CloudPassage

Server Account Management

Setup Guide

Contents:

About Server Account Management

The Server Account Management feature of CloudPassage® Halo® allows you to monitor and audit remote access to your servers by all of the servers' local accounts. Halo scans your servers at a frequency that you specify, gathering account information and login history for all servers, then displaying it in a centralized location for your inspection and remediation.

The feature also provides basic account-management capabilities, allowing you to create, edit, or deactivate server accounts.

In an elastic cloud environment in which you may have hundreds of servers that come and go dynamically, using Halo for these purposes can save you time and also help to ensure complete coverage of your server installation.

Auditing Server Access

Setting up Halo to perform server-access scans and report on account activity is simple. Either (1) enable automatic scanning and choose the frequency of scanning that is best for you, or (2) specify the servers to be scanned and execute a manual scan.

Halo performs the scans and presents detailed results in the Halo portal or API.

Responding to Account-Related Special Events

When scanning a server's accounts, Halo will generate an event (and a Halo issue will be created) if it detects more than one account with root privileges, or more that one account with a given user ID. You can view those issues and events in the Halo portal, and you can use Server Account Management to remediate them.

Administering Server Accounts

Halo also lets you control server accounts centrally from the portal, so that you can remediate account issues uncovered by server-access scanning. For example, you can edit an account to change its permissions, you can deactivate an account that should not exist on a particular server, and you can even create a new server account.

The Halo portal provides you with the convenience of manipulating all server accounts through one user interface. And for even greater convenience, you can use the Halo API to script automated actions across multiple accounts at once.

Setting Up and Running a Server Access Scan

Perform the following steps to set up and run server-access scans.

1. Enable automatic server access scanning.

   For information, in the *Halo Operations Guide*, see Scanner Settings.

2. Perform an automatic or manual scan.

   For information, in the *Halo Operations Guide* see Working with Scans.

3. View and act on scan results.

   - To view server access scan findings, click the status value of a server access scan on the Scans screen of the Environment page. In the *Halo Operations Guide*, see View Scan Findings.

     The scan findings page opens. See Addressing Server Access Findings.

   - To view server access issues, start with the Issues view on the Environment screen, then view the Issue Details Sidebar. In the *Halo Operations Guide*, see Viewing Issue Details.

     To get details of the findings underlying the issue, click the Scans link on the sidebar. The scan findings page opens. For information see Act on Server Access Issues, Findings, and Events.

Addressing Server Access Findings

To accurately assess the level of risk associated with a given server access finding, issue, or event, you may need to examine the details of one or more server access scan findings.

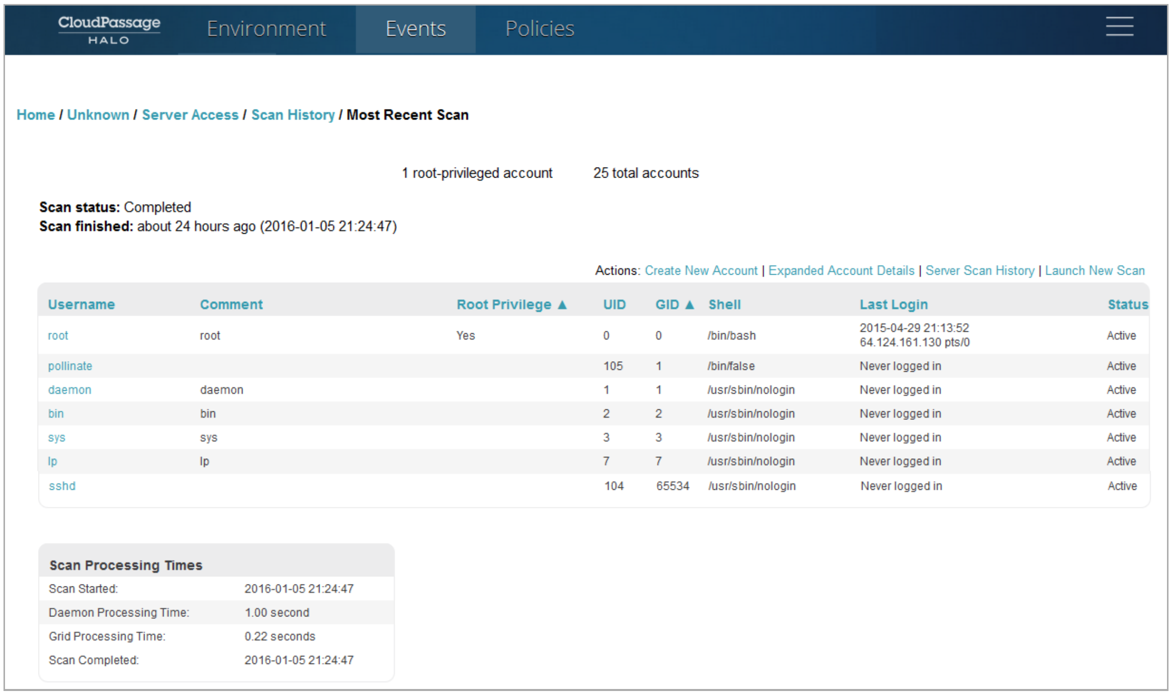
The easiest way to examine server access findings in detail is to click a scan's Status column to display a summary of the scan's results. From there, you can view the individual findings within a given result.

View Server Access Scan Findings

Halo enables you to view the results of server access scans in multiple ways and at varying levels of detail.

View account summaries for a server

After performing at least one server access scan, select an individual server, click Scans, locate a server access scan, then click its status value (for example, "Completed").



Home / Unknown / Server Access / Scan History / **Most Recent Scan**

1 root-privileged account 25 total accounts

Scan status: Completed
Scan finished: about 24 hours ago (2016-01-05 21:24:47)

Actions: Create New Account | Expanded Account Details | Server Scan History | Launch New Scan

Username	Comment	Root Privilege ▲	UID	GID ▲	Shell	Last Login	Status
root	root	Yes	0	0	/bin/bash	2015-04-29 21:13:52 64.124.161.130 pts/0	Active
pollinate			105	1	/bin/false	Never logged in	Active
daemon	daemon		1	1	/usr/sbin/nologin	Never logged in	Active
bin	bin		2	2	/usr/sbin/nologin	Never logged in	Active
sys	sys		3	3	/usr/sbin/nologin	Never logged in	Active
lp	lp		7	7	/usr/sbin/nologin	Never logged in	Active
sshd			104	65534	/usr/sbin/nologin	Never logged in	Active

Scan Processing Times	
Scan Started:	2016-01-05 21:24:47
Daemon Processing Time:	1.00 second
Grid Processing Time:	0.22 seconds
Scan Completed:	2016-01-05 21:24:47

For each server, note its operating-system indicator and its status: Active (the Halo agent has recently communicated with the Halo analytics engine), Deactivated (the server was shut down or the agent was stopped), or Missing (agent-engine communication has been interrupted). Then inspect the account information:

- Root Privilege. At the top of the page, specifies the number of root-privileged accounts on the server (if the server has been scanned). If there is more than one, one is named "root" and the others have a UID or GID of zero. (Some distributions provide only one root-privileged account by default, others may provide several.) Make sure this number is not different from what you expect; extra root-level accounts could be a strong security concern.
- Total Accounts. At the top of the page, the total number of local accounts in the server. This number should not be larger than what you reasonably expect the number of accounts to be. Note also that, if the servers are all in the same server group and you instantiate them from a server template, this number should be the same for all of the servers.
- Last Login. The date and time of the last login, if any, by any account. In the list of accounts, click the Root Privilege column to group the list of accounts with root privileges (UID or GID = 0).

  This value includes only remote logins; it does not account for console logins on the server itself, or for logins in which `su` or `sudo` commands might have been used to perform root-level tasks. (Note that local logins are recorded in the server's log file `var/log/secure`.)

View server account details

To get more information about the accounts on a server, click the number of root accounts or total accounts for that server (in the Root/Total column in the list of servers). The Server Access Scan Results page appears:

This page includes information about the most recent access scan, and displays a line of information about each server account.

Hint: Click a column head to sort the results by that column. For example, to see all accounts with root privileges at the top of the list, sort by "Root Privilege" or "GID".

For each account, note especially these values:

- Username. The account's login name. Check the list of accounts for any unexpected account names or accounts that should have been removed (for example, from ex-employees).

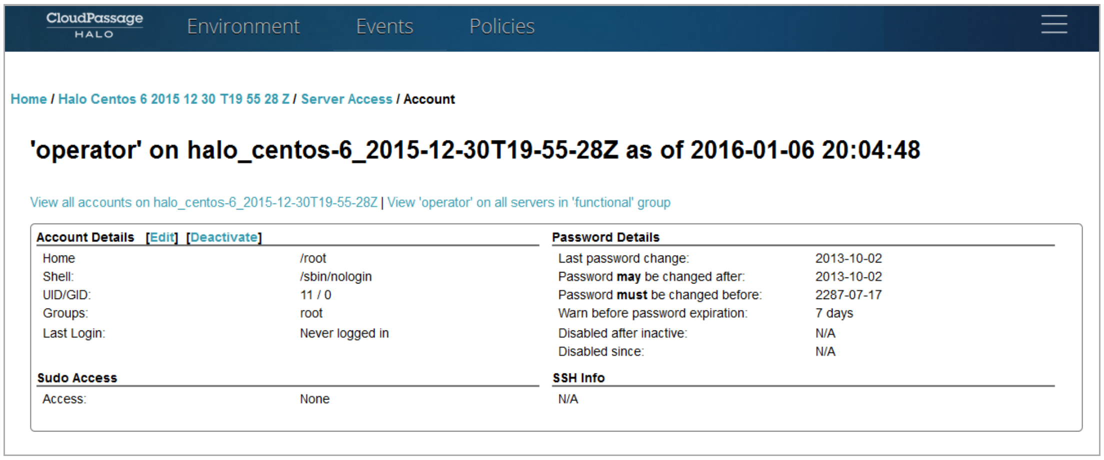
- Root Privilege. "Yes" if the account has root privileges. Make sure there are no accounts with root privileges that shouldn't have them.
- UID and GID. The user ID and group ID of the account. Note that an account with root privileges will have a UID or GID of zero. Make sure that only accounts that should have root privileges have a zero UID or GID.

  Note: "Root privilege" by this definition does not include accounts with membership in the "wheel" group (giving them 'su' capabilities) or accounts with any level of 'sudo' capability.
- Shell. The path to the command shell that the account has used to access the server. If shell access to the server is not allowed, the shell is shown as something like `/bin/nologin` or `/bin/false`. Thus you can easily tell whether a given account has remote access to this server.
- Last Login. The date and time of the last login to the server from this account, plus the IP address of the remote machine from which the user logged and the terminal that was used. This not only tells you whether this account has been active recently, but can also indicate whether the login occurred outside of normal business hours, and whether it came from an unexpected location.

  Note: This value includes only remote logins; it does not account for console logins on the server itself, or for logins in which `su` or `sudo` commands might have been used to perform root-level tasks. (Note that local logins are recorded in the server's log file `/var/log/secure`.)
- Active. Whether the account is active or inactive (deactivated).

View details of one account

On the Server Access Details page, click the username of an account to get even more information about that account. The Account Details page appears:



Home / Halo Centos 6 2015 12 30 T19 55 28 Z / Server Access / Account

'operator' on halo_centos-6_2015-12-30T19-55-28Z as of 2016-01-06 20:04:48

View all accounts on halo_centos-6_2015-12-30T19-55-28Z | View 'operator' on all servers in 'functional' group

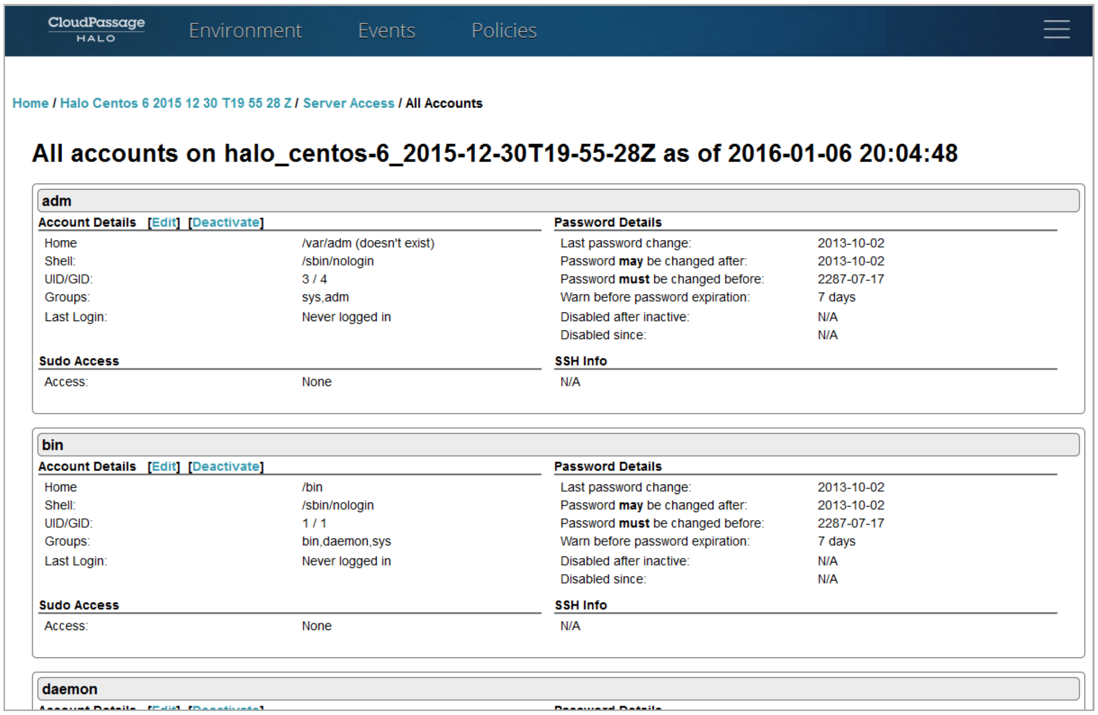
Account Details [Edit] [Deactivate]		Password Details	
Home	/root	Last password change:	2013-10-02
Shell:	/sbin/nologin	Password **may** be changed after:	2013-10-02
UID/GID:	11 / 0	Password **must** be changed before:	2287-07-17
Groups:	root	Warn before password expiration:	7 days
Last Login:	Never logged in	Disabled after inactive:	N/A
		Disabled since:	N/A
Sudo Access		**SSH Info**	
Access:	None	N/A	

This page includes the same account information as the Server Account Details page, and adds more:

- Home. The account's home directory. (It may or may not have been created.)
- Groups. The groups that this account belongs to. If the "wheel" group is listed, this account can use the `su` command to assume root level privileges.
- Sudo access. This section specifies the commands, if any, that this account is allowed to execute as the root-level user.
- Password Details. When the password was last changed (a recent change may be of interest), how soon after the change it is possible to change it again, and the deadline for the next change. Also, whether this account is automatically disabled a certain number of days after its password expires.
- SSH Info. This indicates whether SSH keys are stored for this account, and what permissions are set on the account user’s SSH directory. In the above example, the value of `rwx------` is appropriate, indicating that the account has full permissions on the directory, whereas the account's group and others have no permissions.

Compare all accounts on one server

To see detailed account information for all accounts on a server, click Expanded Account Details on the Server Access Details page, or click View all accounts on ***ServerName*** on the Account Details page. The All Accounts page appears:



Home / Halo Centos 6 2015 12 30 T19 55 28 Z / Server Access / **All Accounts**

All accounts on halo_centos-6_2015-12-30T19-55-28Z as of 2016-01-06 20:04:48

adm

Account Details [Edit] [Deactivate]

Home	/var/adm (doesn't exist)
Shell:	/sbin/nologin
UID/GID:	3 / 4
Groups:	sys,adm
Last Login:	Never logged in

Password Details

Last password change:	2013-10-02
Password **may** be changed after:	2013-10-02
Password **must** be changed before:	2287-07-17
Warn before password expiration:	7 days
Disabled after inactive:	N/A
Disabled since:	N/A

Sudo Access

Access:	None

SSH Info

N/A

bin

Account Details [Edit] [Deactivate]

Home	/bin
Shell:	/sbin/nologin
UID/GID:	1 / 1
Groups:	bin,daemon,sys
Last Login:	Never logged in

Password Details

Last password change:	2013-10-02
Password **may** be changed after:	2013-10-02
Password **must** be changed before:	2287-07-17
Warn before password expiration:	7 days
Disabled after inactive:	N/A
Disabled since:	N/A

Sudo Access

Access:	None

SSH Info

N/A

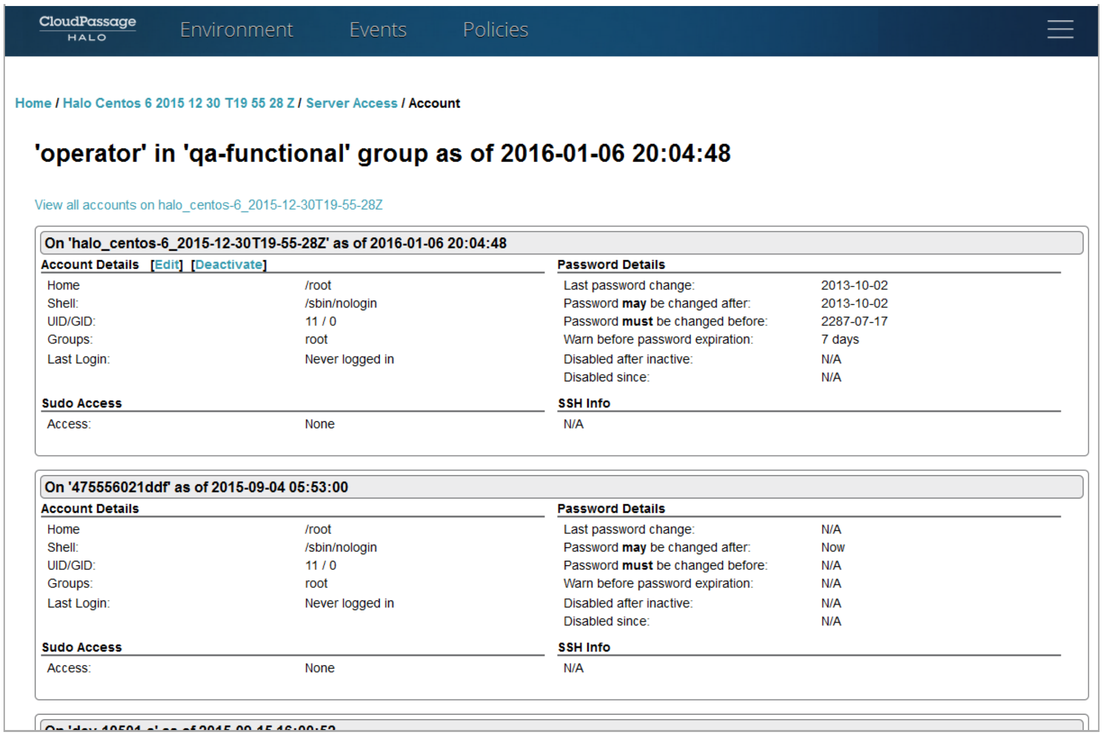
daemon

Account Details [Edit] [Deactivate] **Password Details**

Account details for all of the accounts on the server are displayed on this page. You can quickly scroll down and up to compare different accounts. For example, you can look for "wheel" membership, sudo access, or recent password changes without opening each account's details separately.

Compare one account across all servers

Besides looking at all accounts on one server, you can also analyze login activity by looking at one account across all of your servers. View the Account Details page for an account, then click view '***AccountName***' on all servers in '***GroupName***' group. The following Account in Group page appears:



Home / Halo Centos 6 2015 12 30 T19 55 28 Z / Server Access / Account

'operator' in 'qa-functional' group as of 2016-01-06 20:04:48

View all accounts on halo_centos-6_2015-12-30T19-55-28Z

On 'halo_centos-6_2015-12-30T19-55-28Z' as of 2016-01-06 20:04:48

Account Details [Edit] [Deactivate]		Password Details	
Home	/root	Last password change:	2013-10-02
Shell:	/sbin/nologin	Password **may** be changed after:	2013-10-02
UID/GID:	11 / 0	Password **must** be changed before:	2287-07-17
Groups:	root	Warn before password expiration:	7 days
Last Login:	Never logged in	Disabled after inactive:	N/A
		Disabled since:	N/A
Sudo Access		**SSH Info**	
Access:	None	N/A	

On '475556021ddf' as of 2015-09-04 05:53:00

Account Details		Password Details	
Home	/root	Last password change:	N/A
Shell:	/sbin/nologin	Password **may** be changed after:	Now
UID/GID:	11 / 0	Password **must** be changed before:	N/A
Groups:	root	Warn before password expiration:	N/A
Last Login:	Never logged in	Disabled after inactive:	N/A
		Disabled since:	N/A
Sudo Access		**SSH Info**	
Access:	None	N/A	

With this view, you can easily compare a user's recent activity across all servers being scanned. The account's information should mostly be identical across all servers in a given server group; any differences might be cause for investigation.

Act on Server Access Scan Findings

Server access scans do not directly report security issues. However, by examining scan results, you can infer whether issues exist that should be addressed.

Use server access scan results to evaluate the following:

- Make sure that the reported number of root accounts (accounts whose UID or GID is zero) is not different from what you expect; extra root-level accounts could be a strong security concern.
- The total number of local accounts on a server should not be unreasonably large, and if the servers in the server group are all instantiated from a server template, this number should be the same for all of the servers.
- Note whether there has been any recent remote login activity on that server by one of its privileged accounts. If there has and it is unexpected, it may be a security concern.
- Check the list of accounts for any unexpected account names or accounts that should have been removed (for example, from ex-employees).
- Make sure there are no accounts with root privileges that shouldn't have them.
- Make sure that only accounts that should have root privileges have a zero UID or GID.
- Verify that only accounts that should have shell access to this server do have it, and verify that the permissions on the account's SSH directory are secure enough.
- The date and time of the last login to this server from an account, along with the IP address of the remote machine from which the user logged and the terminal that was used, can indicate whether the login was recent, whether it occurred outside of normal business hours, and whether it came from an unexpected location.
- Ensure that accounts that should be inactive are not active.
- Verify that only accounts that need elevated privileges belong to groups (such as "wheel") with elevated privileges.

- Verify that each account has only the appropriate sudo privileges for that account, and no more.
- Note whether any of the accounts' passwords have changed recently and unexpectedly.

Based on any issues that you discover with any of the accounts, you can then take action:

- Deactivate. If the account is not needed or belongs to someone who has left the organization, deactivate it. If the account belongs to an unknown user, investigate immediately.
- Edit or Create New Account. If the account has unnecessarily high privileges, needs changes to its group memberships, or otherwise needs to be altered, you can edit its information. If the privilege escalation is unauthorized, it may warrant immediate investigation.

  If you want to restore an account that was inadvertently deleted, you can add it as a new account on the server. If the account deletion is suspicious or appears to have been malicious, investigate immediately.
- Launch New Scan. Immediately run another server access scan. You might do this if you have just edited, created, or deactivated some accounts and you want to verify that your edits are reflected in the new scan.

Act On Server Access Issues and Events

The Halo portal reports an event, and an issue is created, whenever a server access scan detects more than one account with root privileges on a server, or more than one account with the same UID.

If the event type is "Multiple Root Accounts Detected" or "Multiple accounts detected with same UID", verify the event by directly accessing the server in question. If you determine that the events violate your organization's security policies,remediate the issue —delete the extra accounts, or remove root privileges and change UIDs, or immediately start an investigation.

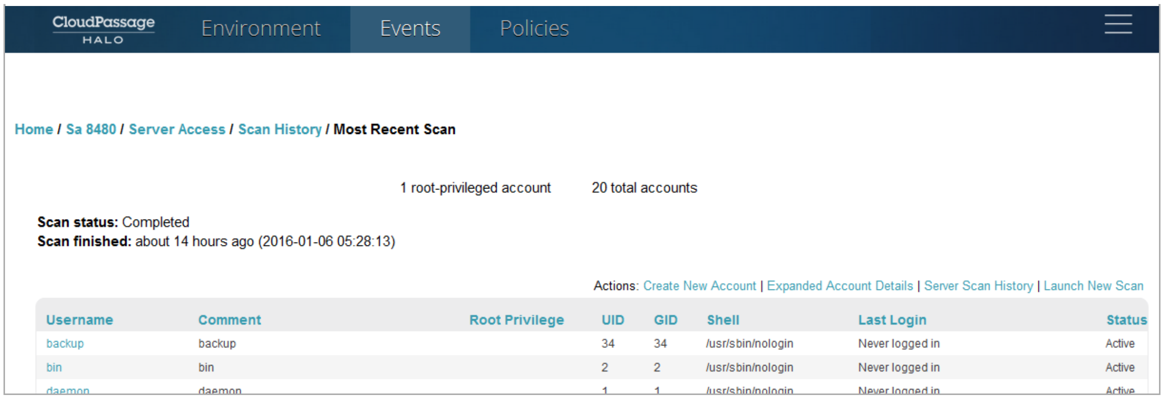
Administering Server Accounts

In the process of auditing user access to your servers, you may need to make certain changes to some of the accounts. From within the Halo portal, you can perform basic account-management tasks, such as editing, deactivating, and creating accounts.

Create a Server Account

Halo also gives you the convenience of creating server accounts from within the Halo portal. To create a new account, do this:

1. On a server's Account Summary page, click Create New Account.



Home / Sa 8480 / Server Access / Scan History / **Most Recent Scan**

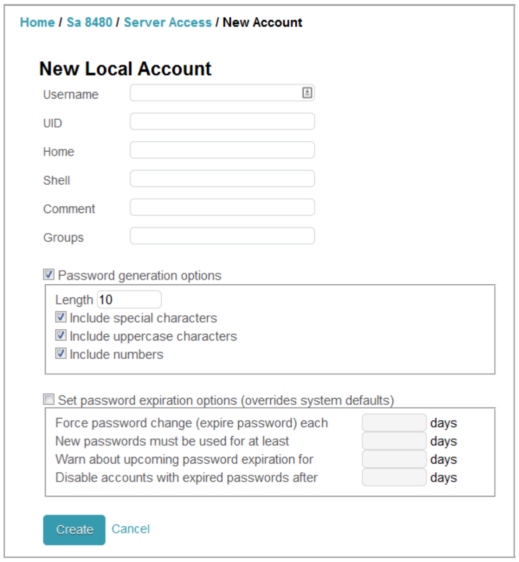
1 root-privileged account 20 total accounts

Scan status: Completed
Scan finished: about 14 hours ago (2016-01-06 05:28:13)

Actions: Create New Account | Expanded Account Details | Server Scan History | Launch New Scan

Username	Comment	Root Privilege	UID	GID	Shell	Last Login	Status
backup	backup		34	34	/usr/sbin/nologin	Never logged in	Active
bin	bin		2	2	/usr/sbin/nologin	Never logged in	Active
daemon	daemon		1	1	/usr/sbin/nologin	Never logged in	Active

Halo displays the New Local Account page.



Home / Sa 8480 / Server Access / **New Account**

New Local Account

Username
UID
Home
Shell
Comment
Groups

☑ Password generation options

Length 10
☑ Include special characters
☑ Include uppercase characters
☑ Include numbers

☐ Set password expiration options (overrides system defaults)

Force password change (expire password) each days
New passwords must be used for at least days
Warn about upcoming password expiration for days
Disable accounts with expired passwords after days

2. Fill in the account details and click Create.

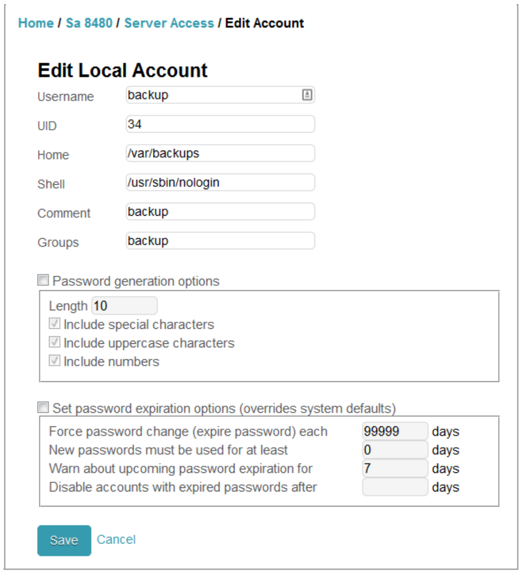
   Halo creates a random password for the user and displays it above the success banner in the Halo portal. You can then provide that password to the new user to supply at initial login.

Note: If you instantiate from a server template, create the account on the template so that all future cloned instances will automatically have the new account.

Edit a Server Account

To edit an account—for example, to remove root privileges, change the login name, or edit password requirements—perform the following steps.

1. On the Account Details display for that account (on the Account Details page, the All Accounts page, or the Account in Group page), click Edit. Halo displays the Edit Local Account page.



Home / Sa 8480 / Server Access / Edit Account

Edit Local Account

Username	backup
UID	34
Home	/var/backups
Shell	/usr/sbin/nologin
Comment	backup
Groups	backup

☐ Password generation options

Length 10
☑ Include special characters
☑ Include uppercase characters
☑ Include numbers

☐ Set password expiration options (overrides system defaults)

Force password change (expire password) each	99999	days
New passwords must be used for at least	0	days
Warn about upcoming password expiration for	7	days
Disable accounts with expired passwords after		days

2. Change any of the available account values, password-generation options, or password-expiration options.

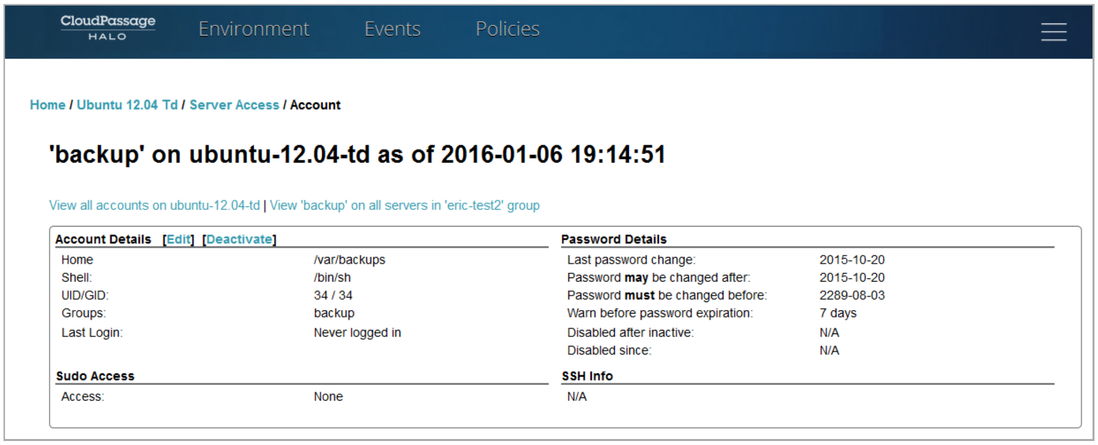
3. Click Save to save your changes.

Note: If you instantiate your servers from a template image, you can make the changes on the template so that all future cloned instances will automatically have the updated account information.

Deactivate a Server Account

To deactivate an account—for example, to get rid of the account of an employee no longer with the organization—take these steps:

1. On the Server Access Details page for a server, click an account to view the account's details, then on the Account Details page, the All Accounts page, or the Account in Group page, click Deactivate.



Home / Ubuntu 12.04 Td / Server Access / Account

'backup' on ubuntu-12.04-td as of 2016-01-06 19:14:51

View all accounts on ubuntu-12.04-td | View 'backup' on all servers in 'eric-test2' group

Account Details [Edit] [Deactivate]		Password Details	
Home	/var/backups	Last password change:	2015-10-20
Shell:	/bin/sh	Password **may** be changed after:	2015-10-20
UID/GID:	34 / 34	Password **must** be changed before:	2289-08-03
Groups:	backup	Warn before password expiration:	7 days
Last Login:	Never logged in	Disabled after inactive:	N/A
		Disabled since:	N/A
Sudo Access		**SSH Info**	
Access:	None	N/A	

2. In the dialog box that opens, click OK confirm that you want to deactivate the user.

Note: To restore a deactivated user, click the Activate link on the Account Details display for that account. (For a de-activated account, the Deactivate link becomes Activate.)