

## How to Connect non-Azure CGFs to a Microsoft Azure Log Analytics Workspace

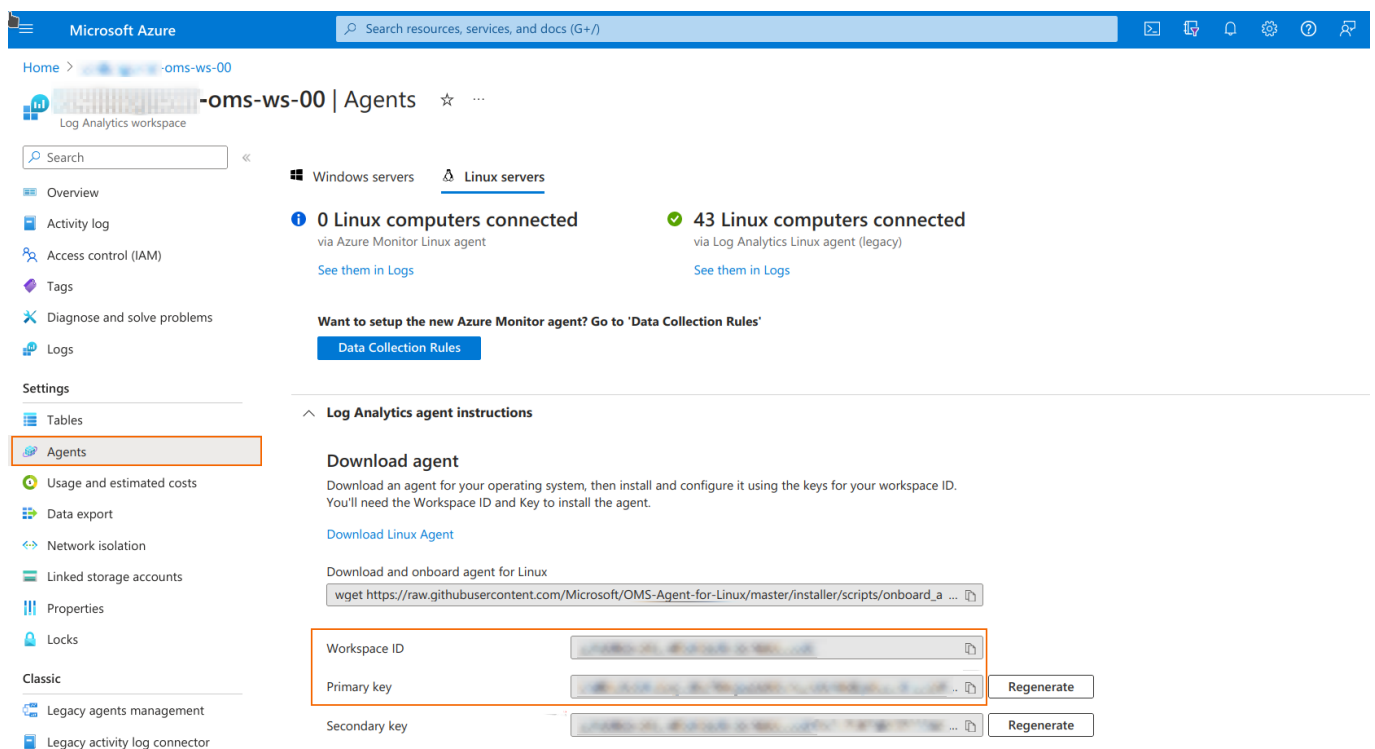
<https://campus.barracuda.com/doc/101711882/>

CloudGen Firewall boxes that run outside the Azure cloud can be connected to a Microsoft Azure Log Analytics workspace. The functionality is the same as for CloudGen Firewalls residing in the Azure Cloud, with a few differences/limitations. The connection is based on a command line tool named "omsctl".

### Prerequisites

In order to connect a CloudGen Firewall to an Azure Log Analytics Workspace, the workspace ID and its primary key must be available.

These can be copied from the Azure portal:



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo and a search bar. The left sidebar contains a list of navigation items, with 'Agents' highlighted. The main content area shows the 'Agents' page for a Log Analytics workspace. It displays two sections: '0 Linux computers connected' and '43 Linux computers connected'. Below these, there is a 'Download agent' section with instructions and a terminal command. A red box highlights the 'Workspace ID', 'Primary key', and 'Secondary key' fields, with 'Regenerate' buttons next to the keys.

or gathered via Azure CLI:

```
az monitor log-analytics workspace show --subscription <subscription_id> --  
resource-group <resource_group_name> --workspace-name <workspace_name>  
az monitor log-analytics workspace get-shared-keys --subscription
```

```
<subscription_id> --resource-group <resource_group_name> --workspace-name  
<workspace_name>
```

## Limitations

Similar to CloudGen Firewalls residing in the Azure Cloud, the following limitations apply to connecting non-Azure CloudGen Firewalls to Azure Log Analytics:

- On CC-managed boxes, the streaming configuration is not automatically created and must be configured manually. For more information, see [How to Configure Log Streaming to Microsoft Azure Log Analytics](#).
- On HA pairs, the primary HA peer must be connected first, so that the streaming configuration gets created, and only afterwards should also the secondary unit be connected.
- Also, for CloudGen Firewalls in the Azure Cloud there is a health check that runs periodically and that can automatically recover from some error conditions that might arise during operation. This health check is not available on non-Azure boxes connected to OMS.

## Connecting and Disconnecting from an Azure Log Analytics Workspace

Both operations are done using the CLI utility `/opt/phion/bin/omsctl`:

```
# omsctl --help  
usage:  
omsctl connect -w <workspace_id> -k <secret_key>  
omsctl disconnect  
omsctl start|stop|status
```

For the initial connection, the tool must be run with the *connect* subcommand and with the workspace ID and key. After the connection has been established, the *status* subcommand can be used to check the results. The tool logs all activities in the `/var/phion/logs/box_Cloud_operational.log` log file, which is the place where eventual troubleshooting should take place. You can use the *disconnect* subcommand to disconnect from the OMS workspace.

*start* and *stop* commands are run automatically for starting and stopping the affected services during bootstrapping and service management operations.

## Figures

1. get\_workspace.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.