Chuco Gives a FAQ 2024: Targeting Offline Endpoints Guide

Version: 1.0

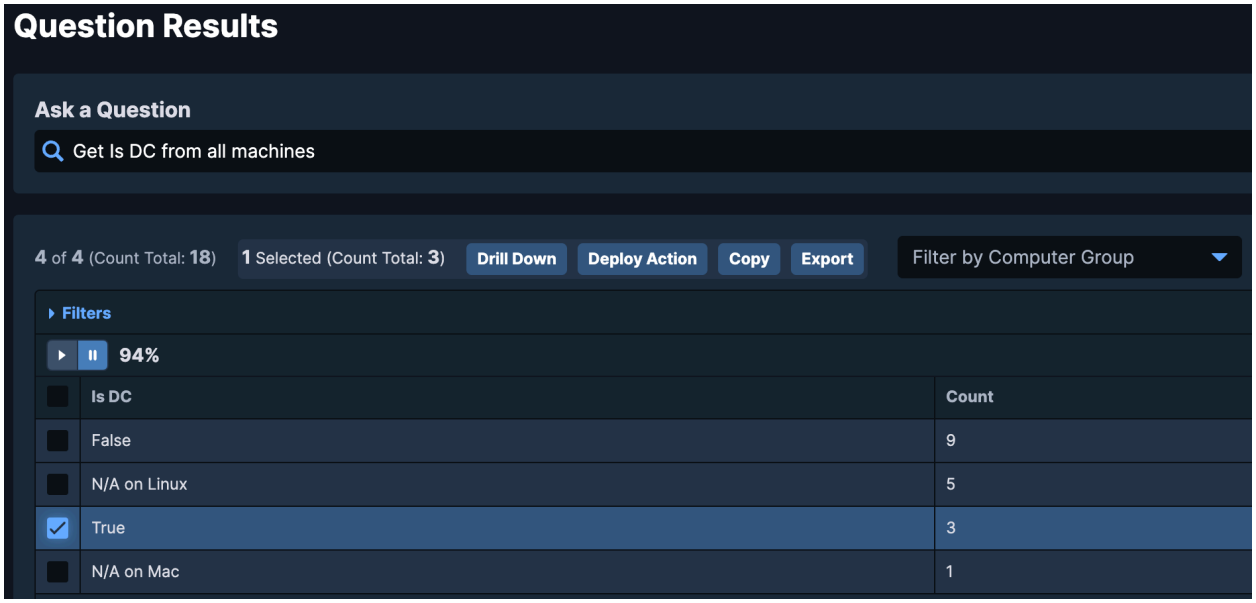
Last Update: Oct 24th, 2024

Table of Contents

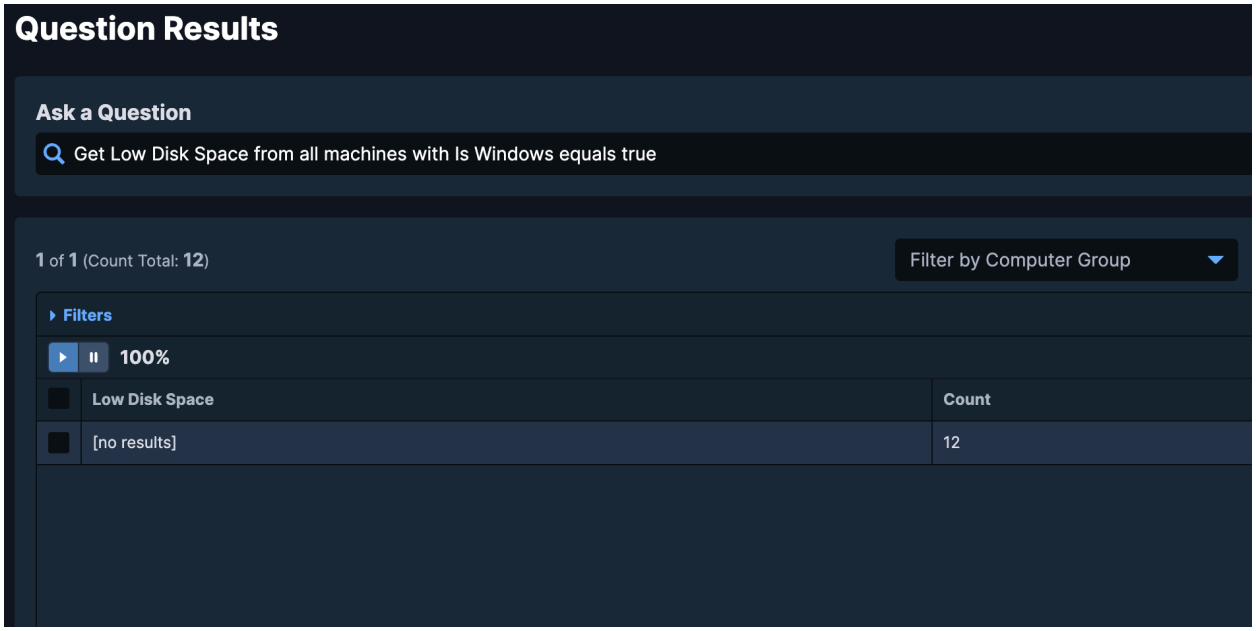
The Issue With Offline Endpoints **3**
The Single Endpoint Approach **4**
The Computer Group Approach **4**
Investigate The Sensor 5
Create a Computer Group 6
Deploy a Package to Offline Endpoints Using a Computer Group 7

The Issue With Offline Endpoints

When deploying a platform package in Tanium is it common to use a counting question for targeting. This gives us a single item to check in the Tanium UI. Like this example where we are targeting all domain controllers.



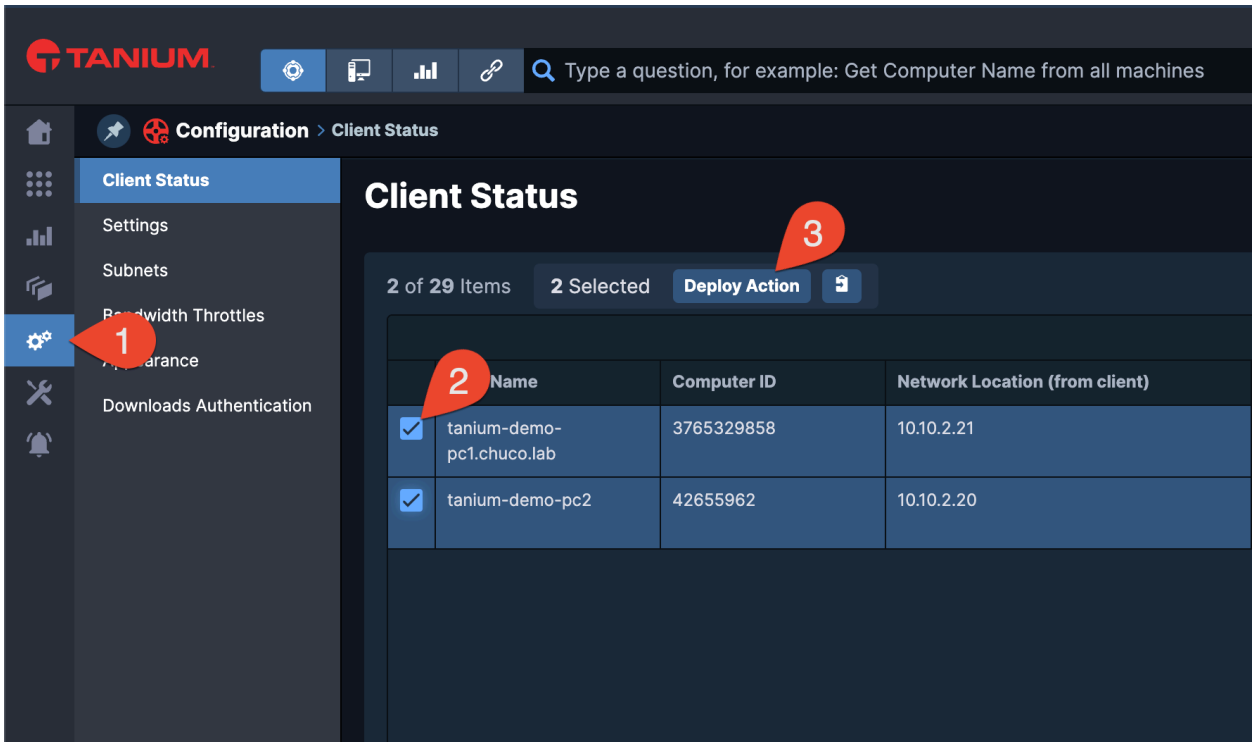
But what if we don't have any endpoints online that meet our criteria, like this example where we are trying to target all Windows endpoints with low disk space?



The Single Endpoint Approach

Tanium does provide a way to target offline endpoints via the Client Status page. This is useful if you know the name of the client you want to target. And you can select multiple endpoints, but you still need to individually check each box.

1. In the Tanium Console, navigate to **Administration > Configuration > Client Status**
2. Select the **desired endpoints**
3. Select **Deploy Action**

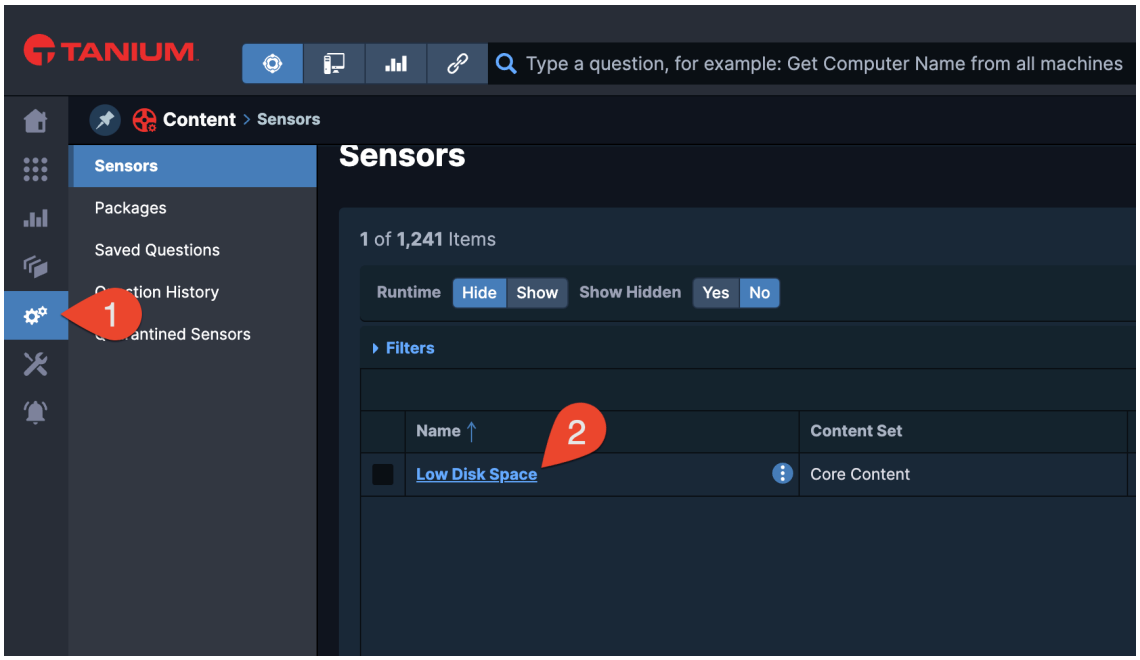


The Computer Group Approach

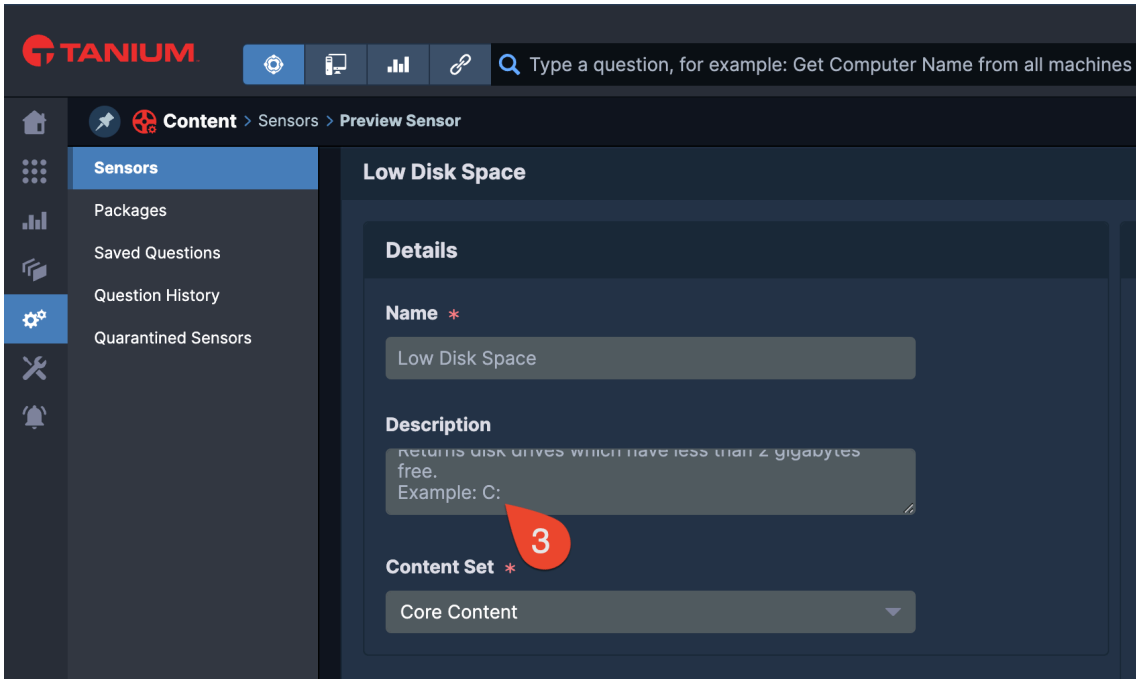
But what if I want to target those offline Windows endpoints with low disk space? We can create a computer group and use that group to deploy a package. But before we make a new computer group, let's look at the low disk space sensor. Since we don't have any Windows clients returning results we need to do a little research to help us build the computer group filter.

Investigate The Sensor

1. In the Tanium Console, navigate to **Administration > Content > Sensors**
2. Select the desired sensor, in this case that's **Low Disk Space**



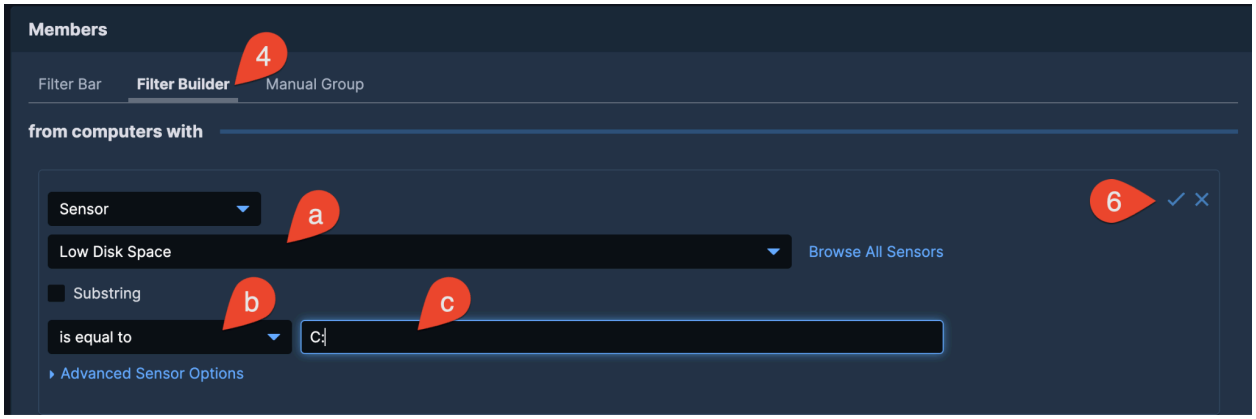
3. Look at the description field. Here we see an example output. This lets us know that we can expect to see the drive letter with low disk space.



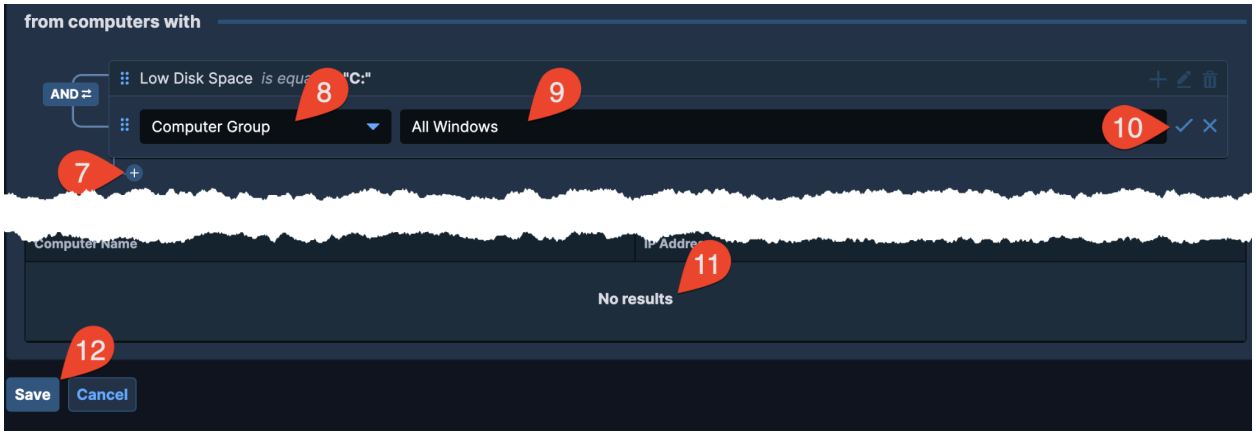
Create a Computer Group

Now that we know what the sensor will return, we can create a computer group that we will use to deploy a platform package.

1. In the Tanium Console, navigate to **Administration > Permissions > Computer Groups**
2. Select **New Computer Group**
3. Fill in the **Name** field
4. Select the **Filter Builder** tab
5. Select Add Row and fill in the following fields (Adjust this for the sensor you need):
    a. **Sensor Name**: Low Disk Space
    b. **Operator**: is equal to
    c. **Value**: C:
6. Select the **Apply** check



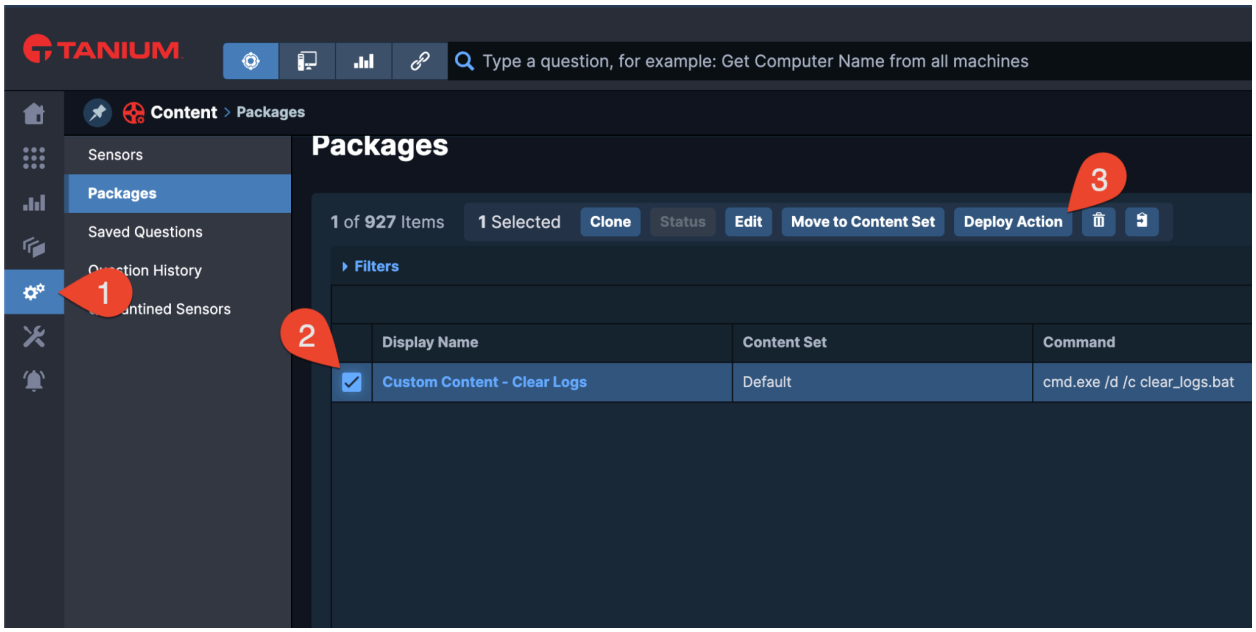
7. Select **Add Row**
8. Switch from Sensor to **Computer Group**
9. Select **All Windows**
10. Select the **Apply** check
11. Since there are no endpoint online that match the filter, we will not see any results
12. Select **Save**



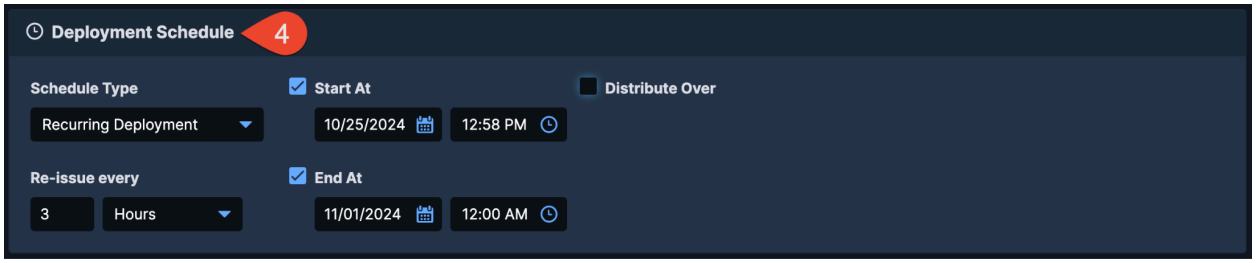
Deploy a Package to Offline Endpoints Using a Computer Group

Now we can use the new computer group to deploy a platform package. For this scenario, imagine we have an application that is generating large log files that are not being cleaned up, thus causing the low disk space issue. We have manually remediated the issue for now, but want to put a workaround in place utilizing a custom package before we have a chance to properly configure log generation for the application.

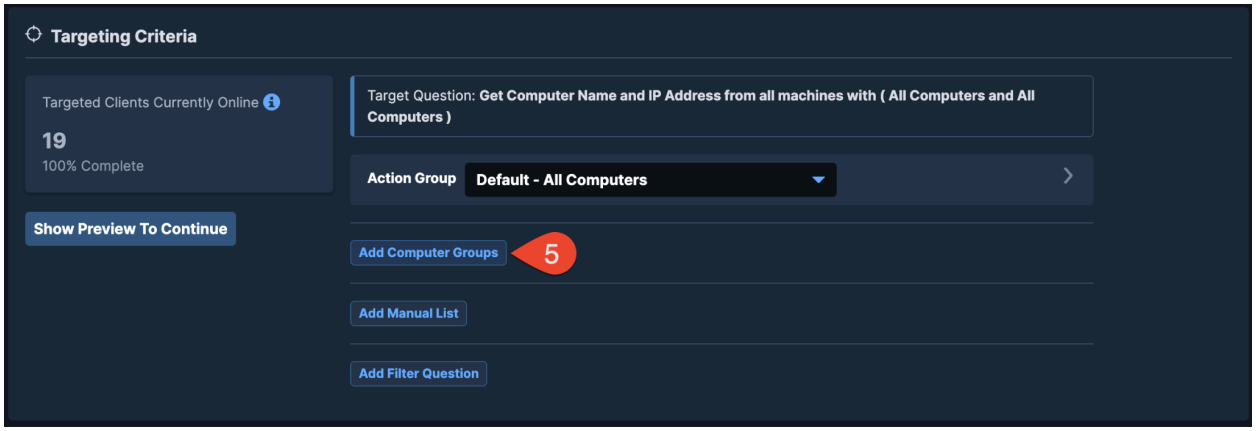
1. In the Tanium Console, navigate to **Administration > Content > Packages**
2. Select the **Check Box** for the desired package
3. Select **Deploy Action**



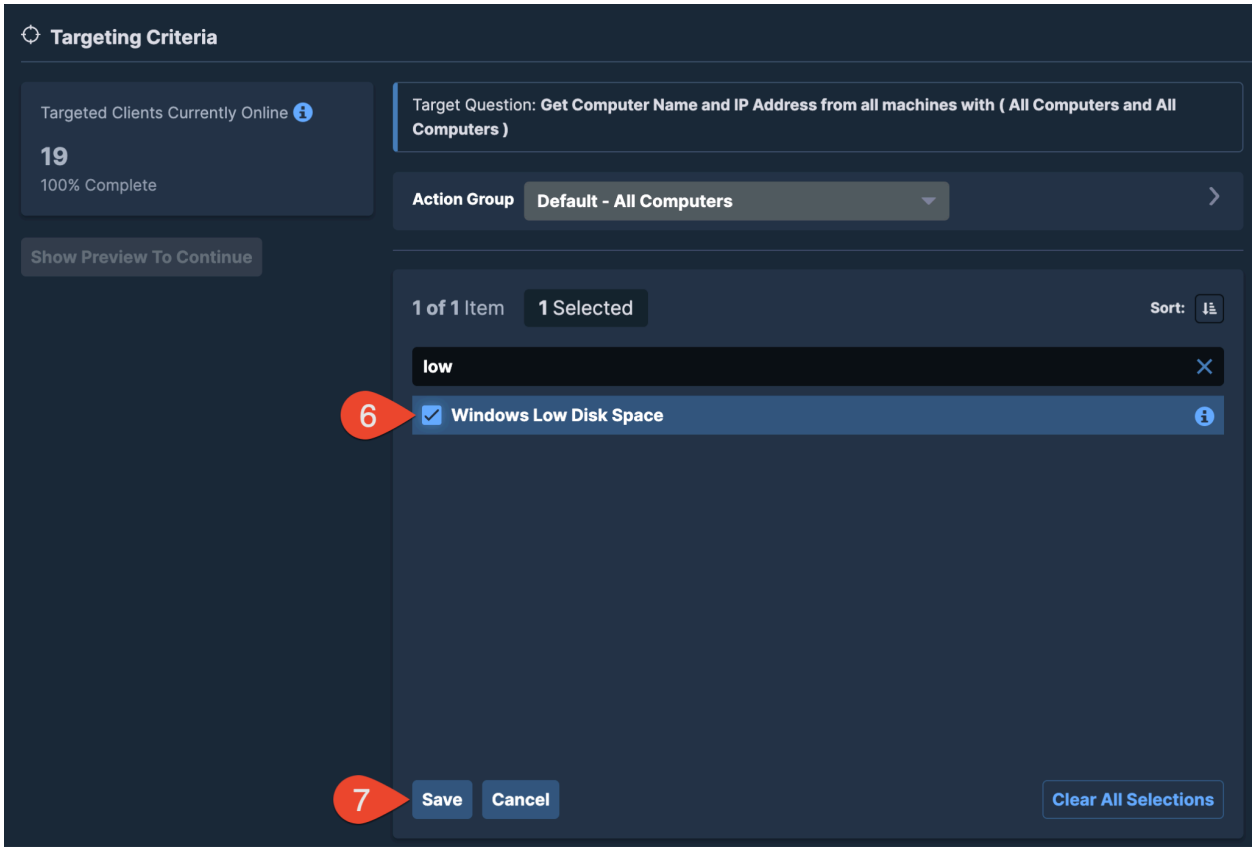
4. In the **Deployment Schedule** section, set **Schedule Type** to **Recurring Deployment**. A frequency of every 3-4 hours is recommended to catch endpoints as they come online.



5. In the **Targeting Criteria** section, select **Add Computer Groups**



6. Select the **Computer Group** created in the steps above
7. Select **Save**



8. Now that we have selected the Computer Group, we can see that the **Targeted Clients** count has changed to 0, this is expected as no endpoints are currently online that match the Computer Group filter. Select **Show Preview to Continue**
9. Select **Deploy Action**