Audit Logs

For supported software information, click here.

Director node audit log files record information about configuration changes, such as creation, modification, and deletion, that are performed on various entities on the Director node. Audit log files also contain entries for user logins and logouts, user password changes, and preference setting changes. The records in audit log files provide documentary evidence of the sequence of actions that occur on a Director node. Each log entry records the time the action occurred or was performed, who performed the action, the value before the change was made, and the value after the change. You can use this information to determine the cause of a problem and help prevent future occurrences of the problem, and to help identify system implementation and operational issues, unusual or suspicious activities, and system and operator errors.

Audit log files are stored in the directory /var/log/vnms/audit on the Director node. The exception is the shell.log file, which is stored in the /var/log directory.

Each log file has the filename extension .log.

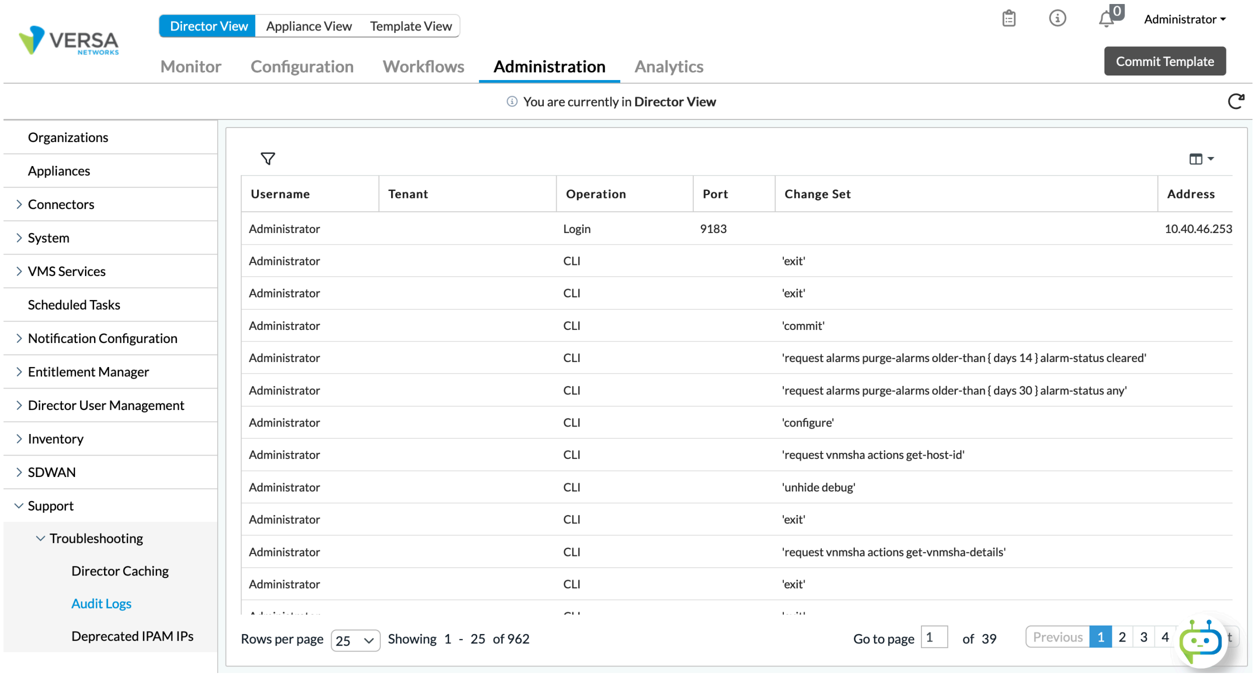
When an audit log file reaches its size limit , which is 15 MB, a new log file is created. Newer logs are named *filename.log.1, filename.log.2,* and so forth. The filename with the highest number contains the newest information.

This article describes how to view the audit logs in the Director GUI, and it describes the contents of the Director audit log files.

View Audit Logs

For Releases 21.2 and later.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Support > Troubleshooting > Audit Logs in the left menu bar. The main pane displays the audit logs for the Director node.



Username	Tenant	Operation	Port	Change Set	Address
Administrator		Login	9183		10.40.46.253
Administrator		CLI		'exit'	
Administrator		CLI		'exit'	
Administrator		CLI		'commit'	
Administrator		CLI		'request alarms purge-alarms older-than { days 14 } alarm-status cleared'	
Administrator		CLI		'request alarms purge-alarms older-than { days 30 } alarm-status any'	
Administrator		CLI		'configure'	
Administrator		CLI		'request vnmsha actions get-host-id'	
Administrator		CLI		'unhide debug'	
Administrator		CLI		'exit'	
Administrator		CLI		'request vnmsha actions get-vnmsha-details'	
Administrator		CLI		'exit'	

Rows per page 25 Showing 1 - 25 of 962

Go to page 1 of 39 Previous 1 2 3 4

ProviderDataCenterSystemAdmin.log File

The ProviderDataCenterSystemAdmin.log files contain one entry is for each operation such as create, modify, and delete performed by Provider Data Center System Admin (PDCSA) user to any Director entity except for organization and organization services.

The following are example file entries. Note that the entries have been reformatted for readability.

```
[09-Sep-2019 11:14:31.835][INFO] Administrator@ProviderDataCenterSystemAdmin, 10.145.0.110:49821,
create, service-chain:qwerty , changeset:devices
 { template{template-jq-bs}
   { config
     { orgs
       { org{Provider-org}
         { service-chains
           { + service-chain{qwerty}
             { + service-node-group + type internal}
           }
         }
       }
      }
    }
  }

[09-Sep-2019 11:15:00.690][INFO] Administrator@ProviderDataCenterSystemAdmin, 10.145.0.110:49821,
modify, service-chain:qwerty , changeset:devices
 { template{template-jq-bs}
   { config
   { orgs
    { org{Provider-org}
     { service-chains
      { service-chain{qwerty}
       { + description description + service-node-group + service-node-group-cluster-list
        { + clusterorsng}
       }
      }
     }
    }
   }
  }
 }

[09-Sep-2019 11:15:05.563][INFO] Administrator@ProviderDataCenterSystemAdmin, 10.145.0.110:49821,
delete, service-chain:qwerty , changeset:
```

SystemUser.log File

The SystemUser.log files contain one entry for each operation such as create, modify and delete performed by Provider Data System Admin (PDSA) users to any Director entity except for organization and organization services.

The following are example file entries. Note that the entries have been reformatted for readability.

```
[25-Jun-2019 09:51:05.031][INFO] Administrator@ProviderDataCenterSystemAdmin, 10.145.0.141:49546,
Login,

[25-Jun-2019 09:51:21.155][INFO] Administrator@ProviderDataCenterSystemAdmin, 10.145.0.141:49546,
ChangePassword, password , changeset:
 {"change-password":
  {"currentpassword":"******","newpassword":"*****     *"}
 }

[25-Jun-2019 09:52:00.596][INFO] Administrator@ProviderDataCenterSystemAdmin, 10.145.0.141:49546,
ChangePassword, password , changeset:
 {"change-password":
  {"currentpassword":"******","newpassword":"*****     *"}
 }
```

This file also logs the CLI commands that you issue. For example:

```
[06-Nov-2019 06:25:03,762]INFO: ProviderAdmin  Administrator, CLI 'exit'
[07-Nov-2019 06:25:04,435]INFO: ProviderAdmin  Administrator, CLI 'configure'
[07-Nov-2019 06:25:04,447]INFO: ProviderAdmin  Administrator, CLI done
[07-Nov-2019 06:25:04,483]INFO: ProviderAdmin  Administrator, CLI 'request alarms purge-alarms older-than {
days 30 } alarm-status any'
[07-Nov-2019 06:25:04,493]INFO: ProviderAdmin  Administrator, CLI done
[07-Nov-2019 06:25:04,506]INFO: ProviderAdmin  Administrator, CLI 'request alarms purge-alarms older-than {
days 14 } alarm-status cleared'
[07-Nov-2019 06:25:04,516]INFO: ProviderAdmin  Administrator, CLI done
[07-Nov-2019 06:25:04,526]INFO: ProviderAdmin  Administrator, CLI 'commit'
```

Tenant-name.log File

The *tenant-name*.log file contains one entry for each operation such as create, modify, and delete performed by PDCSA, PDSA, or TenantAdmin users to organization and organization services hierarchy. This log file also includes system-level changes made by the TenantAdmin user, such as user creation.

The following is an example file entry. Note that the entries have been reformatted for readability.

```
[07-Nov-2019 15:06:36,546]INFO: ChildOrg  TsecurityA@ChildOrg, 10.145.0.119:57169, create, group:dummy,
appliances: BR-NAT , changeset:devices
 { device{BR-NAT}
  { config
   { orgs
    { org-services{ChildOrg}
     { objects
      { address-groups
       { + group{dummy}
       }
      }
     }
    }
   }
  }
 }

[07-Nov-2019 15:08:18,356]INFO: ChildOrg  TsecurityA@ChildOrg, 10.145.0.119:57282, modify, zone:qqqqqq,
appliances: BR-NAT , changeset:devices
 { device{BR-NAT}
  { config
   { orgs
    { org-services{ChildOrg}
     { objects
      { zones
       { zone{qqqqqq}
        { + description des }
       }
      }
     }
    }
   }
  }
 }
```

Shell.log File

The shell.log file contains one entry for each CLI and bash command that is issued on Versa Director. These commands are also captured in tech-support logs, which are used for debugging customer issues.

For example, when you issue the following command:

```
[Administrator@vDir-QA151-Slave3: ~] $ cd /var/versa/packages/vnms/
[Administrator@vDir-QA151-Slave3: vnms] $ cd /var/versa/backups/
[Administrator@vDir-QA151-Slave3: backups] $ logs
[Administrator@vDir-QA151-Slave3: vnms] $ tail -f upgrade.log
```

The following entry is placed into the shell.log file:

```
Apr 14 10:42:25 vDir-QA151-Slave3 Administrator: Administrator [5125]: cd /var/versa/packages/vnms/ [0]
Apr 14 10:42:36 vDir-QA151-Slave3 Administrator: Administrator [5125]: cd /var/versa/backups/ [0]
Apr 14 10:42:41 vDir-QA151-Slave3 Administrator: Administrator [5125]: logs [0]
Apr 14 10:43:09 vDir-QA151-Slave3 Administrator: Administrator [5125]: tail -f upgrade.log  [130]
```

Role-name.log File

The *role-name*.log file contains one entry for each change that a custom user makes to Versa Director. Custom users are those users who are granted privileges to perform a particular set of operations. This file also includes the role assigned to the custom user.

The following is an example file entry:

```
[07-Nov-2019 14:50:22,959]INFO: CURprovider  curptest@CURprovider, 10.129.0.61:63395, deployTemplate,
Template:Test
```

External-user.log File

The *external-user*.log file contains one entry for all operations performed on Versa Director by an external user. When an external user logs in to the Director, the authentication server such as TACACS, RADIUS authenticates the user.

The following are example file entries:

```
[31-Oct-2019 18:20:10,426]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI 'shell'
[31-Oct-2019 18:38:51,599]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI done
[31-Oct-2019 20:32:31,117]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI 'configure'
[31-Oct-2019 20:32:31,129]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI done
[31-Oct-2019 20:33:11,940]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI done
[31-Oct-2019 20:33:24,048]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI 'delete nms
provider default-auth-connector'
[31-Oct-2019 20:33:24,059]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI done
[31-Oct-2019 20:33:29,502]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI 'commit'
[31-Oct-2019 20:33:29,576]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI done
[31-Oct-2019 20:33:31,843]INFO: EXTERNAL_USER  PAdministrator@EXTERNAL_USER, CLI done
```

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- In Release 21.2, you can view audit logs in the Director GUI.