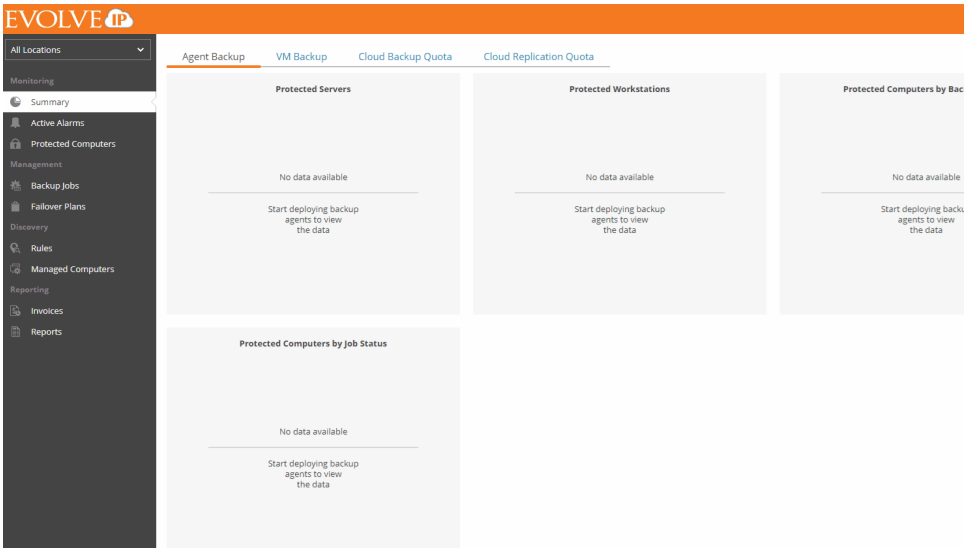
Veeam-Agent-03b-Install Veeam Backup Agent (Discovery, Recommended)

Summary

The third step in backing up your systems is to deploy the Veeam Backup Agent. This can be done via discovery from the master agent (recommended) which can automatically install the Veeam Management Agent followed by the Veeam Backup Agent. If the machines are not reachable by the master agent and don't warrant setting up another location to manage them, they can be installed manually.

Procedure	Example
Prerequisites	
- In order to complete the discovery process you must have already installed a Veeam Master Agent and create a discovery rule. - Make sure you have an account with local Administrator permissions on all computers that you want to discover. - This is not required if you already configured a discovery account on the master agent. - Make sure that remote computers are powered on and configured to allow discovery, the *Remote Scheduled Tasks Management (RPC and RPC-EMAP)* firewall rules must allow inbound traffic. - On remote computers that run a Windows OS, the *Windows Management Instrumentation (WMI-In)* firewall rule must be configured to allow inbound traffic. - If you plan to install Veeam Backup agents as part of the discovery procedure, make sure that remote computers are configured to allow installation: the *File and Printer Sharing (SMB-In)* firewall rule must allow inbound traffic. - If you plan to assign a backup policy as part of the discovery procedure, create a new backup policy or customize an existing predefined policy. Discovery rules can be configured to locate machines through the following methods: - Network-based discovery - This method allows you to discover computers based on a range of IP addresses. - Active Directory discovery - This method allows you to discover computers that are a part of an AD domain. The master agent must be a member of the domain. - Import-based discovery - This method allows you to discover computers by importing a list of IP addresses from a CSV file.	
Create a Discovery Rule	
1. Log into the master agent machine as an Administrator 2. Log into your Availability Console with the administrative credentials provided by EvolveIP. a. If you do not know the URL or your credentials, please contact EvolveIP Support. 3. Click on **Rules** under **Discovery** a. Click on **New** 4. Specify a **Rule Name** and click **Next.** 5. At the **Companies** step, choose one or more companies that the discovery rule will be configured. Use the search field if needed. a. Click the link in the **Locations** column, then click a link in the **Master Agent** column, and select a management agent that will be used as the master agent for discover in each company location. b. If you only have one location and only one master agent installed, you do not need to select a management agent. 6. At the **Discovery Method** step choose the appropriate discovery method and click **Next**.	

a. **Network-based**
    i. Click **Add**
    ii. Enter a desciptive **Networ k Name**.
    iii. In the **IP ranges** field,type a range of IP addresses that will be scanned in the specified network that is accessible to the master agent, click **OK**.
        1. Repeat this step to add all required networks.
    iv. In the **Exclusion mask** field, specify a mask for names of computers that must be excluded from discovery.
        1. The mask can contain the asterisk * that stands for zero or more characters. You can specify multiple masks separated with commas.
    v. Click **Next** once all networks are added.
b. **Active Directory**
    i. Select the appropriate method for discovery:
        1. Select **Search through all Active Directory containers** to discover all computers that are included in the *Domai n Controllers and Computers* organizational units.
        2. Select **Search from organizational units** to discover computers that are included in selected organizational units only.
        3. Select **Run custom query** to discover computers based on results of a custom query. In the text field at the bottom, specify a LDAP query that must return a list of computers to scan.
    ii. In the **Exclusion mask** field, specify a mask for names of computers that must be excluded from discovery.
        1. The mask can contain the asterisk * that stands for zero or more characters. You can specify multiple masks separated with commas.
    iii. Select **Ignore offline computers** to exclude computers from discovery that have not contacted a domain controller for 30 days or longer.

c. **Computers from CSV file**
    i. Create a CSV file with a list of computer IP addresses or DNS names to scan during discovery.
        1. Delimit IP addresses and DNS names in the list with commas:
            a. **Comma delimited list**

```
192.168.1.20,DC01,File01,192.168.1.54
```

        2. Form a file where each new IP or DNS name is one a new line:
            a. **Lined list**

```
192.168.1.20
DC01
File01
192.168.1.54
```

7. At the **Access Account** step of the wizard, specify credentials of an account that the master agent will use to connect to computers within the discovery scope. The account must have local Administrator permissions on all discovered computers.
    a. If you have specified a discovery account in the master agent configuration settings, select the **Use credentials specified in the master agent configuration** check box.
        i. Credentials specified in the master agent take precedence over credentials specified in the discovery rule.

8. At the **Discovery Filters** step, choose what filters you want to enable for discovery. If no filters are specified, all systems within the discovery range are targeted.
    a. To filter computers based on OS type, click **By OS type** and click **Edit**. Select which type of OS to apply discovery to (*Server operating system, Client operating system)* and click **OK**.
    b. To filter computers based on the type of application running click **By application** and click **Edit**. Select applications that must run on the discovered computers (*Microsoft Exchange Server, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint, Oracle, Other Applications)* and click **OK.**
    c. To filter computers based on which platform is running the system, click **By platform** and click **Edit**. Select which type of platform the discovered system must run on (*Vmware vSphere, Hyper-V, Physical Computers, Microsoft Azure, Amazon Web Services, Other*), *Client operating system)* and click **OK**.
    d. If you want discovery to only be applied to accessible computers, select **Do not show inaccessible computers**.
        i. Different types of filter conditions are joined using Boolean AND operator. For example, if you enable filters *Server operating system, Microsoft Active Directory,* and *VMware vSphere*, the list of discovered computers will include only machines running on VMware vSphere that are a Server OS Domain Controller.
9. At the **Email Notification** step, you can enable discovery notifications to provide results based on the discovery rules configured.
    a. Select **Send Notifications** check box and specify a schedule according to which email notifications will be sent.
    b. In the **Subject** field, specify the subject of the email.
    c. In the **To** field, specify an email address at which the email notifications must be sent, typically your IT distribution group email.
    d. Select the **Send notification after the first run** check box if a notification about discovery results must be sent after the first run, regardless of a specified schedule.
    e. Click **Next.**

10. At the **Backup Agent Deployment** step, specify whether you want to install the Veeam Backup Agent on discovered computers.
    a. If you do not want to install the Veeam Backup Agent automatically on discovered computers, select **Discover remote computer without installing backup agent**.
    b. If, after discovery, you want Veeam Backup Agents to be installed enable **Discover Remote computer, install backup agent and assign the selected backup policy.**
        i. From the **Backup policy to apply**, choose a backup policy to assign to the discovered systems.
        ii. Click **Create New** if you do not already have the policies configured, see Create a Backup Policy.
        iii. By default, the read-only access mode is enabled for all Veeam backup agents installed as part of discovery. To disable the read-only access mode set the **Enable read-only UI access for the backup agent** to *Off.*
            1. You can adjust this on a per system basis later.
        iv. Click **Next**.
11. At the **Summary** step, review the settings and click **Finish**.
    a. If you wish to start discovery immediately check the box next to **Launch the discovery rule when I click Finish.**

If you wish to have discovery run on a schedule select the desired discover rule and select **Schedule.** Select a daily schedule for the rule and click **Apply**.