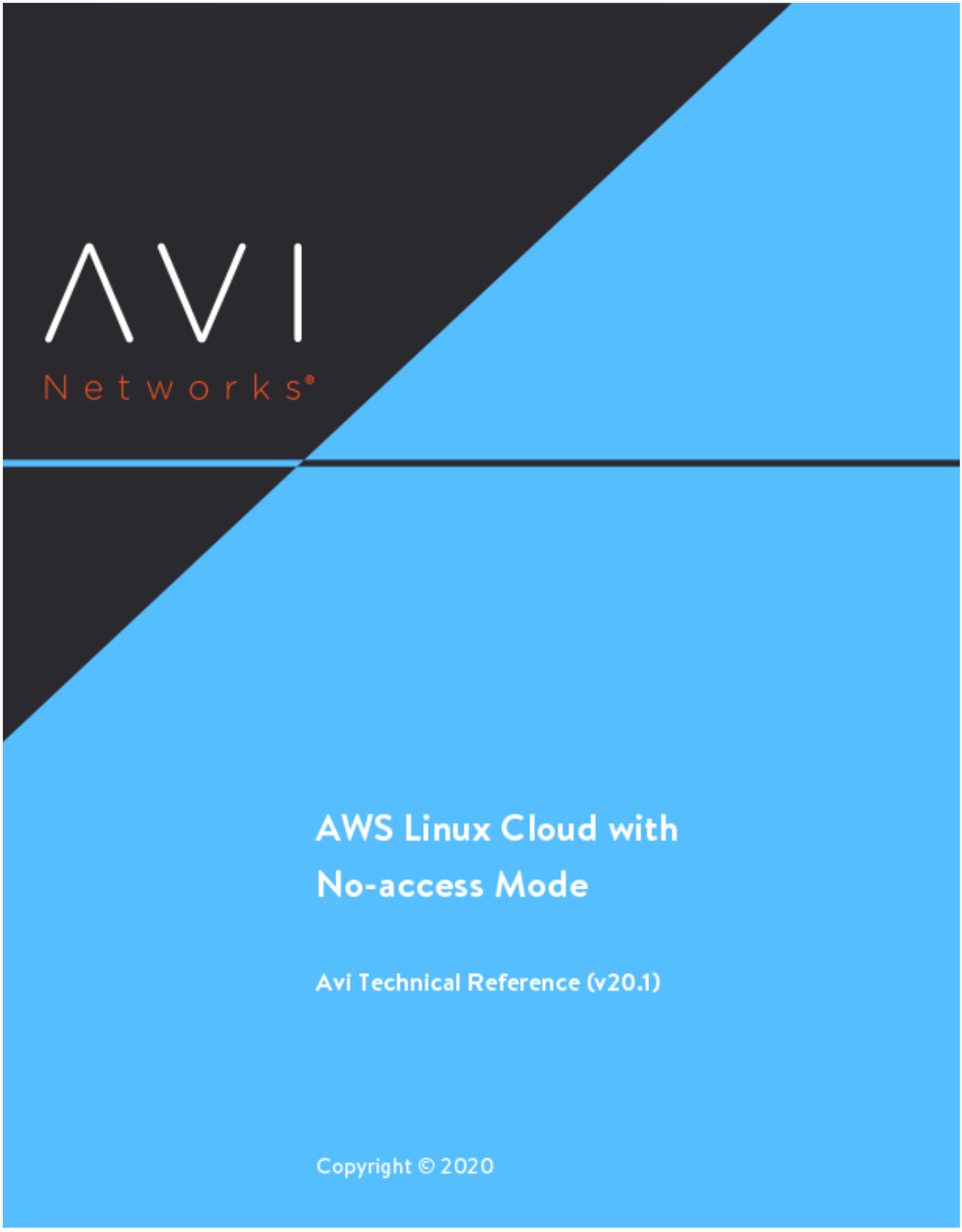

AWS Linux Cloud with No-access Mode

Avi Technical Reference (v20.1)

AWS Linux Cloud with No-access Mode

view online

This article describes how to set up IP address management (IPAM) in an Avi Vantage deployment onto a Linux server cloud in Amazon Web Services (AWS). These steps deploy Avi Vantage into AWS in no access mode.

The setup process consists of the following tasks:

- Create a role in IAM using the supplied JSON file: avicontroller-role-ipam-policy.json
- Launch the Avi Controller using the IAM role. This starts the setup wizard.
- Afer initial setup, use the Avi Controller web interface to edit the Default-Cloud to add Linux server cloud settings, including the IP address management (IPAM) profile.
- Use the Avi Controller CLI to enable no-access settings Avi Service Engines (SEs).

Create a Role in IAM

Use the following JSON file to create a role in IAM. Use the following name for the file: avicontroller-role-ipam-policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1450393199000",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteTags",
                "ec2:DescribeAddresses",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstances",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ResetNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "*"
            ]
        }
```

```
    ]
}
```

Launch and Finish with the Setup Wizard

Launch the avi-controller using this role. Configure an administrator account, and enter DNS and NTP server information. On the Orchestrator page, select No Orchestrator. Exit the wizard.

Configure Cloud Settings

Before beginning these steps, ensure the following for each SE or server host:

- Correct vNIC(s)
- Source-destination checking disabled
- Security group(s): must allow all ports (protocols) for VPC CIDR (at least ports '73', '97', and '63')

To configure the cloud:

1. Navigate to the Avi Controller web interface and go to Infrastructure > Clouds.
2. Click the edit icon in the row for Default-Cloud.
3. Select Linux as the infrastructure type and click Next.
4. Create an SSH user account. (While this account is not required for no-access deployment, the configuration popup still requires it.)
5. Create the IPAM profile:Select Create from the IPAM Profile pull-down list. Enter or select the following values:
    - Name: String
    - Type: AWS
    - DNS Name Server (NS) records: if needed
    - Credential type: IAM role or access key
    - AWS region
    - VPC ID

    The credentials (access key or IAM role) provide the permissions to look up networks and Virtual Machines (VMs), create or delete Elastic Network Interfaces (ENIs), and manage private IP addresses (allocate, deallocate, assign, or de-assign). Additionally, if an IAM role is used, permissions are granted to add, look up, and delete ENI tags.

6. To add servers, click Add new server.
   Note: For no-access mode, do not add any servers.

When the State is Cloud-Ready, the cloud configuration changes are complete.

Create a Virtual Service

1. Navigate to Applications > Dashboard and click Create Virtual Service > Basic Setup.
2. Enter required values:
    - Name: string
    - Type: HTTP, HTTPS, or L4
    - VIP address: either a host address or the subnet from which to select the address
    - Certificate (if type is HTTPS)
3. Click Save.

Note: If no host has any vNICs on the pool subnet(s), enable the the following option: Ignore network reachability constraints for the server pool

Configure Avi SE Settings for No-access Mode

If deploying in no-access mode, some configuration in the Vantage CLI also is required.

Enter the following commands to let the Avi Controller connect to SE nodes without attempting to use SSH for authentication:

```
: > configure controller properties
: controllerproperties> allow_unauthenticated_nodes
: controllerproperties> save
```

Enter the following commands to enable tunneling support for Avi SEs:

```
: > configure serviceengineproperties
: seproperties> se_bootup_properties
: seproperties:se_bootup_properties> se_ip_encap_ipc 1
: seproperties:se_bootup_properties> se_tunnel_mode 1
: seproperties:se_bootup_properties> save
: seproperties> save
```