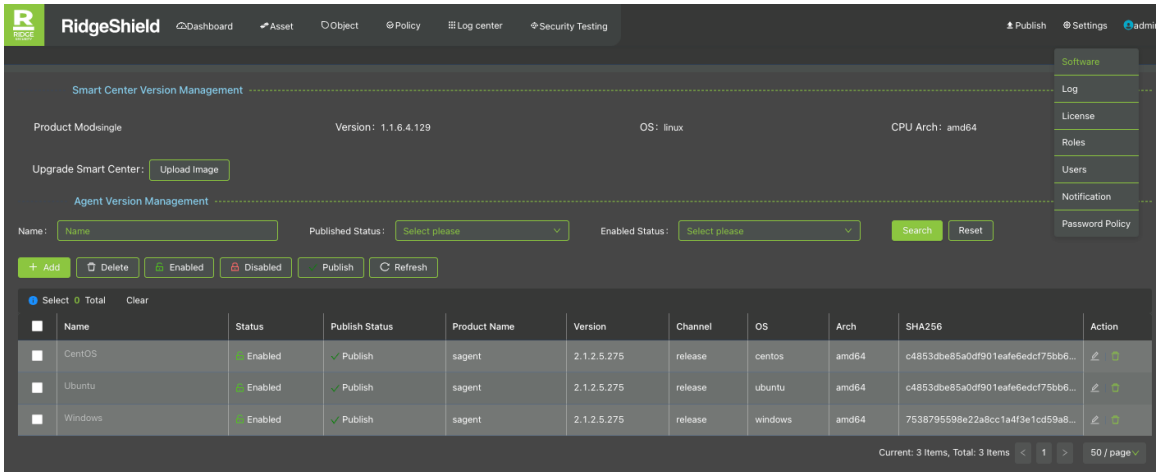
Step 6: Install Agent Software

Download the OS-specific Agent software images at https://ridgesecurity-public.s3.us-west-1.amazonaws.com/sagent-2.1.2.5.357/sagent-2.1.2.5.357.zip.

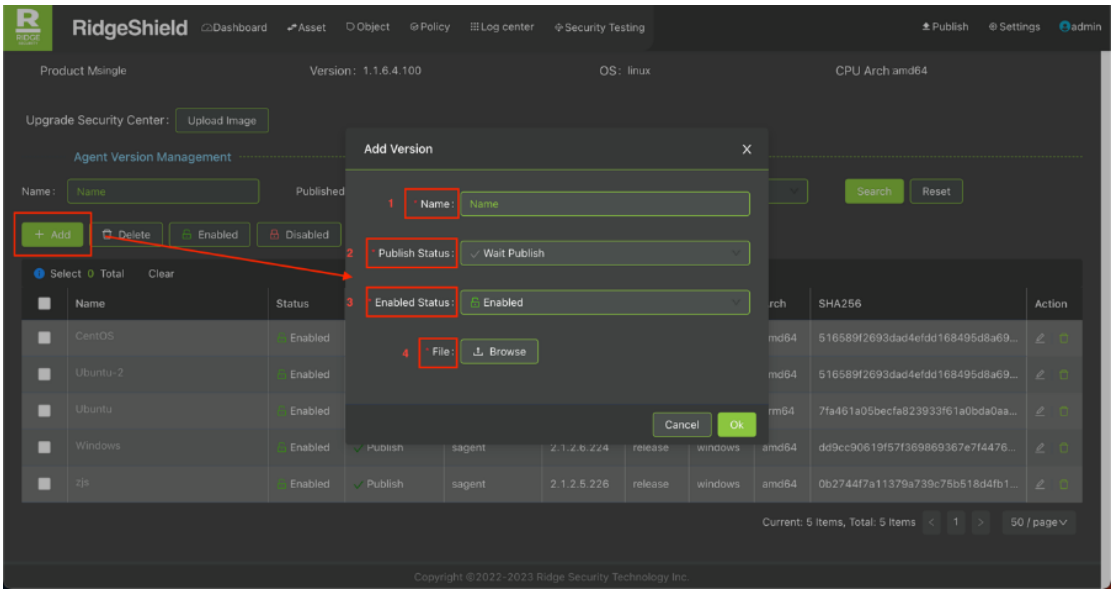
RidgeShield Agent supports Windows and Linux (including RPM-based RedHat, CentOS, SUSE, and Debian-based Ubuntu and Kali). Unzip the agent zip file and get three agents images.



Navigate to **Settings -> Software** in the top-right toolbar to see a display of currently installed software versions, including the RidgeShield Smart Center software as well as Agent software.

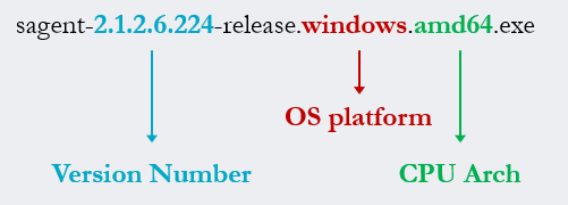


Click the **Add** button to add a new version of Agent software, as shown below. Fill in the fields on the pop-up window, including the version name, software release status (the default is *Wait Publish*), the status (the default is enabled), and select an Agent file to upload.



Note: There are strict requirements of the upload file name. The required format is: sagent-2.1.2.6.224-release.windows.amd64.exe

The information encoded in the file name format is given below.



Agent software must be published before it can be used to create an active Agent for a workload to be onboarded. Publishing the Agent software makes it available and active in the system. To publish an Agent software version, click on the **checkbox** for the Agent row that you want to select and click on the **Publish** button. You can mark the checkboxes on multiple rows and **Publish** all the selected Agent software versions at once.

Step 7: Onboard Workloads

Onboard your workload(s) by creating and uploading a pairing script for each workload and executing the script on the workload server. This creates an Agent for the workload and makes it a managed asset in the system that can then be seen in the asset display as well as the Business Topology.

Example Scenario Description

To illustrate the installation procedure, consider the following example scenario.

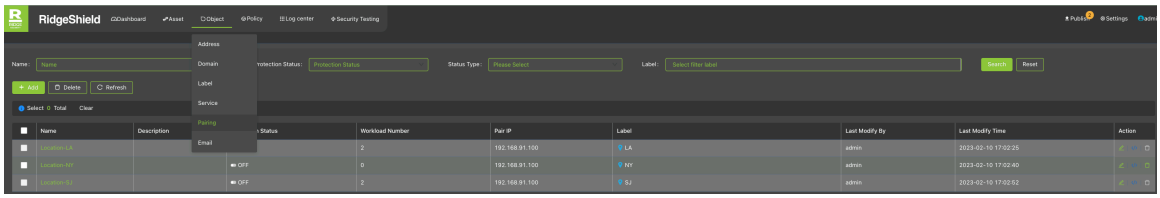
A RidgeShield system must be installed to protect two VMs running an OA application. There is an Office Automation (OA) application in the New York production area. The OA application is deployed with two virtual machines (VMs), one running web services and the other one running the database.

- The web services VM has a Windows Server 2012 R2 OS, and its IP address is 192.168. 91.116
- The database VM has a Linux RedHat 7 OS, and its IP address is 192.168. 91.115. The Linux system already has IPSET components installed.

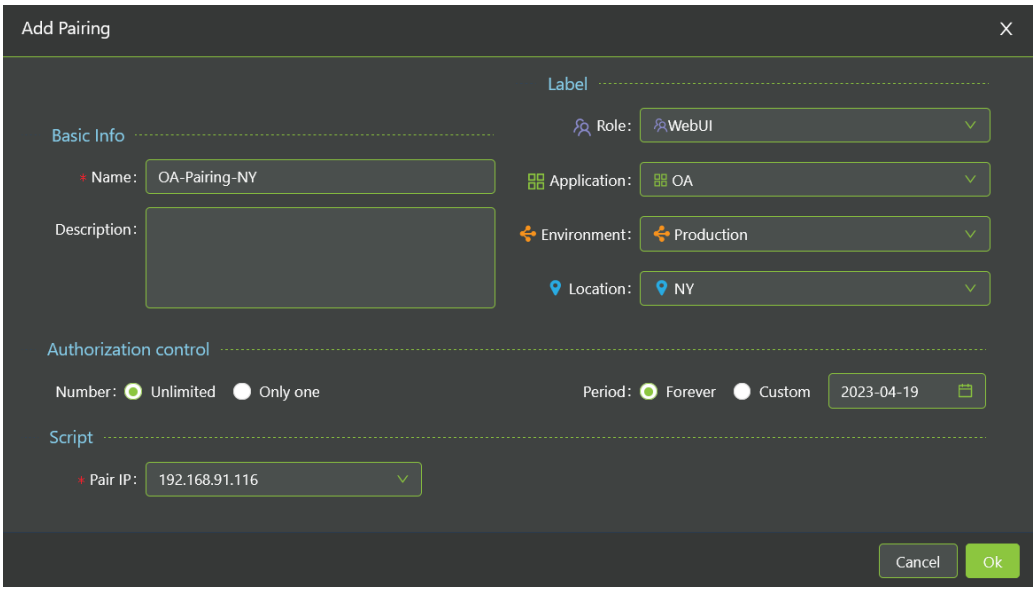
Step 7a: Create Pairing Scripts

To create, install and associate an Agent for the OA example application, you must first create a pairing file. Once successfully installed, RidgeShield can monitor and manage the OA application VM through the Agent (pairing file).

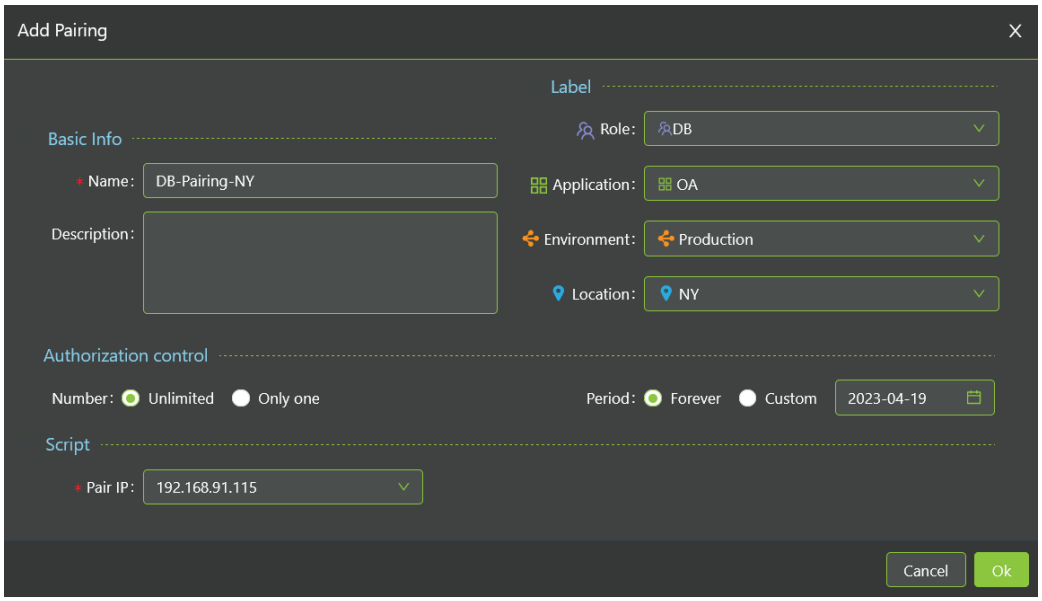
Navigate to **Object -> Pairing** as shown below to create a pairing script for the OA web server.



Click the **Add** button, and in the pop-up window, enter *OA-pairing-NY* as the pairing **name**, select *OA* as the **Application label**, select *Production* as the **Environment label**, select *NY* as the **Location label**, select *WebUI* as the **Role label**, and enter *192.168.91.116* as the **Pair IP** address, as shown below. Then click **OK**.

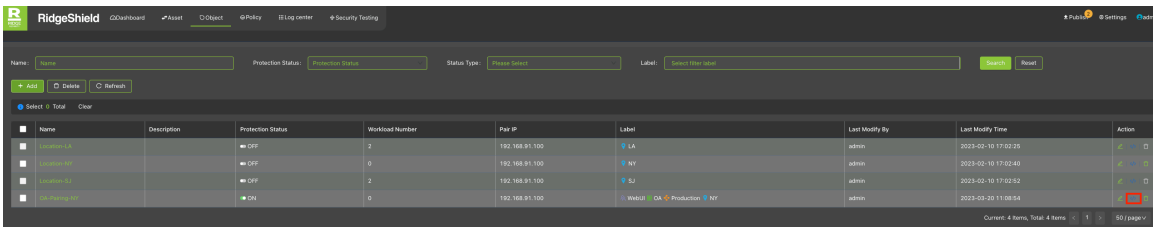


Following the same steps as given above for the OA web server, create a pairing for the DB Server. Enter *DB-Pairing-NY* as the pairing **name**, select *OA* as the **Application label**, select *Production* as the **Environment label**, select *NY* as the **Location label**, select *DB* as the **Role label**, and enter *192.168.91.115* as the **Pair IP** address, as shown below. Then click **OK**.

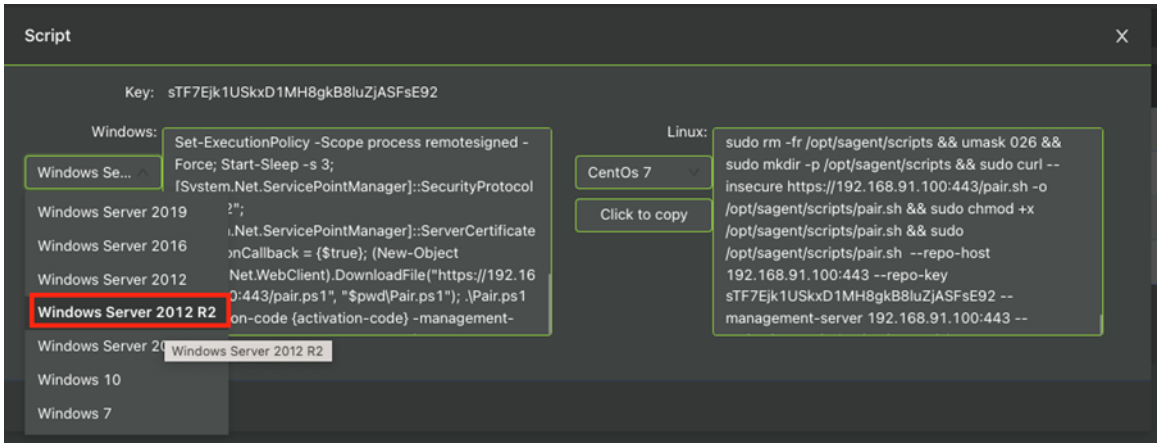


Step 7b: Upload the Pairing Scripts

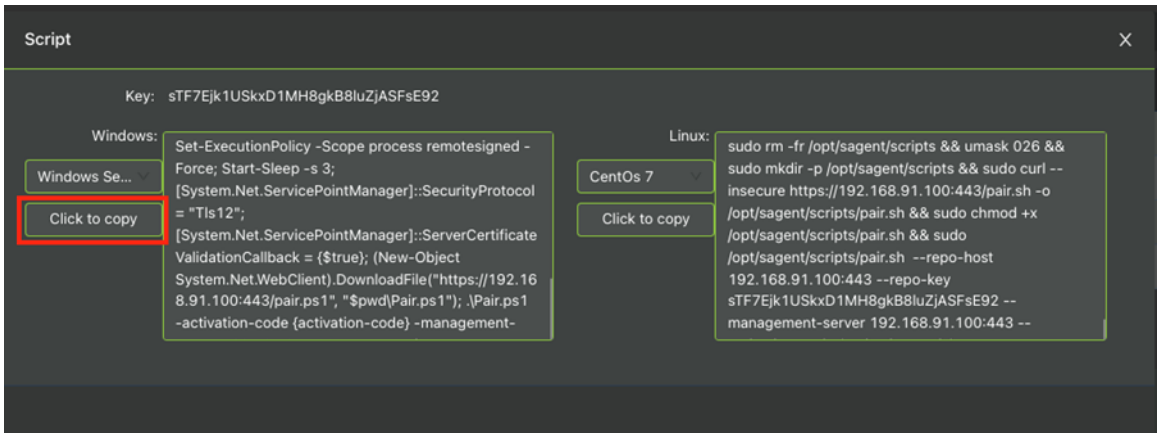
On the **Object -> Pairing** display, click on the pairing script button on the far right of the row for the **OA-Pairing-NY** pairing, as shown below.



On the pop-window that appears, sample pairing scripts are shown. Select **Windows Server 2012 R2** (from the Windows drop-down box on the left of the screen) to match the OS of the web server. This populates the display with the appropriate pairing script for the selected OS server version.

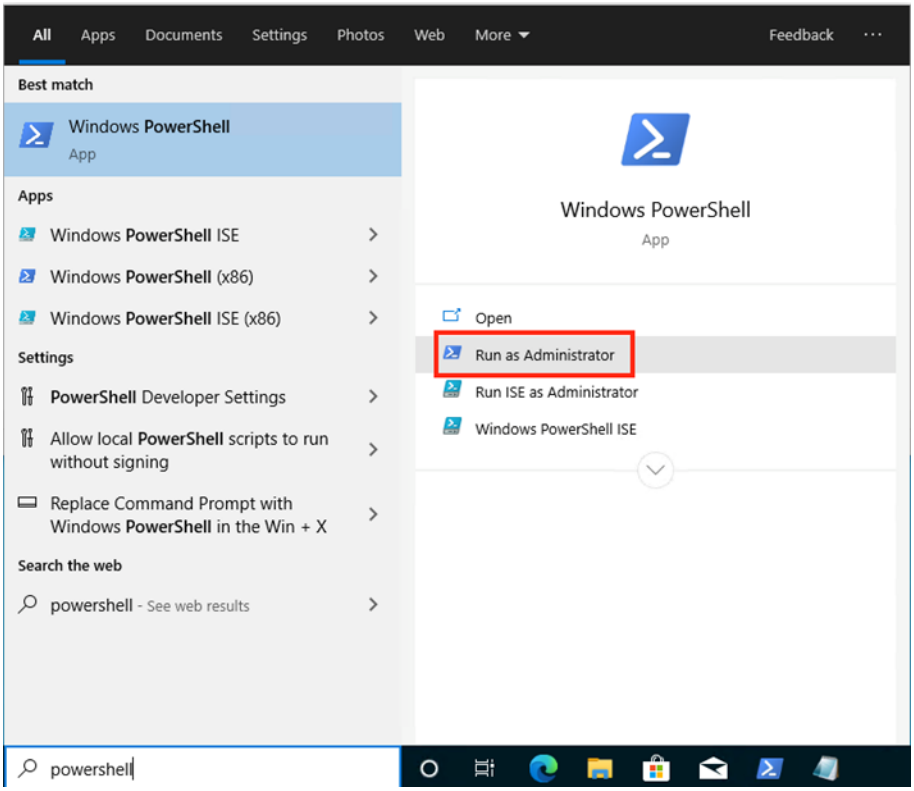


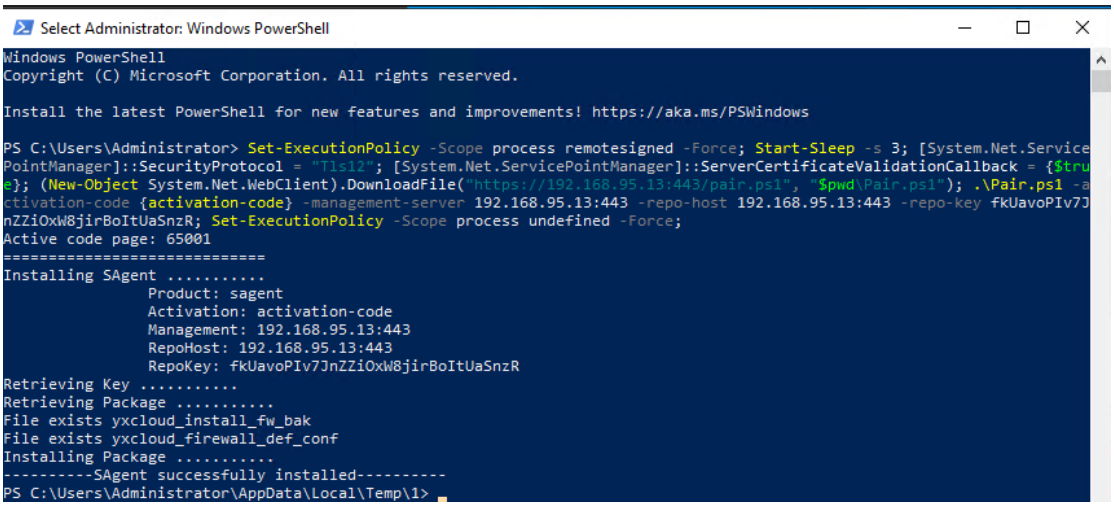
Click the **Click to Copy** button to copy the pairing script.



Step 7c: Execute the Pairing Scripts to Bring the Workloads Online

Log remotely into the web server (IP address 192.168.91.116 in the example scenario), open a PowerShell (as an administrator), and paste in the pairing script. Then execute the script, as shown below.

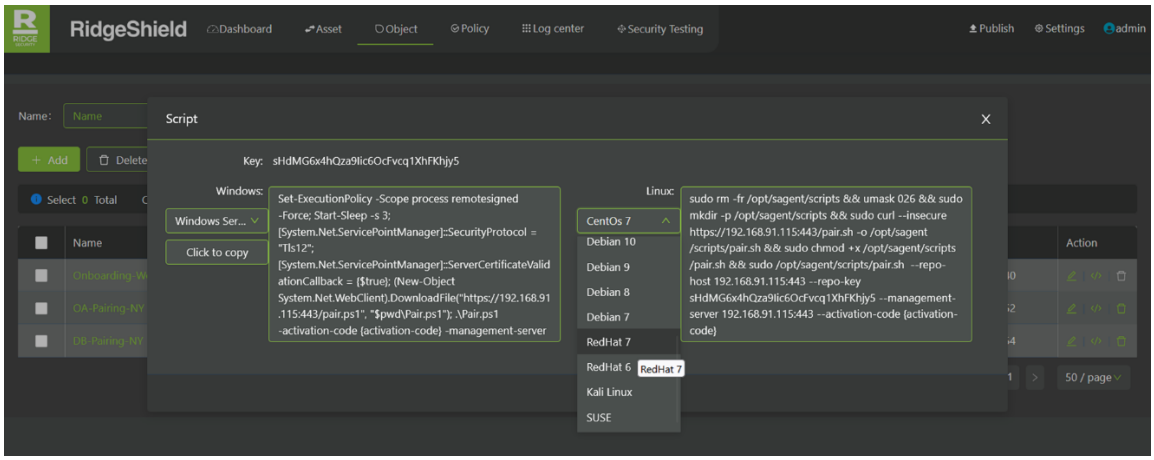




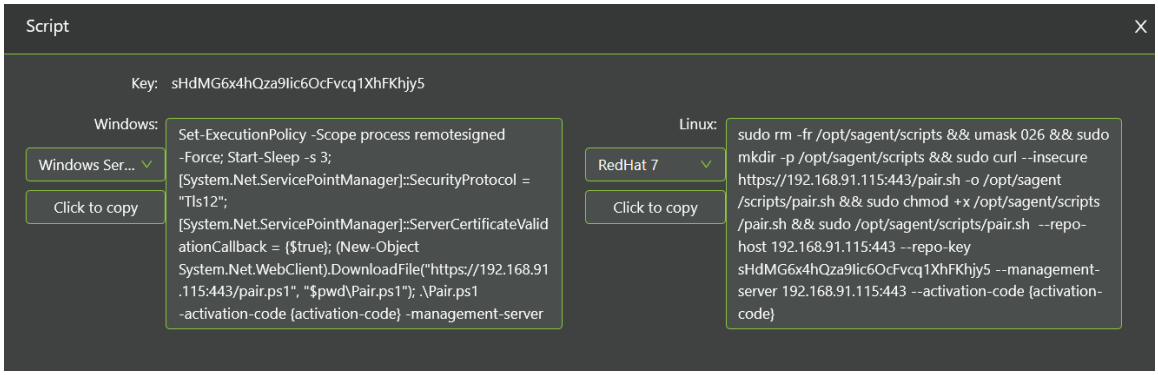
Follow the same steps as above to bring the database server online.

On the **Object -> Pairing** display, click on the pairing script button on the far right of the row for the **DB-Pairing-NY** entry.

On the sample pairing script pop-window for the **DB-Pairing-NY** pairing. Select **RedHat 7** (from the Linux drop-down box on the right of the screen) to match the OS of the database server. This populates the display with the appropriate pairing script for the selected OS server version.



Click the **Click to Copy** button to copy the pairing script.



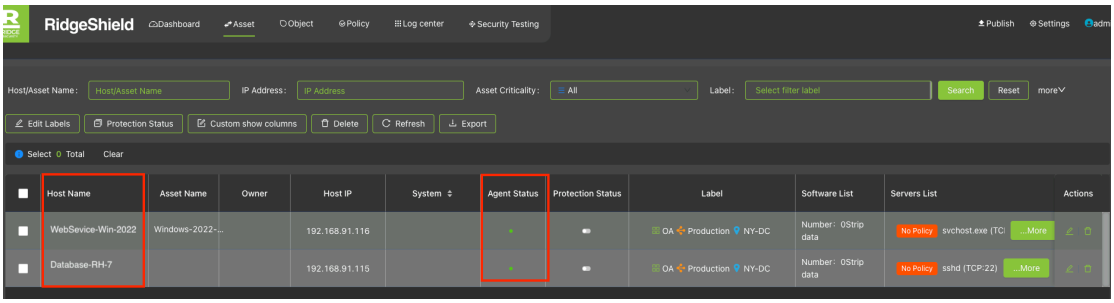
Log remotely into the DB server (IP address 192.168.91.115 in the example scenario) and paste in the pairing script at the command prompt. Then execute the script, as shown below.

```
[root@rh7-linux-1 ~]# sudo rm -fr /opt/sagent/scripts && umask 026 && sudo mkdir -p /opt/sagent/scripts &
& sudo curl --insecure https://192.168.95.13:443/pair.sh -o /opt/sagent/scripts/pair.sh && sudo chmod +x
/opt/sagent/scripts/pair.sh && sudo /opt/sagent/scripts/pair.sh  --repo-host 192.168.95.13:443 --repo-key
 fkUavoPIv7JnZZiOxW8jirBoItUaSnzR --management-server 192.168.95.13:443 --activation-code {activation-cod
e}
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10770  100 10770    0     0  12917      0 --:--:-- --:--:-- --:--:-- 13022

----------Installing SAgent----------
ARCH: amd64
OS: Red_Hat
Key downloading......

Version downloading......

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11.1M    0 11.1M    0     0  2084k      0 --:--:--  0:00:05 --:--:-- 2814k
----------SAgent successfully installed----------
[root@rh7-linux-1 ~]#
```

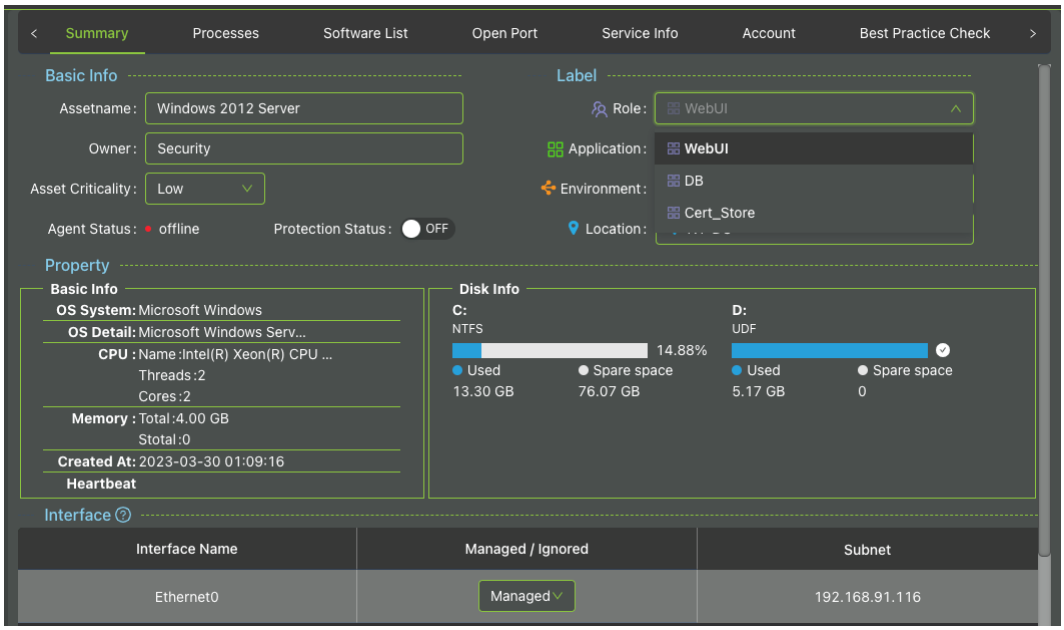
```
[root@rh7-linux-1 ~]# sudo rm -fr /opt/sagent/scripts && umask 026 && sudo mkdir -p /opt/sagent/scripts &
& sudo curl --insecure https://192.168.95.13:443/pair.sh -o /opt/sagent/scripts/pair.sh && sudo chmod +x
/opt/sagent/scripts/pair.sh && sudo /opt/sagent/scripts/pair.sh  --repo-host 192.168.95.13:443 --repo-key
 fkUavoPIv7JnZZiOxW8jirBoItUaSnzR --management-server 192.168.95.13:443 --activation-code {activation-cod
e}
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10770  100 10770    0     0  12917      0 --:--:-- --:--:-- --:--:-- 13022
                                                                          Get the script
----------Installing SAgent----------
                                                                          Execute the script
ARCH: amd64
OS: Red_Hat
Key downloading......

Version downloading......

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11.1M    0 11.1M    0     0  2084k      0 --:--:--  0:00:05 --:--:-- 2814k
----------SAgent successfully installed----------
                                                                          Install successfully
[root@rh7-linux-1 ~]#
```

Step 8: Ensure Correct Labels for Workloads

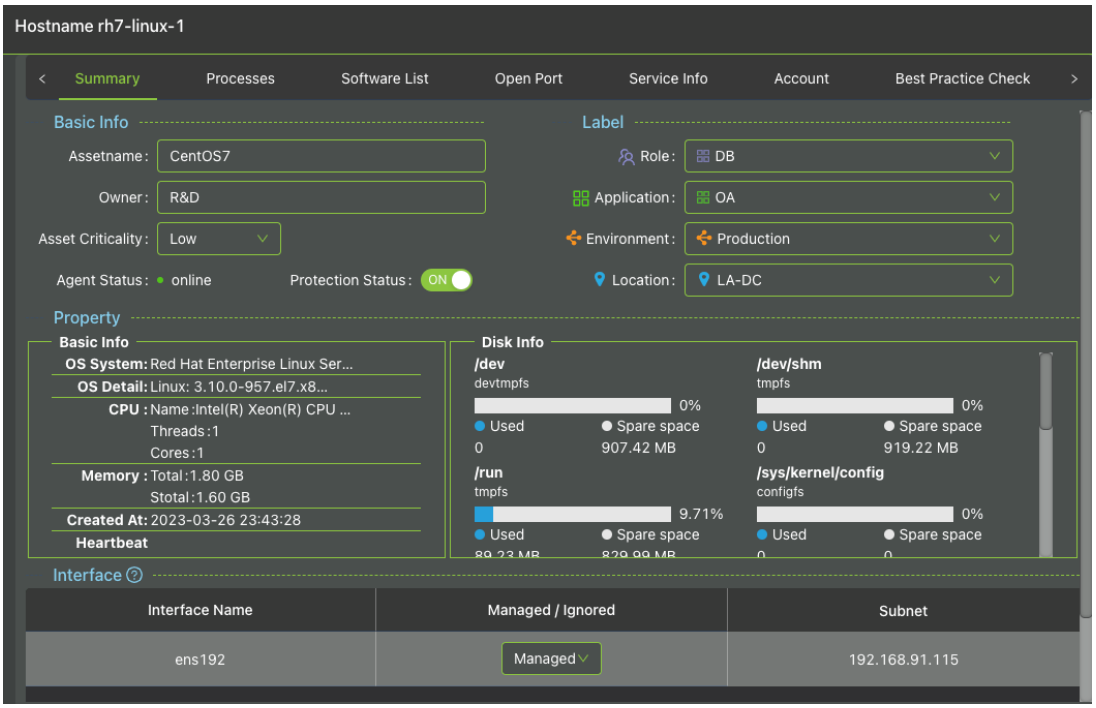
Navigate to the **Asset** display to verify that the OA web server with IP 192.168.91.116 and the OA DB server with IP 192.168.91.115 have been successfully brought online, as shown below.



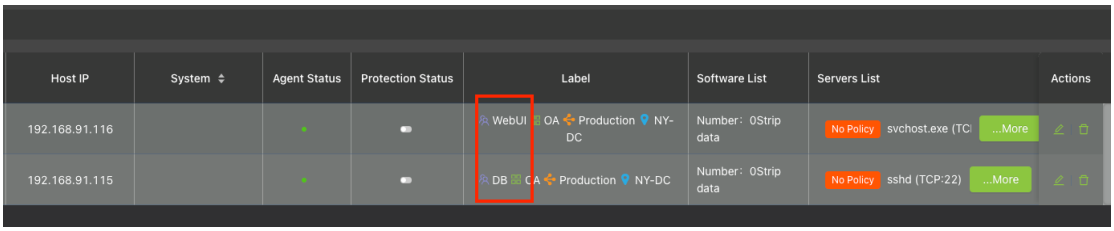
Click on the **Edit** button of the OA web server name in the **Asset** display to show the details of the asset as shown below.



Click on the **Edit** button of the OA DB server name in the **Asset** display to show the details of the asset as shown below.

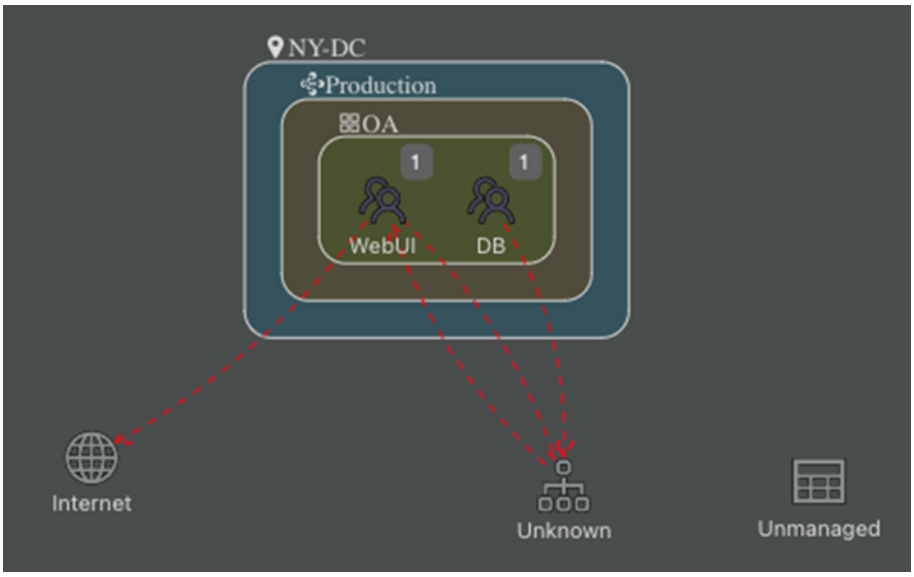


Verify that the role label settings are correct by checking the **Asset** summary display, as shown below.



Step 9: View the Business Topology

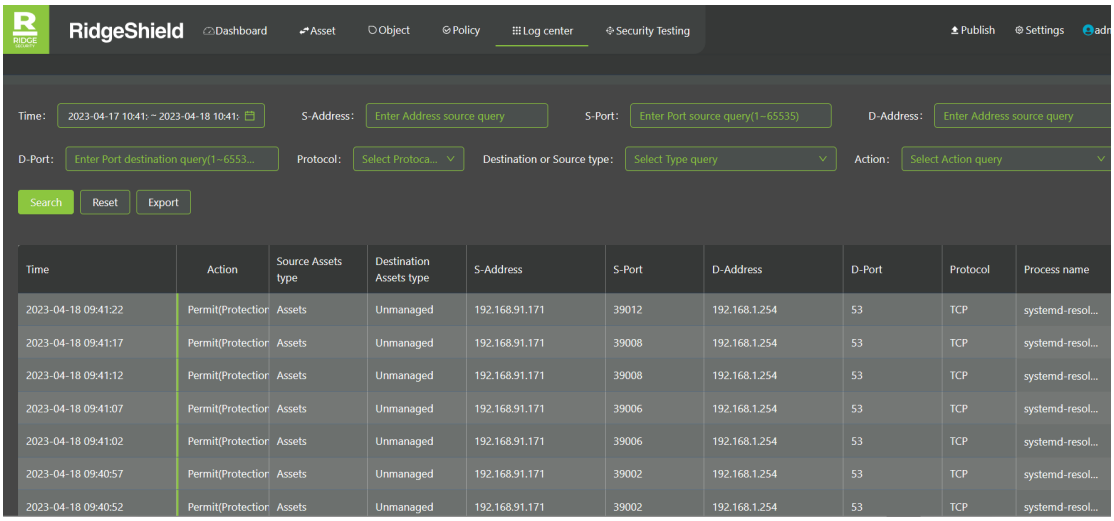
Navigate to the **Dashboard** to view the Business Topology. It shows the OA business group, and the Location, Environment, and Application labels for the business group, as well as the role label of the web server *WebUI*, and the role label of the database as *DB*.



Step 10: Monitor Traffic and Policy Preview

If you are familiar with cloud services and already understand the access (traffic) relationships within the workloads that you have just onboarded, as well as between this workload group and other groups that may already exist in your environment, then you can now go ahead and configure (or refine) the security policies for all your workloads (or workload groups). If not, it is recommended that you observer traffic in the system for a while and use that information to then define/refine the policies in the system.

Observed traffic in the system can be seen in summary on the Business Topology display (navigate to **Dashboard** in the top toolbar). For a more detailed view, navigate to **Log Center -> Flow Log** as shown below.



Time	Action	Source Assets type	Destination Assets type	S-Address	S-Port	D-Address	D-Port	Protocol	Process name
2023-04-18 09:41:22	Permit(Protection	Assets	Unmanaged	192.168.91.171	39012	192.168.1.254	53	TCP	systemd-resol...
2023-04-18 09:41:17	Permit(Protection	Assets	Unmanaged	192.168.91.171	39008	192.168.1.254	53	TCP	systemd-resol...
2023-04-18 09:41:12	Permit(Protection	Assets	Unmanaged	192.168.91.171	39008	192.168.1.254	53	TCP	systemd-resol...
2023-04-18 09:41:07	Permit(Protection	Assets	Unmanaged	192.168.91.171	39006	192.168.1.254	53	TCP	systemd-resol...
2023-04-18 09:41:02	Permit(Protection	Assets	Unmanaged	192.168.91.171	39006	192.168.1.254	53	TCP	systemd-resol...
2023-04-18 09:40:57	Permit(Protection	Assets	Unmanaged	192.168.91.171	39002	192.168.1.254	53	TCP	systemd-resol...
2023-04-18 09:40:52	Permit(Protection	Assets	Unmanaged	192.168.91.171	39002	192.168.1.254	53	TCP	systemd-resol...

Navigate to **Policy -> RuleSet** in the RidgeShield UI and enter the policies your organization require. If you have the *Free Trial* or *Monitor* license, you can only preview the policies, but not actively control traffic. The Business Topology dashboard shows you what traffic flows between your workloads and what your policies would do if they were active.

Policy Management is discussed in detail in the RidgeShield Smart Center User Manual Chapter 6.

Chapter 5. Sample Scenario

This chapter provides sample scenarios to help you implement micro-segmentation by isolating one workload or workload group from each other, as well as from outside elements such as the Internet, business partner network elements, and various servers (such as DNS or FTP) that may exist in the organization.

- There are **within-group** rules which define the policies for traffic within a segment (group or scope).
- There are **between-group** rules which define policies for traffic flowing between segments (groups or scopes).

Example Scenario Description

Consider a situation where there is an OA system in the production environment (segment 1) of an organization's data center with three virtual machines. Two of the VMs are web servers and the other is a database server. Access control is required to allow users in different geographical locations to access the two web servers (but not the database server), while the two web servers may access the database server.

In addition to the web servers and their database (segment 1), the organization's production area also has set of authentication systems (an interface server and its database). The authentication systems must be isolated into segment 2, but some traffic must be permitted between the workloads in segment 1 and those in segment 2 to perform authentication checks.

The steps to achieve this configuration include:

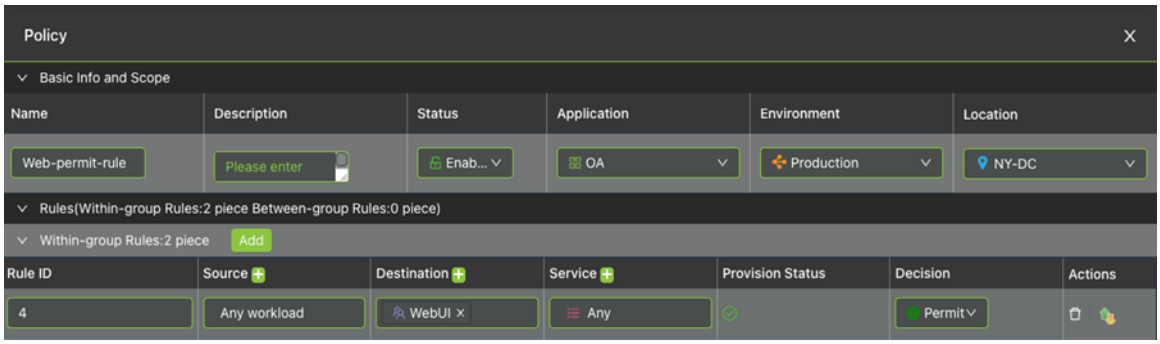
- Segment 1:
  - Add an access policy for traffic from the external network to the web servers
  - Add an access policy for the web servers to the database server
- Segment 2:
  - Add an access policy for the web servers to the authentication servers
  - Add an access policy for traffic from the external network to the authentication servers

Restricting Traffic within a Segment

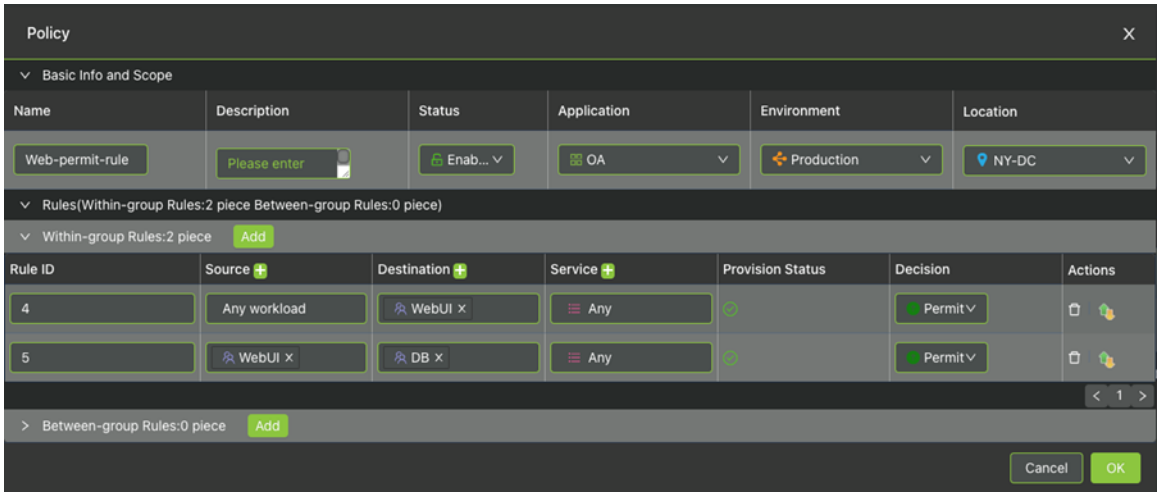
In this section you set up the **within-group** (within-segment) policies for controlling traffic from the external network to web servers. These are the policies to control traffic within segment 1.

Add a policy set with the name *Web-permit-rule*, and set the scope (the three labels that determine the scope of a policy, which includes Application, Environment and Location). Choose Application *OA*, Environment *Production*, and Location *NY.*

Add a within-group rule that allows any source to access the WebUI role (destination), as shown below as Rule #4. This allows external users to access the web servers.

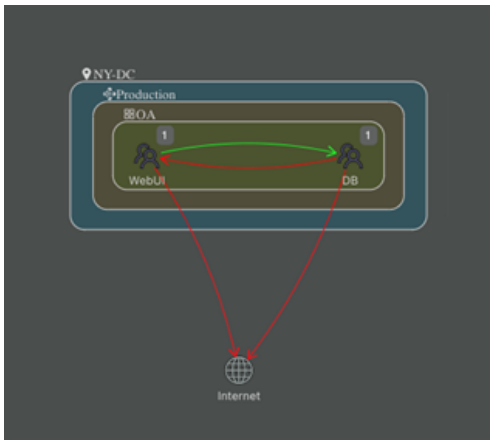


Add another within-group rule that allows the web server (WebUI role as source) to access the database (DB role as destination) as shown below as Rule #5.



Make the policy (rules) active in the system by publishing them.

After some normal traffic has been observed hitting these policies, you can view the workload group on the Business Topology (navigate to **Dashboard** on the toolbar).



Restricting Traffic between Segments

In this section you set up the **between-group** (between segments 1 and 2) policies for controlling traffic between the OA web servers and database (forming the OA group in segment 1) to/from the authentication servers (belonging to group or segment 2).

Steps:

1) Workloads in two sets of business systems are online

2) Enable user access policy configuration to file system

3) Perform policy configuration for file information system access to authentication system and form prohibited access traffic

Policy configuration: