Guia Técnico v6.1 - Alta-Disponibilidade

CONTROL ONE

Conteúdo

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

Introdução

Este documento possui informações detalhadas sobre a funcionalidade de Alta-Disponibilidade (HA) do sistema ControlONE.

Definições

- HA = High-Availability, Alta-Disponibilidade.
- Conference Server = Serviço conference de um Servidor ControlONE. Pode ser local ou remoto.
- Console Server = Serviço server de um Servidor ControlONE participante do Cluster.
- Cluster = Grupo de servidores que compõe um único sistema ControlONE.
- Servidor Mestre = Servidor ControlONE que possui todos os serviços ativos na inicialização e aceita conexões de consoles e integrações.
- Servidor Escravo = Servidor ControlONE que possui os Serviços Console Server e Conference Server desativados enquanto o Servidor Mestre está funcionando.
- Servidor Passivo = Servidor ControlONE para replicação de dados, com serviços de base de dados. Serviços Console Server e Conference Server desativados.
- Estado Espera = Servidor que está aguardando falha em peer para ativar os serviços. *Standby*.
- Estado Ativo = Servidor ativo, com serviços em funcionamento. *Active*.
- Nó = Servidor ControlONE participante do Cluster.
- Peer(s) = Outro(s) nó(s) do cluster.

Descrição da funcionalidade

O ControlONE possui suporte a cluster de alta-disponibilidade (HA), com sincronização de configurações e dados entre servidores. Cada servidor pode ser designado como master, slave ou passive, para as funções, respectivamente, de Servidor Mestre, Servidor Escravo, ou Servidor Passivo.

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

Múltiplos servidores podem ser designados como Mestre, de maneira a segmentar a operação. Isto é útil, principalmente, em sistemas multi-site ou que necessitem distribuir a carga de grande número de Consoles.

A configuração de HA é aplicada em cada servidor, e pode conter diferenças entre eles. Desta maneira, se consegue maior flexibilidade de arquitetura e é possível escolher os servidores a serem replicados e monitorados em cada nó.

Abaixo, uma arquitetura típica de 2 sites com o ControlONE. Além da redundância entre os sites, existe um servidor Escravo em cada.

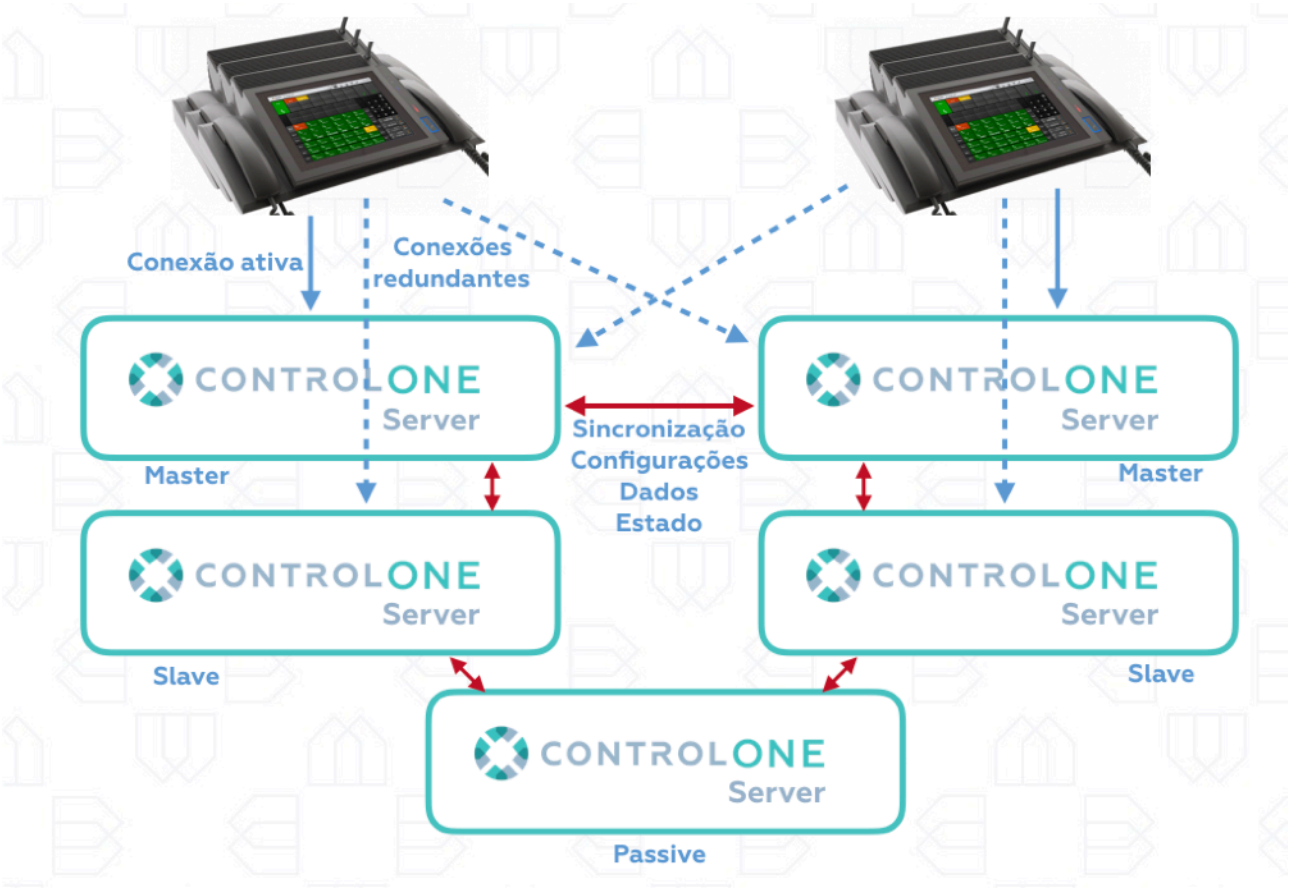

FIG 1. EXEMPLO DE ARQUITETURA DO CONTROLONE COM 2 SITES EM HA

O servidor Passivo pode ser utilizado como estação principal de gerenciamento e auditoria centralizada, pois possui sincronia com todos os outros nós. E quaisquer dos 5 nós, nessa arquitetura, podem ser utilizados para gerenciamento e auditoria, mesmo em caso de isolamento de um ou mais servidores.

Não é necessário qualquer equipamento adicional ou funcionalidade em ambiente de virtualização para o funcionamento de Alta-Disponibilidade do ControlONE.

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

A distribuição de carga é feita na configuração das Consoles.

Pré-Requisitos

A conectividade entre os nós é necessária através das seguintes portas:

- TCP/22 - serviço SSH
- TCP/7551 - serviço Consoles
- TCP/27017 - sincronização base de dados

Para a função de continuidade de chamadas ativas, em caso de chaveamento de servidores, é necessário que os equipamentos SIP conectados suportem o cabeçalho Replaces, segundo RFC 3891.

Licenciamento

Para ativar a funcionalidade é necessária uma licença CO-LICE-HA para cada Servidor Mestre configurado no cluster.

Todas as licenças do sistema são replicadas e válidas para todos os nós.

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

Funcionamento

Sincronização

As configurações são sincronizadas entre todos os nós do cluster, mantendo a integridade do sistema.

O nó onde a modificação foi realizada sincroniza sua configuração para todos os outros que constem na lista de *peers*. Desta maneira, configurações podem ser realizadas em qualquer nó do sistema, sendo replicadas para todo o cluster.

As configurações são replicadas com base no horário de modificação (*timestamp*) e diferenças (*checksum*). Somente configurações diferentes são copiadas, para diminuir o tráfego entre os nós. A última configuração realizada no cluster sempre será prioritária em caso de conflito, caso a mesma configuração esteja sendo modificada em 2 nós ao mesmo tempo.

Em caso de isolamento de um ou mais nós, a sincronização continua ocorrendo entre os servidores que se comunicam. Mesmo os servidores isolados podem ser reconfigurados. Ao serem reconectados ao cluster, enviam e recebem as últimas modificações de configuração realizadas.

Além da sincronização em tempo real, o servidor realiza uma sincronização total periódica, por padrão a cada 1 hora, para garantir a integridade dos dados com todos os seus peers.

Por segurança, arquivos de configuração apagados não são replicados e precisam ser removidos em todos os nós individualmente.

Detecção de falhas

Cada nó realiza auto-monitoramento dos seus serviços. O serviço watchdog1 realiza periodicamente (10 segundos por padrão) requisições SIP para o Conference Server e requisições de Console para o Console Server. Além disto, analisa hardware e sistema operacional, como uso elevado de CPU, memória, disco, entre outros. Em caso de anormalidade que prejudique o funcionamento do sistema, o servidor desativa o Console Server, de maneira a forçar outro servidor em estado ativo ou espera a assumir a operação.

Os equipamentos em estado de espera monitoram ativamente os serviços Console Server (requisições de Console) e Conference Server (requisições SIP) dos nós em estado ativo. Isto garante que não somente falhas gerais, como a desconexão de

rede do servidor, mas também falhas menores de software ou hardware sejam detectadas.

Em caso de detecção de falha, o servidor em estado de espera é promovido a estado ativo. O retorno do servidor configurado como Escravo para estado passivo é opcional, definido na configuração do HA.

Nas Consoles é configurada a lista de servidores, sendo a prioridade definida pela ordem nesta lista. Cada Console permanece com conexão ativa somente com um servidor para todas as funções. Em caso de falha de comunicação, detectada por timeout de resposta (10 segundos por padrão) ou erros de pacotes, a Console tenta conexão com o segundo servidor da lista e assim sucessivamente. Em cada novo processo, o primeiro da lista é verificado novamente. Os outros servidores são testados periodicamente pela Console, para validação de conectividade e prevenção de problemas.

O processo de ativação da conexão da Console em novo Servidor é transparente ao usuário, que pode receber indicações de anormalidade na informação de estado do sistema. Somente em casos críticos, como a falta de conectividade de rede, ou de falha em todos os servidores, é que a Console fica indisponível para o usuário.

Chamadas

Todas as chamadas são gerenciadas e agregadas pelo Conference Server, em cada servidor ControlONE do sistema. A distribuição é realizada por filas (*queues*) definidas pelo número de destino da chamada e possibilita a segmentação em diferentes Servidores, de acordo com a configuração de monitoramento de filas de cada console.

Um servidor, mesmo ativo, não aceita chamadas provenientes de gateways externos para filas que não possuam Consoles conectadas. Desta maneira, provê redundância de entrada de chamadas, com garantia de entrega para os servidores que possam atendê-las. A chamada é rejeitada com mensagem SIP *603 Decline*, de maneira a permitir ao gateway tentar caminho alternativo para a chamada, geralmente outros Conference Server do cluster.

As chamadas de saída são distribuídas pelo servidor onde a Console está conectada para os Conference Server disponíveis em sua configuração (*conference*). Estes, por sua vez, utilizam as regras de roteamento de chamadas (*dialplan*) do sistema, que possibilitam múltiplas rotas de saída.

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

Continuidade de chamadas ativas

Os nós realizam testes periódicos em seus *peers*, através de teste real de protocolo SIP. Em caso de falha no Conference Server, o servidor de maior prioridade, ativo ou em espera, assume todas as chamadas que estavam no Conference Server com falha. Este processo é realizado com requisição do servidor ativo para os Gateways ou Endpoints SIP onde as chamadas estavam estabelecidas, utilizando protocolo SIP.

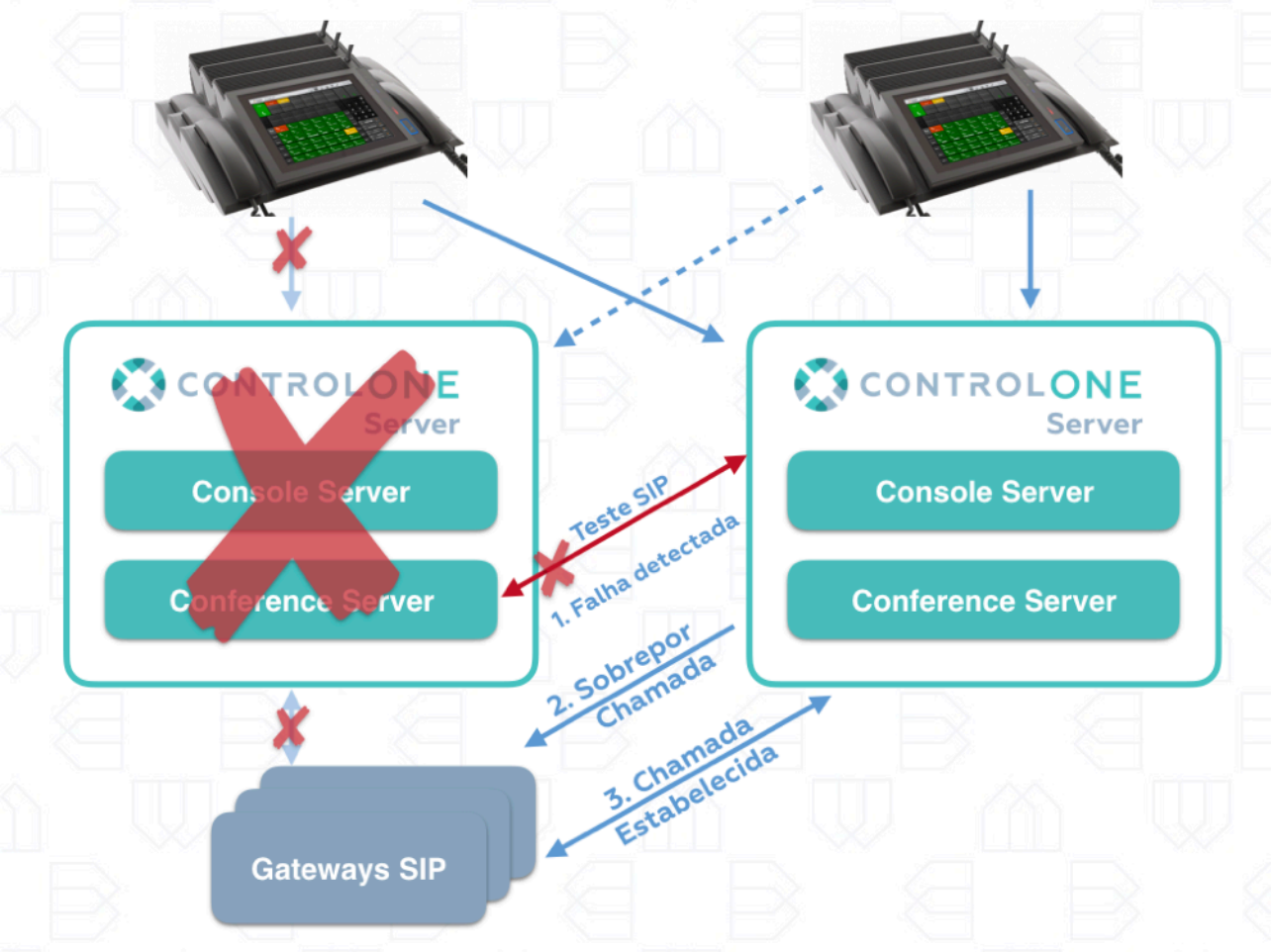

FIG 2. PROCESSO DE TRANSFERÊNCIA DE CHAMADAS PARA SERVIDOR ATIVO

Em um ambiente que atenda os requisitos apresentados, o processo de troca de servidor ocorre de maneira transparente ao usuário, que continuará com as chamadas ativas.

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

As gravações em andamento continuarão a partir do estabelecimento da chamada no novo servidor ativo. O servidor anterior mantém a gravação até o momento da falha e sincronizará os dados com o restante do cluster quando retornar.

Em caso de uso de servidor externo de gravação, este será informado para iniciar nova sessão de gravação, caso esteja sendo realizada a cópia de *stream* de áudio a partir do Conference Server. Caso o *stream* de áudio seja a partir da Console, a gravação continuará normalmente.

Segurança

O Sigilo da sincronização das informações entre os nós é garantido através de criptografia em todas as comunicações, utilizando par de chaves RSA 2048 bits. Estas chaves são geradas durante a implantação do sistema. Além disso é configurada uma senha de HA para o sistema, como medida adicional de segurança, utilizada na autenticação dos processos de cópia de configurações e base de dados.

Ambas informações, chaves RSA e senha HA, precisam estar em conformidade para a conexão ser aceita e as informações serem sincronizadas.

Configuração

Servidor

Para o funcionamento de Alta-Disponibilidade, é necessária a definição de 3 configurações básicas:

1. **Peers:** Lista de hosts a serem monitorados e sincronizados
2. **Função (role):** Função deste servidor: master, slave ou passive
3. **Segredo (secret):** Senha utilizada pelo cluster para sincronização

Esta configuração pode ser realizada pela interface WEB, em **Sistema -> HA**. O serviço *HA* deve ser reiniciado para aplicar as configurações, na opção **Serviços**.

Para configuração via CLI, utilizam-se os comandos:

```
uci set ha.default.peers=PEER1,PEER2, PEER3
uci set ha.default.role=master
uci set ha.default.secret=123456
uci commit
service ha restart
```

Após a configuração, pode-se verificar o estado do cluster através da interface WEB ou via CLI, com o comando:

```
ha status
```

Através do comando é possível visualizar estado do próprio servidor, dos peers, e última sincronização de configurações e dados realizado.

O comando *ha* possui parâmetros adicionais

- **ha sync <item>:** Força a sincronização de determinado item (*config*, *jobs*, *recordings*, *sounds* ou *database*)
- **ha force_passive:** Força mudança do servidor para estado passivo.
- **ha force_active:** Força mudança do servidor para estado ativo.

Console

Através da CLI da console, via SSH ou Serial, deve-se definir a lista de servidores, em ordem de preferência, com o comando:

```
uci set console.default.server=<SERVIDOR1>,<SERVIDOR2>,<SERVIDOR3>
uci commit
service console restart
```

A console manterá conexão ativa preferencialmente com o primeiro da lista, e em caso de falha, tentará o segundo e depois o terceiro servidor.

Parâmetros de *timeout* e número de pacotes perdidos para ativar a mudança de servidor podem ser configurados no processo de implantação.

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920

Related Documents

- The Session Initiation Protocol (SIP) "Replaces" Header - RFC 3891, veja https://tools.ietf.org/html/rfc3891

Rod José Carlos Daux, 4150
Florianópolis SC
+55 11 2102 6920